# Международный журнал информационных технологий и энергоэффективности

Том 8 Номер 5 (31)

2023

Международный журнал информационных технологий и энергоэффективности
Т.8 №5(31) ч.2. 2023 г.

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

## СОДЕРЖАНИЕ / CONTENT

### ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Дементьев С. Ю., Мурыгин А. В. Промышленный интернет вещей в России // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31)ч.2 с. 5–8

Международный журнал информационных технологий и энергоэффективности

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

УДК 65.011.56

# ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ В РОССИИ

**Дементьев С. Ю., Мурыгин А. 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. 31), e-mail: info@sibsau.ru*

**Промышленный Интернет вещей (IIoT) — это новая технология, которая находит все более широкое применение в различных отраслях промышленности по всему миру. Россия также начала внедрять IIoT в своем промышленном секторе. В этой статье исследуется текущее состояние IIoT в России и его потенциал для роста в будущем. Анализируется проблемы, с которыми сталкивается российская промышленность при внедрении IIoT, и меры, принимаемые правительством для преодоления этих проблем. Также подчеркивается преимущества IIoT для российской промышленности и влияние, которое оно может оказать на экономику страны.**

Ключевые слова: Промышленный интернет вещей, IIoT, Россия, промышленность, экономика.

# INDUSTRIAL INTERNET OF THINGS IN RUSSIA

**Dementiev S. Yu., Murygin A.V.**
*Siberian State University of Science and Technology named after Academician M. F. Reshetnev, Krasnoyarsk Russia (660037, Krasnoyarsk Krai, Krasnoyarsk city, prospect named after the newspaper "Krasnoyarsk worker", 31), e-mail: info@sibsau.ru*

**The Industrial Internet of Things (IIoT) is an emerging technology that has been increasingly adopted in various industries across the world. Russia has also started to embrace IIoT in its industrial sector. This article revealed the lack of state of IIoT in Russia and its potential for growth in the future. The problems in which the Russian industry is considered in the implementation of the IIoT are analyzed, and the decisions taken to solve these problems are made. The advantage of IIoT for the Russian industry and the impact that may have an impact on the participation of the country is also amplified**

Keywords: Industrial Internet of Things, IIoT, Russia, industry, economy.

The Industrial Internet of Things (IIoT) is a technology that involves the integration of various physical devices, machines, and sensors with software and network connectivity to collect and analyze data. IIoT has the potential to transform industries by increasing efficiency, reducing costs, and improving productivity. In recent years, IIoT has gained significant attention in Russia, with various industries starting to adopt this technology. This article aims to explore the current state of IIoT in Russia, the challenges faced by industries in adopting it, and the measures taken by the government to promote IIoT in the country.

Russia is a country with a significant industrial base, and IIoT has the potential to enhance the competitiveness of its industries. The adoption of IIoT in Russia is still in its early stages, but various industries have started to implement IIoT solutions. The oil and gas, manufacturing, and

transportation industries are some of the sectors that have started to adopt IIoT in Russia. For example, in the oil and gas industry, IIoT is being used to monitor the condition of pipelines, detect leaks, and predict maintenance requirements.

The adoption of IIoT in Russia is not without challenges. One of the significant challenges is the lack of awareness and understanding of IIoT among Russian industries. Many companies do not fully understand the potential benefits of IIoT, and some are skeptical about the technology. The lack of skilled workers and the high cost of implementing IIoT solutions are also significant challenges faced by Russian industries.

The Russian government has recognized the potential benefits of IIoT and has taken measures to promote its adoption in the country. The government has developed a roadmap for the implementation of IIoT in Russia, which includes the development of standards, the promotion of research and development, and the establishment of IIoT centers of excellence. The government is also providing financial incentives to companies that adopt IIoT solutions and is working to improve the availability of skilled workers in the field [1-2].

There are several examples of the IIoT in. Examples of IIoT in Russia:

1. Smart Oil Field - In Russia, the Smart Oil Field project uses IIoT to monitor oil wells and pipelines, detect leaks, and predict maintenance requirements.
2. Smart Grid - The Russian power grid is being upgraded with IIoT technology to improve efficiency and reduce power outages.
3. Smart Transportation - IIoT is being used to monitor the condition of railway tracks and predict maintenance requirements to improve safety and efficiency.

The effectiveness of the IIoT can be measured in various ways, such as increased productivity, reduced costs, improved safety, and enhanced efficiency. Here are some statistics that demonstrate the effectiveness of IIoT:

1. Increased productivity: According to a study by Accenture, IIoT can increase labor productivity by up to 25%. Another study by GE Digital found that IIoT can increase equipment uptime by up to 10%.
2. Reduced costs: A study by McKinsey & Company found that IIoT can reduce maintenance costs by up to 40% and energy costs by up to 20%. IIoT can also reduce downtime and improve the overall equipment effectiveness (OEE).
3. Improved safety: IIoT can improve workplace safety by identifying and addressing potential hazards before accidents occur. According to a study by Deloitte, IIoT can reduce workplace accidents by up to 25%.
4. Enhanced efficiency: IIoT can optimize processes and workflows, leading to improved efficiency. A study by the International Data Corporation (IDC) found that IIoT can increase equipment efficiency by up to 20%.
5. Economic impact: IIoT has the potential to generate significant economic impact. A study by the Boston Consulting Group (BCG) estimated that IIoT could create up to $11.1 trillion in economic value by 2025 [3-4].

IIoT can be implemented in a wide range of enterprises in Russia, regardless of their size or industry. However, certain enterprises are likely to benefit more from IIoT implementation than others. Here are some enterprises in Russia where it would be most appropriate to implement IIoT:

1. Manufacturing: IIoT can be implemented in manufacturing enterprises to optimize production processes, reduce waste, and improve product quality. Manufacturing enterprises in

Russia can benefit from IIoT by using it to monitor equipment and processes, and to predict maintenance requirements.

2. Energy and utilities: IIoT can be implemented in the energy and utilities sector to optimize power generation and distribution, predict demand, and reduce energy waste. In Russia, IIoT can be used to monitor and manage the power grid, optimize energy consumption, and reduce costs.

3. Transportation and logistics: IIoT can be implemented in transportation and logistics enterprises to optimize routes, reduce fuel consumption, and improve supply chain efficiency. In Russia, IIoT can be used to monitor the condition of railways, roads, and airports, and to optimize transportation routes and logistics processes.

4. Oil and gas: IIoT can be implemented in oil and gas enterprises to optimize drilling, production, and distribution processes, and to improve safety and environmental sustainability. In Russia, IIoT can be used to monitor oil wells and pipelines, detect leaks, and predict maintenance requirements.

5. Agriculture: IIoT can be implemented in agriculture enterprises to optimize crop yields, reduce water usage, and improve crop quality. In Russia, IIoT can be used to monitor soil moisture, crop health, and weather conditions, and to optimize irrigation and fertilization processes.

Overall, any enterprise that relies on industrial processes and equipment can benefit from IIoT implementation in Russia. Enterprises that adopt IIoT can increase productivity, reduce costs, improve safety, and enhance efficiency, leading to significant economic impact.

Benefits of IIoT for Russian industries: The adoption of IIoT can bring significant benefits to Russian industries. IIoT can improve productivity, reduce costs, and increase efficiency. IIoT can also help companies to optimize their supply chains, improve product quality, and reduce downtime. The adoption of IIoT can also enhance safety and environmental sustainability in industries [5-6].

The Industrial Internet of Things is a technology that has the potential to transform industries across the world. Russia has also recognized the potential benefits of IIoT and has started to adopt this technology in its industrial sector. However, there are still challenges that need to be overcome, such as the lack of awareness and understanding of IIoT among industries. The Russian government has taken measures to promote the adoption of IIoT and is providing financial incentives to companies that adopt this technology. The adoption of IIoT can bring significant benefits to Russian industries, including improved productivity, reduced costs, and increased efficiency.

**Список литературы**

1. Shvab, K. Chetvertaja promyshlennaja revoljucija. [Text] / K. Shvab // Bombora. – 2016. – p. 230
2. Dementev, S. Y. Production modernization toolkit for the transition to Industry 4.0 / S. Y. Dementev // . – 2022. – No. 21. – p.p 243-245. – EDN HWTEDK.
3. Dementev, S. Yu. Smart lighting in Industry 4.0 / S. Yu. Dementev, A. V. Murygin // International Journal of Information Technology and Energy Efficiency. – 2023. – Vol. 8, No. 1(27). – p.p. 118-121. – EDN VHGCXQ.
4. Henrik, B. Mashinnoe obuchenie. [Text]. / B. Henrik, M. Feverolf, Dzh. Richards // Piter. – 2017. – p. 336
5. Dement'ev, S. Ju. Metody avtomaticheskoj gruppirovki dlja povyshenija jekonomicheskoj jeffektivnosti v industrii 4.0 / S. Ju. Dement'ev, M. P. Roza // Jekonomika i predprinimatel'stvo.

– 2022. – № 10(147). – p.p. 1390-1393. – DOI 10.34925/EIP.2022.147.10.278. – EDN YDFFDH.

6. Sheffer, Je. Industrija H.O. Preimushhestva cifrovyh tehnologij dlja proizvodstva. [Text]. / Je. Sheffer // 2019. – p .320

**References**

1. Shvab, K. Chetvertaja promyshlennaja revoljucija. [Text] / K. Shvab // Bombora. – 2016. – p. 230
2. Dementev, S. Y. Production modernization toolkit for the transition to Industry 4.0 / S. Y. Dementev // . – 2022. – No. 21. – p.p 243-245. – EDN HWTEDK.
3. Dementev, S. Yu. Smart lighting in Industry 4.0 / S. Yu. Dementev, A. V. Murygin // International Journal of Information Technology and Energy Efficiency. – 2023. – Vol. 8, No. 1(27). – p.p. 118-121. – EDN VHGCXQ.
4. Henrik, B. Mashinnoe obuchenie. [Text]. / B. Henrik, M. Feverolf, Dzh. Richards // Piter. – 2017. – p. 336
5. Dement'ev, S. Ju. Metody avtomaticheskoj gruppirovki dlja povyshenija jekonomicheskoj jeffektivnosti v industrii 4.0 / S. Ju. Dement'ev, M. P. Roza // Jekonomika i predprinimatel'stvo. – 2022. – № 10(147). – p.p. 1390-1393. – DOI 10.34925/EIP.2022.147.10.278. – EDN YDFFDH.
6. Sheffer, Je. Industrija H.O. Preimushhestva cifrovyh tehnologij dlja proizvodstva. [Text]. / Je. Sheffer // 2019. – p .320

Сычев Д.И. Искусственный интеллект и кибербезопасность: будущие тенденции и вызовы // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 9–14

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ: БУДУЩИЕ ТЕНДЕНЦИИ И ВЫЗОВЫ

**Сычев Д.И.**
*ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: s.denis_2001@mail.ru*

**В этой статье исследуется сложная взаимосвязь между искусственным интеллектом (ИИ) и кибербезопасностью с акцентом на будущие тенденции и проблемы, которые могут ждать впереди. В начале представляется краткое введение в ИИ и кибербезопасность, их историческое взаимодействие, после чего следует подробное обсуждение будущих тенденций, включая обнаружение и реагирование на угрозы с помощью ИИ, автоматизированный взлом, роль ИИ в конфиденциальности и защите данных, а также потенциальное влияние квантовые вычисления по искусственному интеллекту и кибербезопасности.**
**Также в статье рассматриваются потенциальные проблемы, такие как проблемы этики и конфиденциальности, уязвимости из-за чрезмерной зависимости от ИИ, проблемы предвзятости в ИИ и необходимость идти в ногу с последними достижениями в области искусственного интеллекта. Приведены реальные примеры из практики, чтобы проиллюстрировать возможности и сложности внедрения инструмента ИИ в кибербезопасность.**

Ключевые слова: Искусственный интеллект, кибербезопасность, безопасность данных.

# ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: FUTURE TRENDS AND CHALLENGES

**Sychev D.I.**
*St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: s.denis_2001@mail.ru*

**This article explores the complex relationship between artificial intelligence (AI) and cybersecurity with an emphasis on future trends and challenges that may lie ahead. At the beginning, a brief introduction to AI and cybersecurity, their historical interaction is presented, followed by a detailed discussion of future trends, including AI threat detection and response, automated hacking, the role of AI in privacy and data protection, as well as the potential impact of quantum computing on artificial intelligence and cybersecurity.**
**The article also addresses potential issues such as ethics and privacy issues, vulnerabilities due to over-reliance on AI, issues of bias in AI, and the need to keep up with the latest advances in artificial intelligence. Real-world examples from practice are given to illustrate the possibilities and difficulties of implementing an AI tool in cybersecurity.**

Keywords: Artificial intelligence, cybersecurity, data security.

**Введение**

В эпоху повсеместной цифровизации технологии продолжают развиваться с поразительной скоростью, коренным образом меняя то, как мы живем, работаем и общаемся. Два важнейших аспекта этой технологической революции — искусственный интеллект (ИИ) и кибербезопасность. В то время как ИИ имитирует процессы человеческого интеллекта посредством обучения, рассуждений и исправлений, кибербезопасность направлена на защиту систем, сетей и данных от цифровых атак. Пересечение, на котором встречаются эти две преобразующие технологии, обладает значительным потенциалом для формирования будущего цифровой безопасности. В этой статье рассматриваются развивающиеся связь между ИИ и кибербезопасностью, исследуются их будущие тенденции и проблемы, которые ждут впереди [1-2].

Искусственный интеллект прошел долгий путь с момента своего концептуального зарождения, от простых систем, основанных на правилах, до сложных моделей машинного и глубокого обучения. За прошедшие годы искусственный интеллект проник в различные области, включая кибербезопасность. С ростом взаимосвязанности систем и ростом производства данных, традиционных мер кибербезопасности уже недостаточно. Сложность и изощренность киберугроз растет, а ориентироваться в среде кибербезопасности становится все труднее.

Интеграция искусственного интеллекта в кибербезопасность представляет собой изменение парадигмы в том, как мы обнаруживаем киберугрозы и реагируем на них. Способность ИИ учиться на прошлых инцидентах, адаптироваться к новым ситуациям и делать прогнозы идеально соответствует требованиям современной кибербезопасности. Инструменты искусственного интеллекта могут анализировать огромные объемы данных для обнаружения угроз, автоматизировать реагирование и даже прогнозировать будущие тенденции атак. Несмотря на эти достижения, использование ИИ в кибербезопасности все еще находится на начальной стадии, и множество возможностей еще не изучено.

## 1. Будущие тенденции

### 1.1. Обнаружение угроз и реагирование на них с помощью ИИ

В динамичном мире кибербезопасности обнаружение угроз и реагирование на них должны быть быстрыми и точными. Возможности ИИ играют важную роль в достижении этого. Алгоритмы машинного обучения могут анализировать огромное количество данных в режиме реального времени и выявлять закономерности или аномалии, которые могут указывать на угрозу.

Эти модели ИИ становятся все более изощренными, извлекая уроки из каждого взаимодействия и улучшая свои прогностические возможности. Они могут понимать цифровую среду, определять нормальное поведение и отмечать аномалии, которые могут указывать на потенциальные киберугрозы. ИИ также может автоматизировать реагирование на эти угрозы, сокращая время отклика и потенциально предотвращая ущерб.

Отличным примером обнаружения угроз с помощью ИИ является использование аналитики поведения пользователей и объектов (UEBA). Инструменты UEBA используют машинное обучение для понимания нормального поведения пользователей и сущностей в системе. Любое отклонение от этого «нормального» поведения помечается как потенциальная угроза, что позволяет быстро реагировать [3-4].

### 1.2. Механизмы автоматизированного взлома и защиты на основе ИИ

Искусственный интеллект является мощным инструментом в сфере кибербезопасности. С одной стороны, он способен значительно укрепить безопасность хранения данных, однако, он также может быть использован для автоматизации и уточнения попыток взлома.

Хакерские инструменты на базе ИИ могут выполнять атаки с повышенной скоростью и точностью, что делает их более эффективными и трудными для обнаружения. Эта тенденция вызывает тревогу у специалистов по кибербезопасности, поскольку может привести к увеличению частоты и серьезности кибератак.

Однако, стоит отметить, что ИИ также может сыграть важную роль в разработке передовых защитных механизмов. Например, ИИ можно использовать в «этическом взломе» или «красной команде», когда он используется для проверки систем на наличие уязвимостей, а затем исправляет слабые места, прежде чем злоумышленник успеет ими воспользоваться. Этот упреждающий подход к кибербезопасности может изменить правила игры, потенциально позволяя на шаг опережать злоумышленников.

### 1.3. ИИ в конфиденциальности и защите данных

Еще одна новая тенденция — роль ИИ в защите данных и конфиденциальности. С ростом ценности данных в современном мире защита личной и конфиденциальной информации никогда не была более важной [5].

ИИ может помочь автоматизировать процесс защиты данных и обеспечить соблюдение правил конфиденциальности, таких как Общий регламент по защите данных (GDPR). Инструменты искусственного интеллекта можно использовать для отслеживания утечек данных, обнаружения несанкционированного доступа к персональным данным и обеспечения того, чтобы методы хранения и обработки данных соответствовали нормативным стандартам.

Кроме того, искусственный интеллект может помочь в разработке более надежных алгоритмов шифрования для защиты данных во время передачи и хранения. Возможность использования ИИ для передовых методов шифрования может стать значительным шагом вперед в обеспечении конфиденциальности и целостности данных.

### 1.4. Квантовые вычисления и кибербезопасность

Появление квантовых вычислений представляет собой новый рубеж для ИИ и кибербезопасности. Квантовые компьютеры с их необычайной вычислительной мощностью потенциально могут сломать традиционные методы шифрования, что создает значительный риск для кибербезопасности.

Однако квантовая технология также предоставляет возможности для повышения кибербезопасности. Квантовое шифрование, или квантовое распределение ключей, обещает «невзламываемой» системы хранения данных, используя принципы квантовой механики. Это может произвести революцию в области безопасной связи.

Но интеграция квантовых вычислений и ИИ в кибербезопасность все еще находится на ранней стадии, и для полного понимания и использования этого потенциала необходимо провести много исследований [6-8].

## 2. Вызовы и проблемы

### 2.1. Вопросы этики и конфиденциальности

Хотя потенциал ИИ для повышения кибербезопасности неоспорим, он также вызывает проблемы этики и конфиденциальности. Например, в своей роли в мониторинге и анализе данных для обнаружения потенциальных угроз ИИ может нарушать права людей на неприкосновенность частной жизни.

Более того, алгоритмы ИИ хороши ровно настолько, насколько хороши данные, на которых они обучаются, и если эти данные содержат предвзятую или конфиденциальную информацию, это может привести к серьезным этическим проблемам. Поэтому крайне важно обеспечить прозрачность и подотчетность систем ИИ, используемых в кибербезопасности.

### 2.2. Зависимость от ИИ и потенциальных уязвимостей

Поскольку мы все больше полагаемся на ИИ для обеспечения кибербезопасности, мы также подвергаем себя новым уязвимостям. Если система ИИ будет скомпрометирована, результаты могут быть катастрофическими, поскольку злоумышленники могут получить доступ к конфиденциальным данным или контроль над критически важными системами.

Обеспечение безопасности самих систем ИИ является серьезной проблемой. Это включает в себя не только защиту системы от внешних атак, но и обеспечение того, чтобы алгоритмы ИИ не могли быть использованы для злонамеренного поведения.

### 2.3. Предвзятость ИИ и кибербезопасность

Системы ИИ учатся на данных, на которых они обучаются, и если эти данные содержат предубеждения, ИИ может перенять эти предубеждения, что приведет к несправедливым или неточным результатам. В контексте кибербезопасности это может означать, что определенные типы угроз игнорируются или что невинное поведение помечается как подозрительное.

Преодоление предвзятости в ИИ является серьезной проблемой. Это требует тщательного сбора и обработки данных, тщательного тестирования моделей ИИ и постоянного мониторинга для обеспечения справедливости и точности.

### 2.4. Задача идти в ногу с достижениями ИИ

ИИ — это быстро развивающаяся область, и идти в ногу с последними разработками может быть сложно. Специалисты по кибербезопасности должны постоянно учиться и адаптироваться, чтобы эффективно использовать ИИ и защищаться от угроз, связанных с ИИ. Этот спрос на постоянное обучение и развитие может стать серьезной проблемой, особенно в сфере, где ставки так высоки.

## 3. Тематические исследования

Ниже рассматриваются два реальных случая, которые иллюстрируют потенциал и проблемы ИИ в кибербезопасности.

Пример 1: ИИ в обнаружении угроз

Darktrace, ведущая компания искусственного интеллекта в области кибербезопасности, использует машинное обучение для обнаружения киберугроз, реагирования на них и смягчения их последствий в режиме реального времени. Их технология искусственного интеллекта, известная как «Иммунная система предприятия», изучает, что является

нормальным в сети, а затем может идентифицировать и реагировать на необычную активность, которая отклоняется от этого «образца жизни».

Способность системы быстро и автономно реагировать на угрозы оказалась очень эффективной. В одном из случаев он обнаружил и остановил атаку программы-вымогателя за считанные секунды, предотвратив значительную потерю данных и нарушение работы.

Пример 2: ИИ и кибератаки

В 2020 году компания Cybereason, занимающаяся кибербезопасностью, сообщила о кампании кибератак, которую они назвали «кибератакой с использованием ИИ». Злоумышленники использовали ИИ для автоматизации создания вредоносных электронных писем, что позволило им рассылать фишинговые электронные письма в гораздо большем объеме и с более убедительным содержанием, чем это было бы возможно вручную.

Этот случай иллюстрирует возможность использования ИИ киберпреступниками, подчеркивая важность разработки передовых защитных механизмов на основе ИИ.

**Вывод**

Отношения между ИИ и кибербезопасностью сложны и развиваются. Как было рассмотрено выше, ИИ обладает значительным потенциалом для повышения кибербезопасности, от обнаружения угроз и реагирования до защиты данных и конфиденциальности. Однако мы также должны решать серьезные проблемы, включая проблемы этики и конфиденциальности, потенциальные уязвимости и необходимость идти в ногу с быстрым технологическим прогрессом.

По мере того, как мы движемся в будущее, становится ясно, что ИИ будет играть все более важную роль в кибербезопасности. Непрерывные исследования, инвестиции и бдительность будут иметь решающее значение для использования преимуществ ИИ при одновременном снижении потенциальных рисков и решении проблем.

Кажется, впереди предстоит захватывающий путь, где симбиоз между ИИ и кибербезопасностью будет продолжать переопределять границы возможного в цифровой безопасности.

**Список литературы**

1. 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.
2. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
3. 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.
4. Пестов И. Е., Христофоров Р. О., Швидкий А. А. Анализ подходов к разработке облачных сервисов// Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 752-757.
5. Красов А. В. и др. Построение доверенной вычислительной среды. – 2019.

6. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 438-440.
7. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022. – №. 4s. – С. 92-101.
8. 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.

**References**

1. 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.
2. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for automation of software testing // Naukosphere. – 2020. – no. 6. - pp. 152-156.
3. 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.
4. Pestov I. E., Khristoforov R. O., Shvidkiy A. A. Analysis of approaches to the development of cloud services // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 752-757.
5. Krasov A. V. et al. Construction of a trusted computing environment. – 2019.
6. Gelfand A. M. et al. Applications of big data analytics in critical information infrastructures // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 438-440.
7. Krasov A. V. et al. Actual threats to the security of information in the field of healthcare and ophthalmology // OPHTHALMOSHURGY. – 2022. – no. 4s. - pp. 92-101.
8. Gelfand A. M. et al. Internet of things (iot): threats to security and privacy // Actual problems of infotelecommunications in science and education (APINO 2021). - 2021. - pp 215-220.

Матвеев В.А. Гибкий подход с использованием КАНБАН в управлении рисками информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 15–19

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# ГИБКИЙ ПОДХОД С ИСПОЛЬЗОВАНИЕМ КАНБАН В УПРАВЛЕНИИ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Матвеев В.А.**
*ФГБОУ ВО «Национальный исследовательский ядерный университет «МИФИ», Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail: veevtammatveev@yandex.ru*

**В настоящее время разработка и внедрение программного обеспечения для нужд бизнеса является одним из важнейших направлений информационных технологий. В этом аспекте актуальность приобретают и вопросы информационной безопасности. От грамотного построения и использования системы защиты информации при разработке ПО зависит не только финансовое положение, но и репутация Компании, а также и соблюдение законодательства РФ. Постоянно меняющееся бизнес-окружение накладывает свои ограничения и правила, поэтому применение подходящих методологий влияет на эффективность управления рисками ИБ. Рассмотрен процесс повышения эффективности управления рисками, более действенное реагирование бизнеса и улучшения определенных SLA по управлению рисками.**

Ключевые слова: Канбан, Agile, Информационная безопасность, SLA, оценка, бот.

# A FLEXIBLE APPROACH USING KANBAN TO MANAGE INFORMATION SECURITY RISK

**Matveev V.A.**
*National Research Nuclear University MEPhI, Moscow, Russia (115409, Moscow Kashirskoye shosse, 31), e-mail: veevtammatveev@yandex.ru*

**Currently, the development and implementation of software for business needs is one of the most important areas of information technology. In this aspect, information security issues also become relevant. Not only the financial position, but also the reputation of the Company, as well as compliance with the legislation of the Russian Federation, depends on the competent construction and use of the information security system in software development. The constantly changing business environment imposes its own restrictions and rules, so the use of suitable methodologies affects the effectiveness of information security risk management. The process of improving the efficiency of risk management, a more effective response of the business and improving certain SLAs for risk management is considered.**

Keywords: Kanban, Agile, Information security, SLA, assessment, bot.

На сегодняшний день, информационные технологии, в частности Интернет, являются важным звеном, дающим возможность успешно развиваться бизнесу. Сайты, онлайн сервисы, мобильные приложения и другие варианты использования технологии Интернет позволяют бизнесу и компаниям улучшать свои финансовые и рейтинговые показатели. Все больше компаний стараются не только внедрить различные сервисы, но и развивать их, делать более удобными для аудитории и для контроля сотрудниками. При разработке программного

обеспечения изначально идет процесс планирования, в котором обсуждается все тонкости программного продукта на выходе. Гибкая методология разработки программного обеспечения ориентирована на использовании итеративного подхода, при котором программный продукт создается поэтапно, реализуя определенный набор требований. При этом предполагается, что требования могут изменяться в процессе из-за появления различных нюансов. Команды, использующие гибкие методологии, формируются из высококвалифицированных и опытных разработчиков, которые распределяют между собой различные задачи в процессе создания программного продукта.

Выбор методики управления рисками информационной безопасности, подходящей для каждой организации, зависит от ряда условий ее деятельности [1]:

- зависимость деятельности организации от информационных технологий и значимость для ее деятельности рисков ИБ;
- необходимость детального изучения рисков ИБ и возможность проведения верхнеуровневой оценки рисков и определения базовых направлений по снижению рисков ИБ;
- наличие человеческих, финансовых и временных ресурсов для реализации процесса управления рисками ИБ;
- требования законодательства, регуляторов и других заинтересованных сторон к процессу управления рисками ИБ.

В зависимости от перечисленных условий для разных организаций будет оптимальным выбор разных методологий управления рисками, но, в любом случае, для успешного управления рисками ИБ, выбираемая или разрабатываемая организацией методология управления рисками должна:

- соответствовать потребностям организации;
- быть применимой к организации с учетом корпоративной культуры и имеющихся ресурсов;
- отражать в виде модели реальную ситуацию с перечнем рисков ИБ, являющихся актуальными для организации;
- обеспечивать повторяемость результатов при использовании ее разными группами экспертов;
- быть понятной и прозрачной для всех заинтересованных сторон, включая руководство компании, представителей регуляторов, внешних и внутренних аудиторов.

Рассмотрен проект одной из ведущей российской e-commerce компании, которой доверяют миллионы пользователей [2]. Соответственно в компании серьёзно подходят к вопросам информационной безопасности внутренних и внешних сервисов: бережно относятся к пользовательским данным и разрабатывают собственные сервисы с учётом рекомендаций по информационной безопасности. При этом все равно существует вероятность появления в них уязвимостей, создавая риски безопасности.

Для этого в компании создан проект RISK. Цель проекта RISK в том, чтобы через "управление" этими рисками/уязвимостями, сделать сервисы компании безопаснее.

RISK — это задача, в которой исследуется и исправляется в рамках SLA один конкретный риск безопасности. В задаче описываются следующие условия:

- фиксируется источник информирования о проблеме безопасности;
- исследование уязвимостей приведших к риску;
- оценка критичности риска;
- оценка предварительных действий по закрытию риска;
- анализ системного характера проблемы;
- анализ решений для устранения или снижения риска;
- приведение ссылок на созданные задачи на исправление в соответствующем проекте.

Помимо того, что это непосредственно задача, есть и более объёмное толкование (на самом деле их несколько, но тут мы будем исходить из одного). Воспользуемся для этого документом OWASP Top Ten 2017: Application Security Risks. Злоумышленники разными способами могут атаковать сервис и нанести сервису ущерб (Рисунок 1). Подобные пути представляют собой риски безопасности, которые могут (или не могут) быть достаточно серьезными, чтобы обращать на них внимание.

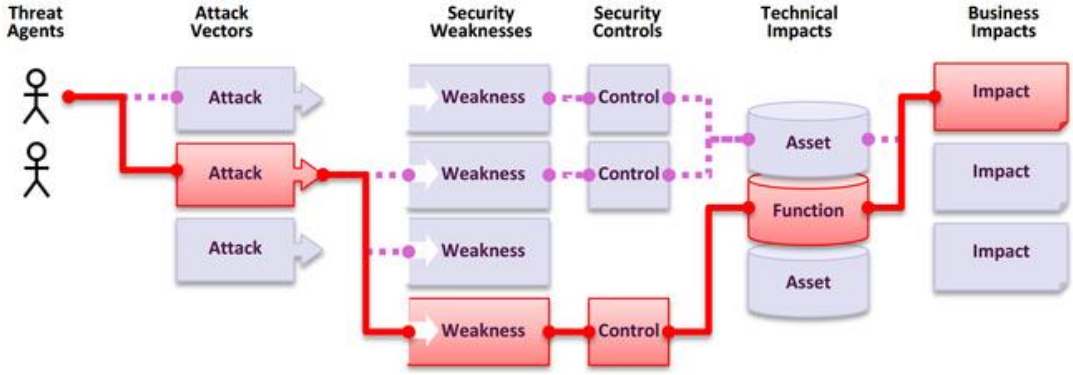



Рисунок 1 – Схема атаки злоумышленника

*Источник: OWASP Top Ten 2017: Application Security Risks [3]*

Иногда эти способы легко найти и эксплуатировать, иногда — очень сложно. Аналогичная ситуация с возможным ущербом: его может не быть совсем или он может дорого стоить бизнесу. Чтобы определить риски, придется оценить вероятности, связанные с источниками угроз, векторами атак и недостатками безопасности, а затем объединить их с оценкой технического и репутационного вреда для компании. Сумма этих факторов определяет совокупный риск.

RISK-тикет заводится тогда, когда каким-либо образом стало известно о какой-либо уязвимости в сервисах компании:

- пришёл репорт от внешнего исследователя безопасности через багбаунти-программу компании;
- статистический анализатор кода обнаружил потенциальную уязвимость.

После проведения первичного исследования, ответственным за исправления риска становится представитель направления или конкретный техлид, в сервисе которого была обнаружена проблема безопасности.

Ответственный за исправления риска следует соответствующей инструкции:

1. Обсудить с инженером ИБ, который завёл тикет, специфику риска безопасности, определить уровень его опасности и согласовать выбранное решение по исправлению;
2. Создать в проекте сервиса соответствующие тикеты на исправление и привязать их к RISK-тикету**;**
3. В соответствие с SLA обеспечить закрытие этих задач и таким образом закрыть RISK;
4. В случае решения тикета, призвать инженера ИБ для проверки исправления.

После того риск безопасности подтвердился инженером ИБ и передан на исправление начинается отчёт времени SLA исправления со стороны сервиса.

Применение элементов искусственного интеллекта в сфере электронной коммерции и услуг является, если и не главным, то одним из основных трендов современных информационных технологий. Среди них наиболее востребованы программируемые модули, так называемые «боты», позволяющие взаимодействовать с пользователями в режиме реального времени.

Боты позволяют минимизировать расходы, связанные с ежедневным и однотипным взаимодействием с большим количеством пользователей. Как и в других сферах бизнеса и производства, автоматизация рабочего процесса целесообразна в том случае, если задачи и цели этого процесса могут быть описаны и конкретизированы. Очевидно, что те функции, которые взяли на себя чат-боты, могут быть реализованы (и успешно реализуются) в более привычной форме – через веб-интерфейс или предустановленные приложения.

В рассмотренной e-commerce компании для форсирования выполнения SLA по исправлению рисков используются следующий процесс:

- Бот ИБ регулярно приходит в неактивные тикеты и уведомляет ответственного о том, что близок или уже исчерпан срок SLA;
- Тикеты эскалируются по следующему алгоритму:
    1. при игнорировании тикета на протяжении трех дней инженер ИБ оповещает ответственного о наличии проблемы;
    2. при очередном двухдневном игнорировании инженер подготавливает эскалацию до руководителей направлений;
    3. при дальнейшем однодневном простое — эскалация идет по тому же принципу с шагом один день до технического директора.

Вывод: в настоящей работе представлено описание возможности применения методологии Канбан в рамках управления рисками информационной безопасности, а также вариант улучшения рабочих процессов с помощью бота, который представляет собой дополнительно разработанный алгоритм по уведомлению и эскалации как инициатора задачи, так и исполнителя.

**Список литературы**

1. Методики управления рисками информационной безопасности и их оценки [Электронный ресурс] – Режим доступа: https://safe-surf.ru/specialists/article/5194/587935/
2. Проект RISK: как мы управляем уязвимостями эффективно [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/ozontech/articles/653517/

3. Application Security Risks [Электронный ресурс] – Режим доступа: https://owasp.org/www-project-top-ten/2017/Application_Security_Risks

**References**

1. Methods of information security risk management and their assessment [Electronic resource] – Access mode:: https://safe-surf.ru/specialists/article/5194/587935//
2. Project RISK: How We Manage Vulnerabilities Effectively [Electronic resource] – Access mode: https://habr.com/ru/companies/ozontech/articles/653517/
3. Application Security Risks [Electronic resource] – Access mode: https://owasp.org/www-project-top-ten/2017/Application_Security_Risks

Сычев Д.И. Основы безопасности облачных данных: преодоление проблем и внедрение передового опыта для надежной защиты // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 20–25

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

# ОСНОВЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ДАННЫХ: ПРЕОДОЛЕНИЕ ПРОБЛЕМ И ВНЕДРЕНИЕ ПЕРЕДОВОГО ОПЫТА ДЛЯ НАДЕЖНОЙ ЗАЩИТЫ

**Сычев Д.И.**
*ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1), e-mail: s.denis_2001@mail.ru*

**На текущем уровне развития информационных технологий, организации все больше полагаются на облачные вычисления для хранения своих данных и потребностей приложений.. Сосредоточив внимание на современных угрозах и стратегиях защиты конфиденциальной информации, ниже обсуждаются проблемы защиты облачных данных, представлен набор передовых методов снижения этих рисков и выделяются потенциальные области для дальнейших исследований. Предоставленная информация призвана помочь организациям разработать комплексные стратегии облачной безопасности, обеспечивающие защиту ценных данных в постоянно развивающемся цифровом ландшафте.**

Ключевые слова: Безопасность облачных данных, информационная безопасность, шифрование.

# BASICS OF CLOUD DATA SECURITY: OVERCOMING PROBLEMS AND IMPLEMENTING BEST PRACTICES FOR RELIABLE PROTECTION

**Sychev D.I.**
*St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, St. Petersburg, Russia (193232, St. Petersburg, Bolshevikov Ave., 22, room 1), e-mail: s.denis_2001@mail.ru*

**At the current level of information technology development, organizations are increasingly relying on cloud computing to store their data and application needs.. Focusing on modern threats and strategies for protecting confidential information, the problems of protecting cloud data are discussed below, a set of best practices for reducing these risks is presented, and potential areas for further research are highlighted. The information provided is intended to help organizations develop comprehensive cloud security strategies that protect valuable data in an ever-evolving digital landscape.**

Keywords: Cloud data security, information security, encryption.

## Введение

В отличие от ранних кибератак, когда злоумышленник атаковал определенный набор IP-адресов или конкретный локализованный центр обработки данных, центы данных в облаке могут быть разбросаны по разным регионам, что расширяет поверхность атаки. Злоумышленники, как правило, используют любую уязвимость, обнаруженную в коде, конфигурациях и развертываниях, что приводит к катастрофическим последствиям для организации.

Данные клиентов и другая конфиденциальная информация являются наиболее важными активами, которыми может обладать та или иная организация, и иногда конкурирующие компании могут использовать услуги киберпреступников, чтобы получить преимущество перед своими конкурентами. Обязанность корпораций состоит в том, чтобы удержать злоумышленников подальше от данных пользователей, используя сочетание самых современных технологий и опытных групп кибербезопасности.

Одна из распространенных ошибок, которую совершают организации, заключается в том, что они считают поставщика облачных услуг гарантом безопасность облачных данных. Большинство поставщиков облачных услуг работают по модели общей ответственности, которая отвечает лишь за обеспечение безопасности базовой инфраструктуры и сетевых компонентов. В то же время именно заказчик несет ответственность за безопасность приложений, серверов и других компонентов, которые он создает в облаке.

Рост удаленной работы и увеличивающаяся зависимость от облачных сервисов усилили важность эффективных стратегий безопасности облачных данных. Цель этой статьи — дать обзор проблем, с которыми сталкиваются организации при защите своих облачных данных, и представить исчерпывающий набор передовых методов, которые помогут справиться с этими сложными проблемами. Понимая риски и применяя соответствующие меры безопасности, предприятия могут защитить свою ценную информацию и сохранить доверие к облачной экосистеме [1-2].

## 1. Проблемы защиты облачных данных

Организации сталкиваются с множеством проблем, когда речь заходит о защите их облачных данных, и понимание этих проблем имеет решающее значение для разработки комплексной стратегии облачной безопасности. Некоторые из наиболее распространенных проблем включают в себя:

- Общая ответственность. Безопасность облачных вычислений часто основывается на модели совместной ответственности, при которой и поставщик облачных услуг (CSP), и заказчик несут ответственность за различные аспекты безопасности. Организации должны четко понимать свои обязанности в этой модели, чтобы гарантировать отсутствие пробелов в безопасности из-за неосведомленности или недопонимания.
- Утечки данных: растущая частота утечек данных является серьезной проблемой для компаний, хранящих конфиденциальную информацию в облаке. Злоумышленники могут использовать уязвимости в облачной инфраструктуре или приложениях для получения несанкционированного доступа к данным, что может привести к значительному финансовому и репутационному ущербу [3].
- Внутренние угрозы. Злонамеренные инсайдеры или скомпрометированные учетные записи внутри организации могут представлять значительный риск для безопасности облачных данных. Сотрудники или подрядчики, имеющие доступ к конфиденциальной информации, могут намеренно или непреднамеренно вызвать утечку данных, подвергая организацию потенциальным юридическим и финансовым последствиям.
- Соблюдение нормативных требований: организации должны соблюдать различные отраслевые нормативные акты и законы о защите данных, такие как GDPR, HIPAA или CCPA, при хранении и обработке данных в облаке. Несоблюдение требований может

привести к крупным штрафам и ущербу для репутации, поэтому компаниям необходимо обеспечить соответствие своих методов обеспечения безопасности в облаке применимым нормам.

- Отсутствие видимости и контроля. В облачной среде организации часто имеют ограниченную видимость своих данных и приложений, что затрудняет эффективный мониторинг и управление безопасностью. Отсутствие контроля может увеличить риск несанкционированного доступа, потери данных или других нарушений безопасности.

Осознавая эти проблемы и оперативно решая их, организации могут создать надежную стратегию облачной безопасности, которая защитит их ценные данные и сведет к минимуму риск инцидентов, связанных с безопасностью [4].

**2. Лучшие практики для защиты облачных данных**

Для эффективной защиты облачных данных и снижения рисков, связанных с проблемами, упомянутыми ранее, организациям следует применять многогранный подход, включающий следующие передовые методы:

- Рекомендуется установление и применение строгой политики контроля доступа, чтобы ограничить доступ к облачным данным и приложениям. Реализуйте принцип наименьших привилегий, гарантируя, что пользователи имеют только необходимые разрешения для выполнения своих рабочих функций. Используйте многофакторную аутентификацию (MFA), чтобы добавить дополнительный уровень безопасности в процесс аутентификации.
- Шифрование конфиденциальных данные как в состоянии покоя, так и во время передачи, чтобы защитить их от несанкционированного доступа. Используйте надежные алгоритмы шифрования и методы управления ключами, чтобы свести к минимуму риск утечки данных.
- Непрерывный мониторинг и аудит облачных сред для выявления потенциальных угроз безопасности, неправильных конфигураций или несанкционированного доступа. Внедряйте автоматизированные инструменты и решения для улучшения видимости и контроля над облачными активами.
- Безопасные резервные копии и планы аварийного восстановления: регулярное сохранение резервных копий важных данных и приложений, чтобы обеспечить быстрое восстановление в случае потери данных или инцидентов безопасности. Разработка и тестирование комплексного плана аварийного восстановления, в котором описаны шаги, которые необходимо предпринять в случае чрезвычайной ситуации.
- Обучение сотрудников методам и политикам безопасности. Проведение регулярных программ обучения и повышения осведомленности, чтобы информировать сотрудников о важности безопасности облачных данных, передовых методиках и организационных политиках. Это может помочь снизить риск внутренних угроз и способствовать развитию культуры безопасности в организации.
- Тесное сотрудничество с поставщиками облачных услуг для обеспечения соответствия требованиям безопасности. Взаимодействие с CSP, чтобы убедиться, что их меры безопасности соответствуют требованиям вашей организации и применимым нормам.

Регулярные оценки безопасности и аудиты вашего CSP для поддержания безопасной облачной среды.

- Внедрение надежного плана реагирования на инциденты. Разработка и поддержка всеобъемлющего плана реагирования на инциденты, в котором излагаются шаги, которые необходимо предпринять в случае нарушения безопасности или других инцидентов. Этот план должен включать четкие роли и обязанности, протоколы связи и процедуры сдерживания, искоренения и восстановления [5].

Применяя эти передовые методы, компании могут разработать надежную и упреждающую стратегию безопасности облачных данных, которая эффективно устраняет проблемы и риски, связанные с хранением конфиденциальной информации в облаке.

### 3. Рекомендации для дальнейших исследований

Поскольку облачные вычисления продолжают развиваться и возникают новые проблемы безопасности, необходимы дальнейшие исследования, чтобы улучшить наше понимание безопасности облачных данных. Некоторые потенциальные области для дальнейших исследований включают [6-7]:

- Изучение применения передовых методов искусственного интеллекта и машинного обучения: исследуйте использование технологий искусственного интеллекта (ИИ) и машинного обучения (МО) для обнаружения и устранения угроз в облачных средах. Эти передовые методы могут помочь автоматизировать идентификацию угроз и реагирование на них, улучшая общее состояние безопасности организации.
- Исследование влияния новых технологий: оцените влияние новых технологий, таких как квантовые вычисления, на методы шифрования и безопасности данных. Понимание того, как эти технологии могут нарушить текущие меры безопасности, поможет организациям подготовиться к будущим угрозам.
- Анализ эффективности различных платформ и сертификатов облачной безопасности. Оцените роль и эффективность различных платформ и сертификатов облачной безопасности в обеспечении защиты данных. Этот анализ может помочь организациям выбрать наиболее подходящие стандарты безопасности и лучшие практики для своих конкретных потребностей.
- Оценка роли государственных постановлений и политик: изучите влияние государственных постановлений и политик на безопасность облачных данных и то, как они могут повлиять на будущее отрасли. Понимание меняющейся нормативно-правовой базы имеет решающее значение для организаций, чтобы соответствовать требованиям и поддерживать безопасную облачную среду.

Проводя дальнейшие исследования в этих областях, предприятия и исследователи могут внести свой вклад в разработку более надежных и адаптивных стратегий безопасности облачных данных, обеспечивающих защиту ценной информации в постоянно меняющемся цифровом ландшафте.

### Вывод

Защита облачных данных — сложная и многогранная задача, требующая комплексного подхода для устранения различных рисков и угроз. Понимая проблемы, связанные с защитой

облачных данных, применяя передовой опыт и получая информацию о последних тенденциях и разработках в области безопасности, организации могут эффективно защищать свою ценную информацию и поддерживать доверие к облачной экосистеме.

По мере того, как облачные вычисления продолжают развиваться и приобретать все большее значение, для предприятий крайне важно оставаться активными в своем подходе к безопасности облачных данных. Это включает в себя не только внедрение лучших практик, изложенных в этой статье, но и формирование культуры осведомленности о безопасности в организации и участие в текущих исследованиях, чтобы опережать возникающие угрозы.

В конечном счете, уделение особого внимания безопасности облачных данных поможет организациям воспользоваться преимуществами облачных вычислений и свести к минимуму риски, связанные с хранением и обработкой конфиденциальной информации в облаке.

**Список литературы**

1. Krasov A. V., Shterenberg S. I. Methods for building a trusted environment in Unix operating systems based on the implementation of a digital watermark //2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). – IEEE, 2020. – С. 253-257.
2. Сахаров Д. В. и др. Разработка модели обеспечения отказоустойчивости сети передачи данных //Известия высших учебных заведений. Технология легкой промышленности. – 2016. – Т. 34. – №. 4. – С. 14-20.
3. Штеренберг С. И., Красов А. В. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки // Учредители: Санкт-Петербургский государственный университет промышленных технологий и дизайна. – №. 1. – С. 26-36.
4. Пестов И. Е. и др. Мониторинг информации инстансов облачной инфраструктуры //Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). – 2023. – С. 216-220.
5. Бугрова Е. С. и др. Анализ методов повышения отказоустойчивости облачной инфраструктуры средствами мониторинга и предсказания состояния компонентов //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 188-192.
6. Пестов И. Е., Христофоров Р. О., Швидкий А. А. Анализ подходов к разработке облачных сервисов //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 752-757.
7. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру //Инновационные решения социальных, экономических и технологических проблем современного общества. – 2021. – С. 113-115.

**References**

1. Krasov A. V., Shterenberg S. I. Methods for building a trusted environment in Unix operating systems based on the implementation of a digital watermark //2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). – IEEE, 2020. – pp. 253-257.

2. Sakharov D. V. et al. Development of a model for ensuring the fault tolerance of a data transmission network // Izvestia of higher educational institutions. Light industry technology. 2016. - T. 34. - No. 4. - pp. 14-20.
3. Shterenberg S. I., Krasov A. V. Bulletin of St. Petersburg state university of technology and design. Series 1: Natural and technical sciences // Founders: St. Petersburg State University of Industrial Technologies and Design. – no. 1. - pp. 26-36.
4. Pestov I. E. et al. Monitoring of information of cloud infrastructure instances // Training of professional personnel in the master's program for the digital economy (PKM-2022). - 2023. - pp. 216-220.
5. Bugrova E. S. et al. Analysis of methods for increasing the fault tolerance of cloud infrastructure by means of monitoring and predicting the state of components // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 188-192.
6. Pestov I. E., Khristoforov R. O., Shvidkiy A. A. Analysis of approaches to the development of cloud services // Actual problems of infotelecommunications in science and education (APINO 2022). - 2022. - pp. 752-757.
7. Pestov I. E., Kosheleva S. A. Attacks on cloud infrastructure // Innovative solutions to social, economic and technological problems of modern society. - 2021. - pp. 113-115.

Пашенко Н. В. Системы безопасности умного дома // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2 с. 26–38

Международный журнал информационных технологий и энергоэффективности

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

УДК 004. 056

# СИСТЕМЫ БЕЗОПАСНОСТИ УМНОГО ДОМА

**Пашенко Н. В.**
*ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», Санкт-Петербург, Россия (195251, Россия, г. Санкт-Петербург, ул. Политехническая, 29), e-mail: pashenko012@gmail.com*

**Системы умных домов активно входят в нашу жизнь и это происходит не просто так, ведь данные системы способны значительно упростить вашу бытовую жизнь, и повысить качество безопасности вашего дома. Уже существуют множества компаний, которые производят различные системы умного дома. вследствие этого возникает вопрос, какую систему умного дома выбрать? Данная статья содержит разбор некоторых ведущих компаний в данной сфере и поможет сделать правильный выбор.**

Ключевые слова: Умный дом, люди с ограниченными возможностями, система, контроллер, мозг.

# SMART HOME SECURITY SYSTEMS

**Pashchenko N. V.**
*St. Petersburg Polytechnic University of Peter the Great , St. Petersburg, Russia (195251, St. Petersburg, Politechnicheskaya str., 29), e-mail: pashenko012@gmail.com*

**Smart home systems are actively entering our lives and this happens for a reason, because these systems can significantly simplify your everyday life and improve the quality of security of your home. There are already many companies that produce various smart home systems. as a result, the question arises, which smart home system to choose? This article contains an analysis of some of the leading companies in this field and will help you make the right choice.**

Keywords: smart home, people with disabilities, system, controller, brain.

## Введение

История развития домашней автоматизации начинается с изобретения первых бытовых приборов, которые использовали электричество для упрощения жизни и были приспособлены к выполнению простых бытовых задач по приготовлению пищи и уборки. Первым бытовым прибором изобретённым стал пылесос, изобретенный в 1901 году, дальше был тостер, домашний холодильник, и т. д. [1,2]

О первых попытках создания умного дома в истории упоминается только в середине двадцатого века, эти единичные попытки домашней автоматизации, выглядели крайне футуристическими экспериментами, которые многих пугали и удивляли. Одним из первых прототипов умного дома был создан американским инженером Эмиля Матиаса, который назывался «Дом с кнопками» (Pash-Button Manor) в 1950 году, в который входит: [3,4]

1. Кнопка управления гаражными дверями.
2. Двигатель с подъемным механизмом гаражных дверей.

3. Датчик охранной сигнализации с выводом сигнала в дом.
4. Кнопка управления гаражными воротами.
5. Включение радио.
6. Спаренный дверной звонок и выключатель света.
7. Автоматические шторы.
8. Автоматические окна
9. Управление окнами
10. Пульт управления светом.

Самое интересное из данного списка, это автоматические окна, в которых отмечался крайне простой принцип работы. Во время дождя вода по водостоку попадает в специальную тарелку, которая находится под напряжением, когда контакты замыкаются, подается напряжение на небольшой двигатель, который через ременную передачу поворачивает рычаг, который в свою очередь тянет трос, трос опускает окно. Когда рычаг доходит до ограничителя, то двигатель выключается. [5,6]

Следующий виток развития в истории домашней автоматизации произошел в 1975 году, когда шотландская организация Pico Electronics [7,8] разработала первый специализированный стандарт управления домашними устройствами который был назван X10. Это развернутый протокол, который позволяет реализовать многие функции умного дома [9,10]. Он задает определенный метод и последовательность действий для передачи управляющих сигналов и различных команд по силовой электропроводке на электронные модули, к которым подключены управляемые электробытовые и осветительные приборы.

Благодаря этому протоколу значительно улучшилась автоматизация управления освещения и управления электроприборами:

1. дистанционно с инфракрасных и радиопультов управления
2. удаленно с помощью телефона и через Интернет
3. по временным сценариям с помощью программируемых таймеров
4. по датчикам освещенности, движения и температуры

Так что же такое умный дом, умный дом – это автоматизированная система, которая позволяет управлять всеми приборами в доме, которые объединены в единую систему. Эта система способна сама принимать и выполнять определенные задачи, без участия непосредственно человека, тем самым значительно упростить ему жизнь. Каждому умному дому можно задать алгоритм, в соответствии с которым система будет управлять различными приборами, такими как освещение, бытовые приборы и т. д. [11,12,13]

Система умного дома многогранна, но в каждом умном доме присутствуют элементы такие как:

1. Контроллер
2. Устройства управления
3. Датчики
4. Актуаторы

Разберем, что делает каждый из этих элементов, начнем с контроллера. Контроллер – это ключевой элемент системы, то есть центр управления, который объединяет все другие части системы друг с другом и предоставляет возможность удаленного доступа.

Устройства управления бывают различных типов:

1. Сенсорная панель, которая находится на центральном контроллере

2. Приложения на смартфоне/планшете
3. С помощью дистанционного пульта
4. С помощью компьютера или ноутбука через специальное ПО
5. С помощью голосового помощника, таких как умные колонки [14,15]

Датчики, которые принимают определенные сигналы из окружающей среды и срабатывают, если происходит определенное событие, например датчик протечек срабатывает, когда под него затекает вода, и он сигнализирует о протечке.

Актуаторы – это исполнительные устройства, которые получают разные команды от контроллера и исполняют их. Это умные розетки, сирены, камеры, свет в доме и т. д. [1]


Рисунок 1 – Система умного дома.

Технологии умного дома помогут в разы облегчить жизнь людям с ограниченными возможностями. Снижение физической активности могут вызывать проблемы с повседневными задачами по дому. Некоторые элементы, которые значительно упростят жизнь людям с ограниченными возможностями:

1. Термостаты
2. Осветительные устройства
3. Дверной замок
4. Дверной звонок
5. Роботизированные пылесосы
6. Гаражные ворота
7. Шторы и жалюзи
8. Детектор окиси углерода

Каждый из элементов дома можно автоматизировать, чтобы элементы системы работали по командам или через приложение на смартфоне, таким образом можно уменьшить зависимость от членов семьи или опекунов. [16]

В качестве примера приведу 35-летнего жителя в Гамильтоне, который живет в специально простроенном доме, автоматизированные функции которого контролируются через приложение на его смартфоне. Благодаря этому его жизнь стала намного проще, не нужно ждать пока откроется входная дверь, чтобы выйти на улицу, или дождаться члена

семьи, чтобы он включил ему свет в комнате и многие другие простые вещи, которые он не может сделать сам. [17,18]

Так, например в статье [9] говорится о вспомогательных технологиях для людей с деменцией, живущих дома, данная категория людей не способна в должной мере ухаживать за собой, в случае модификации их домов, можно значительно упростить им жизнь.

В статье [19] сказано о мониторинге присутствия жильцов дома, и последующей оптимизации энергопотребления здания. Система умного дома поможет сократить потребление электроэнергии.

Статья [20] говорит нам о том, что сейчас внедряют стационарную реабилитацию после инсульта на дому, а благодаря умному дому, можно будет значительно проще проходить реабилитацию.

Целью статьи [21] являлось исследование программ по уходу за больными в домашних условиях с помощью умной одежды и умного дома. Мониторинг помог выявить информацию о повседневной жизнедеятельности и помог оказывать своевременную помощь больным, если что-то идет не так.

Автор статьи [22] проводит качественное исследование по содействию реабилитации пожилых людей, живущих дома. Умный дом, позволяет проводить наблюдение за физическим состоянием пожилых людей, также за состоянием электроприборов в доме, сигнализируя о их неисправности.

Из-за пандемии многие люди перешли на работу из дома. В условиях самоизоляции система умного дома способна создать все условия для работы дома, а именно экономить время за счет автоматизации ежедневных дел, управлять освещенностью во всем доме или в каждой комнате отдельно, следить за рабочим временем, чтобы не было перенапряжения, подавать больше воздуха в помещение, где происходит работа, следить за состоянием работника. [23]

В статье [24] представлены системы управления энергопотреблением умного дома, которые могут демонстрировать цели по снижению энергопотребления в жилом секторе. Система управления энергопотреблением умного дома получает в качестве входных данных прогнозы спроса, возобновляемых источников энергии, тем самым способна сократить количество потребляемой энергии.

Исходя из вышеперечисленных статей, система умный дом завоевывает все большую популярность. Умный дом способен значительно упростить жизнь каждого человека независимо от его физического состояния, но дело не только в упрощении жизни, но и в безопасности жилища, которую умный дом поможет обеспечить. Уже придумали многочисленные системы для сохранения порядка в доме и на прилегающей к нему территории.

**Методы и материалы**

На данный момент в мире открывается все больше и больше различных компаний со своей уникальной технологией умного дома, например такие как Livihom, Xiaomi, Intelliger, Modern Security Solutions, Rubetek, Korolab, Navigator, Бестрон, Insytr Electronics, Razumdom, HouseClever, MOIO, Synilogy [25].

В результате достаточного и, можно сказать, изобильного предложения компаний-производителей данных систем, у потребителя возникает проблема выбора, что указывает на

необходимость подробнее узнать о функционалах определенных систем, предлагаемых компаниями. Из-за многообразия и различных вариаций наполненности систем умного дома, каждый человек может подобрать систему, отвечающую именно его потребностям.

Безопасность умного дома состоит из:

1. Система охранной сигнализации
2. Пожарная сигнализация
3. Система контроля от протечек
4. Контроль доступа

Система охранной сигнализации делится на несколько типов:

1. Охрана внутри дома
2. Охрана периметра дома
3. Охрана периметра участка

В доме это могут быть датчики движения, датчики на размыкание дверей, окон, датчики на разбития стекол. На участке датчики, которые стоят на заборе, и по всему периметру участка, и в случае проникновения на участок они сработают. Так же в каждой комнате расположен пожарный датчик, и в случае возникновения дыма, сработает оповещение о возникновении пожара. Система контроля от протечек устанавливается, в потенциально опасные зоны, такие как ванная комната, кухня, в случае возникновения протечки, перекрывается вода в доме. Контроль доступа может быть разнообразна, можно подключить карточки считывателя вместо ключа, по отпечатку пальца или лица.

Для полноценного проживания в умном доме нужно разобраться в его системе безопасности. Разберем основные критерии оценивания:

1. Центр управления – должен обладать понятными, удобными настройками, оперативно откликаться на поставленные задачи
2. Функционал – чем шире возможности, тем меньше забот у собственника
3. Датчики – должны обладать хорошей чувствительностью, без ошибок передавать полученную информацию
4. Исполнительное оборудование – чем больше техники, бытовых электронных устройств можно адаптировать в «Умный дом», тем выше уровень комфорта
5. Вид связи – подключение к оборудованию и системам оповещения может выполняться с помощью проводов, каналами GSM или Wi-Fi
6. Комплектация – продаются готовые решения и отдельные компоненты, которые позволяют собрать комплекс с учетом индивидуальных потребностей.

Исходя из этого, в работе использовались такие методы, как сравнение, систематизация, обобщение, анализ функционала систем (с использованием данных компаний-поставщиков) и экспертных оценок (на основе отзывов потребителей). В данной работе в качестве потенциального покупателя рассматриваются различные категории людей, например, заказчики с ограниченными физическими возможностями, пожилые люди, люди с временно ограниченной трудоспособностью из-за болезни или травм, а также обычные современные пользователи, стремящиеся к повышению уровня комфорта и обеспечения безопасности своей жизни и жилища.

Заключительным этапом работы являлось проведения анализа и сравнения продукции интернет-магазинов и официальных сайтов представителей компаний, предоставляющих услуги по установке систем умного дома с выбранными критериями оценки для подбора

функционала систем, совместимости с различными приборами и обладающего оптимальными характеристиками, соотношением цены и качества, а также отвечающим потребностям определенного потребителя.

**Результаты**

В мире очень много компаний, которые предоставляют свою продукцию, но чем же руководствоваться при выборе устройств. Для того чтобы выбрать индивидуально подходящую систему нужно исходить из сценариев, которые универсальны для всех. Например, для всех важна безопасность и компании предоставляют датчики протечки и под раковиной, и в ванной комнате, если они регистрируют протечку воды, то автоматически краны перекрывают поступающею воду в квартире или доме. Срабатывание датчика связываются через уведомление на смартфон, например, при срабатывании датчика дыма приходит уведомление о возможном возгорании, затем владелец квартиры или дома может удаленно посмотреть по камерам наличие задымления в помещении и вызвать пожарных находить за сотни километров от дома. На окнах и дверях установлены датчики открытия и вибрации, при срабатывании они подадут сигнал на телефон, а по камерам можно посмотреть не проникли посторонний в помещение.

Чтобы более детально разобраться, что предоставляют компании, рассмотрим некоторые из них и сравним системы безопасности умного дома, которые нам представляют компании: Ayax, Livihom, Xiaomi, Rubitek, Synoligy.

Ayax крайне проста в установке и использовании систем безопасности, он подключается за пару минут, нужно подключить главному мозг всей системы к питанию и к сетевому кабелю интернета, после этого нужно скачать приложение и система готова. К главному мозгу всей системы можно подключать различные модули, которые значительно расширяют возможности безопасности. Например, есть уличная или домашняя сирены, которые включаются если сработал датчик открытия дверей или датчик движения, так же есть датчик движения с камерой, который мгновенно отправит три фотографии вам на смартфон, если кто-то проникнет в дом и таких датчиков много, и каждый из них имеет встроенную батарейку, которая обеспечивает пару лет автономной работы и позволяет быстро подключиться ко всей системе. К главному мозгу всей системы подключаются внешние модули и камеры-сенсора протечек, датчики движения, и в случае, если что-то произойдет, он тут же отправит уведомление на смартфон. Для подключения модулей компания Ayax разработала свой протокол радиосвязь, который называется Jeweler, сигнал передается на чистоте 868 МГц, по заявлению компании он гораздо стабильнее и у него больше радиус действия чем у Wi-Fi, таким образом Jeweler позволяет передавать маленький объем информации на большее расстояния и при этом он очень энергоэффективный. Так же эта система предоставляет датчики задымления и датчики протечки воды, каждый датчик можно установить или на двойной скотч, либо на саморезы, и если в процессе работы датчика его снять, то он тут же сообщит вам об этом. Все сенсоры работают очень быстро, например датчик протечек, меньше, чем за одну секунду сигнализирует вам. Датчик дыма реагирует либо на задымление, либо на температуру выше 60 градусов цельсия, либо на резко возрастающую температуру. Приложение Ayax крайне просто в управлении и слежении за всеми датчиками, которые находятся у вас дома. [26]

Одной из популярных систем безопасности значится компания Livihom. Существует бесплатное мобильное приложение, которое позволяет управлять всем домом в вашем смартфоне, регистрация в данном приложении происходит беспроблемно, остается только подключить все приборы, которые у вас есть. Как говорит их официальный сайт, что для обмена информацией применяются датчики с 128-битнымим AES-алгоритмом шифрования, которые обеспечат проверку подлинности подключённых устройств и исключают риски подмены оборудования, помимо этого обмен данными производится исключительно в зашифрованном виде, что гарантирует надежную защиту от взлома. Устройства компании Livihom гарантируют стабильную работу на протяжении 10 лет, без замены источников питания. Сигналы с датчиков имеют высокую чувствительность и мгновенную передачу информации меньше чем за 10 мс на расстоянии до 1 км на открытом пространстве. Так же датчики работают в любые погодные условия, параметры устройств автоматически подстраиваются под окружающую температуру. Еще одним из преимуществ данной системы является то, что к одной системе можно подключить до 256 различных радиоустройств, то есть задействовать каждое окно или дверь, автоматизировать каждый уголок своего дома. [27,28]

Система от производителей Xiaomi значительно отличается от предшественника. Вся система представляет из себя миниатюрные датчики, которые можно прикрепить к любой поверхности вашего дома. Так же имеется удобное приложение, через которое можно подключить себе все приборы. Установка и настройка достаточно проста, базовый комплект содержит пару инфракрасных датчиков движения, так же датчики открытия окон и дверей и один беспроводной выключатель. Важно упомянуть о том, что система Xiaomi не ограничена базовой комплектацией, в нее можно добавлять различные радиоустройства, но от того же производителя. В отличии от системы Livihom, главный мозг системы Xiaomi нужно подключать на определенном расстоянии от всех приборов, то есть ее обмен данными происходит на небольшом расстоянии, но также быстро. Главная проблема Xiaomi, заключается в том, что хоть и вся продукция находится под единым брендом, но она работает в разных стандартах, какие-то через Wi-Fi, какие-то через Bluetooth и устройства не могут общаться между собой и часто все команды проходят через центральный сервер, который может находиться в Китае. [29]

Компания Rubitek представляет так же, как и Xiaomi миниатюрные датчики, которые, легко можно установить на любой поверхности вашего дома. Центр управления является блоком, который объединяет до 64 устройств, работающих на чистоте RF 868 МГц и позволяет управлять ими удаленно с помощью смартфона, голосовых помощников или сценария. Так же можно всю систему объединить с другими системами, такими как Яндекс, Google, Apple Homekid. Приложение крайне удобно, с его помощью можно отслеживать энергопотребление за определённый период, создать сценарий, по которому будет выполняться работа во всем умном доме и так же оперативно получать уведомление от всех приборов, которые подключены к системе. Так же компания Rubitek представляет беспроводной выключатель, то есть дистанционная панель управления, которую можно поместить в удобных местах по дому, с помощью которой так же удобно управлять всеми электроприборами в доме. [30]

Слоган компания Synology «Безопасность – наш приоритет», компания предлагает усовершенствованные и универсальные решения для обеспечения безопасности, которые позволяют быстрее адаптироваться к развивающимся технологиям, и угрозам. Данная

компания не может похвастаться простотой в установки или миниатюрности своих приборов, но при этом, их продукция на высоком уровне справляется с поставленной задачей. Компания предоставляет надежную систему от взлома и мгновенного оповещения, если он произошел, после оповещение на мобильное устройство, есть выбор, или установление распространение проблемы, или вызова специальных служб, в зависимости, где произошла проблема. Так же данная система, не ограниченная только своими электроприборами, а также способна быть связана и с другими компаниями. [26]

Системы компаний Ayax, Livihom, Xiaomi и Rubitek отличаются высоким спросом, хорошим функционалом, простотой установки и управления, а также своей компактностью. Однако ключевыми различиями и решающими аспектами для покупателя являются такие факторы, как: удаленность, с которой можно получить сигнал; ценовой сегмент, здесь стоит отметить, что системы Rubitek и Livihome в 3 раза превышают стоимость систем Xiaomi; относительная сложность установки оборудования, например, для Livihome характерен непосредственный монтаж оборудования в стены, двери и т. д. Отдельно хотелось бы выделить компанию Synoligy, потому что она значительно выбивается из ценового сегмента, так как электроприборы занимают значительную площадь по сравнению с другими представителями, установка данной системы занимает долгий процесс и цена выше чем у Xiaomi в 15 раз и больше, но тот функционал и качество продукции которое предоставляет данная компания оправдывает такую сумму.

Результатом исследований были выявлены на сколько системы умного дом полезны и много функциональны, благодаря им можно автоматизировать все бытовые приборы, а также беспокоится о своей безопасности, так как вся информация, что происходит дома и на его участке фиксируется. Так же экономить электроэнергию, выставляя сценарии работы электроприборов. Все функции умного дома позволяют сделать домашнюю жизнь более безопасной и менее энергозатратной для человека, как так все за вас будет делать ваш дом.

**Заключение и обсуждение**

Системы умного дома в наше время, это уже не что-то новое и фантастическое, её может приобрести каждый, кто хочет упростить себе жизнь. Он позволит:

1. Переводить квартиру в энергосберегающий режим, когда никого нет дома
2. Задавать сценарии освещения, включать и выключать свет автоматически
3. Перекрывать воду в случае протечки
4. Контролировать влажность и температуру
5. Заботиться о питомцах: подливать воду и насыпать корм, регулировать освещение в аквариуме, выпускать животное на улицу
6. Показывать, что происходит в квартире
7. Помогать в воспитании детей: ограничивать доступ к телевизору или интернету, отслеживать время прихода домой
8. Предупреждать о пожаре
9. Отключать питание электроприборов
10. Убирать, варить кофе и решать за вас прочие бытовые вопросы

Система умного дома не просто может упростить вашу жизнь, а полностью обеспечить вам наилучшую и беззаботное проживание в вашем доме. Время, которое помогает система умного дома сэкономить, можно потратить на свои хобби, то есть, полностью отдаться себе.

В нашей сфере жизни уже существуют множество различных компаний, предоставляющих услуги по установке и продаже систем умного дома с выбранными критериями оценки для подбора функционала систем, совместимости с различными приборами и оптимального соотношения цены и качества, которые готовы предоставить своё видение умного дома, свою продукцию, для усовершенствования вашего дома.

Основные различия будут проявляться в:

1. Стоимости системы умного дома
2. Комплектации системы умного дома
3. Связи со сторонними производителями
4. Материал, из которого состоит система
5. Качество и дальность связи
6. Внешний вид
7. Управление

В остальном продукция различных компаний идентична, везде используется главный контроллер, по которому можно задать сценарий действий умного дома, так же различный датчики, которые подключаются которые управляются контроллером.

Исследование показало на сколько система умного дом полезна и многофункциональна, благодаря ей можно автоматизировать все бытовые приборы. Кроме того, человек может быть уверен в своей безопасности, умный дом, фиксирует всю информацию о доме и его участке, позволяет анализировать все что происходит в доме и создавать удобные сценарии для проживания каждого дня. Также экономить энергию, выставляя в сценариях работы электроприборов.

Так же стоить отметить, что система умного дома продемонстрировала свою актуальность при использовании ее людей с ограниченными возможностями, которые наблюдаются у специалистов. Так же система умного дома помогает упростить жизнь не только людям с ограниченными возможностями, которые проживают в этих дома, но и людям, которые следят за безопасностью и состояние здоровья этих жильцов.

В заключении хотелось бы сказать, что возможности, которые предоставляет система умного дома, значительно помогут упростить жизнь в нем. При нынешних технологиях умного дома наука не собирается останавливаться на месте, а продолжает прогрессировать, провалятся различные эксперименты, разработки в сфере робототехники, которые хотят создать роботизированную машину оснащению искусственным интеллектом. Данные роботизированные машины, сейчас внедряют в различные сферы, такие как:

1. Промышленность
2. Транспорт
3. Добыча полезных ископаемых
4. Банковские сервисы, электронная коммерция

Это малый список того, где активно используются роботизированные машины с искусственным интеллектом, и надеюсь, что в скором времени, создадут такую электронную машину, которая поможет создать наилучшие условия для жизни в домашних условиях.

**Список литературы**

1. История умного дома [Электронный ресурс]. Tech-house.su . – URL: https://tech-house.su/istoriya-poyavleniya-umnogo-doma / (12.03.2022)

2. Степаненко С. "Умный дом" - Микропроцессорное устройство управления. Статья в журнаре – научная статья. Номер 7(89), год 2008, С. 50–53
3. Эмиль Матиас. Отец "Умного дома". «Популярная механика». 27.12.19
4. Pico Electronics [Электронный ресурс]. Picoelectronics.com . – URL: https://picoelectronics.com / (12.03.2022)
5. Игнатов Сергей. Подробное описание протокола X10. «Главный журнал электрики». 28.04.2017
6. Елена Бем. Умный дом: что это такое, зачем он нужен и как он работает. 29.03.2020.
7. Нил Макмахон. Как высокотехнологичный дом может облегчить жизнь людям с ограниченными возможностями. 5 апреля 2015
8. Система "Умный Дом" [Электронный ресурс]. Tech-house.su . – URL: https://tech-house.su/sistema-umnyj-dom-chto-eto-tehnologiya-postrojki-i-upravleniya / (12/03/2022)
9. Колос С.А. Роль умного дома в жизни людей с ограниченными возможностями. ФГБОУ ВО "Брянский государственный университет имени академика И.Г.Петровского". 10.11.2021
10. Керноу, Элеонора, Раш, Роберт, Горска, Сильвия, Фоузит, Кирсти. Различия в вспомогательных технологиях, установленных для людей с деменцией, живущих дома, которые подвергаются риску блуждания и безопасности. BMC Geriatrics. 21(1). Doi 10.1186/s12877-021-02546-7
11. Андрей Ищенко. Лучшие системы "умного дома". 14.10.2021.
12. Хоу, И-Цзюнь, Цзэн, Си-Ин, Линь, Чжун-Чжи, Ян, Цзин-цзы, Хуан, Хуэй-Лин, Чэнь, Мин-Чи, Цай, Сю-Синь, Лян, Джерси, Шю, Да-Англ. Программа ухода на дому с использованием "умной одежды" для семейных опекунов пожилых людей с деменцией и переломом тазобедренного сустава: исследование с использованием смешанных методов. BMC Geriatrics 22(1). Doi 10.1186/s12877-022-02789- y
13. Карлссон, Маргарета, Нойдстрем, Бригитта. Использование и обмен знаниями при внедрении стационарной реабилитации на дому после инсульта: барьеры и факторы, способствующие управлению изменениями. BMC Health Services Research. 22(1)/ doi: 10.1186/s12913-022-07618- икс.
14. Платтс, Кэтрин, Брекон, Джефф, Маршалл, Эллен. Принудительная работа на дому в условиях карантина и ее влияние на благополучие сотрудников: перекрестное исследование. BMC Public Health. 22(1). Doi: 10.1186/s12889-022-12630-1
15. Кольцасаклис, Никилаос, Панапакидис, Лоаннис, Христофедис, Георгиос, Кнапек, Ярослав. Поддержка процессов энергоменеджмента "умного дома" с помощью алгоритмов машинного обучения. Энергетические отчеты. 8. Doi: 10.1016/j.egyr.2022.01.033
16. Пожарная сигнализация [Электронный ресурс]. Livicom.ru . – URL: https://livicom.ru/examples-fire-alarm (27.03.2022)
17. Обзор набора смарт-датчиков Xiaomi Mi Smart Sensor Set. [Электронный ресурс]. Eldorado.ru . – URL: https://blog.eldorado.ru/publications/obzor-xiaomi-mi-smart-sensor-set-obzory-546 (27.03.2022)
18. Комплект интеллектуальных датчиков Mi. [Электронный ресурс]. Megaobzor.com . - URL: https://megaobzor.com/Obzor-Xiaomi-Mi-Smart-Sensor-Set.html (11.04.2022)

19. Степаненко С. "УМНЫЙ ДОМ" - МИКРОПРОЦЕССОРНОЕ УСТРОЙ-СТВО УПРАВЛЕНИЯ. Статья в журнаре – научная статья. Номер 7(89), год 2008, С. 50–53
20. Датчик утечки воды 868 МГц. [Электронный ресурс]. Rubitek.com . – URL: https://rubetek.com/catalog/datchiki/datchik-protechki-vody-rs-3225 / (11.04.2022)
21. Производители систем умный дом [Электронный ресурс]. Производи-тель.рф. – URL: https://xn--b1aedfedwrdfl5a6k.xn--p1ai/producers/sistemy-umnyy-dom (11.04.2022)
22. Сонг, Л. Служба контекстной осведомленности о режиме взаимодействия пользователей Интернета вещей в интеллектуальной среде / Л. Сонг. Служба контекстной осведомленности о режиме взаимодействия пользователей Интернета вещей в интеллектуальной среде. Достижения в области мультимедиа. Doi: 10.1155/2022/2466032 .
23. Лю К., Ван К., Чен Дж., Феng Дж. Частотно-временное внимание для распознавания речевых эмоций с блоками сжатия и возбуждения. Конспекты лекций по информатике (включая подсерии "Конспекты лекций по искусственному интеллекту" и "Конспекты лекций по биоинформатике"). Документ конференции. DOI: 10.1007/978-3-030-98358-1_42
24. Сюй, Дж. Интеллектуальное управление отелями на фоне больших данных. Коммуникации в области вычислительной техники и информатики. Документ конференции. DOI: 10.1007/978-981-19-0852-1_26
25. Прия С.С., Рачана П., Челлани Д. Дополненная реальность и управление речью при демонстрации автомобилей. Материалы 4-й Международной конференции по интеллектуальным системам и изобретательским технологиям. DOI: 10.1109/ICSSIT53264.2022.9716534
26. Сюй З., Ли П. Прогресс в гидрологическом реагировании на урбанизацию: механизмы, методы и решения. Охрана водных ресурсов, 38 (1). DOI: 10.3880/j.issn.1004-6933.2022.01.002
27. Глэденс Л.М., Сангита К.К., Саундхария С., Ревати С., Селван М.П. Система мониторинга "Умного дома" и прогнозирования энергопотребления. Материалы 6-й Международной конференции по компьютерным методологиям и коммуникации. DOI: 10.1109/ICCMC53470.2022.9753722
28. Чжан Х., Юй С., Чжоу Х., Хуан П., Го Л., Ли М. Атака и защита с эмуляцией сигнала для интернета вещей "Умный дом". Транзакции IEEE по надежным и безопасным вычислениям. DOI: 10.1109/TDSC.2022.3169705
29. Мун Х.-С., Сонг Дж., Шин Х., Чан Дж. Блокчейн-платформа для управления домашними устройствами интернета вещей с использованием смарт-контрактов и контрмеры против 51% атак. Серия материалов международной конференции ACM, стр. 191-195. DOI: 10.1145/3512353.3512381
30. Цветанов С., Папапостолу Т., Димитров С., Андонов И. Интеллектуальный контроллер для современных тепловых систем. (2022) Конспекты лекций по сетям и системам, 319, стр. 618-624. DOI: 10.1007/978-3-030-85540-6_78

**References**

1. History of the smart house [Electronic resource]. Tech-house.su .–URL: https://tech-house.su/istoriya-poyavleniya-umnogo-doma / (12.03.2022)

2. Stepanenko S. "Smart House" - Microprocessor control device. An article in the journal is a scientific article. Issue 7(89), year 2008, pp. 50–53
3. Emil Mathias. The father of the "Smart Home". "Popular mechanics". 27.12.19
4. Pico Electronics [Электронный ресурс]. Picoelectronics.com . – URL: https://picoelectronics.com / (12.03.2022)
5. Ignatov Sergey. A detailed description of the X10 protocol. "The Main Journal of Electrics". 28.04.2017
6. Elena Bem. Smart home: what it is, why it is needed and how it works. 29.03.2020.
7. Neil McMahon. How a high-tech home can make life easier for people with disabilities. 5 April 2015
8. System "Smart House" [Electronic resource]. Tech-house.su . – URL: https://tech-house.su/sistema-umnyj-dom-chto-eto-tehnologiya-postrojki-i-upravleniya / (12/03/2022)
9. Kolos S.A. The role of a smart home in the lives of people with disabilities. Bryansk State University named after Academician I.G. Petrovsky. 10.11.2021
10. Kernow, Eleanor, Rush, Robert, Gorska, Sylvia, Fawuzit, Kirsty. Differences in assistive technology established for people with dementia living at home who are at risk of wandering and safety. BMC Geriatrics. 21(1). Doi 10.1186/s12877-021-02546-7
11. Andrey Ishchenko. The best smart home systems. 14.10.2021.
12. Hou, Yi-Jun, Zeng, Si-Ying, Lin, Zhong-Zhi, Yang, Jing-tzu, Huang, Hui-Ling, Chen, Ming-Chi, Tsai, Hsu-Xin, Liang, Jersey, Shu, Da-Ingle. A Smart Clothing Home Care Program for Family Caregivers of Older Adults with Dementia and Hip Fracture: A Mixed-Methods Study. BMC Geriatrics 22(1). Doi 10.1186/s12877-022-02789- y
13. Karlsson, Margareta, Neudström, Brigitte. Using and sharing knowledge in the implementation of inpatient rehabilitation at home after stroke: barriers and factors that contribute to change management. BMC Health Services Research. 22(1)/ DOI: 10.1186/S12913-022-07618- x.
14. Platts, Catherine, Brecon, Jeff, Marshall, Ellen. Forced work from home under quarantine and its impact on employee well-being: a cross-sectional study. BMC Public Health. 22(1). Doi: 10.1186/s12889-022-12630-1
15. Kolsaklis, Nikilaos, Panapakidis, Loannis, Christofeidis, Georgios, Knapek, Jaroslav. Support for smart home energy management processes using machine learning algorithms. Energy reports. 8. Doi: 10.1016/j.egyr.2022.01.033
16. Fire alarm [Electronic resource]. Livicom.ru . – URL: https://livicom.ru/examples-fire-alarm (27.03.2022)
17. Overview of the Xiaomi Mi Smart Sensor Set. [Electronic resource]. Eldorado.ru . – URL: https://blog.eldorado.ru/publications/obzor-xiaomi-mi-smart-sensor-set-obzory-546 (27.03.2022)
18. Mi Smart Sensor Kit. [Electronic resource]. Megaobzor.com . - URL: https://megaobzor.com/Obzor-Xiaomi-Mi-Smart-Sensor-Set.html (11.04.2022)
19. Stepanenko S. "SMART HOME" - MICROPROCESSOR CONTROL DEVICE. An article in the journal is a scientific article. Issue 7(89), year 2008, pp. 50–53
20. 868 MHz water leakage sensor. [Electronic resource]. Rubitek.com . – URL: https://rubetek.com/catalog/datchiki/datchik-protechki-vody-rs-3225 / (11.04.2022)
21. Manufacturers of smart home systems [Electronic resource]. Proizvoditel.rf. – URL: https://xn--b1aedfedwrdfl5a6k.xn--p1ai/producers/sistemy-umnyy-dom (11.04.2022)

22. Song, L. Contextual Awareness Service on the Interaction Mode of Internet of Things Users in an Intelligent Environment / L. Song. Contextual awareness service for IoT user interaction mode in an intelligent environment. Advances in multimedia. Doi: 10.1155/2022/2466032 .
23. Liu K, Wang K, Chen J, Feng J. Frequency-time attention for recognition of speech emotions with compression and excitation blocks. Lecture notes on computer science (including the subseries "Lecture Notes on Artificial Intelligence" and "Lecture Notes on Bioinformatics"). Document of the conference. DOI: 10.1007/978-3-030-98358-1_42
24. Xu, J. Intelligent hotel management against the backdrop of big data. Communications in the field of computer engineering and informatics. Document of the conference. DOI: 10.1007/978-981-19-0852-1_26
25. Priya S.S., Rachana P., Chellani D. Augmented reality and speech control in car demonstrations. Proceedings of the 4th International Conference on Intelligent Systems and Inventive Technologies. DOI: 10.1109/ICSSIT53264.2022.9716534
26. Xu Z., Li P. Progress in hydrological response to urbanization: mechanisms, methods and solutions. Water Resources Protection, 38 (1). DOI: 10.3880/j.issn.1004-6933.2022.01.002
27. Gladens L.M., Sangeeta K.K., Soundhariya S., Revati S., Selvan M.P. Smart Home Monitoring System and Energy Forecasting. Proceedings of the 6th International Conference on Computer Methodologies and Communication. DOI: 10.1109/ICCMC53470.2022.9753722
28. Zhang H., Yu S., Zhou H., Huang P., Guo L., Li M. Attack and protection with signal emulation for the Internet of Things "Smart Home". IEEE transactions for reliable and secure computing. DOI: 10.1109/TDSC.2022.3169705
29. Moon H.-S., Song J., Shin H., Jang J. Blockchain platform for managing home IoT devices using smart contracts and countermeasures against 51% of attacks. ACM International Conference Proceedings Series, pp. 191-195. DOI: 10.1145/3512353.3512381
30. Tsvetanov S., Papapostol T., Dimitrov S., Andonov I. Intelligent controller for modern thermal systems. (2022) Lecture Notes on Networks and Systems, 319, pp. 618-624. DOI: 10.1007/978-3-030-85540-6_78

Киселев Н.С. Построение матричной модели для анализа непрерывно дискретных систем // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31)ч.2 с. 39–47

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.02

# ПОСТРОЕНИЕ МАТРИЧНОЙ МОДЕЛИ ДЛЯ АНАЛИЗА НЕПРЕРЫВНО ДИСКРЕТНЫХ СИСТЕМ

**Киселев Н.С.**
*ФГБОУ ВО " Казанский Государственный Энергетический Университет", Казань Россия (420066, Республика Татарстан, город Казань, Красносельская ул, д. 51)***,** *e-mail: kis_48@mail.ru*

**Рассмотрен метод построения модели для анализа непрерывных и дискретных процессов на примере логических и электронных схем. Предложен метод построения объединенной непрерывно-дискретной модели на основе матрицы смежности.**

Ключевые слова: Модель непрерывно дискретных систем, матрицы смежности, матрицы инцидентности.

# CONSTRUCTION OF A MATRIX MODEL FOR THE ANALYSIS OF CONTINUOUSLY DISCRETE SYSTEMS

**Kiselev N.S.**
*Kazan State Power Engineering University, Kazan, Russia (420066, Republik of Tatarstan, Kazan city, Krasnoselskaya street, 51), e-mail: kis_48@mail.ru*

**The method of constructing a model for the analysis of continuous and discrete processes on the example of logic and electronic circuits is considered. A method for constructing a combined continuous-discrete model based on the adjacency matrix is proposed.**

Keywords: Model of continuously discrete systems, adjacency matrices, incidence matrices.

Многие современные технические системы представляют из себя совокупность устройств с непрерывными и дискретными технологическими процессами. К непрерывным, например, относятся электрические, химические, тепловые, гидродинамические, диффузионные и ряд других. Дискретные процессы реализуют, как правило, системы управления, ручного или автоматического.

Большую часть в этих системах составляют системы, связанные с передачей и преобразованием различного рода потоков - информационные, энергетические, потоки жидкостей и газов и др.

Для анализа таких систем на разных уровнях детализации в качестве моделей используют разнообразный математический аппарат: численные методы решения дифференциальных уравнений, алгебру логики, теорию графов, сети Петри, теорию массового обслуживания и др., с хорошо разработанными методами решения [1, 2, 3].

Разнообразие методов и моделей создает определенные трудности:

- для более полного анализа требуемой задачи необходимо построение нескольких моделей для разных уровней детализации поставленной задачи
- повышаются профессиональные требования к специалистам, поскольку они должны: владеть большим разнообразием методов моделирования на разных уровнях, уметь сопрягать модели разных уровней и интерпретировать результаты их моделирования.

В работе предлагается объединить непрерывные и дискретные модели в рамках единого матричного подхода к построению единой модели.

Рассмотрим построение гибридной модели на примере схемы содержащей электрические (аналоговые) и логические (дискретные) элементы.

Для логических схем в качестве модели удобно использовать матричную модель вида [4]

$$\boldsymbol{S_o = M\ \Theta\ S_i} \quad (1)$$

или

$$\begin{vmatrix} s_{o1} \\ s_{o2} \\ \dots \\ s_{on} \end{vmatrix} = \begin{vmatrix} m_{11} & m_{21} & \dots & m_{n1} \\ m_{12} & m_{22} & \dots & m_{n2} \\ \dots & \dots & \dots & \dots \\ m_{1n} & m_{2n} & \dots & m_{nn} \end{vmatrix} \begin{vmatrix} \odot_1 \\ \odot_2 \\ \dots \\ \odot_n \end{vmatrix} \begin{vmatrix} s_{i1} \\ s_{i2} \\ \dots \\ s_{in} \end{vmatrix} \quad (2)$$

Пусть задана логическая схема и ее граф (Рисунок 1).

Вершинам графа соответствуют элементы схемы, включая входы и выходы, а ребрам – связи между элементами. Направление ребер соответствует направлению передачи сигналов (потоков информации).

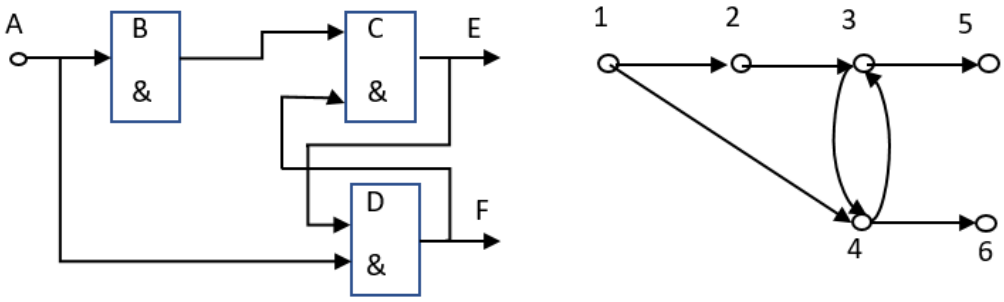



Рисунок 1 – Схема и ее граф

Для графа и схемы построим матрицу смежности и вектор функций элементов (Рисунок 2).

Каждая строка матрицы определяет входы в элемент (например: в элемент – ***B***, вершина графа 2 входом является элемент ***A***, вершина графа 1). Функция элемента ¬& ***(И-НЕ***). Задав начальное значение на входе схемы, можно вычислить значение на элементе ***B*** (строка матрицы 2). Пробегая все строки можно определить состояние всех элементов в некоторый начальный момент времени. Данный алгоритм описывается выражениями 1 и 2.

| № п/п | 1 | 2 | 3 | 4 | 5 | 6 | Функция элементов схемы |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | вход |
| 2 | 1 | | | | | | ¬& |
| 3 | | 1 | | 1 | | | ¬& |
| 4 | 1 | | 1 | | | | ¬& |
| 5 | | | 1 | | | | выход |
| 6 | | | | 1 | | | выход |

Рисунок 2 – Матрица смежности с функциями элементов схемы

При построении математической модели электрических схем также используется граф схемы. При этом вершинам графа соответствуют цепи, а ребрам компоненты (двухполюсные).

Рассмотрим построение матрицы смежности для аналоговой схемы. В качестве примера возьмем рисунки из [5] (Рисунок 3).

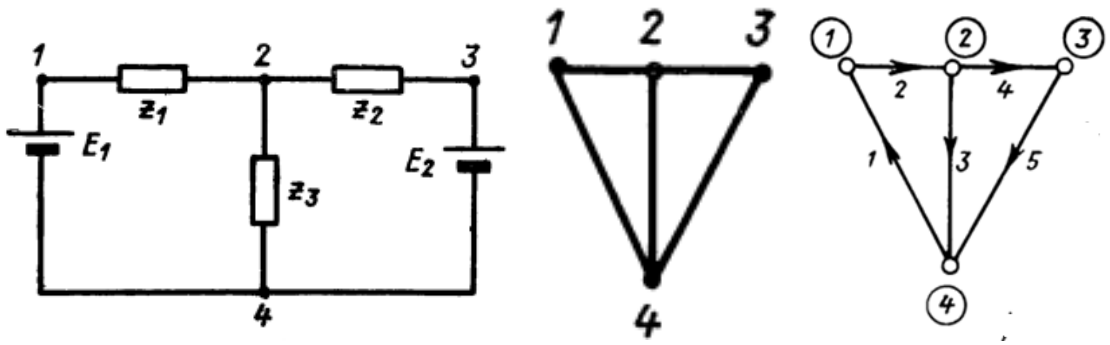



Рисунок 3 – Схема, её граф и ориентированный граф

На основе ориентированного графа можно построить матрицу инциденций (соединений), представленную на Рисунке 4. Матрица показывает соединение узлов и ветвей ориентированного графа. В каждом столбце единицами отмечены в строках, соответствующих узлам, начала (-1) и концы ветвей (1).

| Узлы | Ветви | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| ① | 1 | -1 | | | |
| ② | | 1 | -1 | -1 | |
| ③ | | | | 1 | -1 |
| ④ | -1 | | 1 | | 1 |

Рисунок 4 – Матрица инциденций (матрица соединений)

Известно, что данную матрицу можно использовать для записи законов Кирхгофа. Обозначив матрицу буквой $\boldsymbol{A}$ выражение закона Кирхгофа для токов (ЗКТ) запишется в виде $\boldsymbol{AI=0}$, а для закона Кирхгофа для напряжений $\boldsymbol{A^tU = 0}$, где $\boldsymbol{t}$ – знак транспонирования.

Матрица смежности для этой же схемы представлена на Рисунке 5. имеет блочный вид. Два блока выделены жирными линиями. Обозначим блоки матрицы символами ***B*** для правого верхнего и ***C*** для левого нижнего.

| | ① | ② | ③ | ④ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|
| ① | | | | | 1 | | | | |
| ② | | | | | | 1 | | | |
| ③ | | | | | | | | 1 | |
| ④ | | | | | | | 1 | | 1 |
| 1 | | | | 1 | | | | | |
| 2 | 1 | | | | | | | | |
| 3 | | 1 | | | | | | | |
| 4 | | 1 | | | | | | | |
| 5 | | | 1 | | | | | | |

Рисунок 5 – Матрица смежности

Сопоставляя эти две матрицы можно заметить, что первая матрица ***A*** получается из второй, если у неё взять левый нижний блок, умножить на (-1) и транспонировать, а затем сложить с правым верхним блоком. Также можно получить транспонированную матрицу $\boldsymbol{A^t}$. Для этого левый нижний блок надо умножить на (- 1 ), и сложить с транспонированной правым верхним блоком.

Или $\boldsymbol{A} = \mathrm{B} + \mathrm{C}^{\boldsymbol{t}} * (\boldsymbol{-1})$ (3)

и $\boldsymbol{A^t} = (\boldsymbol{-1}) * \boldsymbol{C} + \boldsymbol{B^t}$ (4)

Полученная модифицированная матрица представлена на Рисунке 6.

| | ① | ② | ③ | ④ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|
| ① | | | | | 1 | -1 | | | |
| ② | | | | | | 1 | -1 | -1 | |
| ③ | | | | | | | | 1 | -1 |
| ④ | | | | | -1 | | 1 | | 1 |
| 1 | 1 | | | -1 | | | | | |
| 2 | -1 | 1 | | | | | | | |
| 3 | | -1 | | 1 | | | | | |
| 4 | | -1 | 1 | | | | | | |
| 5 | | | -1 | 1 | | | | | |

Рисунок 6 – Структурная матрица для ЗК

Уравнения законов Кирхгофа на основе полученной матрицы можно записать следующим образом

$$\begin{bmatrix} \boldsymbol{0} & \boldsymbol{A} \\ \boldsymbol{A^t} & \boldsymbol{0} \end{bmatrix} * \begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{I} \end{bmatrix} = \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix} \quad (5)$$

Для получения полной системы уравнений необходимо добавить компонентные уравнения для токов и напряжений [6].

Построить полную систему уравнений из исходной модели в матричном виде можно, если в граф на Рисунке 3 добавить дополнительные вершины (Рисунок 7.).

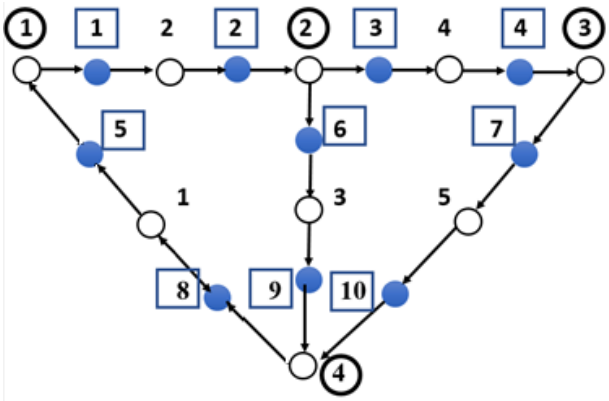



Рисунок 7 – Граф с дополнительными вершинами.

Дополнительные вершины выделены цветом и отмечены номерами в квадратиках. Матрица смежности для данного графа представлена на Рисунке 8.

В полученной матрице невозможно увидеть блоки как-то сходные с блоками матрицы на Рисунке 5. Однако при перестановке строк и одноименных столбцов можно получить матрицу, представленную на Рисунке 9.,

Очевидно, что в новой матрице есть два блока таких же, как и на Рисунке 5, и два единичных блока.

Перестановка строк и одноименных столбцов равносильна перенумерации вершин графа. Дополнительная нумерация на Рисунке 9 соответствует графу на Рисунке 10.

| — | ① | ② | ③ | ④ | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ① | | | | | | | | | | | | | | 1 | | | | | |
| ② | | | | | | | | | | | 1 | | | | | | | | |
| ③ | | | | | | | | | | | | | 1 | | | | | | |
| ④ | | | | | | | | | | | | | | | | | | 1 | 1 |
| 1 | | | | | | | | | | | | | | | | | 1 | | |
| 2 | | | | | | | | | | 1 | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | 1 | | | | |
| 4 | | | | | | | | | | | | 1 | | | | | | | |
| 5 | | | | | | | | | | | | | | | | 1 | | | |
| 1 | 1 | | | | | | | | | | | | | | | | | | |
| 2 | | | | | | 1 | | | | | | | | | | | | | |
| 3 | | 1 | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | 1 | | | | | | | | | | | |
| 5 | | | | | 1 | | | | | | | | | | | | | | |
| 6 | | 1 | | | | | | | | | | | | | | | | | |
| 7 | | | 1 | | | | | | | | | | | | | | | | |
| 8 | | | | 1 | | | | | | | | | | | | | | | |
| 9 | | | | | | | 1 | | | | | | | | | | | | |
| 10 | | | | | | | | | 1 | | | | | | | | | | |

Рисунок 8 – Матрица смежности для графа с дополнительными вершинами

| | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ① | ② | ③ | ④ | 1 | 2 | 3 | 4 | 5 | 5 | 2 | 9 | 4 | 10 | 8 | 1 | 6 | 3 | 7 |
| | ① | | | | | | | | | | 1 | | | | | | | | | |
| | ② | | | | | | | | | | | 1 | | | | | | | | |
| | ③ | | | | | | | | | | | | | 1 | | | | | | |
| | ④ | | | | | | | | | | | | 1 | | 1 | | | | | |
| | 1 | | | | | | | | | | | | | | | 1 | | | | |
| | 2 | | | | | | | | | | | | | | | | 1 | | | |
| | 3 | | | | | | | | | | | | | | | | | 1 | | |
| | 4 | | | | | | | | | | | | | | | | | | 1 | |
| | 5 | | | | | | | | | | | | | | | | | | | 1 |
| 1 | 5 | | | | | 1 | | | | | | | | | | | | | | |
| 2 | 2 | | | | | | 1 | | | | | | | | | | | | | |
| 3 | 9 | | | | | | | 1 | | | | | | | | | | | | |
| 4 | 4 | | | | | | | | 1 | | | | | | | | | | | |
| 5 | 10 | | | | | | | | | 1 | | | | | | | | | | |
| 6 | 8 | | | | 1 | | | | | | | | | | | | | | | |
| 7 | 1 | 1 | | | | | | | | | | | | | | | | | | |
| 8 | 6 | | 1 | | | | | | | | | | | | | | | | | |
| 9 | 3 | | 1 | | | | | | | | | | | | | | | | | |
| 10 | 7 | | | 1 | | | | | | | | | | | | | | | | |

Рисунок 9 – Матрица с переставленными строками и столбцами

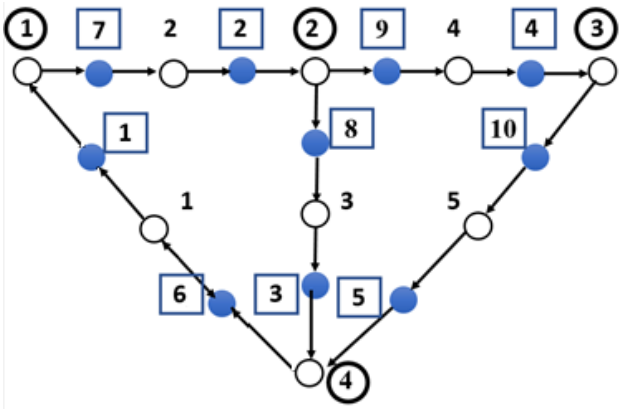



Рисунок 10 – Граф с перенумерованными вершинами

В символьном виде матрицу на Рисунке 7 можно представить следующим образом:

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \boldsymbol{B} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I} \\ \mathbf{0} & \boldsymbol{I} & \mathbf{0} & \mathbf{0} \\ \boldsymbol{C} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \quad (6)$$

А с учетом преобразований 3 и 4.

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \boldsymbol{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \boldsymbol{I} \\ \mathbf{0} & \boldsymbol{I} & \mathbf{0} & \mathbf{0} \\ \boldsymbol{A^t} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \quad (7)$$

Выражение (7) является основой для системы уравнений для токов, напряжений и компонентных уравнений.

В результате полученных рассуждений видно, что системы уравнений электрических схем можно получить не только из матриц инциденций, но и из матриц смежности. При этом получаются как топологические, так и компонентные уравнения. Таким образом, использование матриц смежности, как для логических, так и электрических схем, с методологической точки зрения упрощает алгоритм построения разнородных моделей.

**Список литературы**

1. Парийская Е.Ю., Сравнительный анализ математических моделей и подходов к моделированию и анализу непрерывно–дискретных систем. Дифференциальные уравнения и процессы управления, №1, 1997, Электронный журнал, с.91-120
2. Якимов И.М., Кирпичников А.П., Мокшин В.В. Моделирование сложных систем в среде имитационного моделирования GPSS W с расширенным редактором. Вестник казанского технологического университета, Том: 17, №: 4 2014, с.: 298-303
3. Киселев Н.С. Матричный метод моделирования непрерывно-дискретных схем //Информатика 87. 2 Всесоюзная конференция. Ереван: Арм.ССР,1987.- с.251
4. Киселев Н.С. Матричная модель для анализа логических схем большой размерности//Исследования по информатике. Выпуск 1. Научно-практическое издание. Институт проблем информатики АН РТ. Сборник трудов. Казань: Отечество, 1999, с.95-100
5. Ильин В.И. Машинное проектирование электронных схем. - М.: Энергия, 1972
6. Шиманская-Семенова, Т.А. Применение матричных моделей для расчета и анализа режимов электрических сетей: методическое пособие по выполнению курсовой работы и изучению дисциплины «Математические модели в энергетике» для студентов специальности 1-43 01 02 «Электроэнергетические системы и сети» / Т.А. Шиманская-Семёнова. – Минск: БНТУ, 2010. – 158 с.

**References**

1. Pariyskaya E.Yu., Comparative analysis of mathematical models and approaches to modeling and analysis of continuous–discrete systems. Differential Equations and Control Processes, No. 1, 1997, Electronic Journal, pp.91-120
2. Yakimov I.M., Kirpichnikov A.P., Mokshin V.V. Modeling of complex systems in the GPSS W simulation environment with an extended editor. Bulletin of Kazan Technological University, Volume: 17, no.: 4 2014, pp.: 298-303
3. Kiselev N.S. Matrix method of modeling continuous-discrete circuits //Informatics 87. 2 All-Union Conference. Yerevan: Arm.SSR, 1987.- p.251
4. Kiselev N.S. Matrix model for the analysis of large-dimensional logic circuits//Computer science research. Issue 1. Scientific and practical edition. Institute of Computer Science Problems of the Academy of Sciences of the Republic of Tatarstan. Collection of works. Kazan: Fatherland, 1999, pp.95-100
5. Ilyin V.I. Machine design of electronic circuits. - M.: Energiya, 1972
6. Shimanskaya-Semenova, T.A. Application of matrix models for calculation and analysis of modes of electric networks: a methodological guide for the course work and the study of the

discipline "Mathematical models in power engineering" for students of specialty 1-43 01 02 "Electric power systems and networks" / T.A. Shimanskaya-Semenova. – Minsk: BNTU, 2010. – p.158

Кириллина Ю.В., Чуркин А.С. Реинжиниринг процесса управления файлами бортовой базы данных интеллектуальной системы автоматизированного вождения поездов// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 48–53

Международный журнал информационных технологий и энергоэффективности

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

УДК 625

# РЕИНЖИНИРИНГ ПРОЦЕССА УПРАВЛЕНИЯ ФАЙЛАМИ БОРТОВОЙ БАЗЫ ДАННЫХ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ВОЖДЕНИЯ ПОЕЗДОВ

**[1] Кириллина Ю.В., [2]Чуркин А.С.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: [1]jvk05@mail.ru, [2]churkin.a.s@edu.mirea.ru*

**В статье рассматривается текущее исполнение процесса управления файлами бортовой базы данных интеллектуальной системы автоматизированного вождения поездов, применяемой ОАО «РЖД» и затрагивающей деятельность нескольких организаций. Анализ процесса позволил выявить основные проблемы в его исполнении и предложить изменения на основе применения единой информационной системы, для чего была представлена общая схема выполнения процесса. Новый вариант исполнения процесса управления файлами бортовой базы данных интеллектуальной системы автоматизированного вождения поездов позволяет отказаться от необходимости физического присутствия локомотива для осуществления обновления файлов.**

Ключевые слова: Интеллектуальная система автоматизированного вождения поездов, процесс управления файлами бортовой базы данных системы, проблемы исполнения процесса, реинжиниринг процесса.

# REENGINEERING OF THE FILE MANAGEMENT PROCESS OF THE ON-BOARD DATABASE OF THE INTELLIGENT AUTOMATED TRAIN DRIVING SYSTEM

**[1] Kirillina Y.V., [2] Churkin A.S.,**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: [1]jvk05@mail.ru, [2]churkin.a.s@edu.mirea.ru*

**The article discusses the current execution of the file management process of the on-board database of the intelligent automated train driving system used by JSC "Russian Railways" and affecting the activities of several organizations. The analysis of the process made it possible to identify the main problems in its execution and propose changes based on the use of a unified information system, for which a general scheme of the process was presented. A new version of the file management process of the on-board database of the intelligent automated train driving system allows you to eliminate the need for the physical presence of the locomotive to update the files.**

Keywords: Intelligent automated train driving system, the process of managing the files of the onboard database of the system, process execution problems, process reengineering.

Сегодня у подавляющего большинства компаний наблюдается тенденция уменьшения роли человека в процессах, происходящих в организации, а также тенденция снижения их стоимости за счёт оптимизации расхода ресурсов. ОАО «РЖД» не является исключением. Одно из направлений оптимизации расходования ресурсов в последние 20 лет — это

автоматизация управления подвижным составом с помощью внедрения интеллектуальной системы автоматизированного вождения поездов (ИСАВП-РТ) в каждый грузовой локомотив. Автоматизированное управление с использованием интеллектуальной системы автоматизированного вождения поездов повышенной массы и длины с распределенными по длине локомотивами осуществляется в режиме оптимального расхода электроэнергии при точном выполнении времени хода. Использование ИСАВП-РТ способствует повышению безопасности движения и облегчает труд машиниста. Для получения максимальной выгоды от использования системы автоматизированного ведения поезда необходимо регулярно и своевременно актуализировать бортовую базу данных. [2, 3, 4, 5]

Основная задача сотрудников, занятых в железнодорожной отрасли, в рамках процесса управления файлами бортовой базы данных системы ИСАВП-РТ состоит в поддержании бортовой базы данных системы в актуальном состоянии.

Процесс управления файлами бортовой базы данных системы ИСАВП-РТ обширен, затрагивает работу сразу нескольких крупных структур: дирекция управления движением ОАО «РЖД», дирекция тяги ООО «РЖД», ООО «АВП Технология», ООО «ЛокоТех-Сервис», эксплуатационные и сервисные (ремонтные) депо. [1]

Начало процесса — это формирование расписания движения поездов и составления набора параметров, необходимых для корректной работы ИСАВП-РТ, в дирекции управления движением ОАО «РЖД». Далее расписание и набор параметров попадает в ООО «АВП Технология», где происходит их преобразование в файлы, предназначенные для ИСАВП-РТ. В свою очередь файлы вновь попадают в дирекцию управления движением ОАО «РЖД», после чего происходит их размещение на сервере ОАО «РЖД» с последующим копированием на сервер ООО «ЛокоТех-Сервис», где файлы хранятся до востребования. Одновременно с этими процессами дирекция управления движением ОАО «РЖД» уведомляет дирекцию тяги ООО «РЖД» о выходе нового расписания движения и обновлении набора параметров для ИСАВП-РТ, последняя в свою очередь рассылает приказы о необходимости обновления БД ИСАВП-РТ в эксплуатационное депо. После руководителями эксплуатационного депо (ТЧЭ) и ремонтного депо (ТЧР) формируются заявки на обновление БД ИСАВП-РТ, организуется перегонка локомотивов в установленной очереди из ТЧЭ в ТЧР, где и происходит обновление файлов БД ИСАВП-РТ. [1]

Общая схема выполнения процесса управления файлами бортовой базы данных системы ИСАВП-РТ представлена на Рисунке 1.

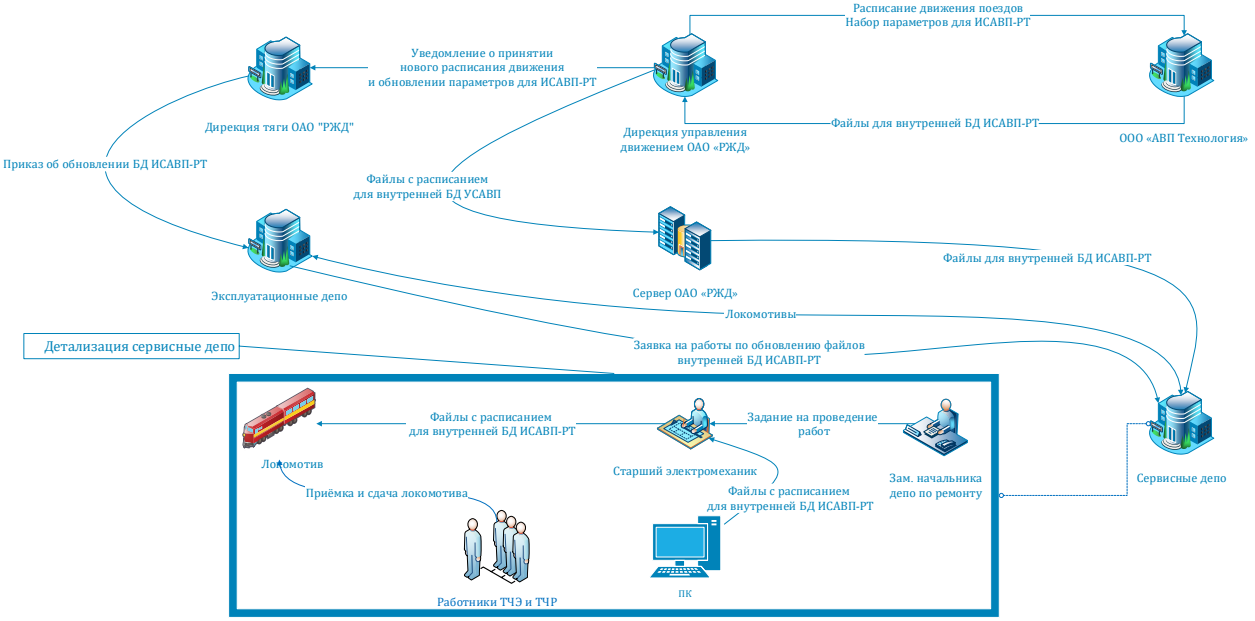



Рисунок 1 – Общая схема процесса «Управление файлами бортовой базы данных системы ИСАВП-РТ» (as is)

В настоящее время обновление файлов базы данных ИСАВП-РТ часто происходит совместно с одним из видов технического обслуживания (ТО) или сервисных работ (СР), производящихся по заранее составленному графику. Реже обновление происходит, как отдельный вид модернизации локомотива. График проведения данных видов работ на локомотиве, в подавляющем большинстве случаев, составляется без учёта графика изменения расписания движения поездов, он так же не привязан к изменениям параметров, необходимых для корректной работы ИСАВП-РТ. Очень часто обновление не производится поскольку текущая информация в базе данных ИСАВП-РТ на момент проведения ТО или СР всё ещё актуальна, но это не означает, что изменения не вступят в силу в ближайшее время. [1]

Получается, что ИСАВП-РТ, установленная на локомотиве, продолжает работать с базой данных, информация в которой может потерять актуальность в любой момент, а восстановить актуальность данных получится только в рамках следующего цикла ТО или СР.

В результате анализа текущего исполнения процесса было выявлено, что:

1. Процесс управления файлами бортовой базы данных системы ИСАВП-РТ в настоящее время слабо автоматизирован и требует вовлечения большого числа сотрудников, что приводит к увеличению материальных и временных затрат на его проведение. Из-за отсутствия автоматизации повышаются риски, связанные с человеческим фактором, которые могут понести за собой катастрофические последствия, связанные с выходом из строя локомотивного оборудования.

2. Процесс сбора и передачи данных системой информирования машиниста с функцией электронного маршрута машиниста (АСИМ-ЭММ), напротив, автоматизирован полностью, но информация, получаемая в рамках данного процесса, почти не задействуется для оптимизации железнодорожного движения. На данный момент информация используется при ведении расследований в отношении железнодорожных инцидентов.

3. Данные, участвующие в обоих процессах, имеют разных владельцев и носят критический характер в отношении железнодорожной инфраструктуры, что сильно повышает требования к обеспечению их безопасности при хранении, обработке и передаче. Попадание этих данных в руки злоумышленников ставит под угрозу функционирование всей железнодорожной отрасли, что влечёт за собой экономические убытки в особо крупных объёмах, как для ОАО «РЖД», так и для её партнёров.

В качестве решения для устранения выявленных проблем предлагается использовать единую систему хранения информации о состоянии ИСАВП-РТ каждого локомотива, осуществлять централизованное обновление файлов базы данных ИСАВП-РТ, что исключит ошибки при обновлениях, связанных с человеческим фактором, приводящих к выходу из строя ИСАВП-РТ. Также предполагается сбор и централизованное хранение информации из АСИМ-ЭММ для формирования аналитических отчётов, на основании которых можно производить более тонкую настройку ИСАВП-РТ.

На Рисунке 2 показана общая схема процесса удаленного управления файлами бортовой базы данных ИСАВП-РТ, сбора и обработки данных АСИМ-ЭММ в новом варианте.

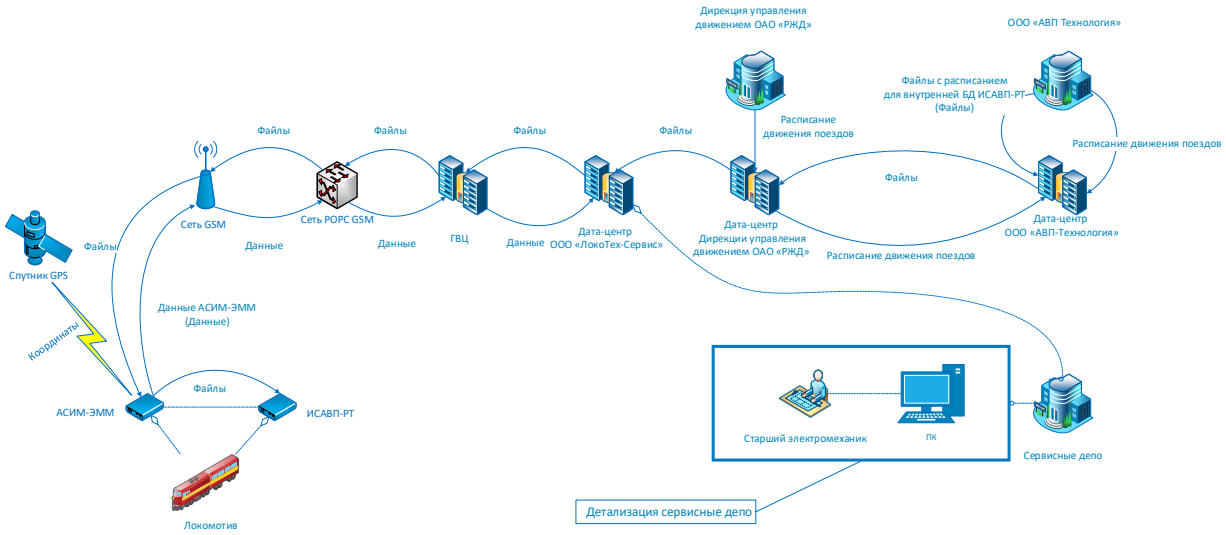



Рисунок 2 – Общая схема процесса «Управление файлами бортовой базы данных системы ИСАВП-РТ» (to be)

Благодаря реинжинирингу процесса путем его автоматизации временные и материальные затраты на процесс сократятся, поскольку физическое присутствие локомотива в ТЧР более не требуется, а значит не требуется задействовать персонал для его перемещения из ТЧЭ в ТЧР и по территории последнего, для его последующей приёмки на модернизацию, проведения модернизации, заполнения множества сопроводительных документов, а также работ по приёмке локомотива в эксплуатацию с последующей перегонкой из ТЧР назад в ТЧЭ. Эти нововведения позитивно отразятся на коэффициенте полезного действия локомотива и сотрудников ТЧЭ, ТЧР. [6]

**Список литературы**

1. Положение о порядке взаимодействия ремонтного локомотивного депо — структурного подразделения дирекции по ремонту тягового подвижного состава— филиала ОАО «РЖД» и эксплуатационного локомотивного депо — структурного подразделения дирекции тяги — филиала ОАО «РЖД» (В ред. Распоряжений ОАО «РЖД» от 27.03.2013 N 728р, от 08.08.2013 N 1724р, от 02.12.2013 N 2636р), (Утверждено распоряжением ОАО «РЖД» от 29 декабря 2012 г. N 2763р).
2. Система ИСАВП-РТ 2ЭС4К (3ЭС4К) Инструкция по загрузке программного обеспечения АЮВП.468382.027ИС, 2018.
3. Система ИСАВП-РТ 2ЭС5 Руководство по эксплуатации АЮВП.468382.021РЭ, 2015.
4. Система информирования машиниста автономная с функцией электронного маршрута машиниста АСИМ-ЭММ. [Электронный ресурс] — Режим доступа: https://www.avpt.ru/products/dlya-gruzovykh-lokomotivov/sistema-informirovaniya-mashinista-avtonomnaya-s-funktsiey-elektronnogo-marshruta-mashinista-asim-em/, свободный. — Загл. с экрана. — Яз. рус. Дата обращения (01.05.2023).
5. Система информирования машиниста автономная с функцией электронного маршрута машиниста АСИМ-ЭММ. Руководство по эксплуатации АЮВП.467249.002РЭ, 2020.
6. Цифровое депо. Новый уровень ремонта локомотивов. Аргументы и факты. Иркутск. [Электронный ресурс]. — Режим доступа: https://irk.aif.ru/society/cifrovoe_depo_novyy_uroven_remonta_lokomotivov, свободный. — Загл. с экрана. — Яз. рус. Дата обращения (01.05.2023).

**References**

1. Regulation on the procedure for interaction between the repair locomotive depot — structural subdivision of the Directorate for the repair of traction rolling stock —— branch of JSC "Russian Railways" and the operational locomotive depot — structural subdivision of the Directorate of traction — branch of JSC "Russian Railways" (As amended. Orders of JSC "Russian Railways" dated 27.03.2013 N 728r, from 08.08.2013 N 1724r, from 02.12.2013 N 2636r), (Approved by the order of JSC "Russian Railways" dated December 29, 2012 N 2763r).
2. ISAVP-RT system 2ES4K (3ES4K) Instructions for downloading the software AYUP.468382.027 IS, 2018.
3. ISAVP-RT 2ES5 system Operating Manual ONVP.468382.021RE, 2015.
4. The driver's information system is autonomous with the function of the driver's electronic route ASIM-EMM. [Electronic resource] — Access mode: https://www.avpt.ru/products/dlya-gruzovykh-lokomotivov/sistema-informirovaniya-mashinista-avtonomnaya-s-funktsiey-elektronnogo-marshruta-mashinista-asim-em/, Cover from the screen. — Yaz. rus. Date of application (01.05.2023).
5. The driver's information system is autonomous with the function of the driver's electronic route ASIM-EMM. Operating manual AUVP.467249.002RE, 2020.
6. Digital depot. A new level of locomotive repair. Arguments and facts. Irkutsk. [electronic resource]. — Access mode:

https://irk.aif.ru/society/cifrovoe_depo_novyy_uroven_remonta_lokomotivov, Cover from the screen. — Yaz. rus. Date of application (01.05.2023).

Макеева О.В., Шарипов А.А. Проектирование автоматизированной информационной системы медицинских учреждений // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2. с. 54–60

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

**[1] Макеева О.В., Шарипов А.А.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: [1]makeeva-oks@yandex.ru*

**Статья посвящена процессу разработки автоматизированной информационной системы для медицинских учреждений на базе средства разработки Django. В статье будет рассмотрена модульная архитектура системы, основные функциональные возможности и преимущества использования данной системы для медицинских учреждений так же будет рассмотрен процесс разработки, описание ключевых элементов системы и ее основных модулей.**

Ключевые слова: Автоматизированная информационная система, Медицинская информационная система, медицинские учреждения, модульность, пользовательский интерфейс, управление медицинской информацией, эффективность, качество услуг, Django, Python, PostgreSQL

# DESIGN OF AN AUTOMATED INFORMATION SYSTEM OF MEDICAL INSTITUTIONS

**[1] Makeeva O.V, A.A. Sharipov**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: [1]makeeva-oks@yandex.ru*

**The article is devoted to the process of developing an automated information system for medical institutions based on the Django development tool. The article will consider the modular architecture of the system, the main functionality and advantages of using this system for medical institutions, as well as the development process, a description of the key elements of the system and its main modules.**

Keywords: automated Information system, medical information system, medical institutions, modularity, user interface, medical information management, efficiency, quality of services, Django, Python, PostgreSQL.

Медицинские учреждения имеют дело с большим объемом информации о пациентах, медицинских записях, результатами обследований, назначениями и назначенными лекарствами. Управление этой информацией может быть очень сложным и затратным процессом, особенно если это делается вручную. В таких случаях автоматизированные информационные системы могут существенно упростить этот процесс и повысить эффективность работы медицинских учреждений [1].

Медицинская информационная система — это не просто система для управления клиникой, а элемент медицинской экосистемы, где МИС её ядро [8].

В коммерческих медицинских учреждениях информационные процессы организованы вокруг МИС, в то время как в государственных учреждениях значительная часть информационного обмена связана с региональной МИС. Региональная МИС, в свою очередь, является важной составляющей экосистемы Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ). МИС выступает связующим звеном в этой схеме взаимодействия.

Экосистема создается путем привлечения к информационному взаимодействию всех участников процесса. На Рисунке 1 представлены основные участники, с которыми взаимодействуют медицинские учреждения различных типов.

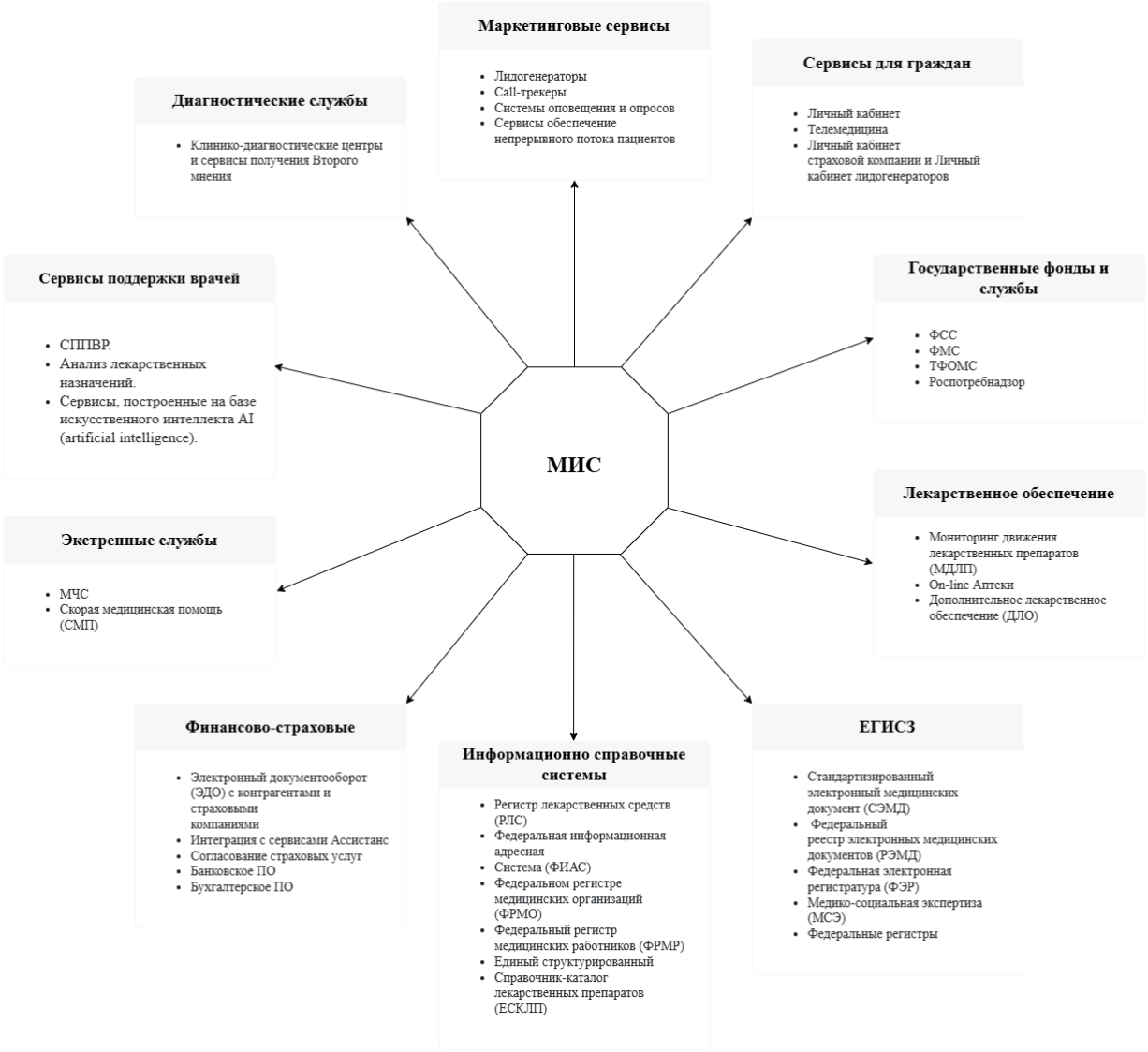



Рисунок 1 – Участники цифровой экосистемы

**Преимущества данного решения**

1. Быстрый старт: Django имеет множество встроенных функций и модулей, которые упрощают создание веб-приложений. Это позволяет быстро начать работу над МИС, не тратя много времени на разработку базовой функциональности.
2. Гибкость и масштабируемость: Django позволяет создавать приложения любого уровня сложности и масштабировать их по мере необходимости. Благодаря использованию шаблонов и механизмов маршрутизации, Django упрощает разработку сложных функций МИС.
3. Безопасность: Django предоставляет множество инструментов для обеспечения безопасности приложений, включая защиту от атак CSRF и XSS, проверку вводимых пользователем данных и управление доступом.
4. Поддержка: Django имеет активное сообщество разработчиков и официальную документацию, что делает его легким в использовании и обновлении.
5. Интеграция: Django может интегрироваться с другими приложениями и сервисами, такими как базы данных, облачные хранилища, почтовые сервисы и т.д.
6. Стоимость: Использование Django для создания МИС может снизить общую стоимость проекта за счет сокращения времени и ресурсов, затрачиваемых на разработку.

В дальнейшем тексте будут более подробно описаны ключевые элементы и модули системы, а также преимущества использования данной системы для медицинских учреждений.

**Существующие ИС для управления медицинскими учреждениями на базе Django**

Существует множество информационных систем для управления медицинскими учреждениями, разработанных на базе Django. Одним из наиболее популярных примеров такой системы является "GNU Health".

GNU Health — это бесплатная система управления медицинской информацией, которая используется в медицинских учреждениях по всему миру. Она также разработана на базе Django + Python и PostgreSQL и предоставляет полный набор функций для управления информацией о пациентах, медицинских записях, назначениях и назначенных лекарствах.

Кроме того, существуют другие ИС на базе Django + Python, которые могут быть адаптированы для использования в медицинских учреждениях в зависимости от конкретных требований и потребностей. Такие системы могут быть как открытыми, так и коммерческими, что предоставляет медицинским учреждениям широкий выбор вариантов для управления медицинской информацией.

**Анализ требований к проектируемой системе**

АИС для медицинских учреждений должна быть модульной, с отдельными модулями для каждой функции, чтобы упростить разработку и поддержку системы, а также обеспечить гибкость при изменениях и добавлении новых функций. Конфиденциальность медицинской информации - ключевое требование, которое система должна обеспечивать, а также управление информацией о пациентах, включая диагнозы, историю болезни, лечение и другие медицинские записи. Система должна быть способна хранить и обрабатывать большие объемы информации и обеспечивать быстрый и удобный доступ к ней.

**Требования к системе**

Основываясь на анализе требований к проектируемой системе, можно выделить следующие конкретные требования к системе:

- *Модульность:* система должна быть разбита на отдельные модули, каждый из которых будет выполнять определенную функцию, для упрощения разработки, поддержки и гибкости.
- *Надежность***:** система должна быть стабильной, безопасной и защищенной от взломов и несанкционированного доступа. Также система должна иметь возможность восстанавливаться в случае сбоев и отказов.
- *Конфиденциальность:* система должна обеспечивать высокий уровень конфиденциальности и защиты персональных данных пациентов.
- *Управление информацией о пациентах:* система должна обеспечивать возможность управления информацией о пациентах, включая информацию о диагнозах, истории болезни, лечении и прочих медицинских записях.
- *Хранение и обработка больших объемов информации***:** система должна иметь возможность хранения и обработки больших объемов информации и обеспечивать быстрый и удобный доступ к ней.
- *Интеграция с другими системами***:** система должна обеспечивать возможность интеграции с другими системами, используемыми в медицинских учреждениях, такими как системы лабораторной диагностики, системы заказа медицинского оборудования и т.д.
- *Удобство использования***:** система должна быть удобной и легкой в использовании, иметь простой и понятный интерфейс для пользователей, включая медицинских специалистов и административный персонал, и обеспечивать быстрый и удобный доступ к информации.
- *Расширяемость:* система должна иметь возможность расширяться и добавлять новые функции в будущем, с целью удовлетворения изменяющихся потребностей медицинских учреждений.

Удовлетворение этих требований является ключевым для создания успешной и эффективной автоматизированной информационной системы для медицинских учреждений.

**Архитектура системы**

На Рисунке 2 представлена архитектура системы для автоматизированной информационной системы для медицинских учреждений, которая должна быть разработана таким образом, чтобы удовлетворять вышеперечисленным требованиям и обеспечивать эффективное управление медицинской информацией [2].

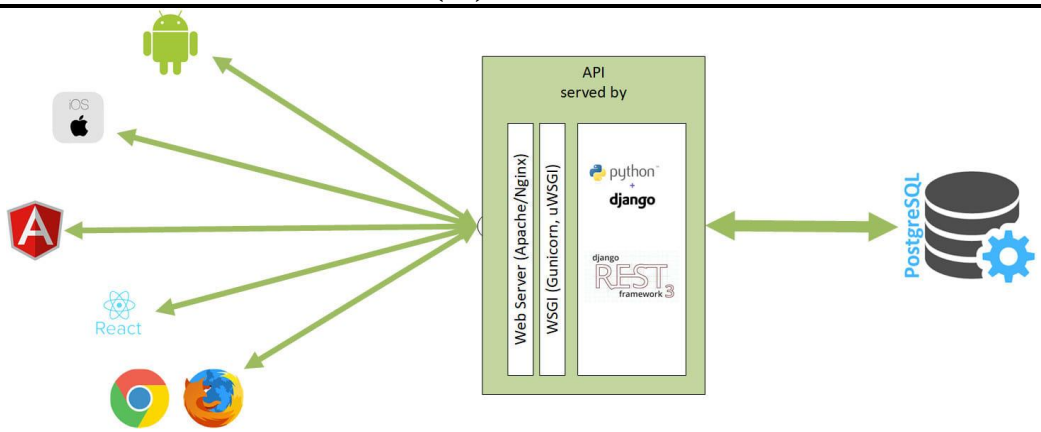



Рисунок 2 – Архитектура системы

Основной инструментарий для разработки данной системы - Django, Python и PostgreSQL, известные своей гибкостью, эффективностью и надежностью [5].

Система состоит из нескольких модулей, каждый из которых выполняет определенную функцию и обеспечивает логическую связь между сущностями и информационными потоками. Рассмотрим основные модули системы:

1. Модуль управления информацией о пациентах: основной модуль системы, который содержит информацию о пациентах, включая их личные данные, историю болезни, диагнозы, результаты обследований и тестов, назначения и лекарства, протоколы лечения и другие медицинские данные.
2. Модуль управления назначениями и лекарствами: модуль, который обеспечивает возможность ввода и управления назначениями и лекарствами, включая рецепты, дозы, частоту приема и другую информацию.
3. Модуль управления приемами и записями: модуль, который обеспечивает возможность записи на прием, управления расписанием врачей, уведомлений и напоминаний, а также управления прочими процессами, связанными с приемами.

**Описание реализации системы**

Для создания автоматизированной информационной системы для медицинских учреждений были использованы инструменты и технологии, такие как Django Framework, Python и PostgreSQL [7]. Django предоставляет гибкость и возможность создавать сложные веб-приложения, благодаря множеству встроенных функций, таких как ORM, маршрутизация URL-адресов, шаблонизация, административный интерфейс и др. Python обладает высокой скоростью разработки, широкими возможностями и обширной библиотекой сторонних модулей, и является главным языком, используемым в Django. PostgreSQL является мощной реляционной базой данных с открытым исходным кодом, которая обеспечивает надежность, масштабируемость и безопасность данных [6].

Реализация системы была осуществлена с использованием модульной архитектуры, где каждый модуль был реализован в соответствии со своей функциональностью, и все они были интегрированы в единую систему. Для каждого модуля был создан пользовательский интерфейс, который позволяет пользователям легко взаимодействовать с системой и

выполнять необходимые задачи. Интерфейсы были реализованы с использованием шаблонов Django и HTML/CSS/JavaScript [3, 4].

Административный интерфейс Django был создан для управления данными и настройками приложения, а также для просмотра и удаления записей. Для обеспечения безопасности и защиты данных система поддерживает протокол HL7 (Health Level Seven), который является международным стандартом для обмена информацией в здравоохранении. Этот протокол позволяет нашей системе интегрироваться со значимыми медицинскими сервисами и повышать конкурентоспособность клиники.

В заключении отметим, что современные медицинские учреждения должны быть интегрированы в медицинское информационное пространство, а не использовать самостоятельные медицинские системы или специализированные программы. Чтобы быть конкурентоспособными, они должны взаимодействовать с другими участниками медицинской инфраструктуры. Таким образом, необходимо искать решения, которые позволят клиникам быть полноценно включенными в медицинское информационное пространство. Без взаимодействия с другими участниками создание полноценно работающего решения невозможно.

**Список литературы**

1. Квашнина, Е. А. Проектирование медицинских информационных систем: учебно-методическое пособие / Е. А. Квашнина, Е. Е. Трубилина. - Новосибирск: Изд-во НГТУ, 2020. - С. 22-34.
2. Мартин Р. Чистая архитектура. Искусство разработки программного обеспечения. СПб.: Питер, 2019. С. 35-39.
3. Полуэктова Н.Р., Разработка веб-приложений: учебное пособие для вузов/ Н.Р.Полуэктова.— Москва: Издательство Юрайт, 2023. С. 50-90.
4. Солодушкин, С. И. Разработка программных комплексов на языке JavaScript: учебное пособие / С. И. Солодушкин, И. Ф. Юманова; под общ. ред. В. Г. Пименова; Министерство науки и высшего образования Россйской Федерации, Уральский федеральный университет. - Екатеринбург: Изд-во Уральского ун-та, 2020. - С. 6-75.
5. Стасышин В.М. Базы данных: технологии доступа: учебное пособие для вузов/ В.М.Стасышин, Т.Л.Стасышина.— 2-е изд., испр. и доп.— Москва: Издательство Юрайт, 2023. С. 127-229.
6. Сысолетин Е.Г. Разработка интернет-приложений: учебное пособие для вузов/ Е.Г.Сысолетин, С.Д.Ростунцев; под научной редакцией Л.Г.Доросинского.— Москва: Издательство Юрайт, 2023 С. 12-22.
7. Чернышев С.А. Основы программирования на Python: учебное пособие для вузов/ С.А.Чернышев.— Москва: Издательство Юрайт, 2023. С. 221-243.
8. Smart Delta Systems: Медицинские информационные системы (МИС). [Электронный ресурс]. URL:https://sdsys.ru/blog/aktualnyj-vzglyad-na-mediczinskuyu-informaczionnuyu-sistemu/ (дата обращения:12.05.2023)

**References**

1. Kvashnina, E. A. Designing medical information systems: an educational and methodical manual / E. A. Kvashnina, E. E. Trublina. - Novosibirsk: NSTU Publishing House, 2020. - pp. 22-34.
2. Martin R. Pure Architecture. The art of software development. St. Petersburg: St. Petersburg, 2019. pp. 35-39.
3. Poluektova, N. R. Development of web applications: a textbook for universities / N. R. Poluektova. — Moscow: Yurayt Publishing House, 2023. pp. 50-90.
4. Solodushkin, S. I. Development of software complexes in JavaScript: textbook / S. I. Solodushkin, I. F. Yumanova; under the general editorship of V. G. Pimenov; Ministry of Science and Higher Education of the Russian Federation, Ural Federal University. - Yekaterinburg: Publishing House of the Ural University, 2020. - pp. 6-75.
5. Stasyshin, V. M. Databases: access technologies: a textbook for universities / V. M. Stasyshin, T. L. Stasyshina. — 2nd ed., ispr. and add. — Moscow: Yurayt Publishing House, 2023. pp. 127-229.
6. Sysoletin, E. G. Development of Internet applications: a textbook for universities / E. G. Sysoletin, S. D. Rostuntsev; under the scientific editorship of L. G. Dorosinsky. — Moscow: Yurayt Publishing House, 2023. pp. 12-22.
7. Chernyshev, S. A. Fundamentals of Python programming: a textbook for universities / S. A. Chernyshev. — Moscow: Yurayt Publishing House, 2023. pp. 221-243.
8. Smart Delta Systems: Medical Information Systems (MIS). [electronic resource]. URL:https://sdsys.ru/blog/aktualnyj-vzglyad-na-mediczinskuyu-informaczionnuyu-sistemu / (date of request:12.05.2023)

Кириллина Ю.В., Мовсисян Л.К. Модернизация информационной системы поддержки управления проектами // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2. с. 61–67

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# МОДЕРНИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПОДДЕРЖКИ УПРАВЛЕНИЯ ПРОЕКТАМИ

**[1] Кириллина Ю.В., [2] Мовсисян Л.К.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: [1]jvk05@mail.ru, [2] movsisyan.l.k@edu.mirea*

**В статье рассматривается применение информационной системы поддержки управления проектами в рамках осуществления основной деятельности агентством интернет-маркетинга ООО «СТК-ПРОМО» и определяются процессы и подразделения компании, которые не охвачены автоматизацией. Для устранения недостатков выполнения процесса управления проектами во взаимодействии с иными процессами организации предлагается расширить функционал используемой информационной системы. Для решения задачи формируется модель процесса «как будет», а также определяются функциональные требования к отдельным частям модернизируемой информационной системы.**

Ключевые слова: Интернет-маркетинг, управление проектами, информационная система поддержки управления проектами, расширение функционала информационной системы.

# MODERNIZATION OF THE PROJECT MANAGEMENT SUPPORT INFORMATION SYSTEM

**[1] Kirillina Y.V., [2] Movsisyan L.K.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: [1]jvk05@mail.ru, [2] movsisyan.l.k@edu.mirea.ru*

**The article discusses the use of an information system to support project management in the framework of the implementation of the main activities of the Internet marketing agency LLC "STK-PROMO" and identifies the processes and divisions of the company that are not covered by automation. To eliminate the shortcomings of the project management process in cooperation with other processes of the organization, it is proposed to expand the functionality of the information system used. To solve the problem, a model of the "as it will be" process is formed, and functional requirements for individual parts of the upgraded information system are determined.**

Keywords: Internet marketing, project management, project management support information system, expansion of the information system functionality.

Рынок интернет-маркетинга обоснованно считается быстрорастущим и перспективным направлением цифровой экономики. Количество пользователей сети Интернет с каждым годом все увеличивается. В Российской Федерации общий объем рынка рекламы по итогам 2022 года составил 578,3 млрд. рублей, увеличившись на 22% по сравнению с предыдущим годом. Направление интернет-маркетинга составило больше половины всех рекламных

бюджетов в стране. Об этом свидетельствуют данные Ассоциации коммуникационных агентств России (АКАР), которые были обнародованы в середине марта 2022 года. [3, 4]

К услугам интернет-маркетинга относится достаточно большой спектр работ, осуществляемый специализированными агентствами интернет-маркетинга:

1. Продвижение сайтов (SEO продвижение) — данная услуга позволяет добиться лидирующих позиций в результатах поисковых системах. Данный комплекс мер увеличивает посещаемость сайта по целевым запросам.
2. Услуга контекстной рекламы — настройка и ведение контекстной рекламы ориентирована на привлечение потенциальных клиентов.
3. Поддержка сайтов — это работа над наполнением и внешним видом сайта клиента.
4. Юзабилити аудит — данная услуга направлена на исследование, которое проводится с целью оценки удобства использования ресурса клиента. Работы в рамках данной услуги проводятся для выявления недостатков продукта, которые становятся преградами к увеличению клиентской базы.
5. SEO аудит — данная услуга позволяет выявить узкие места, которые мешают сайту подняться на первые позиции в поисковых системах.
6. Консалтинговые услуги — данная услуга направлена на формирование устных и письменных консультаций со стороны сотрудника компании, цель которых улучшение методов его продвижения и качества самого ресурса.
7. Медийная реклама — данный механизм применяется с целью привлечения внимания аудитории с помощью рекламного продукта, который ориентирован на зрелищное восприятие. Примером данной услуги является брендирование ресурса заказчика.
8. Реклама в социальных сетях (SMM продвижение) — цель данной услуги — повышение активности ресурса клиента в социальных сетях.
9. Разработка на фреймворках — примером данной услуги является разработка сайта с использованием, заранее выбранного и согласованного с клиентом, фреймворка.
10. Управление репутацией — включает в себя первичное тестирование различных гипотез, опираясь на большой список показателей, а также постоянный мониторинг информационного пространства на наличие различных ситуаций с клиентами, что положительно сказывается, например, на позиции в органическом SEO.

Работа в агентствах интернет-маркетинга, в большинстве случаев, организуется в проектных группах.

Согласно: ГОСТ Р 54869-2011 Проектный менеджмент. Требования к управлению проектами, управление проектной деятельностью заключается в управлении возникшими изменениями на протяжении всего жизненного цикла. [1]

Процесс управления проектами включает в себя следующие этапы:

1. Инициация.
2. Планирование.
3. Исполнение и контроль.
4. Анализ и регулирование.
5. Завершение.

Этапы выполнения работ в рамках оказания маркетинговых услуг проецируются на структуру управления согласно ГОСТ следующим образом:

1. Оформление и обработка заявки. Это принятие решения о начале выполнения проекта. Подпроцесс связан с выполнением задач в рамках формирования информации о клиенте, постановкой проблем ресурса заказчика, определением целей проекта, определением предпочитаемой услуги (метода) продвижения ресурса заказчика.
2. Планирование работ в рамках проекта: определение задач проекта и их основных показателей, выбор услуги, составление и согласование разного рода документации, обеспечивающей работу проектной группы (техническое задание, договор, документы оплаты оказываемых услуг).
3. Организация выполнения работ и их контроль в рамках проекта — это процесс координации сотрудников и других ресурсов для выполнения плана.
4. Анализ хода выполнения работ в рамках проекта. В рамках данного подпроцесса проводится анализ отклонений и их причин, оценка возможных альтернатив и принятие корректирующих воздействий, их согласование, утверждение и применение.
5. Закрытие этапа проекта — это формализация выполнения проекта и подведение его к запланированному финалу. Включает такие работы как: презентация проекта заказчику, предоставление разъяснений, сдача проекта заказчику, формирование пакета закрывающих документов (акт приемки выполненных работ, сводный отчет о завершении проекта, протокол переговоров и т.д.).

Для оперативного управления командами, целью которой является обеспечение роста эффективности реализации проектной деятельности, а также повышения качества предоставляемых услуг посредством непрерывного взаимодействия с заказчиком для получения обратной связи о тех или иных изменениях, необходимо использование информационной системы.

Каждая компания самостоятельно решает вопрос о том, какую систему управления проектами использовать, например, либо приобретать готовый программный продукт, представленный на рынке или же проектировать и разрабатывать собственную информационную систему (ИС). [4]

В агентстве интернет-маркетинга ООО «СТК-ПРОМО» используется собственная разработка для поддержки управления проектами, на Рисунке 1 отражены процессы, которые поддерживаются информационной системой (прямоугольники, залитые светло-зеленым цветом). На данной схеме можно увидеть основные этапы выполнения процесса, информационные потоки, а также вовлечённые подразделения компании ООО «СТК-ПРОМО».

Процессы, выделенные красным на Рисунке 1, требуют автоматизации и, по своей сути, не имеют кросс-процессного технологического взаимодействия с использованием единого информационного пространства.

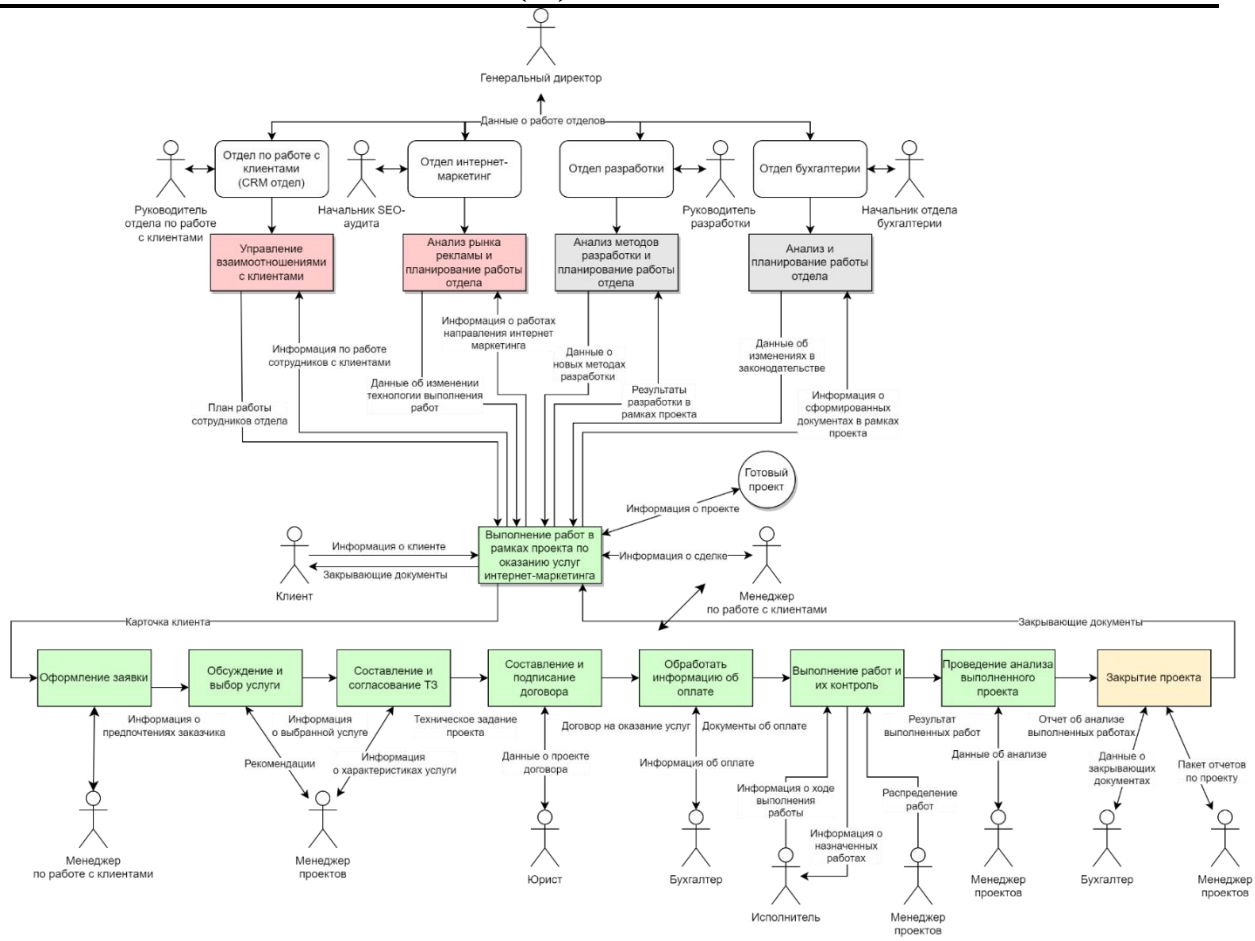



Рисунок 1 – Общая схема функционирования отделов в агентстве ООО «СТК-ПРОМО»

Исходя из требования устранить существующие недостатки при выполнении процесса:

1. Отсутствие автоматизации обработки информации на стратегическом уровне управления.
2. Отсутствие единого информационного пространства среди отделов.
3. Отсутствие стандартных форм документов и отчетов по стратегическому планированию деятельности предприятия.
4. Отсутствие инструментов прикладной аналитики.
5. Отсутствие функций по работе с уровнем лояльности клиентской базы, и осуществить расширение функционала используемой информационной системы поддержки управления проектами была смоделирована модель процесса «как будет» (Рисунок 2) и определены изменения вносимые в модернизируемую ИС. [5]

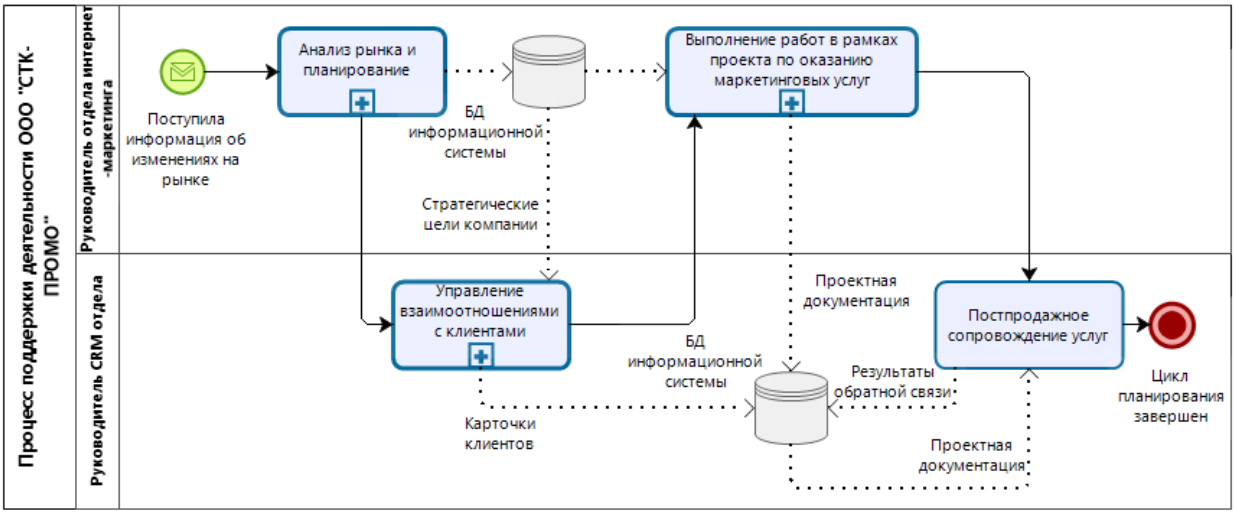



Рисунок 2 – Контекстная модель реализации основной деятельности ООО «СТК-ПРОМО» в нотации BPMN 2.0 с применением модернизируемой ИС

Таблица 1 – Описание процесса с применением модернизируемой ИС

| **Название вложенного процесса (подпроцесса)** | **Описание вносимых изменений в ИС (функциональные требования)** |
|---|---|
| **1** | **2** |
| Детализации подпроцесса анализа рекламного рынка и планирование деятельности агентства | Используется подсистема МИС, автоматизирующая процессы: обработки KPI поставщиков трафика, формирования рекомендаций по обновлению протокола создания рекламных кампаний, формирования рекомендованных целевых показателей эффективности рекламных кампаний, формирования рекомендаций по обновлению паттернов проведения кампаний |
| Детализации подпроцесса управления взаимоотношениями с клиентами | Запись всех потоков информации при обработке заявки клиента производится в хранилище CRM-подсистемы, являющейся частью единого информационного пространства и находится в составе распределенной базы данных ИС поддержки деятельности агентства. Так же добавляются процессы, связанные с получением информации об уровне удовлетворенности заказчика оказанными услугами. |
| Детализации подпроцесса выполнения работ в рамках проекта по оказанию маркетинговых услуг | ИС поддержки управления проектами преобразуется в соответствующую подсистему в составе ИС поддержки деятельности компании |

Продолжение таблицы

| 1 | 2 |
|---|---|
| Детализации подпроцесса выполнение работ по SEO-продвижению в рамках проекта | Используется подсистема МИС, автоматизирующая процессы формирования карточки клиента и карточки проекта, отправки автоматического уведомления заказчику с целью оценки качества. Данные изменения позволят разгрузить исполнителя, повысив тем самым его продуктивность и эффективность операционных затрат на весь процесс в целом |
| Детализации подпроцесса выполнение работ по SMM-продвижению в рамках проекта | ИС поддержки управления проектами преобразуется в соответствующую подсистему в составе ИС поддержки деятельности компании |
| Детализации подпроцесса выполнение работ по контекстной рекламе в рамках проекта | Используется подсистема МИС, автоматизирующая процессы подбора ключевых слов, а также использующая инструменты прикладной аналитики для обработки статистических данных предыдущих проектов с целью предоставления рекомендаций по настройки времени и географии показов |
| Детализации подпроцесса выполнение работ по таргетированной рекламе в рамках проекта | Используется подсистема МИС, автоматизирующая процессы сегментации аудитории, выбора площадок для продвижения |
| Детализации подпроцесса выполнение работ по разработке сайта в рамках проект | ИС поддержки управления проектами преобразуется в соответствующую подсистему в составе ИС поддержки деятельности компании. Также информационные потоки распределены по хранилищам соответствующих подсистем |
| Детализации подпроцесса анализа выполнения работ | |

Таким образом, расширение функционала, используемой в организации информационной системы, позволяет сформировать единое информационное пространство в рамках осуществления основной деятельности организации.

**Список литературы**

1. ГОСТ Р 54869-2011 Проектный менеджмент. Требования к управлению проектами. [Электронный ресурс] — Режим доступа: https://docs.cntd.ru/document/1200089604 — Загл. с экрана. — Яз. рус. (Дата обращения 05.05.2023)

2. Обзор лучших систем управления проектами. [Электронный ресурс] — Режим доступа: https://www.fewskills.com/workflow-project-app/ — Загл. с экрана. — Яз. рус. (Дата обращения 06.05.2023)
3. Объем рекламы в средствах распространения в январе-сентябре 2020 года. [Электронный ресурс] — Режим доступа: https://www.akarussia.ru/knowledge/market_size/id9399 — Загл. с экрана. — Яз. рус. Дата обращения (01.02.2023)
4. Рейтинги digital-рынка России. [Электронный ресурс] — Режим доступа: https://ruward.ru/all/ — Загл. с экрана. — Яз. рус. Дата обращения (01.02.2023)
5. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. — М.: Манн, Иванов и Фербер, 2013. — С. 136-139

**References**

1. GOST R 54869-2011 Project management. Project management requirements. [Electronic resource] — Access mode: https://docs.cntd.ru/document/1200089604 — Cover from the screen. — Yaz. rus. (Date of application 05.05.2023)
2. Overview of the best project management systems. [Electronic resource] — Access mode: https://www.fewskills.com/workflow-project-app/ — Cover from the screen. — Yaz. rus. (Date of application 06.05.2023)
3. The volume of advertising in the distribution media in January-September 2020. [Electronic resource] — Access mode: https://www.akarussia.ru/knowledge/market_size/id9399 — Cover from the screen. — Yaz. rus. (Date of application 01.02.2023)
4. Ratings of the Russian digital market. [Electronic resource] — Access mode: https://ruward.ru/all/ — Cover from the screen. — Yaz. rus. (Date of application 01.02.2023)
5. Repin V.V., Eliferov V.G. Process approach to management. Modeling of business processes. — M.: Mann, Ivanov and Ferber, 2013. — pp. 136-139

Курманбакеев В.А. Тренды и перспективы развития информационной безопасности// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2 с. 68–71

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

# ТРЕНДЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Курманбакеев В.А.**
*ФГБОУ ВО "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: slavan787@gmail.com*

**Информационная безопасность становится все более актуальной в нашей цифровой эпохе, когда все больше информации хранится и передается через сети. С каждым годом уровень угрозы для информационной безопасности растет, и в настоящее время существует несколько трендов и перспектив, которые влияют на развитие этой области.**

Ключевые слова: Информационная безопасность.

# TRENDS AND PROSPECTS OF INFORMATION SECURITY DEVELOPMENT

**Kurmanbakeev V.A.**
*Bonch-Bruevich St. Petersburg State University of Telecommunications*, St. Petersburg, *Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail: slavan787@gmail.com*

**Information security is becoming more and more relevant in our digital age, when more and more information is stored and transmitted through networks. Every year the threat level for information security is growing, and currently there are several trends and prospects that affect the development of this area.**

Keywords: Information security.

Одним из основных трендов является увеличение количества кибератак на корпоративные сети и государственные учреждения. Стремительное развитие технологий и внедрение новых приложений и сервисов создают новые уязвимости, которые могут быть использованы злоумышленниками. Вместе с тем, многие организации не обладают достаточной квалификацией и опытом в области информационной безопасности, что делает их еще более уязвимыми.

Другим трендом является увеличение объема данных, которые собираются и обрабатываются организациями. Это может привести к возникновению проблем с конфиденциальностью и утечкой данных, если не принимать соответствующие меры для защиты информации. Поэтому важно уделять больше внимания не только защите сетей и устройств, но и защите данных, которые они обрабатывают.

Одной из перспектив развития информационной безопасности является использование искусственного интеллекта и машинного обучения. Это может помочь автоматизировать процессы по обнаружению угроз и анализу данных, что упростит задачу защиты информации.

Также возможно использование блокчейн технологии для защиты данных, что обеспечит их целостность и надежность.

Вместе с тем, развитие информационной безопасности может быть затруднено недостатком высококвалифицированных специалистов. В настоящее время существует дефицит квалифицированных специалистов в этой области, что может привести к тому, что организации не будут иметь достаточных ресурсов для защиты своей информации.

Таким образом, тренды и перспективы развития информационной безопасности указывают на необходимость усиления мер по защите информации и обучению специалистов в этой области. Необходимо развивать новые технологии и подходы к защите данных, а также повышать осведомленность среди пользователей и работников организаций о методах и мероприятиях по защите информации.

Также важно учитывать международные стандарты и регуляторные требования по защите данных, такие как GDPR в Европейском союзе или HIPAA в США.

Эти стандарты определяют правила сбора, хранения и обработки данных, а также наказания за их нарушение.

С учетом этих факторов можно сделать вывод, что информационная безопасность является ключевой проблемой для организаций и государственных учреждений. Необходимо принимать все возможные меры для защиты информации и обучения специалистов, чтобы справиться с растущими угрозами и сохранить доверие пользователей и клиентов. Только так можно обеспечить стабильный и безопасный развитие цифровой экономики и общества в целом.

Еще одним важным аспектом развития информационной безопасности является международное сотрудничество и обмен информацией между государствами. Многие кибератаки имеют международный характер, и их успешная предотвращение требует координации усилий различных стран. Для этого необходимо создание международных платформ и механизмов сотрудничества, которые позволят эффективно обмениваться информацией о киберугрозах и совместно принимать меры по их предотвращению.

Также необходимо учитывать социальные и этические аспекты информационной безопасности. Существуют опасности связанные с использованием личной информации пользователей, такие как дискриминация, нарушение приватности и даже кража личности. Поэтому необходимо уделять больше внимания правам и свободам пользователей, а также развивать механизмы контроля за использованием персональных данных.

В целом, развитие информационной безопасности является сложным и многогранным процессом, который требует участия различных заинтересованных сторон. Необходимо учитывать текущие тренды и перспективы в этой области, а также принимать соответствующие меры для защиты данных и повышения осведомленности пользователей и работников. Только так можно создать безопасную и надежную среду для хранения и передачи информации в цифровой эпохе.

Еще одним перспективным направлением в развитии информационной безопасности является использование искусственного интеллекта и машинного обучения для автоматизации процессов защиты данных. Инструменты и алгоритмы искусственного интеллекта могут помочь в обнаружении и анализе киберугроз, а также в автоматической защите от них. Машинное обучение может помочь в создании адаптивных систем защиты, которые могут быстро реагировать на новые угрозы и атаки.

Также стоит упомянуть о развитии квантовых технологий, которые могут изменить парадигму информационной безопасности. Квантовые компьютеры могут быстро взламывать существующие системы шифрования, поэтому необходимо разрабатывать новые квантово-устойчивые методы защиты данных.

Наконец, важно отметить, что информационная безопасность должна рассматриваться как неотъемлемая часть общественной безопасности и защиты прав и свобод граждан. Существующие угрозы в области информационной безопасности могут привести к серьезным последствиям, включая угрозы жизни и здоровью людей. Поэтому необходимо уделять больше внимания этой проблеме и принимать меры для ее решения.

В заключение, можно сказать, что информационная безопасность является важным и перспективным направлением развития в цифровой эпохе. Существующие тренды и перспективы в этой области показывают, что необходимо принимать все возможные меры для защиты данных и повышения осведомленности пользователей и работников о киберугрозах. Только так можно создать безопасную и стабильную среду для развития цифровой экономики и общества в целом.

Еще одним важным аспектом, который следует упомянуть при рассмотрении трендов и перспектив развития информационной безопасности, является роль человеческого фактора в кибербезопасности. Несмотря на все технологические инновации и новые методы защиты данных, человеческий фактор остается одним из самых слабых звеньев в цепи безопасности.

Все чаще хакеры используют социальную инженерию и фишинговые атаки, чтобы получить доступ к конфиденциальной информации. Поэтому необходимо уделять больше внимания обучению и повышению культуры кибербезопасности среди пользователей и работников. Компании и государственные организации должны проводить регулярные тренинги и обучения, чтобы повысить осведомленность своих сотрудников о возможных угрозах и обучить их правильному поведению в сети.

Кроме того, важно улучшать законодательную базу в области кибербезопасности и ужесточать ответственность за нарушение правил и мер безопасности. Только так можно создать эффективную систему защиты данных и обеспечить безопасность в интернете.

В целом, развитие информационной безопасности в наши дни является сложной и многогранной задачей. Необходимо учитывать множество факторов, включая технологические инновации, роль человеческого фактора, социально-экономические тенденции и геополитические риски. Однако, при правильном подходе и принятии необходимых мер, можно создать безопасную и устойчивую среду для развития цифрового мира.

**Список литературы**

1. Петров А. Информационная безопасность: теория и практика. - М.: Издательство Юрайт, 2020.
2. Лукин А. М., Старкова Н. В. Информационная безопасность: угрозы, защита, нормативно-правовое обеспечение. - М.: КНОРУС, 2021.
3. Поляков А. Б., Булыгин Е. В. Кибербезопасность: введение в проблематику. - СПб.: Питер, 2020.

4. Малышев В. Н. Информационная безопасность и защита информации: учебник для студентов высших учебных заведений. - М.: Юрайт, 2021.
5. Безопасность в информационных системах и технологиях. Учебное пособие / Под ред. Ю. А. Шумилина. - М.: Издательство МГТУ им. Н.Э. Баумана, 2020.
6. 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.
7. 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.
8. 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.

**References**

1. Petrov A. Information security: theory and practice. - M.: Yurait Publishing House, 2020..
2. Lukin A. M., Starkova N. V. Information security: threats, protection, regulatory and legal support. - M.: KNORUS, 2021
3. Polyakov A. B., Bulygin E. V. Cybersecurity: introduction to the problematics. - St. Petersburg: Peter, 2020.
4. Malyshev V. N. Information security and information protection: a textbook for students of higher educational institutions. - M.: Yurayt, 2021.
5. Security in information systems and technologies. Textbook / Ed. by Y. A. Shumilin. - Moscow: Bauman MSTU Publishing House, 2020.
6. 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.
7. Gelfand A. M. et al. Internet of Things (IoT): threats to security and privacy // Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
8. Gelfand A. M. et al Study 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.

Большаков А.О. Архитектура системы мониторинга и инвентаризации информационно-технологической инфраструктуры, применяемой в учебном процессе // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 72–82

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.42

# АРХИТЕКТУРА СИСТЕМЫ МОНИТОРИНГА И ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРЫ, ПРИМЕНЯЕМОЙ В УЧЕБНОМ ПРОЦЕССЕ

**Большаков А.О.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: ewaypeople@gmail.com*

**Объектом исследования выступает предметная область тенденция развития IT. Целью научно-исследовательской работы выступает анализ предметной области для дальнейшего проектирования системы мониторинга и инвентаризации информационно-технологической инфраструктуры, применяемой в учебном процессе. В ходе данного исследования использовались: статистические методы наблюдения и анализа.**
**Результаты проведенного исследования могут быть использованы в целях дальнейшего проектирования систем мониторинга и инвентаризации информационно-технологической инфраструктуры, применяемой в учебном процессе. Кроме того, результаты статьи могут использоваться другими разработчиками, целью которых является создание своих систем.**

Ключевые слова: Мониторинг учебных компьютеров, поддержка процессов администрирования, инвентаризация информационно-технологической инфраструктуры, базы данных, графический интерфейс.

# SYSTEM ARCHITECTURE FOR MONITORING AND INVENTORY OF THE INFORMATION TECHNOLOGY INFRASTRUCTURE USED IN THE EDUCATIONAL PROCESS

**Bolshakov A.O.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: ewaypeople@gmail.com*

**The object of the research is the subject area of the IT development trend. The aim of this scientific research is to analyze the subject area for further design of a system for monitoring and inventorying the information technology infrastructure used in the educational process. During this research, statistical observation and analysis methods were used.**
**The results of the conducted research can be used for the purpose of further designing systems for monitoring and inventorying the information technology infrastructure used in the educational process. In addition, the results of the article can be used by other developers whose aim is to create their own systems.**

Keywords: Monitoring of educational computers, support of administration processes, inventorying of information technology infrastructure, databases, graphical interface.

## Введение

В связи с развитием информационных технологий, сегодня сложно представить крупное предприятие или образовательное учреждение, в котором не используются стационарные компьютеры. Человеку сложно контролировать устройства на наличие нужного и отсутствие запрещенного программного обеспечения, а также на добросовестное использование со стороны сотрудников или обучающегося. Кроме того, проблема администрирования устройств отчетлива видна в высших учебных заведениях, только на один класс приходится более двадцати компьютеров.

Эффективность решения этой задачи во многом зависит не только от личных качеств администратора, но и в программном обеспечении, которое используется им. Чтобы контролировать такое количество устройств необходимо автоматизировать большинство процессов, таких как сбор общей информации о компьютерах, информация о использовании программного обеспечения, запрет на использование конкретных программ.

Большинство программных средств такого типа имеют низкий спрос в высших учебных заведениях из-за недостатка функциональности. На сегодняшний день в сфере образования существует мало альтернатив таким программным продуктам, кроме того, за последний год страна имеет дефицит отечественных разработок, в том числе и систем мониторинга и инвентаризации.

Целью работы является оптимизация контроля использования машин и поддержки процессов администрирования в высших учебных заведениях, при этом задействовать как можно большее количество пользователей.

## 1. Анализ предметной области

### *1.1. Обзор существующих решений для мониторинга и инвентаризации информационно-технологической инфраструктуры*

Термин «управление компьютерным классом» сегодня широко используется для описания задач, которые выполняет соответствующий класс программных продуктов – Classroom Management Software (CMS). Основными функциями CMS являются: проведение демонстрации материала с компьютера преподавателя на все компьютеры студентов; мониторинг учебных компьютеров в режиме реального времени с компьютера преподавателя; удаленное управление учебными компьютерами; контроль доступа в интернете и использования программ; функции текстового, аудио и видеочатов; распределение файлов, функции создания и планирования занятий, запись происходящего на экране любого компьютера в видеоролик; функции тестирования.

Использование таких программных средств дает ряд преимуществ для администрирования компьютеров. Если рассуждать абстрактно об процессе контроля пользователей и затронуть все факторы, которые влияют на его эффективность, можно выделить несколько критериев, которые отображены в Таблице 1.

Таблица 1 – Описание критериев сравнения контроля пользователей

| Наименование критерия | Описание критерия |
|---|---|
| 1 | 2 |
| 1. Возможность наглядно представить обучающий материал | Наличие возможности демонстрации материала |

| Продолжение таблицы | |
|---|---|
| 1 | 2 |
| 2. Возможность контролировать учебный процесс | Наличие возможности повлиять на процесс со стороны администратора |
| 3. Время обучения | Время, затраченное на обучение, распределение времени |
| 4. Эффективное количество обучаемых | Количество обучаемых, рекомендованное для получения максимального эффекта от обучения с помощью того или иного метода |
| 5. Требуется собирать людей в одной аудитории | Присутствие в аудитории |

Опираясь на эти критерии, можно выяснить, какие преимущества и недостатки есть от использования систем CMS. В следующей таблице будет проведено сравнение, которое даст понять почему учебные учреждения и компании прибегают к использованию средств управления компьютерным классом.

Таблица 2 – Сравнительная таблица подходов к процессу контроля пользователей

| Критерий | С использованием CMS | Без использования CMS |
|---|---|---|
| 1. Возможность наглядно представить обучающий материал | Не ограничена | Ограничена |
| 2. Возможность контролировать учебный процесс | Возможность просматривать сразу несколько рабочих мест | Возможность просматривать одно рабочее место |
| 3. Время обучения | Меньшие затраты на организационные вещи | В зависимости от восприятия аудитории |
| 4. Эффективное количество обучаемых | Ограничена | Не ограничена |
| 5. Требуется собирать людей в одной аудитории | Не требуется | Требуется |

Данные, которые приведены в таблице, свидетельствуют о том, что использование систем CMS имеет преимущество по многим критериям. [6]

### *1.2. Сравнительная оценка подходов контроля учебных компьютеров*

1.2.1. LanSchool от компании Lenovo

Разработано для образовательных центров, оно обеспечивает проникновение экрана преподавателя на компьютеры студентов.

LanSchool позволяет установить в общей сложности 250 различных каналов. Студент, который синхронизирует определенный канал, увидит экран, относящийся к данному учителю.

Кроме того, с помощью LanSchool можно осуществлять надзор за деятельностью на компьютерах студентов, отменять их экраны, чтобы не допускать отвлечения, и ограничить их доступ к определенным приложениям, таким как веб-браузеры. [2]

LanSchool позволит учителю оставаться на своем месте и иметь контроль над компьютером студента.

Максимальное количество студентов достигает 144. Можно также указывать сайты, к которым они будут иметь доступ, а к каким нет.

Преимущества программного обеспечения:

- Контроль за всеми подчиненными компьютерами
- Обширность функций

Недостатки программного обеспечения:

- Стоимость
- Уязвимости, например, подчиненный компьютер может отключиться от сети, и пользователь главного компьютера не получит никакого сообщения.

1.2.2. iTALC от компании Veyon Solutions

iTALC (intelligently Teaching And Learning with Computer - интеллектуальное преподавание и изучение с помощью компьютера) является программой для удаленного управления компьютерным классом, и успешно работает в операционных системах Linux и Windows XP / Vista / 7 / 8 / 8.1 / 10, включая 64-битные и 32-битные версии. iTALC позволяет учителям удаленно контролировать и управлять компьютерами учеников. Он позволяет учителю демонстрировать свой рабочий стол (Демо), закрыть окна и выключить компьютер. Программа была разработана в качестве бесплатной альтернативы MasterEye. Полностью на русском языке. [3]

Первоначально iTALC была доступна только для Linux. В середине 2006 года, в ходе портирования при помощи Qt4, добавлена поддержка NT-разрядных версий Windows. Кроме того, iTALC прозрачно работает в смешанных вычислительных средах, например, компьютер учителя на Linux может получить доступ к ученическому компьютеру на Windows, и наоборот.

Все функции управления основаны на протоколе RFB. Поскольку iTALC работает полностью с TCP подключениями, то имеет преимущество, которое позволяет демо и дистанционное управление в локально-вычислительных сетях. Алгоритмы быстрого и эффективного сжатия позволяют соединение даже с частными ученическими компьютерами на дому, при условии прямого доступа.

Преимущества программного обеспечения:

- Режим обзора (разрешает предварительный просмотр экранов каждого компьютера ученика в небольшом окне предварительного просмотра);
- Демонстрационный режим (или во фрейме или в окне) - который транслирует экран учителя всем компьютерам учеников в режиме реального времени;
- Блокирование компьютера;
- Отправка текстовых сообщений на подчиненные компьютеры;
- Включение и перезагрузка отдельных или всех компьютеров по сети (Wake on LAN);

- Снимки экрана, например, во время нарушения каких-либо правил, установленных программой;
- Удаленное управление компьютером ученика;

1.2.3. Программное средства NetOp School

NetOp School является одним из самых мощных пакетов для обучения в компьютерном классе среди продуктов CMS, успешно применяется в школах, высших учебных заведениях, негосударственных учебных центрах, на курсах повышения квалификации. Кроме того, продукт может использоваться в качестве платформы для организации удаленного обучения через интернет. Программный комплекс NetOp School представляет собой две взаимодействующие части, одна из которых устанавливается на компьютер преподавателя, другая – на компьютер студента. Организация связи осуществляется по одному из популярных коммуникационных протоколов (TCP/IP, NetBios, IPX, Wireless). [4] Данный программный продукт служит альтернативой интерактивной доске, так как с его помощью можно демонстрировать монитор педагога или студента, передавать управление действиями любому участнику процесса обучения; создавать планы занятий и их записей в видеофайл. Демонстрационный модуль позволяет запустить медиафайл либо веб-страницу одновременно на всех компьютерах виртуального класса. Программный инструментарий позволяет преподавателю отслеживать процесс обучения и оказывать своевременную помощь. В программной части студента предусмотрена возможность вызова помощи преподавателя. После получения сигнала преподаватель имеет возможность организовать переписку либо канал для видео общения или в аудио формате. Преподаватель может подключиться к «Рабочему столу» обучаемого, выделить с помощью маркеров область экрана для привлечения внимания, продемонстрировать ее на весь виртуальный класс, а также передать управление для работы другому студенту. Все эти действия можно записать на видео, что становится просто незаменимой функцией для разбора типичных ошибок.

### *1.3. Исследование необходимости расширения функционала*

Исходя из раздела выше, можно сделать вывод, что все программные средства объединяет отсутствие средств инвентаризации, осуществление основных функций по локальной сети, отсутствие организации отдельной базы данных. В образовательной области, в ваших учебных заведениях число стационарных компьютеров может достигать в несколько сотен, контроль наличия и сбор информации об использовании необходимого программного обеспечения становится проблемной задачей, а также сбор информации о системных параметрах.

Программное обеспечение такого типа должно обладать возможностью работать при помощи соединения с интернет подключением, а не только в рамках локальной сети, чтобы охватить большое количество устройств, за пределами одного помещения. Из-за большого количества пользователей, необходимо организовать хранение информации на базе данных. Наличие средств инвентаризации существенно упрощает контроль установленных программ, помогает оптимизировать занимаемую память, на починенных компьютерах. Цель создать инструментарий для контроля использования учебных машин и поддержки процессов администрирования.

## 2. Архитектура

Такого рода сервисы, как правило, реализованы в виде десктопного приложения – наиболее подходящий способ. Преимущество такой реализации – сокрытие информации и удобство администрирования, предприятие имеет обособленную базу данных от других высших заведений, использующих программный продукт. Для реализации обмена информации при помощи сети интернет необходимо разделить программу на несколько частей, одна для подчиненных компьютеров, другая для главного компьютера. Связи со спецификой разработки схема приложения будет выглядеть следующим образом:

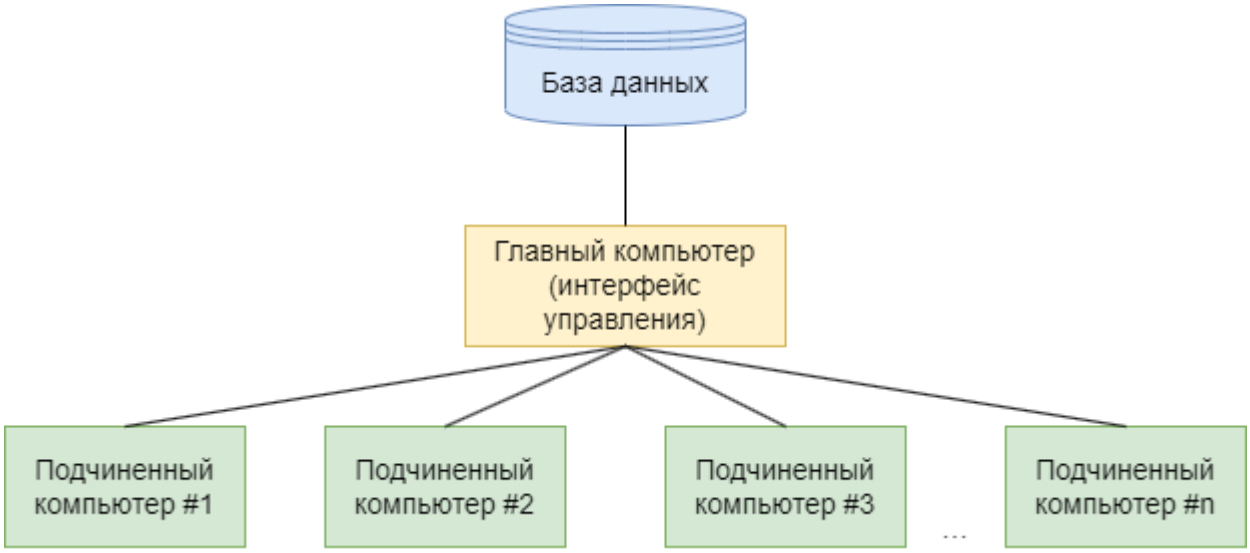



Рисунок 1 – Структурная схема

Если рассмотреть схему отдельно получим приложение следующего вида:

Функциональная схема - отображает взаимодействие компонентов системы и информационных потоков, состав данных в потоках с указанием используемых устройств. Для формирования функциональной схемы необходимо использовать общепризнанный стандарт.

Функциональные схемы содержат больше информации о работе системы, чем структурные. Несмотря на это, блок-схемы также важны, при таком подходе тщательно прорабатываются спецификации межпрограммных интерфейсов, поскольку от качества их описания зависит количество наиболее затратных ошибок. Поскольку на этапе тестирования выявляются ошибки при комплексном тестировании, потребуется повторное тестирование уже отлаженных тестов. [1]

Исходя из предыдущего пункта, функциональная схема будет состоять из трех частей: интерфейс управления, серверная часть, база данных.

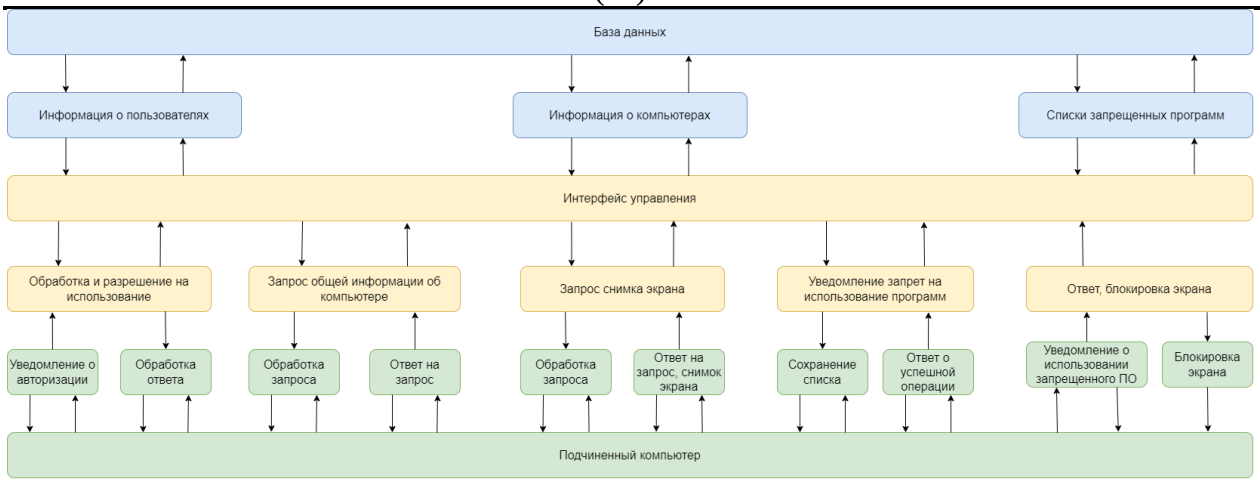



Рисунок 2 – Функциональная схема

Опишем функции, представленные в функциональной схеме:

- Обработка и разрешение на использование – авторизация

пользователя, для определения какой машиной пользуется человек, пока не будет пройдена, пользоваться компьютером невозможно.

- Запрос общей информации об компьютере – отправляет на интерфейс управления информацию о операционной системе и комплектующих устройства, установленных программах.
- Запрос снимка экрана – отправляет на интерфейс управления информацию о текущем изображении экрана
- Запрет использования программ – создает список программ, запрещенных для использования на подчиненных компьютерах.
- Блокировка экрана – при выявлении использования запрещенной программы, блокирует возможность использования компьютера, до одобрения администратором.

Серверная часть может быть разработана на основе множества языков программирования. Например, на таких как: Python, Ruby, PHP, Java, C#. В большинстве случаев выбор остается на PHP, поскольку язык обладает совместимостью со всеми основными платформами, поддерживает большинство серверов, имеет большую поддержку со стороны сообщества, поскольку существует множество фреймворков. Но в основном выбирается в качестве разработки веб-приложений, в нашем случаи необходимо разработать десктопное приложение и выбрать подходящий для этого инструментарий.

Наиболее подходящий язык для реализации программного продукта C# работающий на платформе .NET, которая предоставляет технологии для реализации такого рода программ.

C# является объектно-ориентированным и в этом плане много перенял у Java и C++. Объектно-ориентированный подход позволяет решить задачи по построению крупных, но в тоже время гибких, масштабируемых и расширяемых приложений. И C# продолжает активно развиваться, и с каждой новой версией появляется все больше интересных функциональностей, как, например, лямбды, динамическое связывание, асинхронные методы и т.д. [8]

Когда говорят C#, нередко имеют в виду технологии платформы .NET (WPF, ASP.NET). И, наоборот, когда говорят .NET, нередко имеют в виду C#. Однако, хотя эти понятия связаны, отождествлять их неверно. Язык C# был создан специально для работы с фреймворком .NET, однако само понятие .NET несколько шире. Фреймворк .NET представляет мощную платформу для создания приложений. Можно выделить следующие ее основные черты.

Поддержка нескольких языков. Основой платформы является общеязыковая среда исполнения Common Language Runtime (CLR), благодаря чему .NET поддерживает несколько языков: наряду с C# это также VB.NET, C++, F#, а также различные диалекты других языков, привязанные к .NET, например, Delphi.NET. При компиляции код на любом из этих языков компилируется в сборку на общем языке CIL (Common Intermediate Language) - своего рода ассемблер платформы .NET. Поэтому мы можем сделать отдельные модули одного приложения на отдельных языках. [5]

Кроссплатформенность. .NET является переносимой платформой (с некоторыми ограничениями). Например, последняя версия платформы на данный момент .NET Framework поддерживается на большинстве современных ОС Windows (Windows 10/8.1/8/7/Vista). А благодаря проекту Mono можно создавать приложения, которые будут работать и на других ОС семейства Linux, в том числе на мобильных платформах Android и iOS.

Мощная библиотека классов. .NET представляет единую для всех поддерживаемых языков библиотеку классов. И какое бы приложение мы не собирались писать на C# - текстовый редактор, чат или сложный веб-сайт - так или иначе мы задействуем библиотеку классов .NET.

Разнообразие технологий. Общеязыковая среда исполнения CLR и базовая библиотека классов являются основой для целого стека технологий, которые разработчики могут задействовать при построении тех или иных приложений. Например, для работы с базами данных в этом стеке технологий предназначена технология ADO.NET. Для построения графических приложений с богатым насыщенным интерфейсом - технология WPF и Windows Forms. Для создания веб-сайтов - ASP.NET и т.д. [7]

## 3. Сравнительная оценка характеристик проекта и аналогов

Проведем сравнительную оценку характеристик разрабатываемого сервиса с аналогом. Показатели, по которым будет осуществлять данный анализ, представлены в Таблице 3.

Таблица 3 – Сравнительная оценка характеристик

| Критерии | Разрабатываемый сервис | NetOp School |
|---|---|---|
| 1 | 2 | 3 |
| Мониторинг подчиняемых компьютеров | Есть | Есть |
| Взаимодействие в сети интернет | Есть | Отсутствует |
| Демонстрация экрана главного компьютера | Отсутствует | Есть |

| Продолжение таблицы | | |
|---|---|---|
| 1 | 2 | 3 |
| Наличие базы данных | Есть | Отсутствует |
| Запрет использования программ | Есть | Отсутствует |
| Инвентаризация | Есть | Отсутствует |

Подробнее рассмотрим перечисленные критерии, указанные в таблице, чтобы обосновать необходимость разработки сервиса.

Первый критерий - мониторинг подчиняемых компьютеров, необходимый функционал в подобных программах, должен содержать информацию об устройствах и пользователе, который его использует.
Второй критерий, взаимодействие в сети интернет, так как разрабатываемый сервис намерен выйти за рамки одной аудитории, ему необходима возможность передачи данных через интернет. Недостаток аналога заключается в ограниченном количестве одновременно задействованных машин, в отличии от него разрабатываемый продукт намерен контролировать множество устройств, кроме того за границами учебного заведения.

Третий критерий, демонстрация экрана главного компьютера, полезная функция для ведения занятий, есть в аналоге, в нашем случаи особое внимание уведено процессу инвентаризации, облегчение администрирования, наличие такой функции избыточно и противоречит целям разработки.

Четвертый критерий, наличие базы данных, в случаи с аналогом её отсутствие никак не сказывается на эффективности использования программы. Разрабатываемый продукт требует наличие хранилища данных, но также может использоваться без отдельной базы данных и хранить в виде зашифрованных текстовых файлов информацию о пользователях и запрещенным программам для использования, будет иметь возможность делегировать разработчикам реализацию некоторых функций в том числе и способ хранения данных.

Пятый критерий, запрет использования программ, важная функция, которой не хватает в большинстве программных продуктах такого типа. Администратор при большом количестве подчиненных устройств не сможет контролировать действия всех пользователей, наличие такой функции автоматизирует этот процесс. Аналог не имеет такого функционала, разрабатываемый продукт предполагает наличие такой опции.

Шестой критерий, инвентаризация, позволяет выявлять установленные программы, отслеживать контроль версии установленного программного обеспечения, выявлять частоту использования, а также собирать сведения о устройстве. Крайне необходимый функционал для крупных учебных учреждений, позволяет экономить время для проверки устройств на наличие необходимого программного обеспечения, а также проверки целостности систем. Аналог не имеет данных функций, разрабатываемый продукт подразумевает наличие данных функций.

Итак, подведем итоги сравнительного анализа. NetOp School справляется с задачами, для которых был создан. Однако, некоторый функционал отсутствует, взаимодействие в сети

интернет даст возможность расширить количество устройств для администрирования, запрет использования программ облегчит контроль пользователей, инвентаризация позволит выявить недостающее программное обеспечение. Все эти нововведения позволят сформировать более качественный инструмент введения мониторинга устройств. Исходя из этого можно сказать, что разработка сервиса в целях повышения оптимизации контроля использования машин и поддержки процессов администрирования в высших учебных заведениях, при этом задействовать как можно большее количество пользователей, целесообразна.

**Список литературы**

1. ГОСТ 19.701-90 ЕСПД. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения [Электронный ресурс]: Режим доступа: http://docs.cntd.ru/document/gost-19-701-90-espd/ [Дата обращения: 21.02.23];
2. Система LanSchool CMS от компании Lenovo [Электронный ресурс]: Режим доступа: https://support.lenovo.com/ru/ru/solutions/ht510381-lanschool air-classroom-management-software [Дата обращения: 21.02.23]; Система iTALC от компании Veyon Solutions [Электронный ресурс]: Режим доступа: https://xn--90abhbolvbbfgb9aje4m.xn--p1ai/italc-udalennoeupravlenie-kompyuternym-klassom/ [Дата обращения: 02.03.23];
3. Система NetOp School [Электронный ресурс]: Режим доступа: http://netopschool.ru/ [Дата обращения: 09.03.23];
4. Askarian F. et al. Staphylococcus aureus modulation of innate immune responses through Toll-like (TLR),(NOD)-like (NLR) and C-type lectin (CLR) receptors //FEMS microbiology reviews. – 2018. – Т. 42. – №. 5. – С. 656-671.
5. Gage N. A. et al. The relationship between teachers' implementation of classroom management practices and student behavior in elementary school//Behavioral disorders. – 2018. – Т. 43. – №. 2. – С. 302-315.
6. Guérin B. A. ASP. NET con C# en Visual Studio 2017: diseno y desarrollo de aplicaciones Web. – Ediciones ENI., 2018.
7. Troelsen A., Japikse P. Pro C# 7: With. net and. net Core. – Apress, 2017. – Т. 1328.

**References**

1. GOST 19.701-90 ESD. Diagrams of algorithms, programs, data, and systems. Conventional symbols and rules for execution. [Electronic resource]: Access mode: http://docs.cntd.ru/document/gost-19-701-90-espd/ [Date of the application: 21.02.23];
2. LanSchool CMS system from Lenovo. [Electronic resource]: Access mode: https://support.lenovo.com/ru/ru/solutions/ht510381-lanschool air-classroom-management-software [Date of the application: 21.02.23];
3. iTALC system from Veyon Solutions company. [Electronic resource]: Access mode: https://xn--90abhbolvbbfgb9aje4m.xn--p1ai/italc-udalennoe upravlenie-kompyuternym-klassom/ [Date of the application: 02.03.23];
4. System NetOp School [Electronic resource]: Access mode: http://netopschool.ru/ [Date of the application: 09.03.23];
5. Askarian F. et al. Staphylococcus aureus modulation of innate immune responses through Toll-like (TLR),(NOD)-like (NLR) and C-type lectin (CLR) receptors //FEMS microbiology

reviews. – 2018. – Т. 42. – №. 5. – pp. 656-671.
6. Gage N. A. et al. The relationship between teachers' implementation of classroom management practices and student behavior in elementary school//Behavioral disorders. – 2018. – Т. 43. – №. 2. – pp. 302-315.
7. Guérin B. A. ASP. NET con C# en Visual Studio 2017: diseno y desarrollo de aplicaciones Web. – Ediciones ENI., 2018.
8. Troelsen A., Japikse P. Pro C# 7: With. net and. net Core. – Apress, 2017. – Т. 1328.

Беляева К.В. Безопасность веб-разработки: HTTPS, CORS, XSS, CSRF, CSP // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 83–85

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

# БЕЗОПАСНОСТЬ ВЕБ-РАЗРАБОТКИ: HTTPS, CORS, XSS, CSRF, CSP

**Беляева К.В.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: kaleriaa@bk.ru*

**В данной статье рассматриваются основные понятия и термины в области безопасности веб-разработки, которые необходимо знать для создания безопасных веб-приложений. Описываются такие уязвимости, как XSS, CSRF, а также методы защиты данных, такие как HTTPS. Знание этих основных понятий и терминов позволит разработчикам создавать более безопасные веб-приложения и минимизировать риски возникновения угроз в безопасности.**

Ключевые слова: Веб-разработка, безопасность, HTTPS, CORS, XSS, CSRF, CSP.

# WEB DEVELOPMENT SECURITY: HTTP, CARS, XSS, CSRF, CSP

**Belyaeva K.V.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: kaleriaa@bk.ru*

**This article covers the basic concepts and terms in the field of web development security that you need to know to create secure web applications. Vulnerabilities such as XSS, CSRF are described, as well as data protection methods such as HTTPS. Knowing these basic concepts and terms will allow developers to create more secure web applications and minimize the risk of security threats.**

Keywords: Web development, security, HTTPS, CORS, XSS, CSRF, CSP.

Много лет назад веб-страницы были довольно простыми и имели мало функциональности. Язык JavaScript использовался главным образом для создания эффектов и анимации на страницах, а также для проверки правильности заполнения форм. Однако со временем развитие технологий привело к тому, что JavaScript стал намного мощнее, добавились методы для сетевых запросов и многое другое, что позволяет создавать сложные приложения, работающие как на клиентской, так и на серверной сторонах (Node.js). Так, с увеличением функциональности JavaScript существует риск возникновения уязвимостей в безопасности, поэтому важно правильно использовать этот инструмент и следовать современным методам безопасности при разработке веб-приложений. Следование правилу, что скрипт с одной страницы не мог получить доступ к содержимому другой страницы, было основой веб-безопасности многие годы. Хотя даже это правило разработчики научились обходить, используя разные способы, например, отправка форм на другой сервер, использование в атрибуте src тега script любой домен.

В итоге, запросы на другой источник можно делать с некоторым ограничением – необходимо согласие сервера. CORS (Cross-Origin Resource Sharing) – механизм, который ограничивает доступ к контенту, расположенному на других доменах. Без использования CORS браузеры будут блокировать запросы, которые пытаются получить доступ к ресурсам, находящимся на других доменах. При отправке запроса на другой ресурс, браузер автоматически добавляет в запрос заголовок Origin, который содержит информацию об источнике, откуда был отправлен запрос. Сервер проверяет источник и если доступ разрешен, то добавляется особый заголовок к ответу, содержащий источник либо *. CORS позволяет контролировать доступ к сторонним ресурсам и предотвращает возможность атак межсайтовой подделки запроса (CSRF).

CSRF (Cross-Site Request Forgery) — это атака, при которой злоумышленник может выполнить определенное действие от имени пользователя без его согласия [2]. Это может быть смена пароля в системе, перевод денег и т.д., зависит, конечно же, от системы. Для осуществления вредоносных действий пользователь должен перейти по ссылке или выполнить что-то на подготовленном сайте, которые отправят определенный запрос. Многие сайты используют слабое звено авторизации – хранение сессии пользователей в куках, поэтому классический сценарий с отправкой формы позволит преступникам исполнить свои намерения. То есть, целевой сайт проверяет куки, видит, что посетитель авторизован и обрабатывает форму. Для защиты от CSRF необходимо использовать специальные секретные ключи (создается при авторизации и сохраняется в сессии пользователя) и генерированные на их основе токены, которые добавляются в каждый запрос и проверяются на стороне сервера. Кроме того, можно использовать HTTP заголовки Origin или для отслеживания источника запроса.

XSS (Cross-Site Scripting) – это тип атаки на веб-приложения, когда злоумышленник внедряет вредоносный код на страницу или в формы на сайте. Одним из простых сценариев использования уязвимости может быть: при вводе текста в поле и при последующим его отображением на страницу браузер будет обрабатывать текст между тегами <script> как JS-код, тоже происходит и с другими тегами. Теперь, когда пользователи зайдут на страницу, то вредоносный код загрузится вместе с текстом из поля ввода и/ или при вводе кода в параметре URL, если текст из поля дублируется в запросе. Однако, такое сработает только, если текст из поля не был обработан должны образом, то есть экранированием. Для защиты от XSS можно использовать механизмы фильтрации пользовательского ввода, HTML-экранирование и Content Security Policy (CSP).

CSP (Content Security Policy, политика безопасности контента) — это механизм безопасности веб-приложений, которые позволяют ограничить и контролировать источники загрузки ресурсов на странице. CSP может помочь защитить сайт от целого ряда атак, таких как XSS, clickjacking, подделка запросов и других. Для этого на страницу добавляется HTTP-заголовок Content-Security-Policy и директивы. CSP задает список допустимых источников для загрузки ресурсов, таких как скрипты, стили, изображения, шрифты, видео, звук и другие. Если ресурсы загружаются из недопустимых источников, то браузер блокирует их загрузку и сообщает об ошибке. Данная политика может быть установлена как HTTP-заголовок, тег мета или атрибут HTML-элемента. Обычно ее следует использовать вместе с другими механизмами защиты, такими как HTTPS, CORS и другими.

Таким образом, знание о существующих уязвимостях может помочь их своевременно обнаружить и предотвратить неправомерный действия, а понимание механизмов/ стандартов в области веб-безопасности поможет правильно их применять на практике, сохраняя данные пользователей конфиденциальными.

**Список литературы**

1. Fetch: запросы на другие сайты // Современный учебник JavaScript URL: https://learn.javascript.ru/fetch-crossorigin (дата обращения: 21.05.2023).
2. Атака CSRF // Современный учебник JavaScript URL: https://learn.javascript.ru/csrf (дата обращения: 21.05.2023).
3. CSP // Skillfactory Media URL: https://blog.skillfactory.ru/glossary/csp/ (дата обращения: 21.05.2023).
4. Что такое XSS-уязвимость и как тестировщику не пропустить ее // Habr URL: https://habr.com/ru/articles/511318/ (дата обращения: 21.05.2023).

**References**

1. Fetch: requests to other sites // Modern JavaScript tutorial URL: https://learn.javascript.ru/fetch-crossorigin (accessed on: 21.05.2023).
2. CSRF attack // Modern JavaScript textbook URL: https://learn.javascript.ru/csrf (accessed on: 21.05.2023).
3. CSP // Skillfactory Media URL: https://blog.skillfactory.ru/glossary/csp/ (дата обращения: 21.05.2023).
4. What is an XSS vulnerability and how can a tester not miss it) // Habr URL: https://habr.com/ru/articles/511318/ (accessed 21.05.2023).

Аникин Д.А. Логирование для отладки и профилирования JAVA-приложений // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 86–91

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.432.2

# ЛОГИРОВАНИЕ ДЛЯ ОТЛАДКИ И ПРОФИЛИРОВАНИЯ JAVA-ПРИЛОЖЕНИЙ

**Аникин Д.А.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: danil-anikin-98@mail.ru*

**Настоящая статья посвящена обзору инструментов логирования Java-приложений и рассмотрению методов отладки и профилирования с помощью рассмотренных технологий. В ходе разработки программ необходимо иметь инструмент, благодаря которому проводится отслеживание состояний пользовательских сессий во время работы приложения, автоматизированные инструменты управления логами направлены на решение указанной проблемы. В результате их анализа были выявлены общие принципы и руководства по реализации логирования в разрабатываемых программах.**

Ключевые слова: Информатика, логирование, джава, программирование, отладка и профилирование.

# LOGGING FOR DEBUGGING AND PROFILING JAVA APPLICATIONS

**Anikin D.A.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: danil-anikin-98@mail.ru*

**This article is devoted to an overview of Java application logging tools and a review of debugging and profiling methods using the technologies considered. During the development of programs, it is necessary to have a tool through which the states of user sessions are monitored during the operation of the application, automated log management tools are aimed at solving this problem. As a result of their analysis, general principles and guidelines for the implementation of logging in the developed programs were identified.**

Keywords: Computer science, logging, java, programming, debugging and profiling.

Разработка программных приложений для различных средств электронно-вычислительной техники – это огромная часть современной жизни и тренды развития науки и общества явно указывают на то, что область действия информационных технологий будет продолжать расширять собственную зону влияния. При разработке приложений разработчики сталкиваются с проблемой выявления ошибок и отладки кода, далеко не всегда программисты безошибочно реализуют необходимую бизнес-логику и в ходе работы возникают ситуации, которые не были предусмотрены изначальным замыслом. В такой момент к обязанностям разработчика добавляется отслеживание выполнения кода и поиск ошибок, допущенных при написании, определению, что именно и в какой момент привело к некорректному поведению программы [5].

В данной статье будут рассмотрены принципы использования логирования для отладки и профилирования на примере Java-приложений, а также разобраны различные фреймворки

и инструменты, предназначенные для решения задачи мониторинга и анализа исполнения приложений. Кроме того, будут рассмотрены преимущества и недостатки логирования при отладке Java-приложений и будут представлены рекомендации, основанные на опыте использования различных фреймворков. Улучшение производительности разработчиков является одной из важнейших задач в производстве программного обеспечения, и в этой статье будут представлены рекомендации для быстрой и эффективной разработки Java-приложений.

Как уже было установлено, в задачи разработчика входит не только написание кода, но и отслеживание его выполнения и поиск ошибок. Одним из наиболее популярных и распространённых решений этой проблемы является логирование. Логирование - это процесс ведения журнала событий, которые происходят в компьютерной системе. Логи – это отдельные файлы, которые и составляют журнал логирования [1]. Они должны быть структурированы и подходить под единый шаблон, выведенный в рамках разработки приложения.

При обработке пользовательских сессий может возникнуть множество различных ситуаций, каждая из которых должна быть записана в журнал логов. Так как журнал является тем средством, которое впоследствии будет проанализировано программистом с целью проверки корректности работы или поиска ошибки, то одним из важнейших факторов является читаемость и удобство восприятия логов. Во всех высоконагруженных системах с большим количеством параллельных сессий лог-файлы будут стремительно наполняться большим количеством записей, анализ которых в скором времени станет очень трудной задачей. С целью повышения читаемости и контроля количества сохраняемой информации была разработана концепция уровней логирования.

Уровни логирования явным образом указывают на тип, который записывается в лог-файл. Каждый уровень следует принимать только в подходящем контексте, в противном случае это может привести к еще более запутанному наполнению журнала [3]. Иерархия уровней представлена на Рисунке 1.


Рисунок 1 – Иерархия уровней логирования

ALL: включает в себя все уровни логирования. Он может быть полезен при обработке большого объёма данных, когда необходимо получить полную картину действий приложения.

TRACE: представляет наиболее подробную информацию о работе программы, которая может быть полезна во время разработки и отладки. Могут быть записаны все состояния объектов, значения переменных, ошибки и другие данные, которые помогут разработчику понять, что происходит во время исполнения.

DEBUG: уровень для информации, которая пригодится только при отладке программы. Этот уровень используется для записи дополнительных данных, которые помогут разработчику разобраться в процессе выполнения программы. Это может быть информация о значениях переменных, результатах выполнения условных операторов, вызовах функций и т.д.

INFO: уровень для информации, которая может помочь при анализе работы программы и выявлении её проблем. Этот уровень используется для сообщений о промежуточных результатах работ, в том числе о запуске и остановке, успешных операциях, вызове функций и методов, а также о состоянии программы в момент её выполнения.

WARNING: уровень для сообщений об ошибках или непредвиденных ситуациях, которые были обработаны программой. Этот уровень используется для сообщений о незначительных проблемах, которые не привели к аварийной остановке, но требуют внимания и устранения.

ERROR: уровень для сообщений об ошибках, которые не позволяют продолжить работу программы. Этот уровень используется для сообщений о критических сбоях, которые приводят к завершению работы программы.

FATAL: самый высокий уровень, он используется для сообщений о критических ошибках, которые могут привести к потере данных, повреждению системы или другим серьезным последствиям.

Java - один из самых популярных языков программирования в мире, который имеет широкую функциональность и позволяет создавать мультиплатформенное программное обеспечение. Именно на его примере будет рассмотрено практическое применение и реализация различных фреймворков для ведения логов.

Логирование в Java-приложениях имеет свои преимущества и недостатки [2]. Среди основных достоинств можно выделить:

- Диагностика и устранение проблем. Запись событий в лог-файлы позволяет разработчикам узнать, что происходило в приложении во время возникновения ошибок или других проблем. Это помогает быстрее и эффективнее диагностировать и устранять ошибки.
- Мониторинг и анализ работы приложения. Лог-файлы могут содержать информацию о работе приложения, такую как пропущенные элементы, время ответа и т.д., которая может быть очень полезна при анализе работы приложения.
- Обнаружение угроз безопасности. Логирование приложений может обнаружить запуск несанкционированных процессов или другие аномалии, которые могут свидетельствовать о попытке взлома приложения.
- Улучшение пользовательского опыта. Логирование приложений может помочь разработчикам понять, как пользователи используют приложение, и определить, какие части наиболее часто вызывают проблемы или создают неудобства.

Однако использование логов часто чревато следующими негативными последствиями:

- Снижение производительности. Запись большого количества данных в лог-файлы может повысить нагрузку на приложение, что может привести к снижению его производительности.
- Непоследовательность. Логирование приложений может быть непоследовательным и зависеть от настроек или ошибок конфигурации, что может затруднить понимание того, что происходит в приложении.
- Угроза конфиденциальности. Лог-файлы могут содержать конфиденциальную информацию о пользователях, такую как: логины, пароли, данные банковских карт и т.д. Если эти данные попадут в чужие руки, это может привести к серьезным последствиям.
- Переполнение хранилища данных. Если приложение не управляет размером лог-файлов или их количеством, то это может привести к переполнению хранилища данных, что в свою очередь может замедлить работу приложения.

Поэтому важно проанализировать потребности разработки и выбрать подходящий фреймворк или инструмент для логирования. Для автоматизации процесса разработки системы логирования Java предоставляет различные фреймворки, в которых реализован практически весь функционал, необходимый для составления и обработки log-файлов. Наиболее популярными являются:

JUL (Java Util Logging) - стандартный механизм логирования для Java. JUL обладает всеми базовыми функциями и позволяет записывать логи в файл или консоль. Однако он не позволяет настраивать уровни логирования в реальном времени.

Log4j - одна из самых популярных библиотек для логирования Java приложений. Позволяет выбрать уровень логирования, настроить различный вывод записей, начиная с консольного и файлового, заканчивая системами управления базами данных. Она используется во множестве проектов, однако на данный момент является устаревшей.

Log4j2 - обновленная версия Log4j с расширенным функционалом. Она была переработана с целью обеспечения большей производительности и поддержки асинхронного логирования, а также для достижения более простой конфигурации и использования.

Logback - обладает большими возможностями для настройки и управления логированием, так что её можно настроить для разных типов приложений и сред. Она также поддерживает асинхронное логирование, администрирование через JMX и расширенные функции форматирования.

SLF4J (Simple Logging Facade for Java) - это фреймворк для протоколирования, который является абстракцией над такими библиотеками, как Log4j, Logback и JUL. SLF4J представляет собой обобщенный интерфейс для различных систем и не зависит от конкретной реализации [4].

Рассмотренные библиотеки позволяют снизить влияние технических недостатков записи логов, однако без грамотного управления ими любая система в конечном счете придёт к неорганизованным и перегруженным журналам. Для сохранения порядка следует придерживаться лучших практик организации логирования [7]:

- Запись в журнале лога должна чётко отражать реальную ситуацию и иметь соответствующий ей уровень. Не следует рядовые исключения обработки содержимого формы помечать уровнем ERROR, также как и нежелательно помечать критические ошибки уровнем WARN.

- При разработке веб-приложений следует логировать входящий http-запрос и исходящий htttp-ответ, это позволит определить, что в возникновении исключительной ситуации виновен сервис, который обрабатывает запрос [6].
- Не стоит записывать все события и все промежуточные состояния в журнал, так как на операции чтения и записи затрачиваются вычислительные ресурсы машины, это приводит к понижению скорости работы системы, а файлы увеличиваются в размерах непропорционально полезной информации, которая представлена в них.
- Стоит записывать сообщения, напрямую связанные с исполнением бизнес-логики приложения. Это позволяет отследить корректность решения поставленной задачи.
- Использовать уникальные идентификаторы пользовательских сессий, запросов, это позволяет упростить поиск и фильтрацию записей.
- Использовать понятный и легко интерпретируемый формат. Стандартом отрасли на данный момент является JSON-строка, которая позволяет хранить в себе состояние возможных объектов. Читаемый вид позволяет упростить анализ и восприятие журнала.
- Не записывать конфиденциальную информацию. Утечка персональных данных пользователя может привести к сильному репутационному удару компании или же привести к прямому урону жизни пользователей, чьи данные были потеряны.

В результате анализа концепции логирования и рассмотрения готовых фреймворков для её реализации были выявлены советы по их использованию и организации ведения логов в разрабатываемом приложении. Указанные практики позволяют обеспечить эффективное логирование и анализ работы приложений, повысить безопасность, стабильность и производительность системы. Были рассмотрены как преимущества, так и недостатки, но, несмотря на них, сохранение истории работы приложения является необходимым средством, без которого невозможно дальнейшее развитие информационных систем.

**Список литературы**

1. Anton, Chuvakin Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management / Chuvakin Anton, Schmidt Kevin. — Amsterdam. — Netherlands : , 2012. — 413 с. — Текст : непосредственный.
2. Java Logging Technology // Java documentation URL: https://docs.oracle.com/javase/8/docs/technotes/guides/logging/index.html (дата обращения: 10.05.2023).
3. Introduction to java logging // Baeldung URL: https://www.baeldung.com/java-logging-intro (дата обращения: 10.05.2023).
4. SLF4J Documentation // slf4j URL: https://www.slf4j.org/docs.html (дата обращения: 10.05.2023).
5. Peters, T. (1993). The history and development of transaction log analysis. Library Hi Tech., 42(11), 41−66
6. Robert, C, Martin Clean Code / C, Martin Robert. — Massachusetts : Courier in Stoughton, 2009. — 462 с. — Текст : непосредственный.
7. Robert, C,Martin Clean Architecture / C,Martin Robert. — Massachusetts : Courier in Stoughton, 2018. — 429 с. — Текст : непосредственный.

Аникин Д.А. Логирование для отладки и профилирования JAVA-приложений // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 86–91

**References**

1. Anton, Chuvakin Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management / Chuvakin Anton, Schmidt Kevin. — Amsterdam. — Netherlands : , 2012. — p. 413— Text: direct.
2. Java Logging Technology // Java documentation URL: https://docs.oracle.com/javase/8/docs/technotes/guides/logging/index.html (дата обращения: 10.05.2023).
3. Introduction to java logging // Baeldung URL: https://www.baeldung.com/java-logging-intro (accessed on: 10.05.2023).
4. SLF4J Documentation // slf4j URL: https://www.slf4j.org/docs.html (accessed on: 10.05.2023).
5. Peters, T. (1993). The history and development of transaction log analysis. Library Hi Tech., 42(11), 41−66
6. Robert, C, Martin Clean Code / C, Martin Robert. — Massachusetts : Courier in Stoughton, 2009. — p. 462— Text: immediate.
7. Robert, C,Martin Clean Architecture / C,Martin Robert. — Massachusetts : Courier in Stoughton, 2018. — p. 429— Text: immediate.

Бичаева В.А., Макуха Л.В. ВЕБ приложение для ветеринарной клиники // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 92–98

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.4

# ВЕБ ПРИЛОЖЕНИЕ ДЛЯ ВЕТЕРИНАРНОЙ КЛИНИКИ

**Бичаева В.А., Макуха Л.В.**
*ФГАОУ ВО «Сибирский федеральный университет", Красноярск, Россия (660041, Красноярский край, город Красноярск, Свободный пр-кт, д.79), e-mail: Makuha23@yandex.ru*

**В статье приводится описание работы веб приложения, разработанного для ветеринарной клиники с возможностью использования личного кабинета для записи на предоставляемые услуги и получения персональных бонусов., для легко и удобного общения владельца питомца с врачами клиники.**
**В процессе работы, внутри веб приложения создан личный кабинет пользователя, администратора и врача для автоматизации записи пациентов на прием и удаленного общения с клиникой.**
**Пользователь может пользоваться веб приложением как с личным кабинетом, так и без него. Но, зарегистрированный пользователь в отличии от незарегистрированного имеет бонусы – скидка 5% от суммы заказа при записи на услуги клиники через личный кабинет; простота записи – личные данные пользователя хранятся внутри личного кабинета и при записи на услуги нет необходимости вводить их каждый раз; удобство – в личном кабинете можно просмотреть статус записи, список уже пройденных услуг и общаться с врачами клиники по интересующим вопросам.**
**Личный кабинет администратора помогает с разы упростить работу клиники. Так администратор назначает дату и время для поступившей к нему записи на представленную услугу, отмечать статус записи, удалять и добавлять новые категории и услуги клиники, указывать цены на них.**
**Для врача личный кабинет будет нести информативный характер. В нем он сможет отслеживать пройденные у него записи и, при необходимости, связываться с пациентами в текстовом чате.**
**Автоматизируя процесс записи на прием, ветеринарная клиника может сэкономить время и ресурсы, а также снизить риск перепланировки или двойного бронирования. Все эти меры могут привести к повышению удовлетворенности клиентов и их удержанию, а также к повышению производительности труда персонала.**

Ключевые слова: Телеветеринария, ветеринарная клиника, разработка web-сайта, лечение питомцев, врач, пациент, администратор.

# WEB APP FOR VETERINARY CLINIC

**Bichaeva V.A., Makukha L.V.**
*Siberian Federal University, Krasnoyarsk, Russia (660041, Krasnoyarsk Territory, Krasnoyarsk city, Svobodny Ave., 79), e-mail: Makuha23@yandex.ru*

**The article describes the operation of a web application developed for a veterinary clinic with the ability to use a personal account to sign up for the services provided and receive personal bonuses, for easy and convenient communication between the pet owner and the clinic doctors.**
**In the course of work, a personal account of the user, administrator and doctor was created inside the web application to automate the appointment of patients and remote communication with the clinic.**
**The user can use the web application with or without a personal account. But, a registered user, unlike an unregistered one, has bonuses - a 5% discount on the order amount when registering for clinic services through a personal account; ease of recording - the user's personal data is stored inside the personal account and when registering for services there is no need to enter them every time; convenience - in your personal account you can**

**view the status of the appointment, the list of services already completed and communicate with the doctors of the clinic on issues of interest.**

**The administrator's personal account helps to simplify the work of the clinic from time to time. This is how the administrator sets the date and time for the record received by him for the provided service, marks the status of the record, deletes and adds new categories and clinic services, and indicates prices for them.**

**For a doctor, a personal account will be informative. In it, he will be able to track his records and, if necessary, contact patients in a text chat.**

**By automating the appointment process, the veterinary clinic can save time and resources, and reduce the risk of rescheduling or double bookings. All of these measures can lead to improved customer satisfaction and retention, as well as increased staff productivity.**

Keywords: Televeterinary medicine, veterinary clinic, website development, pet treatment, doctor, patient, administrator.

Из-за территориальной удаленности часто отсутствует возможность личного общения, поэтому на помощь к людям приходят телефоны, мессенджеры и видеоконференции.

Видеоконференция в современном мире является приоритетным методом общения. В ходе видеоконференции задействовано большее число органов чувств, чем во время телефонного звонка (не только слуховые, но и зрительные, что позволяет добиться более прочного понимания между участниками, чем при обычном телефонном общении). Благодаря простоте и эффективности данного средства общения, появился такой термин, как телемедицина.

Телемедицина – это консультация с врачом через социальные мессенджеры, по телефону или по видеосвязи. Например, благодаря видеосвязи, врач видит пациента, имеет возможность зрительно оценить его состояние и на основе полученных данных, может опираться не только на слова пациента, но и на свои собственные наблюдения. Для большего понимания работы телемедицины, будет рассмотрена меньшая ее часть – телеветеринария [1].

Телеветеринария существует относительно недавно, причем аналогична по исполнению телемедицины для людей. Владелец животного может самостоятельно передавать информацию ветеринарному врачу в удаленном формате, сообщать о замеченных симптомах и, по просьбе лечащего врача, предпринимать определенные шаги, чтобы помочь поддержать или улучшить состояние питомца.

Телеветеринария хороша тем, что в формате удаленной консультации можно оценить, являются ли замеченные симптомы реальным поводом для беспокойства, выяснить, нужно ли срочное вмешательство; определить, какие меры можно предпринять самостоятельно.

Поскольку все больше и больше людей обращаются к Интернету за информацией и услугами, веб-сайта для ветеринарной клиники с автоматизированным назначением встреч позволил бы значительно улучшить качество и время обслуживания клиентов [2].

Кроме того, хорошо оформленный веб-сайт может предоставить ценную информацию об услугах, персонале и оснащении ветеринарной клиники, также помогая установить доверие к ней.

Стоит отметить, что очное посещение ветеринарных клиник никто не отменял. Посещение клиник остается главной задачей ответственного владельца домашнего питомца.

В процессе создания сайта были поставлены и решены такие задачи, как разработка структуры веб-сайта (Рисунок 1); проектирование веб-сайта и разработка веб-сайта (Рисунок 2) [3].

Для решения поставленных задач был выбран язык программирования PHP и реляционная база данных с поддержкой транзакции MySQL [4][5].

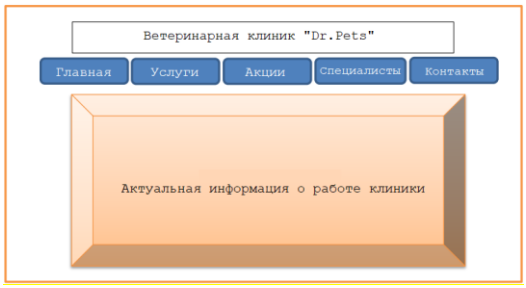



Рисунок 1 – Изначальный шаблон сайта

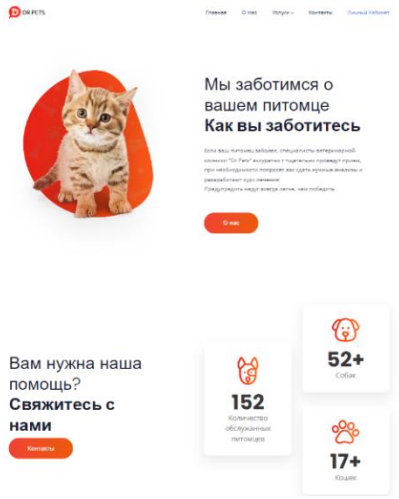



Рисунок 2 – Итоговый результат

Диаграммы вариантов использования (Рисунок 3) полезны для информирования заинтересованных сторон о функциональных требованиях к системе и часто создаются на ранних этапах процесса разработки программного обеспечения как способ выявления и проверки требований. В работе с сайтом задействованы три роли: пользователь, администратор клиники и врач клиники [6].

Пользователь может просматривать актуальную информацию о работе клиники, записываться на предоставляемые услуги, пользоваться личным кабинетом при желании, поддерживать связь с клиникой и врачами.

Администратор занимается отслеживаем записей на услуги, определяет дату, время приема и статус заказа. Также может добавлять новые и удалять имеющиеся категории услуг.

Врач в личном кабинете может просматривать записи на уже прошедшие услуги и поддерживать связь с пациентами.

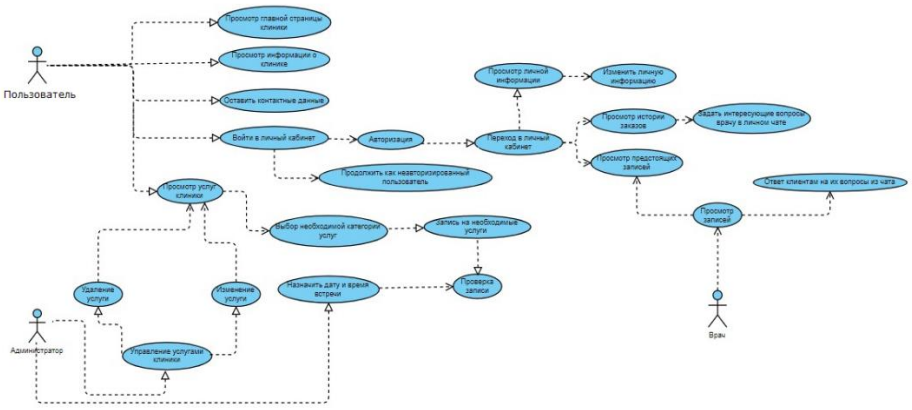



Рисунок 3 – Диаграмма взаимодействий

Регистрация пользователя на сайте происходит посредством установки логина и пароля, которые в будущем будут храниться в базе данных (Рисунок 4). Авторизация предусмотрена для зарегистрированного пользователя. При авторизации происходит обращение к базе данных для проверки хранящихся в ней логинов и паролей. Если после обращения данные

совпадают, то происходит авторизация пользователя в личном кабинете, в противном случае, если незарегистрированный пользователь попытается авторизоваться, он получит ошибку о том, что пользователь с таким логином не зарегистрирован. Окна регистрации и авторизации пользователя показаны на Рисунке 5.

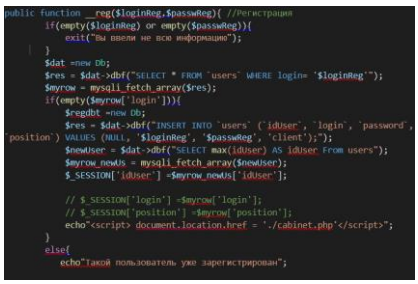



Рисунок 4 – Регистрация пользователя

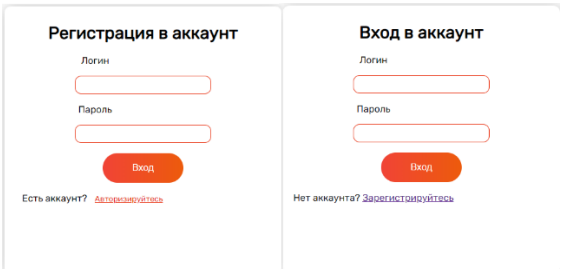



Рисунок 5 – Окна регистрации и авторизации пользователя

Хотелось бы отметить, что запись на услуги зарегистрированного пользователя отличается от записи пользователя (Рисунок 6), который не имеет личного кабинета.

Так, пользователь, имеющий личный кабинет на сайте клиники, имеет личные бонусы - скидка 5% от суммы заказа при записи на услуги через личный кабинет на сайте ветеринарной клиники. Скидка применяется только для авторизированного на сайте пользователя, если его idUser не пустой (Рисунок 7).

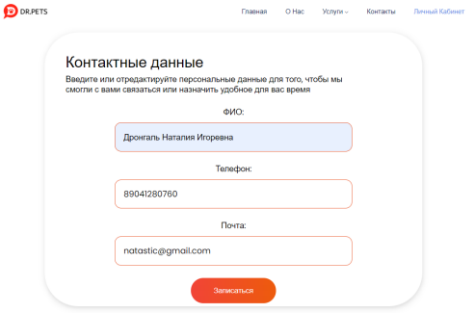



Рисунок 6 – Указание личных данных при записи незарегистрированного пользователя

```php
if(!empty($_POST)){
    $fio = $_POST["fio"];
    $tel = $_POST["tel"];
    $email = $_POST["email"];
    $idUser = $_POST["idUser"];
    $price = $_POST["price"];
    if($idUser !== ""){
        $sale = $price * 0.05;
        $price = $price - $sale;
```

Рисунок 7 – Автоматический расчёт скидки зарегистрированного пользователя

Зарегистрированный пользователь указывает личные данные внутри личного кабинета в специальной форме однократно, откуда они записываются в базу данных и сохраняются там. При записи на услуги клиники через личный кабинет, пользователь получает уведомление о том, что заявка принята в обработку (Рисунок 8). В это время, данные о записи поступают в личный кабинет администратора (Рисунок 9).

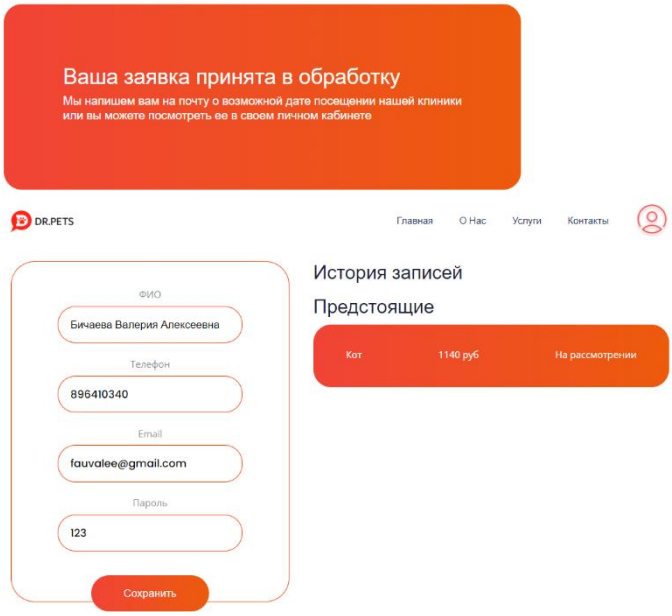



Рисунок 8 – Работа личного кабинета пользователя

Для отслеживания заказов и добавления новых услуг и категорий был разработан кабинет администратора.

Здесь администратор входит в систему для управления каталогом услуг и записями, просматривает все записи и их детали, включая ФИО клиента, номер телефона для связи и статус записи.

Администратор может обновить статус записи (на рассмотрении, ожидание и пройдено). Каждый статус записи несет за собой определенную информацию. На рассмотрении – заявка направлена администратору и в ближайшее время будет назначены дата и время встречи; ожидание – дата и время назначено и врач ожидает пациента на прием; пройдено – пациент посетил ветеринарную клинику и услуга оказана.

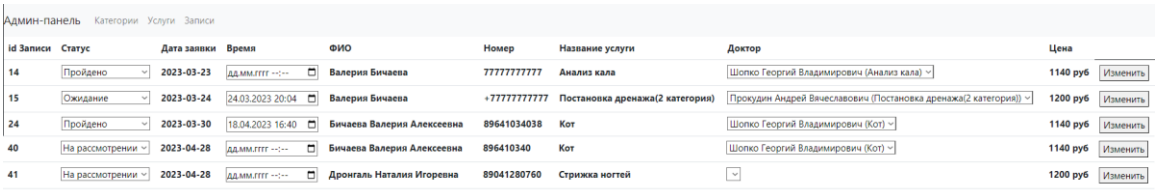



Рисунок 9 – Окно просмотра записей администратором

Как уже говорилось выше, администратор может добавлять услуги и категории, изменять и удалять их.

На Рисунке 10 наглядно продемонстрирован процесс добавления новой услуги администратором. Для этого необходимо заполнить несколько полей: указать название услуги, отнести ее к уже имеющейся категории услуг, но, если требуемая категория отсутствует, по подобному алгоритму администратор может создать новую, указать стоимость новой услуги и добавить описание, если это нужно. После нажатия на кнопку «Добавить», новая услуга добавляется в конец уже имеющегося списка услуг.

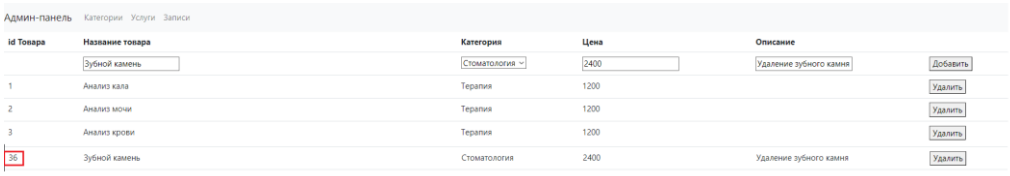



Рисунок 10 – Удаление и добавление услуг администратором

Личный кабинет врача имеет немного ограниченный функционал. Врач заходит в личный кабинет и просматривает личные записи клиентов, а также отвечает на их вопросы в чате. На Рисунке 11 из личного кабинета врача видно, что в нем отображаются записи, которые в личном кабинете администратора уже отмечены статусом «Пройдено».

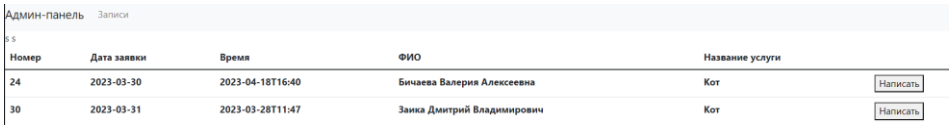



Рисунок 11 – Личные записи врача

На Рисунке 12 запись с id 40 имеет статус «На рассмотрении», соответственно, обращаясь к информации на Рисунке 11 можно увидеть, что запись у врача не отображается. Как только администратор установил статус записи «Пройдено» стало видно, что запись стала отображаться теперь и у врача, где автоматически становится открытым личный чат для связи с пациентом.

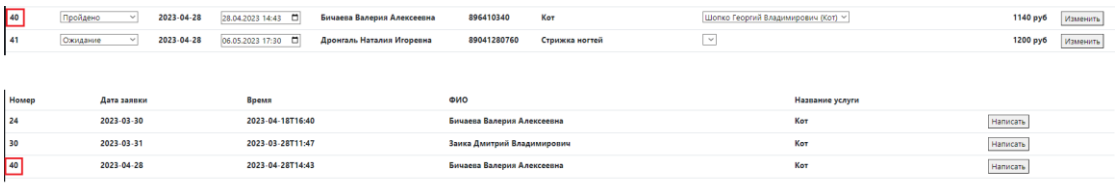



Рисунок 12 – Работа взаимодействия личных кабинетов администратора и врача

Таким образом, при помощи языка программирования PHP и базы данных MySQL был создан функционирующий сайт, отвечающий поставленным задачам и первоначальным задумкам. В процессе работы над веб-приложением удалось разграничить права доступа при работе с различными типами пользователей, автоматически применять скидку авторизированным пользователям при записи на услуги клиники, создать удобный личный кабинет для всех ролей в системе, отвечающий поставленным требованиям.

**Список литературы**

1. Что такое телеветеринария и как она работает? [Электронный ресурс]. – URL https://direct.farm/post/chto-takoye-televeterinariya-i-kak-ona-rabotayet-16899.
2. Правила оказания платных ветеринарных услуг [Электронный ресурс]. – URL: https://studfile.net/preview/3962133/page:11/.
3. Веб-программирование на HTML. [Электронный ресурс]. – URL: http://kurepin.ru/main.phtml.
4. Коггзолл Д. PHP 5: полное руководство [текст] / Д. Коггзолл М. - 2009. - 752 с.
5. Работа с MySQL в PHP. [Электронный ресурс]. – URL: https://htmlacademy.ru/blog/php/mysql.
6. Создание ролей пользователей на сайте [Электронный ресурс]. – URL: https://bezramok-tlt.ru/blog/posts/sozdanie-roley-polzovateley-na-sayte.

**References**

1. What is tele-veterinary medicine and how does it work? [electronic resource]. – URL https://direct.farm/post/chto-takoye-televeterinariya-i-kak-ona-rabotayet-16899 .
2. Rules for the provision of paid veterinary services [Electronic resource]. – URL: https://studfile.net/preview/3962133/page:11 /.
3. Web programming in HTML. [electronic resource]. – URL: http://kurepin.ru/main.phtml.
4. Coggsoll D. PHP 5: the complete guide [text] / D. Coggsoll M. - 2009. - 752 p.
5. Working with MySQL in PHP. [electronic resource]. – URL: https://htmlacademy.ru/blog/php/mysql.
6. Creating user roles on the website [Electronic resource]. – URL: https://bezramok-tlt.ru/blog/posts/sozdanie-roley-polzovateley-na-sayte.

Курманбакеев В.А. Применение нейросетей в сфере защиты информации // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2 с. 99–102

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

# ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

**Курманбакеев В.А.**
*ФГБОУ ВО "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: slavan787@gmail.com*

**В последние годы интернет и цифровые технологии стали неотъемлемой частью жизни людей, а также бизнеса и государства. С этим связаны как преимущества, так и недостатки, в частности - риск потери и утечки конфиденциальной информации. В такой ситуации защита информации становится критически важной задачей, и здесь важную роль играют нейронные сети.**

Ключевые слова: Нейросети, нейронные сети, кибербезопасность, информационная безопасность.

# APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY

**Kurmanbakeev V.A.**
*Bonch-Bruevich St. Petersburg State University of Telecommunications*, St. Petersburg, *Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail: slavan787@gmail.com*

**In recent years, the Internet and digital technologies have become an integral part of people's lives, as well as business and the state. This has both advantages and disadvantages, in particular, the risk of loss and leakage of confidential information. In such a situation, information protection becomes a critical task, and neural networks play an important role here.**

Keywords: Neural networks, neural networks, cybersecurity, information security.

Нейронные сети - это компьютерные алгоритмы, которые могут обрабатывать большие объемы данных и выявлять скрытые зависимости между ними. Эти свойства делают их прекрасным инструментом для работы с защитой информации. Рассмотрим несколько способов применения нейронных сетей в этой области.

Первым способом является обнаружение аномалий в сети. Этот метод используется для выявления подозрительного трафика, который может указывать на попытки взлома или кражи данных. Нейронные сети могут обучаться на основе нормального трафика и затем выявлять аномальные пакеты данных, которые не соответствуют норме. Это может помочь обнаружить атаки и предотвратить утечки информации.

Вторым способом является анализ поведения пользователей. Нейронные сети могут использоваться для создания профилей пользователей, которые определяют, какие действия являются типичными для этого пользователя, а какие - нет. Это может помочь выявить

необычное поведение пользователей, что может свидетельствовать о попытке несанкционированного доступа к данным.

Третьим способом является шифрование информации. Нейронные сети могут использоваться для создания шифрованных сообщений, которые трудно поддаются взлому. Это может помочь защитить данные от несанкционированного доступа и утечек.

Наконец, четвертым способом является распознавание образов. Нейронные сети могут использоваться для распознавания образов на изображениях, что может помочь в обнаружении попыток использования фальшивых документов или идентификаторов.

Несмотря на все преимущества, применение нейронных сетей в сфере защиты информации также имеет свои недостатки и ограничения. Один из основных недостатков - это высокая стоимость разработки и обучения нейронных сетей, особенно если требуется обработка большого объема данных. Кроме того, нейронные сети могут быть взломаны, если хакеры найдут способ обмануть систему и ввести ложные данные.

Другой ограничением является ограниченность точности нейронных сетей в условиях непредсказуемых и нестандартных ситуациях, что может привести к ошибкам при обработке информации и выявлении угрозы.

Несмотря на эти ограничения, применение нейронных сетей в сфере защиты информации все еще является многообещающим. При правильной настройке и использовании, нейронные сети могут помочь значительно улучшить защиту конфиденциальной информации и снизить риск утечек.

Таким образом, использование нейронных сетей в сфере защиты информации представляет собой эффективный способ обнаружения и предотвращения угроз. Несмотря на ограничения и недостатки, применение этой технологии является актуальной и многообещающей темой для исследований и разработок в области кибербезопасности.

Нейронные сети могут быть применены в различных аспектах защиты информации, таких как обнаружение атак, предотвращение утечек данных, распознавание аномалий, аутентификация пользователей и многое другое.

Одной из самых распространенных областей применения нейронных сетей в сфере защиты информации является обнаружение вредоносного программного обеспечения (малварь). Нейронные сети могут быть обучены распознавать особенности и поведение вредоносных программ, чтобы предотвратить их воздействие на компьютерную систему.

Еще одним примером использования нейронных сетей является распознавание скомпрометированных пользователей. Эта технология может использоваться для обнаружения незаконного доступа к системам или аккаунтам с помощью анализа поведения пользователя. Например, нейронные сети могут обучаться распознавать, когда пользователь выполняет действия, которые не соответствуют его типичному поведению, такие как попытки доступа в неправильное время или из неправильного места.

Также нейронные сети могут быть использованы для защиты данных на уровне приложений, например, при распознавании спама в электронной почте или при защите от фишинговых атак. Нейронные сети могут помочь автоматически распознавать и блокировать нежелательные сообщения, таким образом снижая риск утечки информации.

Наконец, нейронные сети могут быть использованы для анализа больших объемов данных и выявления тенденций и паттернов, которые могут указывать на возможные угрозы.

Это может помочь организациям разработать эффективные стратегии защиты информации, основанные на реальных данных и анализе рисков.

В целом, применение нейронных сетей в сфере защиты информации позволяет существенно улучшить кибербезопасность и снизить риск утечек конфиденциальной информации. Однако, для того чтобы использовать эту технологию эффективно, необходимы профессиональные знания и навыки в области машинного обучения и кибербезопасности, а также доступ к достаточным вычислительным ресурсам для обучения и развертывания нейронных сетей.

Кроме того, нейронные сети могут быть подвержены атакам со стороны злоумышленников, которые могут попытаться обойти или обмануть систему защиты, использующую нейронные сети. Поэтому важно постоянно обновлять и адаптировать системы защиты, чтобы они оставались эффективными в изменяющихся условиях.

В заключение, использование нейронных сетей в сфере защиты информации представляет собой мощный инструмент, который может помочь организациям более эффективно защищать свои данные и предотвращать кибератаки. Однако, необходимо учитывать, что эта технология является лишь одним из инструментов в борьбе за кибербезопасность, и успешность ее применения зависит от профессионализма и компетентности специалистов, которые ее используют.

Также следует отметить, что использование нейронных сетей в сфере защиты информации имеет свои ограничения и ограничения. Например, некоторые атаки могут быть слишком сложными для обнаружения с помощью нейронных сетей, и может потребоваться дополнительная технология для их обнаружения. Кроме того, нейронные сети могут ошибаться при распознавании определенных типов данных или при наличии шума в данных, что может привести к ложным срабатываниям.

Таким образом, использование нейронных сетей в сфере защиты информации является перспективным направлением развития, которое может помочь организациям более эффективно защищать свои данные и предотвращать кибератаки. Однако, чтобы успешно применять эту технологию, необходимо учитывать ее ограничения, а также обеспечить высокий уровень профессионализма и компетентности специалистов, которые ее используют.

**Список литературы**

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. IEEE Symposium on Security and Privacy.
3. Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE Symposium on Security and Privacy.
4. Xu, W., Evans, D., & Qi, Y. (2019). Feature squeezing: Detecting adversarial examples in deep neural networks. IEEE Symposium on Security and Privacy.
5. 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.

6. 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.
7. Косов Н. А., Мазепин П. С., Гришин Н. А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
8. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

**References**

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
2. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. IEEE Symposium on Security and Privacy.
3. Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE Symposium on Security and Privacy.
4. Xu, W., Evans, D., & Qi, Y. (2019). Feature squeezing: Detecting adversarial examples in deep neural networks. IEEE Symposium on Security and Privacy.
5. 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.
6. 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.
7. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for automation of software testing // Naukosphere. – 2020. – №. 6. – pp. 152-156.
8. Shterenberg S. I. Methodology for constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology // OPHTHALMIC surgery. – 2022. – No. 4s. – pp. 51-57.

Николаев-Аксенов И.С. ВЕБ-приложение для управления паролями // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 103–108

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ УПРАВЛЕНИЯ ПАРОЛЯМИ

**Николаев-Аксенов И.С.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: 9frischmann@gmail.com*

**Данная работа направлена на создание веб-приложения для управления паролями. В ходе выполнения данной работы был произведен обзор существующих конкурентных решений, выбор инструментов и методов для создания веб-приложения, спроектирована и разработана архитектура, клиентская и серверная часть, модель жизненного цикла и схема базы данных веб-приложения для управления паролями. Результатом работы является разработанное веб-приложения для управления паролями.**

Ключевые слова: Веб-приложение, управление паролями, проектирование приложения, хранение паролей, интернет.

# WEB APPLICATION FOR MANAGING PASSWORDS

**Nikolaev-Aksenov I.S.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: 9frischmann@gmail.com*

**This work is aimed at creating a web application for managing passwords. In the course of this work, a review of existing competitive solutions was made, the choice of tools and methods for creating a web application, the architecture, client and server parts, the life cycle model and the database schema of a web application for password management were designed and developed. The result of the work is the developed web application for password management.**

Keywords: Web application, password management, application design, password storage, interne.

## Введение

В настоящее время появляется все больше сайтов, на которых пользователям необходимо регистрироваться, для предотвращения угрозы взлома учетных записей рекомендуется не повторять пароли при регистрации на разных сайтах, часто обновлять пароли, использовать пароли длиной более 8 символов [1].

Также рекомендуется не использовать пароли, которые легко угадать, по статистике пользователи используют чаще всего следующие пароли в 2023 году [2]: «123456», «123456789», «qwerty», «password», «12345», «qwerty123», «1q2w3e», «12345678», «111111», «1234567890».

В 33% пользователи используют клички своих питомцев, в 22% свое имя, в 15% имя своего партнера и в 14% случаев имя своего ребенка [3]. Чаще всего люди используют пароли размером 8 и 6 символов [2].

Но на практике этими правилами зачастую пренебрегают, так как запомнить множество комбинаций паролей представляется невозможным. Так как сложный для взлома пароль должен иметь как минимум 10 символов, из них как один символ верхнего регистра, цифру и специальный символ [4].

Для решения этой проблемы были созданы менеджеры паролей – это программное обеспечение, которое позволяет хранить пароли в одном месте, для доступа к ним необходимо лишь придумать мастер-пароль.

Программное обеспечение для управления паролями делится на три основных категории:

- установленные на ПК или мобильное устройство – представляют собой программное обеспечение с локальной базой данных, зачастую не имеют выхода в Интернет;
- переносные устройства – это некое устройство, в основном USB-флеш-накопитель, на котором имеется ПО для управления базой данных паролей;
- облачные сервисы – эта категория, в которой база данных паролей находится на внешнем сервере, доступ к ней предоставляется пользователю посредством сети Интернет. Эта категория является наиболее удобной для конечного пользователя, так как не требует дополнительных настроек среды выполнения, а также является более надежной, так как база данных паролей находится не у конечного пользователя, а значит в случае неисправностей у него останется доступ ко всем его паролям.

В рамках данной работы сфокусируемся на создании менеджера паролей последней категории, так как она является наиболее распространенной, это и будет целью работы.

**Обзор существующих конкурентных решений**

Выделим для обзора 7 существующих конкурентных решений:

- KeePassXC – бесплатная программа менеджер паролей с открытым исходном кодом, является ответвлением программы KeePass с добавлением библиотек Qt5 для достижения кроссплатформенности и предания более современного вида. Использует в качестве базы данных зашифрованный файл в расширении kdbx;
- LastPass – условно-бесплатная программа для хранения паролей, разработанная компанией LastPass, пароли хранятся в «облаке» и могут быть синхронизованы между устройствами;
- Bitwarden – менеджер паролей с открытым исходном кодом, использует для сохранения данных облачный сервис, также есть возможность развертывания решения локально;
- 1Password – программа для хранения паролей разработанная AgileBits Inc. Предоставляет возможность хранить различные пароли, данные банковских карт и т.д;

- Kaspersky Password Manager – инструмент управления учетными записями в интернете и приложениях от Лаборатории Касперского. Вся информация хранится в специальной базе данных на компьютере в зашифрованном виде;
- Zoho Vault – веб-приложение для управления паролями с закрытым исходном кодом;
- Dashlane Password Manager – сервис представляющий доступ к своим услугам хранения паролей по подписке.

**Выбор инструментов и методов создания веб-приложения**

Для реализации серверной части веб-приложение выберем строго типизированный объектно-ориентированный язык программирования общего назначения Java, универсальный фреймворк с открытым исходным кодом Spring.

Разрабатывать клиентскую часть будем на языке программирования TypeScript, данный язык расширяет возможности JavaScript и предоставляет возможность явного статического назначения типов, что должно повысить скорость разработки, облегчить читаемость кода, рефакторинг и т.д. Также будем использовать фреймворк Next.js, данный инструмент позволяет разрабатывать приложения на основе React с Server Side Rendering, а также генерировать статические вебсайты.

В качестве базы данных выберем свободную объектно-реляционную систему управления базами данных PostgreSQL.

Для контейнеризации приложения будем использовать Docker. Это программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации.

**Проектирование и разработка веб-приложения**

В качестве архитектуры веб-приложения был выбран паттерн MVC (Model-View-Controller).

В качестве модели жизненного цикла веб-приложения была выбрана каскадная модель. В рамках данной модели процесса разработки программного обеспечения, жизненный цикл выглядит как поток, последовательно проходящий фазы анализа требований, проектирования, реализации, тестирования, интеграции и поддержки. Данная модель является наиболее предпочтительной в виду наличия стабильности требований в течение всего жизненного цикла разработки, определенности и понятности шагов модели и простоты ее применения, этапы работ выполняются в логической последовательности и позволяют планировать сроки завершения всех работ.

В клиентской части веб-приложения реализуем следующие страницы: главная страница, страница регистрации, страница аутентификации, страница профиля пользователя. В качестве примера приведем реализацию страницы профиля пользователя на Рисунке 1.


Рисунок 1 – Демонстрация страницы профиля пользователя

На стороне сервера следует создать конечные точки интерфейса RESTful API. Данные точки должны позволять добавлять, изменять, удалять, обмениваться сущностями. Также нужно предусмотреть точки получения как всех сущностей, так и по идентификационному номеру в базе данных.

В базе данных создадим 9 таблиц: таблица пользователей, таблица сохраненных платежных карт, таблица сохраненных паролей, таблица сохраненных адресов, таблица сохраненных заметок, также создадим 4 вспомогательные таблицы, в которых будет идентификационный номер сущности и список электронных адресов пользователей, которые имеют доступ к этой сущности. Приведем схему базы данных в качестве демонстрации на Рисунке 2.

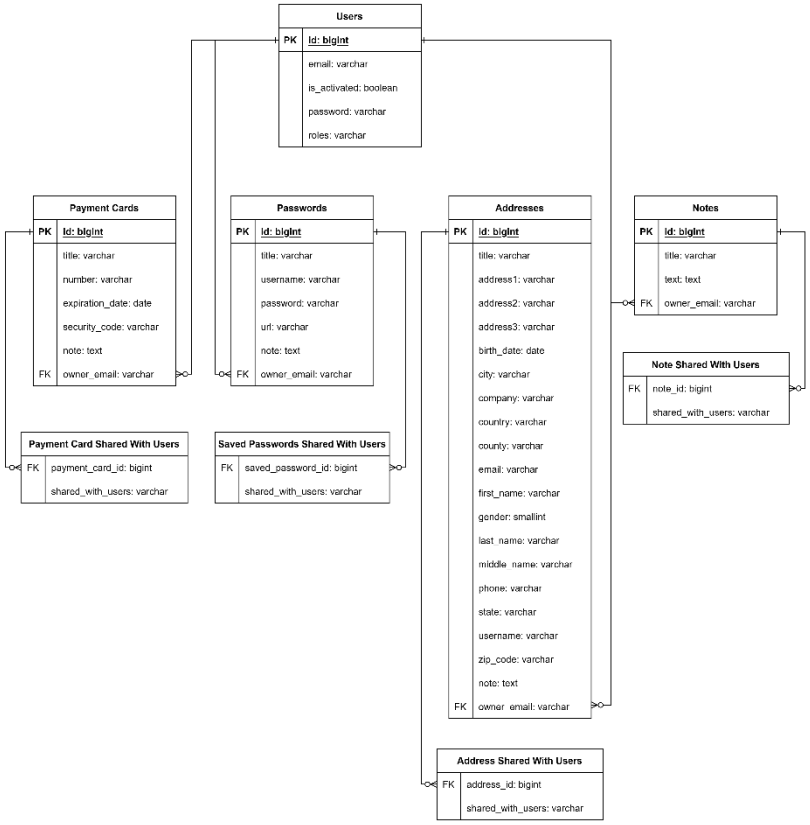



Рисунок 2 – Демонстрация схемы базы данных

**Заключение**

В ходе выполнения данной работы был проведен обзор существующих конкурентных решений, выбор инструментов и методов создания веб-приложения, выполнено проектирование веб-приложения. В результате произведенных действий удалось разработать веб-приложение для управления паролями.

**Список литературы**

1. 7 Bad Password Habits to Break Now : сайт. — URL: https://blog.lastpass.com/2021/01/7-bad-password-habits-to-break-now-2/ (дата обращения: 19.05.2023).
2. Most common passwords: latest 2023 statistics : сайт. — URL: https://cybernews.com/best-password-managers/most-common-passwords/ (дата обращения: 19.05.2023).
3. The United States of P@ssw0rd : сайт. — URL: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf (дата обращения: 19.05.2023).
4. How Safe Is Your Password? : сайт. — URL: https://www.statista.com/chart/26298/time-it-would-take-a-computer-to-crack-a-password/ (дата обращения: 19.05.2023).

**References**

1. 7 Bad Password Habits to Break Now : сайт. — URL: https://blog.lastpass.com/2021/01/7-bad-password-habits-to-break-now-2/ (Accessed on 19.05.2023).
2. Most common passwords: latest 2023 statistics : сайт. — URL: https://cybernews.com/best-password-managers/most-common-passwords/ (Accessed on 19.05.2023).

3. The United States of P@ssw0rd : сайт. — URL: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf (Accessed on 19.05.2023).
4. How Safe Is Your Password? : сайт. — URL: https://www.statista.com/chart/26298/time-it-would-take-a-computer-to-crack-a-password/ (Accessed on 19.05.2023).

Чудинов Е.Д. Методика интеграции несовместимых SDK для обновления ANDROID приложений // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 109–115

Международный журнал информационных технологий и энергоэффективности

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

УДК 004. 4

# МЕТОДИКА ИНТЕГРАЦИИ НЕСОВМЕСТИМЫХ SDK ДЛЯ ОБНОВЛЕНИЯ ANDROID ПРИЛОЖЕНИЙ

**Чудинов Е.Д.**
*ФГБОУ ВО «Челябинский государственный университет», Челябинск, Россия (454001, Челябинская область, город Челябинск, ул. Братьев Кашириных, д.129), e-mail: zotreex@ya.ru*

**В статье рассматривается применение возможностей механизма In-app-update при использовании несовместимых пакетов SDK в рамках магазинов приложений. Представленная реализация использует асинхронный подход к обновлению состояния. Рассмотрено на примерах Google Play SDK и Rustore SDK.**

Ключевые слова: Андроид; обновление в приложении; разработка мобильных приложений; Android-приложение; Rustore SDK

# METHODOLOGY FOR INTEGRATING INCOMPATIBLE SDKS TO UPDATE ANDROID APPS

**Chudinov E.D.**
*Chelyabinsk State University, Chelyabinsk, Russia (454001, Chelyabinsk region, Chelyabinsk, Bratya Kashirin street 129), e-mail: zotreex@ya.ru*

**The article discusses the application of In-app-update mechanism capabilities when using incompatible SDKs within application stores. The presented implementation uses asynchronous state update approach. It is considered on the examples of Google Play SDK and Rustore SDK.**

Keywords: Android; in-app-update; mobile application development; android application, rustore sdk.

Для современных мобильных приложений регулярные обновления стали обязательным условиям для поддержания функциональности и безопасности. Разработчикам необходимо регулярно актуализировать существующий функционал под новые требования операционной системы Android, а также удовлетворять запросу бизнеса на своевременную и оперативную доставку нового функционала пользователю. Здесь возникает проблема, многие пользователи отключают автоматическое обновление приложений и сообщить пользователю о выходе новой версии приложения становится затруднительно.

Для решения этой проблемы, существует механизм in-app-updates, позволяющий разработчикам, реализовать процесс обновления непосредственно из приложения, обеспечивая более плавный и быстрый процесс обновления для пользователей. Это помогает улучшить пользовательский опыт, обеспечить дополнительную безопасность и функциональность приложения.

Такое решение предоставляет каждый магазин приложений (Google Play[1], RuStore, Huawei Appgallery), однако в правила этих магазинов запрещают реализовывать сторонний механизм in-app-updates. Например, в Google play нельзя загрузить приложение с использованием RuStore SDK[2] (часть отвечающая за in-app-updates).

Flavors[3] отлично решают проблему использования разных SDK. На основе этой технологии будет рассмотрена методика интеграции несовместимых SDK In-app-updates и предложена практическая рекомендация для разработчиков по применению этого механизма. При реализации, будет использован подход, отличный от имеющихся примеров в документации, соответствующих SDK.

После разбиения проекта на несколько Flavors [1], проект должен обрести несколько новых sourceDir например:

- app/src/google/kotlin – Для сборки с Google Play SDK
- app/src/rustore/kotlin – для сборки с RuStore SDK
- app/src/main/kotlin – исходный код приложения независимый от внешних SDK

Для package main, необходимо создать интерфейс InAppUpdateManager

```
interface InAppUpdateManager {
    val updateState: MutableStateFlow<InAppUpdateState?>
    fun startUpdateFlow()
    fun updateAppInfo()
}
```

Рисунок 1 – Интерфейс InAppUpdateManager.

Здесь, updateState – Flow[4] с текущем состоянием обновления (Null, Available, Installing, Downloading, Downloaded)

startUpdateFlow() – метод для старта загрузки обновления (например, если пользователь нажмёт соответствующую кнопку)

updateAppInfo() – дополнительный метод, позволяющий принудительно обновить состояние обновления, необходим для реализации swipe-to-refresh механизма.

Здесь стоит обратить внимание, что в интерфейсе применяется ассинхронный подход к обновлению состояния по средствам использования потока данных – Flow[4]. При этом, руководства и Rustore SDK и Google Play SDK предлагает изначально только синхронный подход, основанный на использовании callbaks.

Для того чтобы продолжить релазизацию, необходимо подключить SDK, необхобимо перейти build.gradle(:app) и прописать следующие зависимости:

- rustoreImplementation "ru.rustore.sdk:appupdate:0.1.0"
- googleImplementation 'com.google.android.play:app-update:2.0.1'

Благодаря Flavors, сборщик Gradle автоматически будет подключать нужный SDK в соответствующую сборку. Нам же необходимо объяснить приложению, как работать одновременно с двумя SDK. Для этого был создан универсальный интерфейс, о котором будет знать всё приложение, без привязки на конкретное SDK, фактически, здесь применяется принцип инверсии зависимостей.

В Android разработке, часто применяется библиотека Dagger 2, которая позволяет реализовывать этот принцип относительно просто, помогает в целом хорошо структурировать код и строить чистую архитектуру. Чтобы объяснить библиотеки Dagger о том, что у нас будет несколько реализаций, нам потребуется реализовать сразу два модуля (Рисунок 2), с одинаковыми названиями, но лежащие в разных пакетах приложения (/src/google и /src/rustore).

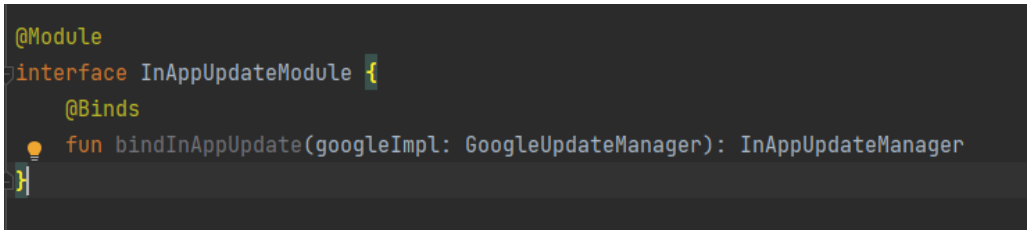



Рисунок 2 – Модуль InAppUpdateModule.

Предварительно, в компонент Dagger`ра, добавлен этот модуль, из-за особенностей реализации, его имя пакета для иморта всегда одино и тот же, для обоих вариаций сборки, а значит не возникнет проблемы, отсутствия этого модуля.

Всё отличие этих двух модулей, будет лишь в методе bindInAppUpdate, в котором параметром передаётся реализация нашего интерфейса. В таком случае, Dagger автоматически построит граф зависимостей для нужной нам сборки, в котором подменит интерфейс InAppUpdateManager на нужную реализацию. Тем самым, реализовав принцип инверсии зависимостей.

Разберём пример реализации GoogleUpdateManager.

Следуюя руководству SDK, необходимо проинциализировать AppUpdateManagerFactory. Создадим класс GoogleUpdateManager и добавим преременную updateManager, которая будет экземпляром AppUpdateManager из Google SDK.

Помимо этого, ещё существует AppUpdateInfo – класс, хранящий информацию о доступности обновлении и прочих вещей для разработчиков. У него есть важная особенность, он используется для старта “Загрузки” передаваясь туда параметром, после чего используемый экземпляр класса перестаёт быть валидным и требудется перезапросить его, используя соответствующий метод из SDK.

```
class GoogleUpdateManager @Inject constructor(
    private val context: Context,
    private val fragmentActivityHolder: FragmentActivityHolder
) : InAppUpdateManager {

    private val updateManager = AppUpdateManagerFactory.create(context)
    private var appUpdateInfo: AppUpdateInfo? = null

    private val listener = InstallStateUpdatedListener { it: InstallState
        handleNewState(it.installStatus(), it)
    }

    private fun getPercentDownloadedText(installState: InstallState?): String {...}

    private fun handleNewState(it: Int, installState: InstallState? = null) {...}

    init {
        updateAppInfo()
    }

    override fun updateAppInfo() {...}

    override val updateState: MutableStateFlow<InAppUpdateState?> =
        MutableStateFlow<InAppUpdateState?>( value: null)

    override fun startUpdateFlow() {...}
}
```

Рисунок 3 – Класс GoogleUpdateManager.

Как было сказано ранее, чтобы наш класс имел смысл, нам необходимо получить от SDK информацию, а именно AppUpdateInfo, для этого в init блок класса, помещается вызов функции updateAppInfo(). Этот метод будет доступен “снаружи” для механизмов принудительного обновления состояния класса.

```
override fun updateAppInfo() {
    updateManager
        .appUpdateInfo
        .addOnSuccessListener { it: AppUpdateInfo!
            appUpdateInfo = it
            if (
                it.updateAvailability() == UpdateAvailability.UPDATE_AVAILABLE ||
                it.updateAvailability() == DEVELOPER_TRIGGERED_UPDATE_IN_PROGRESS
            ) {
                handleNewState(it.installStatus())
            }
        }
}
```

Рисунок 4 – Метод updateAppInfo.

Метод updateAppInfo() – вызывает updateManager, запрашивает информацию appUpdateInfo и синхронным способом, через листенер (он же callback) ожидает результата. Если информация получена успешно, локально сохраняет информацию appUpdateInfo и проверяет два требования:

- Обновление доступно для пользователя
- Обновление уже происходит

Только в этих ситуациях, нам есть необходимость обновить данные во flow, так как иначе null значение, будет расцениваться как отсутствие обновления. Если мы прошли эти проверки, вызываем другой метод – handleNewState, передавая ему информацию о статусе установки (на самом деле, там хранится и информация о доступности обновления)

```
private fun handleNewState(it: Int, installState: InstallState? = null) {
    CoroutineScope(Dispatchers.IO).launch { this: CoroutineScope
        when (it) {
            InstallStatus.DOWNLOADED -> {
                updateAppInfo()
                updateState.emit(InAppUpdateState.Downloaded)
            }
            InstallStatus.DOWNLOADING ->
                if (updateState.value is InAppUpdateState.Downloading)
                    InAppUpdateState.Downloading.percent =
                        getPercentDownloadedText(installState)
                else updateState.emit(
                    InAppUpdateState.Downloading
                )
            InstallStatus.INSTALLING -> updateState.emit(InAppUpdateState.Installing)
            else -> updateState.emit(InAppUpdateState.Available)
        }
    }
}
```

Рисунок 5 – Метод handleNewState.

Данный метод перехватывает возвращаемый SDK Int и проверяет на соответствие определённому состоянию. Его основная задача вызывать updateState.emit передав текущее состояние доступности обновления (здесь уже невозможен вариант отсутствия обновления). В случае, если загрузка уже идёт, перед передачей данных в flow, дополнительно рассчитывается процент из скачанных и общего числа байт.

Остался последний ключевой метод startUpdateFlow() – его задача вызывать интерфейс из SDK для запроса хочет ли пользователь установить, скаченное обновление.

```
override fun startUpdateFlow() {
    appUpdateInfo?.let { it: AppUpdateInfo
        if (it.installStatus() == InstallStatus.DOWNLOADED) {
            updateManager
                .completeUpdate() ^let
        } else {
            fragmentActivityHolder.activity?.let { activity ->
                updateManager.startUpdateFlow(
                    it,
                    activity,
                    AppUpdateOptions.newBuilder(AppUpdateType.FLEXIBLE)
                        .setAllowAssetPackDeletion(true).build()
                ).addOnSuccessListener { resultCode ->
                    if (resultCode == Activity.RESULT_OK) {
                        updateManager.registerListener(listener)
                    } else {
                        updateAppInfo()
                    }
                }

            } ^let

        }
    }
}
```

Рисунок 6 – Метод startUpdateFlow.

Удостоверившись, что метод вызван не ошибочно, вызывается метод completeUpdate из SDK, чтобы произвести обновление приложения уже в системе, так как для этого уже скачена новая версия приложения, а так же пользователь подтвердил установку.

Блок else так же используется, в него мы попадем, если пользователю доступно обновление для скачивания, от него требуется подтверждение, что он хочет произвести загрузку обновления. В листенере, при положительном ответе, будет проинициализирован слушатель, который будет получать информацию о состоянии загрузки. Если пользователь откажет, то нам необходимо перезапросить информацию об обновлении вновь, т.к исчерпаем лимит на использование данных в updateAppInfo.

Для Rustore SDK[2] реализация будет аналогичная. Изменятся только импорты в классе, т.к отечественная реализация полностью совпадает с вариантом от Google.

Рассмотренные в статье реализации механизма InAppUpdates необходимо применять при разработке современных мобильных приложений. Разработанная методика предоставляет

последовательность действий для использования InAppUpdates в ситуациях с применением несовместимых SDK. Предоставленная реализация механизма значительно упрощает применение и поддержку работы InAppUpdate в приложении, публикуемым в несколько магазинов приложений. Подключение подобных SDK в проект может проходить затруднительно, но для этого есть все инструменты и подробная инструкция из этой статьи. Данная технология позволяет решать достаточно много задач, обеспечивая более плавный и быстрый процесс обновления для пользователей.

**Список литературы**

1. Google documentation In-app updates. URL: https://developer.android.com/guide/playcore/in-app-updates (дата обращения 03.05.2023).
2. RuStore Документация разработчика URL: https://help.rustore.ru/rustore/for_developers/developer-documentation (дата обращения 03.05.2023).
3. Advanced Android Flavors Part 2 — Enter Flavor Dimensions. URL: https://proandroiddev.com/advanced-android-flavors-part-2-enter-flavor-dimensions-4ad7f486f6 (дата обращения 03.05.2023).
4. Документация Kotlin. URL: https://kotlinlang.org/docs/flow.html (дата обращения 03.05.2023).

**References**

1. Google documentation In-app updates. URL: https://developer.android.com/guide/playcore/in-app-updates (Accessed on 03.05.2023).
2. RuStore Документация разработчика URL: https://help.rustore.ru/rustore/for_developers/developer-documentation (Accessed on 03.05.2023).).
3. Advanced Android Flavors Part 2 — Enter Flavor Dimensions. URL: https://proandroiddev.com/advanced-android-flavors-part-2-enter-flavor-dimensions-4ad7f486f6 ((Accessed on 03.05.2023).
4. Documentation Kotlin. URL: https://kotlinlang.org/docs/flow.html (Accessed on 03.05.2023).

Беляева К.В. Различные методы оптимизации скорости загрузки сайта и их влияние на опыт пользователя // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2. с. 116–119

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# РАЗЛИЧНЫЕ МЕТОДЫ ОПТИМИЗАЦИИ СКОРОСТИ ЗАГРУЗКИ САЙТА И ИХ ВЛИЯНИЕ НА ОПЫТ ПОЛЬЗОВАТЕЛЯ

**Беляева К.В.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: kaleriaa@bk.ru*

**Статья посвящена описанию способов оптимизации скорости загрузки сайтов. Существует несколько методов оптимизации скорости загрузки сайта, которые можно использовать для улучшения опыта пользователя, снижения отказов и увеличения конверсии, некоторые из которых нашли отражение в данной статье.**

Ключевые слова: Скорость загрузки сайтов, веб-разработка, seo-оптимизация, методы оптимизации, пользовательский опыт.

# DIFFERENT METHODS FOR OPTIMIZING SITE LOADING SPEED AND THEIR IMPACT ON USER EXPERIENCE

**Belyaeva K.V.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: kaleriaa@bk.ru*

**The article is devoted to the description of the high speed of loading sites. There are several site discovery rate detection methods that can be used to explore user experience, graceful bounces, and increased conversions, some of the reflections found in this article.**

Keywords: Site loading speed, web development, seo-optimization, optimization methods, user experience.

В современном мире достаточно трудно представить жизнь без использования интернета, который является огромным источником информации, развлечений и возможностей для коммуникации. А точнее речь пойдет об использовании его веб составляющей, то есть система сайтов и приложений, которые позволяют пользователям получить доступ к информации, продуктам и услугам через браузер. Для создания и поддержки веб-сайтов и приложений используется специальная область знаний – веб-разработка.

Скорость загрузки сайтов имеет огромное значение как на пользователей, так и на владельцев сайта, чей бизнес может зависеть от онлайн присутствия и удобства использования его веб-ресурсов. Каждый пользователь хоть раз сталкивался с проблемой долгой загрузки

контентной части сайта – это вызывает по меньшей части неудовлетворенность, по большей части – негативное отношение к бренду и нежелание возвращаться. Конечно, это может привести к снижению продаж и конверсии. По данным исследования Google, агрегированные анонимные данные Google Analytics из выборки мобильных веб-сайтов, которые согласились делиться эталонными данными n = 3,7 тыс., 53% пользователей покинут страницу, если страница загружается больше 3 секунд [1].

Оптимизация скорости загрузки сайта позволяет снизить bounce rate (количество пользователей, которые покидают сайт после просмотра только одной страницы), увеличить retention rate (количество пользователей, которые остаются на сайте или возвращаются на него). Кроме того, Google и другие поисковые системы используют скорость загрузки сайта в качестве фактора ранжирования, то есть чем быстрее сайт загружается, тем больше шансов, что он будет выведен ближе к верху поисковой выдачи.

Для начала определим, что быстро загружающийся сайт – сайт, контент и все элементы которого полностью загружены, интерактивны и отображаются на экране пользователя за максимально короткое время. Она может зависеть от различных факторов, таких как размеры файлов, скорость ответа сервера, количество запросов и т.д. Так, для решения данной проблемы используют различные методы оптимизации, описанные далее.

Кэширование. Кеширование позволяет делать копию веб-страницы (HTML, CSS, JS), храня результат в браузере пользователя и предотвращая загрузку одного и того же контента при каждом посещении страницы. Во-первых, это позволяет сохранять информацию о странице без повторной загрузки, сокращая время. Во-вторых, использование кеша позволяет уменьшить нагрузку на сервер, что может быть особенно полезно в случае большого количества пользователей. Также это может снизить затраты на трафик, поскольку количество передаваемых данных будет меньше.

Уменьшение размера изображений: использование изображений высокого качества может замедлить загрузку страницы. Однако, в случае с маркетплейсами, где фотографии товаров – важная составляющая, стоит обратить внимание на оптимизацию изображений. Можно использовать инструменты оптимизации изображений, такие как TinyPNG или Kraken.io, чтобы уменьшить размер файла, не теряя изначальное качество. Таким образом, пользователь может наслаждаться быстро загружающейся страницей с изображениями высокого разрешения.

Использование Content Delivery Network (CDN). CDN – это сеть распределения контента, обеспечивающая доставку статических и динамических ресурсов (например, изображения, видео, HTML-файлы) пользователям со скоростью и эффективностью, недостижимой для обычных серверов. CDN работает путем размещения кэшей контента на серверах в различных географических точках и автоматической маршрутизации запросов от пользователя к серверу, находящемуся ближе всего к пользователю [3]. Это значительно ускоряет загрузку контента и повышает производительность веб-сайтов.

Оптимизация CSS и JavaScript файлов: объединение и минификация CSS и JavaScript файлов может уменьшить размер файлов и ускорить загрузку страниц.

Оптимизация CSS файлов может быть достигнута:

- Удаление ненужных стилей и комментариев;
- Сокращение синтаксиса цветов и использование аббревиатур свойств;

- Объединение в один файл.

Оптимизация JS файлов:

- Удаление неиспользуемых переменных и комментариев;
- Использование модулей;
- Использование скриптов с defer/ async.

Однако, данные действия выполняют сборщики приложений (например, Webpack или ESBuild) автоматически в рамках процесса сборки проекта. Эти инструменты позволяют не только оптимизировать CSS и JavaScript файлы (tree shaking/ minify), но и проводить множество других полезных операций для оптимизации проекта: работу с изображениями, import/ export, babel и многое другое.

Оптимизация скорости загрузки сайта является важным фактором для успеха онлайн бизнеса. Быстрая загрузка страниц привлекает пользователей, что может увеличить количество сделок и прибыль владельцев сайтов. В результате, оптимизация скорости загрузки сайта может иметь значительное влияние не только на опыт пользователя, но и на SEO-метрики сайта. Чтобы достичь быстрой загрузки сайта, можно провести оптимизацию кода, минимизировать размер файлов, использовать сжатие данных, а также оптимизировать изображения и другие ресурсы. Для этих целей могут использоваться различные инструменты и технологии, включая сборщики проектов.

Таким образом, все данные методы помогают ускорить загрузку сайта и улучшить его общую производительность. Скорость загрузки сайта становится ключевым фактором для повышения конверсии клиентов и улучшения общего опыта взаимодействия пользователей с сайтом.

**Список литературы**

1. How to make every mobile moment a brand-builder // Think with Google URL: https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/consumer-mobile-brand-content-interaction/ (дата обращения: 21.05.2023).
2. Оптимизация скорости загрузки сайта, или почему не стоит гнаться за цифрами // VC.RU URL: https://vc.ru/seo/165551-optimizaciya-skorosti-zagruzki-sayta-ili-pochemu-ne-stoit-gnatsya-za-ciframi (дата обращения: 21.05.2023).
3. Что такое CDN и как это работает? // Habr URL: https://habr.com/ru/companies/selectel/articles/463915/ (дата обращения: 21.05.2023).
4. Скрипты: async, defer // Современный учебник JavaScript URL: https://learn.javascript.ru/script-async-defer (дата обращения: 21.05.2023).
5. Уменьшение размеров бандлов с помощью Webpack Analyzer и React Lazy/Suspense // Habr URL: https://habr.com/ru/companies/ruvds/articles/468225/ (дата обращения: 21.05.2023).

**References**

1. How to make every mobile moment a brand-builder // Think with Google URL: https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/consumer-mobile-brand-content-interaction/ (accessed on: 21.05.2023).

2. Optimization of site loading speed, or why you should not chase numbers // VC.RU URL: https://vc.ru/seo/165551-optimizaciya-skorosti-zagruzki-sayta-ili-pochemu-ne-stoit-gnatsya-za-ciframi (accessed on: 21.05.2023).
3. What is a CDN and how does it work? Habr URL: https://habr.com/ru/companies/selectel/articles/463915/ (accessed on: 21.05.2023).
4. Scripts: async, defer // Modern JavaScript textbook URL: https://learn.javascript.ru/script-async-defer (accessed: 21.05.2023).
5. Reducing bundle sizes using Webpack Analyzer and React Lazy/Suspense // Habr URL: https://habr.com/ru/companies/ruvds/articles/468225/ (accessed: 21.05.2023).

Аникин Д.А. Анализ методов авторизации и аутентификации REST API // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 120–124

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.422

# АНАЛИЗ МЕТОДОВ АВТОРИЗАЦИИ И АУТЕНТИФИКАЦИИ REST API

**Аникин Д.А.**
*ФГБУО ВО «МИРЭА - Российский технологический университет», Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: danil-anikin-98@mail.ru*

**Настоящая статья посвящена рассмотрению и анализу различных методов аутентификации и авторизации, которые могут быть использованы при проектировании приложения, основанного на REST API. Современные информационные системы в большинстве случаев основаны на технологии обработки пользовательских запросов, для реализации контроля доступа используются различные технологии. В результате их анализа была дана подробная характеристика каждой из них, выявлены сильные и слабые стороны и выработаны рекомендации по выбору технологии.**

Ключевые слова: Информационные технологии, REST API, программирование, авторизация, аутентификация.
.

# ANALYSIS OF REST API AUTHORIZATION AND AUTHENTICATION METHODS REST API

**Anikin D.A.**
*MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: danil-anikin-98@mail.ru*

**This article is devoted to the consideration and comparative analysis of various authentication and authorization methods that can be used when designing an application based on the REST API. Modern information systems in the vast majority of cases are based on the technology of processing user requests, various technologies are used to implement access control. Because of their analysis, a detailed description of each of them was given, strengths and weaknesses were identified and recommendations on the choice of technology were developed.**

Keywords: Information technology, REST API, programming, authorization, authentication.

По мере развития информационных технологий приложения, разрабатываемые программистами, стремительно усложнялись. К новым более совершенным системам не были применимы те же подходы, методики разработки и организации кода, которые были актуальны ранее. Для решения приходящих проблем были разработаны различные решения.

В ходе разработки приложений, к которым должны были иметь доступ множество пользователей, возникли следующие проблемы [1]:

- Необходимость разделения клиентской и серверной частей приложения, так как серверу приходится обрабатывать запросы не только одного пользователя на локальной машине.

- Необходимость добиться кроссплатформенного доступа к сервису, чтобы пользователи не зависели от операционной системы, установленной на их клиентской машине.
- Необходимость создания универсального стиля взаимодействия веб-приложений, использующих общепризнанные сетевые протоколы. Обращение к сервисам не должно было зависеть от языка программирования и средства реализации серверной части приложения.
- Необходимость добиться более простой масштабируемости для всё более разрастающихся и развивающихся систем.

С целью решения вышеперечисленных проблем была разработана технология REST API. Representational State Transfer (REST) Application Programming Interface (API) – это не единственный строго определённый протокол взаимодействия компонентов программы, это архитектурный стиль разработки. Он описывает процесс проектирования интерфейса разработчиком для взаимодействия своего приложения со внешними элементами. Принципы и ограничения данного архитектурного стиля были определены Роем Филдингом в 2000 году, он является одним из создателей протокола HTTP, если интерфейс полностью соответствует принципам, то он называется RESTful [2].

Принцип работы REST API заключается в следующем: клиент отправляет запрос на сервер, сервер обрабатывает клиентский запрос, сохраняет логи обработки, подготавливает ответ и возвращает его клиенту. Однако далеко не все клиенты должны иметь доступ ко всем методам, предоставляемым сервером, так как в таком случае создается угроза безопасности и защиты данных, объектов или материалов, которые предоставляет API. Для решения этой проблемы была разработана концепция авторизации.

Авторизация – это предоставление конкретному лицу или группе лиц прав на выполнение определённых действий, а также процесс проверки, подтверждения данных прав при попытке выполнения этих действий, зачастую этот процесс подразумевает проверку подлинности логина и пароля пользователя или токена доступа [3].

Помимо авторизации, процесс обеспечения защиты подразумевает идентификацию и авторизацию пользователей. Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе. Аутентификация — процедура проверки подлинности.

Недостаточно точно организованный процесс разделения доступа к API может привести к таким последствиям, как: неограниченное количество запросов пользователей к определённым методам, что приведет к замедлению их обработки на серверной части приложения, отсутствие связки конкретного пользователя с историей его запросов, защита целостности данных информационной системы от злоумышленников, невозможность отследить, какие точки доступа используются чаще всего без использования сторонних средств [4].

Проведём анализ наиболее популярных методов авторизации REST API.

Basic Authentication: является одним из самых простых методов аутентификации, который применяется в веб-приложениях. В его основе лежит процесс передачи логина и пароля, для которых используется закодированное значение в заголовке запроса, обычно кодирование производится с помощью алгоритма Base64. При получении запроса сервером производится дешифровка сообщения и проверка заголовка, который содержит логин и

пароль, в зависимости от результата проверки будет принято решение принять или отклонить запрос [5].

Token-based Authentification (Аутентификация на основе токенов) основана на том, что токен используется для авторизации пользователя. Токеном является специальный код, который генерируется для каждого отдельного пользователя и который предоставляет различные уровни доступа. Этот токен может содержать как и информацию о пользователе, так и любые другие сведения, важные для приложения [6].

OAUTH 2.0: позволяет пользователям предоставлять доступ к своим данным другим приложениям без необходимости предоставления собственных данных для входа. В основе своей он имеет отдельный сервер аутентификации для связи с сервером API. Ключевой чертой, по которой можно выявить использование данного метода – наличие возможности авторизации с помощью учётной записи сторонних сервисов.

Данный протокол работает по следующему принципу: пользовательское приложение отправляет ключ приложения и секретные данные на страницу входа в систему на сервере аутентификации, при успешном прохождении сервер аутентификации присваивает и возвращает пользователю токен для доступа к основному сервису. Запрос с полученным токеном перенаправляется на сервер с необходимыми ресурсами. Токен доступа добавляется в заголовок в качестве параметра Bearer, сам сервер проверяет токен доступа и принимает решение об обработке запроса [7]. Диаграмма последовательности для работы протокола OAuth 2.0 представлена на Рисунке 1.

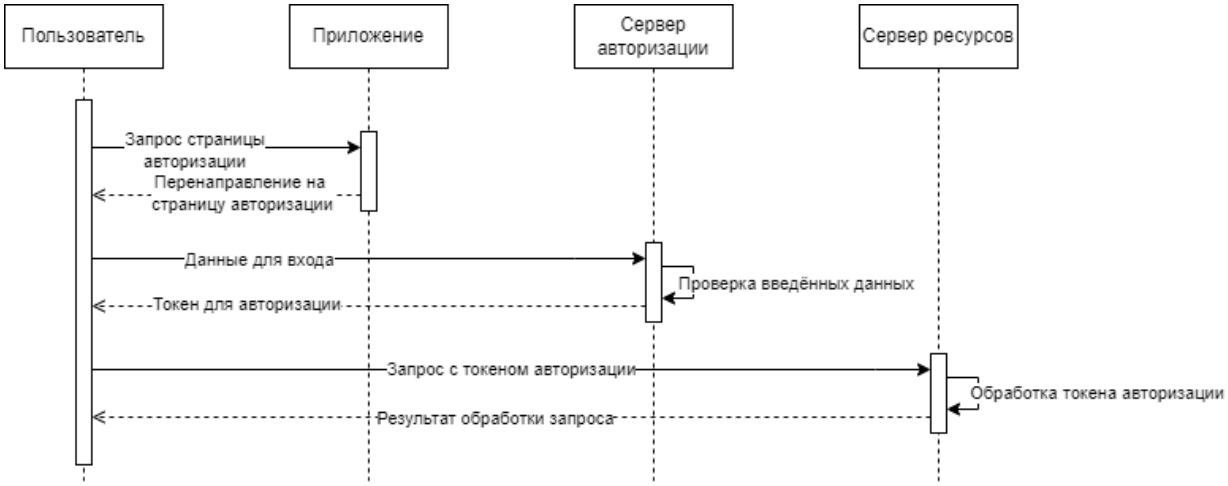



Рисунок 1 – Диаграмма последовательности авторизации OAuth 2.0

Bearer token (Токен-маркер): представляет собой маркер доступа, который используется для аутентификации, хранится он, в свою очередь, на стороне клиента и передаётся в качестве одного из параметров заголовка запроса.

API KEY: заключается в передачи ключевой пары, обычно состоящей из секретного и открытого ключа. Открытый ключ входит в состав запроса, закрытый же используется только при обмене данными между серверами [8].

AWS Signature: метод аутентификации, который используется для обеспечения безопасности доступа к API Amazon Web Services. Signature HMAC-SHA1 или Signature Version 4 — это две версии, которые используются при аутентификации AWS. Первая версия (HMAC-SHA1) используется для старых версий API Amazon [9]. Вторая версия (Version 4) для

более новых версий API. AWS Signature основывается на передаче ключевой пары, которая используется для создания контрольной суммы, обеспечивающей авторизацию пользователя.

Исходя из проведённого анализа, можно определить, что выбор метода аутентификации API зависит от планируемого использования и выдвинутых требований приложения, описанных в техническом задании. Рекомендуется выбрать метод, который наиболее точно отвечает на потребности в безопасности и простоте доступа к сервису.

Таким образом, обеспечение авторизации и аутентификации REST API является крайне важным этапом, позволяющим обеспечить безопасность передаваемых данных, а также управлять доступом к ресурсам и методам серверной части приложения. Были рассмотрены такие методы авторизации, как: Basic Authentication, Token-based Authentification, OAUTH 2.0, JSON Web Tokens, Bearer token, API KEY, AWS Signature, была дана развёрнутая характеристика каждого из них и были рассмотрены основные принципы работы. Из проведённого анализа было установлено, что выбор метода авторизации целиком и полностью основывается на том, какие требования были выдвинуты к разрабатываемому приложению по части безопасности и контроля уровней доступа, нет какого-то одного ультимативного выбора для всех ситуаций, существуют различные технологии, которые применимы в различных ситуациях.

**Список литературы**

1. Brenda, Jin Designing Web APIs / Jin Brenda, Sahni,&,Amir Saurabh. — First edition. — Sebastopol : O’Reilly Media, 2018. — 232 с. — Текст : непосредственный.
2. Mark, Masse REST API Design Rulebook / Masse Mark. — First edition. — Sebastopol : O’Reilly Media, 2012. — 93 с. — Текст : непосредственный.
3. Neil, Madden API Security in Action / Madden Neil. — First edition. — : y Manning Publications Co, 2020. — 43 с. — Текст : непосредственный.
4. Andrew, Hoffman Web Application Security / Hoffman Andrew. — First edition. — : O'Reilly Media, 2020. — 331 с. — Текст : непосредственный.
5. HTTP authentification. — Текст : электронный // mdn web docs : [сайт]. — URL: https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication (дата обращения: 12.05.2023).
6. Token-based Authentication. — Текст : электронный // jetbrains : [сайт]. — URL: https://www.jetbrains.com/help/youtrack/server/2fa-with-token.html (дата обращения: 12.05.2023).
7. OAuth 2.0. — Текст : электронный // oauth : [сайт]. — URL: https://oauth.net/2/ (дата обращения: 12.05.2023).
8. OAuth 2.0. — Текст : электронный // OpenAPI guide : [сайт]. — URL: https://swagger.io/docs/specification/about/ (дата обращения: 12.05.2023).
9. Signing AWS API requests. — Текст : электронный // aws : [сайт]. — URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-signing.html (дата обращения: 12.05.2023).

**References**

1. Brenda, Jin Designing Web APIs / Jin Brenda, Sahni,&,Amir Saurabh. — First edition. — Sebastopol : O'Reilly Media, 2018. — p. 232 — Text: immediate.
2. Mark, Masse REST API Design Rulebook / Masse Mark. — First edition. — Sebastopol : O'Reilly Media, 2012. — p. 93 — Text: immediate.
3. Neil, Madden API Security in Action / Madden Neil. — First edition. — y Manning Publications Co, 2020. — p. 43 — Text: immediate.
4. Andrew, Hoffman Web Application Security / Hoffman Andrew. — First edition. — O'Reilly Media, 2020. — p. 331 — Text: immediate.
5. HTTP authentification. — Text: electronic // mdn web docs: [site]. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication (accessed: 12.05.2023).
6. Token-based Authentication. — Text: electronic // jetbrains: [site]. Available at: https://www.jetbrains.com/help/youtrack/server/2fa-with-token.html (accessed: 12.05.2023).
7. OAuth 2.0. — Text: electronic // oauth: [site]. Available at: https://oauth.net/2/ (accessed: 12.05.2023).
8. OAuth 2.0. — Text: electronic // OpenAPI guide: [site]. Available at: https://swagger.io/docs/specification/about/ (accessed: 12.05.2023).
10. Signing AWS API requests. — Текст : электронный // aws : [сайт]. — URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-signing.html (дата обращения: 12.05.2023).

Уманский Д.М. Умный дом: архитектура, технологии и системы // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2. с. 125–134

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# УМНЫЙ ДОМ: АРХИТЕКТУРА, ТЕХНОЛОГИИ И СИСТЕМЫ

**Уманский Д.М.**
*ФГАОУ ВО «Национальный исследовательский университет "Московский институт электронной техники», Москва, Россия (124498, город Москва, город Зеленоград, пл. Шокина, д. 1), e-mail: umanskiy.dan@gmail.com*

**Система "умный дом" является ключевым элементом умного потребления сети. Это интерактивное взаимодействие между энергосистемой и пользователями в режиме реального времени, которое расширяет возможности комплексного обслуживания энергосистемы, а также обеспечивает интеллектуальное и интерактивное использование электроэнергии, дополнительно улучшает режим работы энергосистемы и схемы использования пользователями для повышения энергоэффективности конечных пользователей. Умный дом — это платформа для жилых помещений, которая использует IoT, компьютерные технологии, технологии управления, технологии отображения изображений и коммуникационные технологии для подключения различных объектов через сеть для удовлетворения требований автоматизации всей системы и обеспечения более удобного контроля и управления. В этой статье анализируются характеристики умного дома, приводится состав умного дома и применение ключевого оборудования; а также ключевые технологии умного дома, чтобы проиллюстрировать дизайн системы электроснабжения умного дома и связанных с ней коммуникационных систем.**

Ключевые слова: Умный дом, система контроля потребления электроэнергии, автоматизация, умные розетки, интрасеть.

# SMART HOME: ARCHITECTURE, TECHNOLOGIES AND SYSTEMS

**Umansky D.M.**
*National Research University "Moscow Institute of Electronic Technology", Moscow, Russia (124498, Moscow, Zelenograd, Shokina sq., 1), e-mail: umanskiy.dan@gmail.com*

**The smart home system is a key element of smart network consumption. This is an interactive interaction between the power system and users in real time, which expands the possibilities of comprehensive maintenance of the power system, as well as provides intelligent and interactive use of electricity, further improves the operation mode of the power system and user usage patterns to improve the energy efficiency of end users. A smart home is a residential platform that uses IoT, computer technology, control technology, image display technology and communication technology to connect various objects through a network to meet the automation requirements of the entire system and provide more convenient control and management. This article analyzes the characteristics of a smart home, provides the composition of a smart home and the use of key equipment; as well as key smart home technologies to illustrate the design of the smart home power supply system and related communication systems.**

Keywords: Smart home, power consumption monitoring system, automation, smart sockets, intranet.

Умный Дом является органичным сочетанием различных подсистем, относящихся к домашней жизни через передовые технологии, такие как волоконно-оптический кабель дома [1]. Он способен и делить ресурсы, и общаться внутри дома, и может обмениваться

информацией с внешней сетью вашего дома через умный порт. Его главной задачей является предоставить эффективную, комфортную, безопасную, удобную и благоприятную для окружающей среды среду обитания, объединяющую систему, сервис и управление.

Умный дом — это использование компьютерных технологий, технологий управления, технологий отображения изображений и коммуникационных технологий, которые будут соединены через сеть различных объектов вместе для удовлетворения требований автоматизации всей системы, чтобы обеспечить более удобный контроль и управление [2]. Традиционное осуществление работы умного дома, как правило, заключается в управлении компонентами здания и обеспечивает связь между ними с помощью проводных линий, трудно избавиться от ограничений, связанных с различными кабелями, стоимость установки высока, а масштабируемость системы также оставляет желать лучшего. Система умный дом, основанная на технологии беспроводной сенсорной сети, позволяет не только избавиться от оков проводов, снизить стоимость установки, но и значительно повысить масштабируемость системы.

Далее следуют основные функции умного дома [1]:

1. умный дом может осуществлять взаимодействие между пользователем и электросетевым предприятием, получать информацию о потреблении электроэнергии и цене на электроэнергию, устанавливать план потребления электроэнергии и так далее, направлять научное и рациональное использование электроэнергии и «навязывать» семье стремление к энергосбережению и защите окружающей среды;
2. умный дом может повысить комфорт, безопасность, удобство и интерактивность домашней жизни, а также оптимизировать стиль жизни людей;
3. умный дом может поддерживать удаленную оплату;
4. умный дом может контролировать и взаимодействовать с домом через стационарный телефон, мобильный телефон и удаленную сеть, обнаруживать ненормальные и своевременные обработки;
5. умный дом реализует считывание показаний счетчика в режиме реального времени и службу безопасности счетчика воды, счетчика электроэнергии и газового счетчика, которые обеспечивают гораздо более удобные условия для высококачественного обслуживания;

Через создание внутренней сети связи в семье, мы реализуем систему кондиционирования воздуха и управление другими умными приборами сети через подключение к силовой волоконно-оптической сети. Через интеллектуальные интерактивные терминалы, умные розетки, умные приборы и т.д. мы достигаем того, что бытовые приборы автоматически собирают информацию об электричестве, анализируют ее, управляют ею; а бытовая техника обеспечивает экономичную эксплуатацию и контроль энергопотребления [3, 4]. С помощью стационарного телефона, сотового телефона, интернета и других средств система может дистанционно управлять домом и другими услугами. С помощью интерактивного терминала управления системой мы также можем обнаружить утечки дыма, газа, обеспечить защиту от краж, экстренную помощь и другие функций домашней безопасности, а также осуществляем автоматический сбор и управление информацией о счетчиках воды, газовых счетчиках и сотовой сети центра поддержки и управления имуществом, а также осуществляем авторизованную одностороннюю передачу информации о безопасности дома и другие услуги. На Рисунке 1 показана структура умного дома.

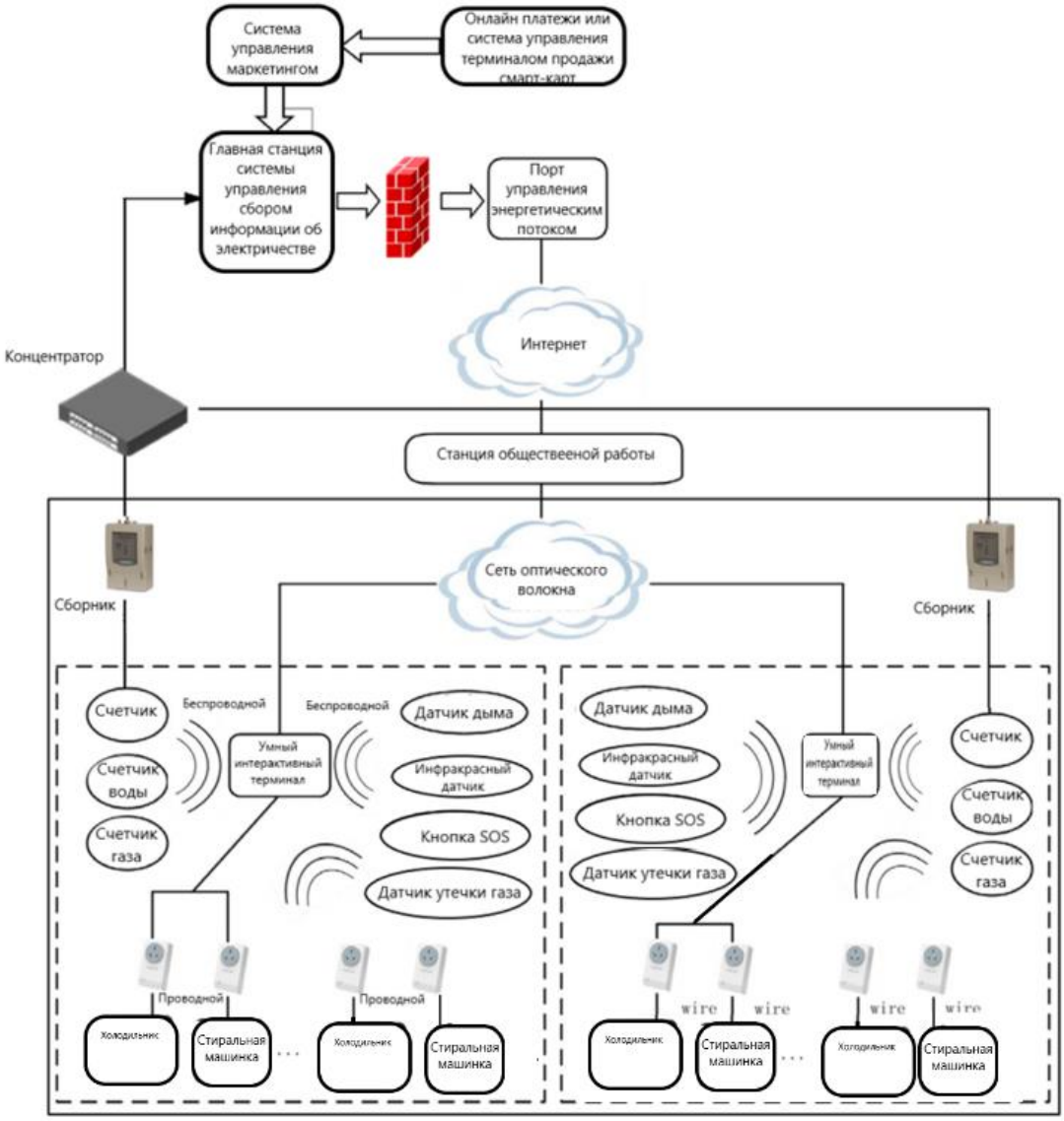



Рисунок 1 – Архитектура умного дома

Услуга интерактивного сайта позволяет настроить формат получаемой информации об электричестве дома, дистанционном управлении оборудованием, оплате, газете, руководстве по обслуживанию и других интерактивных функциях обслуживания.

Умный дом, как система по автоматическому управлению домашним хозяйством, имеет несколько технологий для:

- эффективного управления электроснабжением;
- умного оказания коммунальных услуг.

Система электроснабжения "умный дом" является вспомогательной платформой для мониторинга, анализа и контроля потребления электроэнергии бытовыми пользователями, а также важным способом реализации упорядоченного управления электроэнергией и интеллектуального обслуживания энергоэффективности [9]. На Рисунке 2 показана структура системы энергоснабжения умного дома.

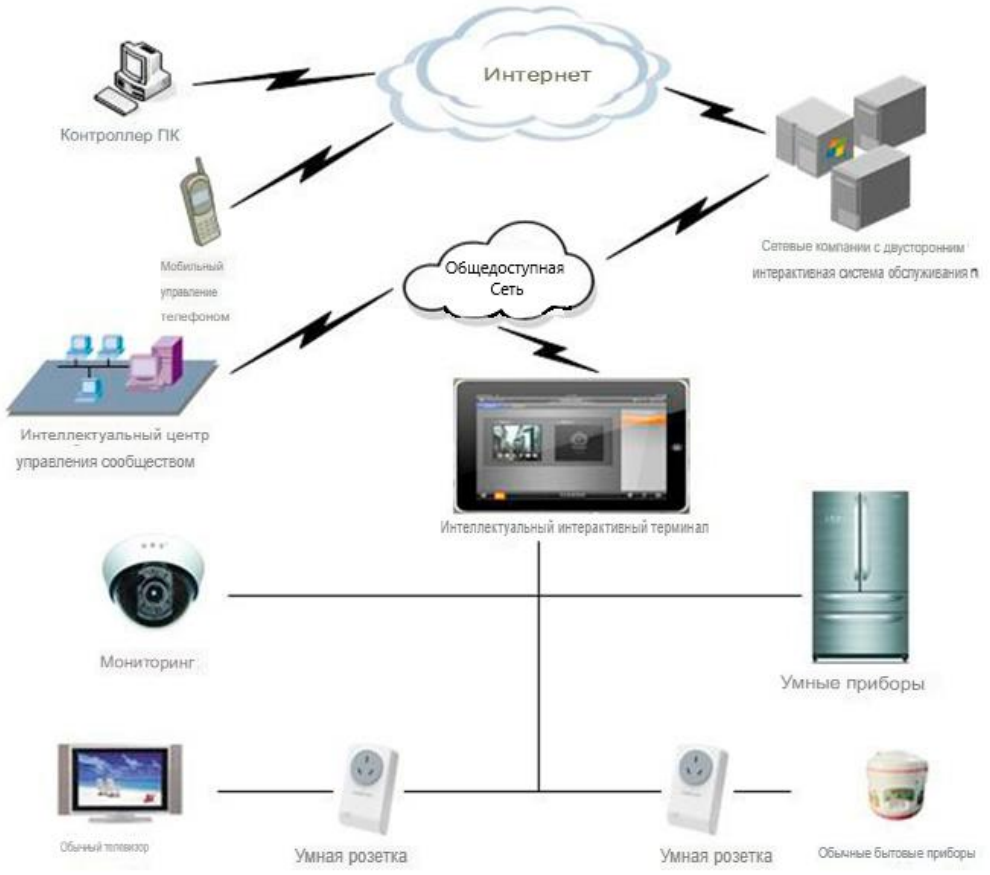



Рисунок 2 – Структура системы энергоснабжения умного дома

Система энергоснабжения умного дома главным образом состоит из базовой станции, канала связи, домашнего интерактивного терминала управления системой и умного электрического устройства из 4 частей:

1. главная система состоит их сервера базы данных, сервера приложений, интерфейсной машины, роутера, оборудования безопасности и так далее;
2. канал связи делится на сеть междугородней связи и локальную, удаленная связь, использующая сети связи общего пользования, локальная сеть связи подбирается из волоконно-оптического композитного кабеля, широкополосной связи по линии электропередачи, беспроводной связи;
3. домашний интерактивный терминал управления системой является ядром системы умный дом, является главной станцией и контактным центром пользователя, а также центром управления электрооборудованием;
4. интеллектуальное электрооборудование включает в себя умные приборы, средства безопасности и так далее. В настоящее время, из-за отсутствия популярности умных приборов, умные розетки могут использоваться для управления бытовой техникой или для сбора информации о бытовой техники, чтобы удовлетворить потребности в управлении неумными приборами и сборе электрической информации.

Ключевым оборудованием Умного Дома являются:

1. Мастер система. Основная система включает в себя серверы, сети связи, рабочие станции и внутреннюю взаимосвязь с 4 частями маркетинговой системы. И маркетинговые

приложения, услуги интерактивных сайтов и другие приложения для подключения в основном через сервер интерфейса, оборудование безопасности и другое оборудование для завершения.

2. Семейный интерактивный терминал управления системой. Домашний интерактивный терминал управления системой устанавливается в положении, удобном для работы пользователей и для установления связи и взаимодействия с умной розеткой, устройством "умный дом" и устройством домашней безопасности.

Существует 3 основных умных электрических устройств:

1. умная розетка, которая устанавливается между электрической розеткой и обычными бытовыми приборами и устанавливает связь с домашним интеллектуальным интерактивным терминалом.

2. умные приборы, что включает в себя интеллектуальные кондиционеры, умные телевизоры, умные холодильники, умные стиральные машины, умные пылесосы, умные рисоварки с двусторонними интерактивными функциями.

3. устройства домашней безопасности, такие как датчики дыма, инфракрасные датчиков, аварийные кнопки, датчики утечки газа, камер и другого оборудования.

Умная розетка может собирать точные и чувствительные данные о нагрузке потребления электроэнергии в режиме реального времени, выбирать наиболее подходящий режим связи в соответствии с реальной ситуацией [10], а основными функциями являются: отображение измерений, управление включением-выключением и прозрачная передача команд управления бытовой техникой.

Модель неумной бытовой техники, подключенные с через умную розетку выполняет следующие функции:

- собирает данные о значениях напряжения, тока, мощности и коэффициента мощности бытовой техники в режиме реального времени и сохраняет его, а также загружает необходимые данные;
- интеллектуальная розетка регулирует мощность на приборе, для достижения энергосбережения;
- умной розеткой можно управлять с помощью интерактивного терминала управления системой, узла сбора данных, сетевого клиента, мобильного телефона и других носителей, а затем с помощью умной розетки управляется выключение бытового прибора.

Модель умной бытовой техники поставляется с модулем беспроводной связи ближнего действия и умной розеткой (с использованием соответствующего модуля беспроводной связи), используемой в сочетании с реализацией следующих функций:

- собирает значение напряжения, тока, мощности и коэффициента мощности бытовой техники в режиме реального времени и сохраняет его, а также загружает необходимые данные;
- интеллектуальная розетка регулирует мощность на приборе, для достижения энергосбережения;
- команды управления, инициируемые интеллектуальным интерактивным терминалом, прозрачно передаются на бытовую технику через беспроводной модуль умной розетки и используются для запуска, настройки и управления бытовой техникой.

- умной розеткой можно управлять с помощью интерактивного терминала управления системой, узла сбора данных, сетевого клиента, мобильного телефона и других носителей, а затем с помощью умной розетки можно управлять выключением бытового прибора.
- режим интегрированного сетевого устройства

Все функции умной розетки полностью интегрированы в умные приборы, чтобы обеспечить прямое управление терминальными умными приборами. Конкретные функции заключаются в том, что они могут не только собирать значения в реальном времени, такие как напряжение, ток и мощность бытовой техники, но также включать и выключать бытовую технику, а также запускать, настраивать и управлять бытовой техникой для выполнения всех функций неумных приборов и сетевых устройств и достижения максимальной интеллектуальности.

Приборы, безопасные для сети (GFA) в основном используют встроенную технологию для автоматического отключения электрической сети от энергосистемы, когда частотный сигнал энергосистемы обнаруживается ниже заданного порога, отслеживая переменное напряжение или частотный сигнал сети в режиме реального времени. Когда многие GFA выполняют эту функцию, это помогает защитить сетку и предотвратить колебания сетки.

GFA эквивалентен небольшой электронной платформе управления, которая вычисляет основную частоту переменного тока сигнала напряжения сети, чтобы предотвратить искажение выходного сигнала и колебания частоты сети. Основными компонентами GFAs является:

1. Модуль управления нагрузкой - Мониторинг GFA.
2. Домашний шлюз - осуществляет беспроводную связь с модулем управления нагрузкой и пересылает сигнал на внутренний сервер через широкополосный кабельный модем или ADSL-соединение.
3. Фоновый сервер - периодически получает данные от каждого домашнего шлюза.

Коммуникационную систему умного дома можно разделить на 3 части: внешнюю сеть, шлюз и внутреннюю сеть.

Внешняя сеть может быть сотовой локальной сетью, сетями кабельного телевидения, телефонными сетями и Интернетом, в основном использующими более зрелые технологии. Интранет (без доступа посторонних) используется для соединения различных бытовых приборов внутри семьи, оборудования, локальной сети, из-за огромного разнообразия подключенных устройств сеть также продемонстрировала большое разнообразие форм.

Домашние сети в основном делятся на три категории в соответствии с их функциями: управляющая сеть для управления функциями, сеть передачи данных для обмена сообщениями данных и мультимедийная сеть для передачи аудио и видео. Домашний шлюз — это сетевое соединительное устройство, которое соединяет домашнюю интрасеть и экстранет (защищённая сеть) и осуществляет доступ из интрасети в экстранет, чтобы предоставить экстранету функцию управления соединяющимися устройствами в доме. В то же время домашний шлюз позволяет дому внедрять различные сетевые технологии и использовать шлюзы, обеспечивающие возможность соединения для различных коммуникационных подсетей, так что сетевые устройства в каждой подсети могут взаимодействовать друг с другом. Основными подсетями умного дома являются:

1. сеть бытовой техники: бытовая техника (холодильники, кондиционеры, телевизоры, микроволновые печи, стиральные машины, освещение и т.д.) образует сети посредством проводных или беспроводных соединений для обмена информацией;

2. сеть безопасности: включая охрану прилегающей территории, домашний видеодомофон, контроль доступа, охранную сигнализацию, пожар, утечки газа, разливы воды и т.д.;

3. высокоскоростной доступ к информации: интернет, доступ к сотовой локальной сети в дом;

4. жилищные услуги: центр управления сообществом может контролировать оборудование и окружающую среду и управлять ими в его юрисдикции.

Основным элементом системы умного дома является домашняя внутренняя сеть связи, которая в основном включает в себя две части: шлюз умного дома и умный датчик узла дома. Шлюз Умного Дома — это центр управления семейными ресурсами и настройки для выполнения домашней сети, управления узлами и других функций.

Шлюз умного дома соединяет каждый узел переключения датчика в домашней сети с помощью сетевой технологии, осуществляет управление внутренней сетью умного дома с помощью стандартного протокола связи и служит интерактивным интерфейсом информации домашней сети и внешней сети. Интеллектуальный дом может выполнять множество функций, таких как: мониторинг дома, внутренний и внешний обмен информацией, управление энергопотреблением, безопасность дома, настройки сцены неотделимы от поддержки шлюза умного дома, многие функции основаны на шлюзе умного дома и достигаются.

Система умный дом — это своего рода система управления, основанная на однокристальном компьютере, который может получать доступ к домашним устройствам и управлять ими через телефон и Интернет. Интеллектуальная система управления домашней сетью с помощью модуля сбора данных, командного управления и модуля протокола TCP / IP для обеспечения безопасности сети мониторинга командное управление разделено на три режима: 1) дистанционное управление по телефону; 2) сетевое дистанционное управление; 3) работа на месте. Структура системы показана на рис. 3.

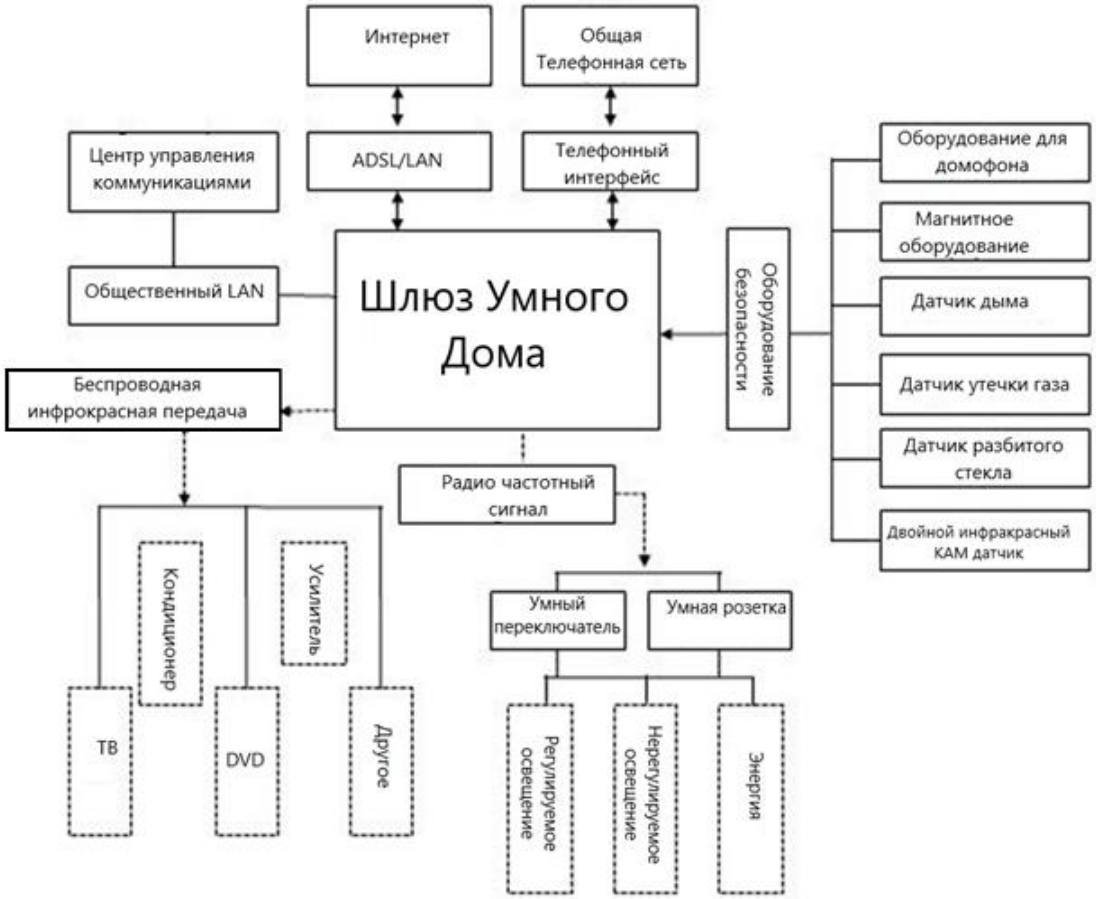



Рисунок 3 – Структура системы

Как ключевая часть умного потребления электроэнергии в сети, услуга умный дом является важным средством для реализации интерактивного взаимодействия между сетью и пользователями в режиме реального времени, расширения возможностей комплексного обслуживания сети, удовлетворения потребностей интерактивного маркетинга и повышения уровня обслуживания, а также усиления обмена информацией между пользователями и сетью и взаимодействия в режиме реального времени, для реализации интеллектуального и интерактивного использования электроэнергии, для дальнейшего улучшения режима работы электросети и режима использования энергии пользователем, а также для повышения энергоэффективности конечных пользователей. В соответствии с фактическими потребностями пользователей, укомплектованы умные интерактивные терминалы, телевизионные приставки, умные розетки и другие домашние умные сенсорные устройства, сетевые программы и интеллектуальная платформа управления услугами электроснабжения исследования и разработано соответствующее оборудование и программные платформы для достижения умного управления бытовой техникой и использования энергии; завершен типовой проект системы сбора информации об электроэнергии в режиме гибридной сети и разработано устройство и система сбора информации об электроэнергии на основе беспроводной сети и режима широкополосной гибридной сети электропитания для

обеспечения надежного электроснабжения бытовых пользователей при одновременном расширении возможностей умного дома.

**Список литературы**

1. Чан, М., Кампо, Э., Эстев, Д., и Фурньольс, Дж. Ю. (2009). Умные дома - текущие функции и перспективы на будущее. Матуритас, 64(2), 90с.
2. Фанг, Х., Мисра, С., Сюэ, Г., и Ян, Д. (2012). Smart grid — новая и усовершенствованная энергосистема: обзор. Опросы и учебные пособия по коммуникациям IEEE, 14(4), С.944-980.
3. Янг, С., Мистретта, Э., Чайчиан, С., и Сиау, Дж. (2017). Сетевая архитектура системы "Умный дом".
4. Хан, Д. М., и Лим, Дж. Х. (2010). Проектирование и внедрение систем энергоменеджмента "умного дома" на базе zigbee. Транзакции IEEE в области бытовой электроники, 56(3), С.1417-1425.
5. Цяо, Х. М., Чжай, Ю., Мэн, П., Чжан, Р. Р. и Ван, С. (2013). Исследование и применение интеллектуальной интерактивной технологии электроснабжения, основанной на оптоволокне, в домашних условиях. Информационно-коммуникационные технологии в электроэнергетике.
6. Канеко, М., Арима, К., Мураками, Т., Ишики, М., и Сугимура, Х. (2017). Разработка и внедрение интерактивной системы управления для умных домов. Международная конференция IEEE по потребительской электронике С.283-284. IEEE.
7. Палм, Дж. (2009). Управление чрезвычайными ситуациями в шведской электросети с точки зрения домашних хозяйств. Журнал непредвиденных обстоятельств и антикризисного управления, 17(1), С.55-63.
8. Буэно, А. Д. О. (2016). От умных городов к социальным: технологии для поддержки общественной жизни. Расширенные тезисы докладов конференции CHI, посвященные человеческим факторам в вычислительных системах С.198-202. ACM.
9. Лин, Л. И., Яо, Г., и Тан, Х. (2016). Строительство интерактивной системы электроснабжения для умного дома китайско-сингапурского эко-города Тяньцзинь.Распределение и утилизация.
10. Келес, С., Карабибер, А., Акчин, М., Кайгусуз, А., Алагоз, Б. Б., и Гюль, О. (2015). Концепция интеллектуального управления энергопотреблением здания: приложения smartsocket с распределением постоянного тока. Международный журнал электроэнергетики и энергетических систем, 64, С.679-688

**References**

1. Chan, M., Campo, E., Estev, D., and Fourniols, J. Y. (2009). Smart homes - current functions and prospects for the future. Maturitas, 64(2) p. 90
2. Fang, X., Misra, S., Xue, G., and Yang, D. (2012). Smart grid — a new and improved power system: an overview. IEEE Communications Surveys and Tutorials, 14(4), pp. 944-980.
3. Yang, S., Mistretta, E., Chaichian, S., and Siau, J. (2017). Network architecture of the Smart Home system.

4. Khan, D. M., and Lim, J. H. (2010). Design and implementation of smart home energy management systems based on zigbee. IEEE Transactions in Consumer Electronics, 56(3), pp.1417-1425.
5. Qiao, H. M., Zhai, Yu, Meng, P., Zhang, R. R. and Wang, S. (2013). Research and application of intelligent interactive power supply technology based on fiber at home. Information and communication technologies in the electric power industry.
6. Kaneko, M., Arima, K., Murakami, T., Ishiki, M., and Sugimura, H. (2017). Development and implementation of an interactive control system for smart homes. IEEE International Conference on Consumer Electronics pp.283-284. IEEE.
7. Palm, J. (2009). Emergency management in the Swedish electricity grid from a household perspective. Journal of Unforeseen Circumstances and Crisis Management, 17(1), pp.55-63.
8. Bueno, A. D. O. (2016). From smart cities to social ones: technologies to support public life. Extended abstracts of the CHI Conference devoted to human factors in computing systems pp.198-202. ACM.
9. Lin, L. I., Yao, G., and Tang, H. (2016). Construction of an interactive power supply system for a smart home of the Chinese-Singaporean eco-city of Tianjin.Distribution and disposal.
10. Keles, S., Karabiber, A., Akchin, M., Kaigusuz, A., Alagoz, B. B., and Gul, O. (2015). The concept of intelligent building energy management: smartsocket applications with DC distribution. International Journal of Electric Power Engineering and Energy Systems, 64, pp.679-688

Палий А.В., Андреева И.М., Одинец Е.Д. Применение искусственного интеллекта в промышленной робототехнике // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31)ч.2 с. 135–139

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

# ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОМЫШЛЕННОЙ РОБОТОТЕХНИКЕ

**Палий А.В., Андреева И.М., Одинец Е.Д.**
*Политехнический институт (филиал) ФГБОУ ВО "Донской государственный технический университет", Таганрог, Россия (347904, Ростовская область, город Таганрог, Петровская ул., д.109а), e-mail: andreeva2012irina@yandex.ru*

**В статье подробно рассмотрены такие понятия, как «искусственный интеллект», подходы к созданию, что в себя включает его применение и использование, а также как применяется искусственный интеллект в промышленной робототехнике.**

Ключевые слова: Искусственный интеллект, нейронные сети, автоматизация производства, робототехника, промышленность.

# APPLICATION OF ARTIFICIAL INTELLIGENCE IN INDUSTRIAL ENGINEERING

**Paliy A.V., Andreeva I.M., Odinets E.D.**
*Polytechnic Institute (branch) of the Don State Technical University, Taganrog, Russia (347904, Rostov region, Taganrog, Petrovskaya street, 109a), e-mail: andreeva2012irina@yandex.ru*

**The article discusses in detail such concepts as "artificial intelligence", approaches to creation, which includes its application and use, as well as how artificial intelligence is used in industrial robotics.**

Keywords: Artificial intelligence, neural networks, production automation, robotics, industry.

Рост социотехнического влияния искусственного интеллекта (ИИ) и робототехники, основывавшейся на базе ИИ, реализуется в различных производственных и организационных процессах. Данный механизм используется во многих областях, где требуется анализ больших объемов данных, высокая точность и скорость обработки, а также принятие решений на основе сложных алгоритмов.

Применения ИИ включают автоматический анализ данных, обработку естественного языка, компьютерное зрение, игры и другие области, в том числе робототехнику. [1]

Одним из наиболее распространенных примеров применения ИИ в промышленной робототехнике является автоматизация процессов сборки и манипуляции. Роботы, оснащенные ИИ, могут выполнять задачи, которые требуют высокой точности и скорости, например, сборка сложных электронных устройств или сортировка товаров на складах.

Кроме того, ИИ может быть использован для управления роботами на основе обратной связи. Такой подход позволяет роботам адаптироваться к изменениям в окружающей среде и корректировать свое поведение на основе полученных данных. [2]

Использование ИИ также может улучшить безопасность на производстве. Роботы могут быть оснащены ИИ–системами, которые позволяют им автоматически реагировать на опасные ситуации и прекращать свою работу в случае необходимости. Таким образом, применение искусственного интеллекта в промышленной робототехнике имеет огромный потенциал для улучшения производительности, безопасности и эффективности процессов.

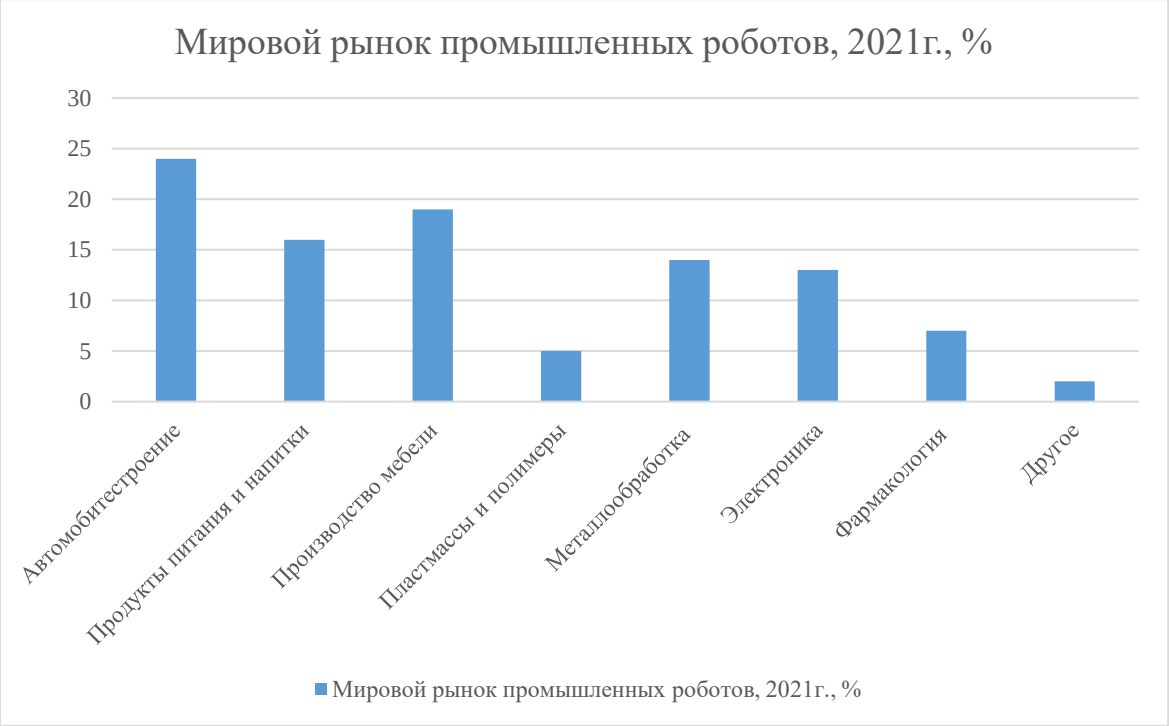



Рисунок 1 – Глобальный рынок роботов в 2021 году.

На Рисунке 1 показан глобальный рынок роботов, которые использовались для совместной работы с человеком в 2021 году. Согласно ему более 24% рынка в 2021 году принадлежало автомобильному сектору, который, по прогнозам, значительно увеличится в течение следующих пяти лет. [5]

В настоящее время искусственный интеллект (ИИ) применяется в робототехнике для управления и автоматизации различных задач, таких как:

1. Промышленные роботы: ИИ используется для программирования роботов в промышленности, чтобы они могли выполнять различные задачи в автоматическом режиме, такие как сборка и пакетирование продуктов;
2. Роботы-помощники: ИИ может помочь в создании роботов-помощников, которые могут выполнять различные задачи в повседневной жизни, такие как уборка дома, приготовление пищи и т.д.;
3. Автономные транспортные средства: ИИ используется для создания автономных транспортных средств.
4. Медицинские роботы: ИИ применяется для создания медицинских роботов, которые могут выполнять сложные хирургические операции.

5. Роботы-экзоскелеты: ИИ используется для управления роботами-экзоскелетами, которые могут помочь людям с ограниченными возможностями.

6. Контроль качества: Искусственный интеллект может использоваться для контроля качества продукции, анализа изображений и диагностики дефектов;

7. Автоматизация производства: Искусственный интеллект может помочь автоматизировать производственные процессы.

8. Прогнозирование сбоев: Искусственный интеллект может помочь предсказывать сбои в оборудовании и устранять их до того, как они приведут к остановке производства;

9. Анализ больших данных: Искусственный интеллект может помочь анализировать большие объемы данных, например, данные о производственных процессах и качестве продукции.

Нужно отметить, что искусственный интеллект, используемый в робототехнике, помогает людям обезопасить, облегчить работу в различных сферах, включая производство, здравоохранение, автоматизацию и повышение качества жизни.

В целом, роботы с искусственным интеллектом могут улучшить производительность, снизить затраты, повысить качество жизни и помочь людям в различных сферах.

Это только некоторые из примеров применения ИИ в робототехнике. Разработчики продолжают искать новые способы использования ИИ для автоматизации различных задач и улучшения качества жизни людей. [3]

По последним данным, в России общий объем рынка ИИ по итогам составил около 635 млрд руб., что на 15% больше, чем годом ранее. Применение ИИ принесло российской экономике более 300 млрд руб. В целом использование данных технологий даст дополнительно 1-2% к темпам роста валового внутреннего продукта (ВВП) страны до 2030 г.

В будущем искусственный интеллект будет продолжать развиваться в нескольких направлениях:

1. Развитие алгоритмов и методов: Искусственный интеллект будет продолжать развиваться в направлении улучшения алгоритмов и методов машинного обучения, что позволит создавать более точные и эффективные системы;

2. Большие данные: Рост объема данных и развитие технологий обработки данных, таких как Big Data и облачные вычисления, будет способствовать развитию искусственного интеллекта;

3. Развитие робототехники: Робототехника, основанная на искусственном интеллекте, будет продолжать развиваться, в том числе с более сложными и тонкими задачами;

4. Разработка умных систем: Разработка умных систем на основе искусственного интеллекта будет продолжаться, что позволит создавать более интеллектуальные и автономные системы в различных областях;

5. Совместная работа с человеком: Разработка искусственного интеллекта будет направлена на совместную работу с человеком, что позволит создавать более гибкие и адаптивные системы, способные обучаться от людей и делать выводы на основе их опыта. Развитие нейронных сетей:

6. Развитие нейронных сетей, которые являются частью искусственного интеллекта, будет продолжаться, что позволит создавать более точные и быстрые системы;

7. Развитие искусственного обучения: Развитие искусственного обучения будет продолжаться, включая создание более сложных систем глубокого обучения и рекуррентных нейронных сетей.

В целом, искусственный интеллект будет продолжать развиваться в различных направлениях, что позволит создавать более умные, интеллектуальные и эффективные системы.

В данной статье было рассмотрено применение искусственного интеллекта в промышленной робототехнике. Были описаны основные принципы работы искусственного интеллекта, а также рассмотрены конкретные примеры его применения в робототехнике.

Искусственный интеллект имеет огромный потенциал для оптимизации производственных процессов, повышения эффективности и качества продукции, а также сокращения затрат на производство. С помощью искусственного интеллекта роботы могут выполнять сложные задачи, обучаться новым навыкам и адаптироваться к изменяющимся условиям производства.

Применение искусственного интеллекта в промышленной робототехнике является одним из ключевых трендов современной промышленности и может привести к значительным улучшениям в производственных процессах и повышению конкурентоспособности предприятий. [4]

Однако следует учитывать, что применение искусственного интеллекта может также вызывать определенные риски, такие как потеря рабочих мест, сокращение человеческого контроля над производственными процессами, а также возможность появления новых видов угроз безопасности. Поэтому необходимо внимательно относиться к вопросам этики и безопасности при использовании искусственного интеллекта в промышленной робототехнике.

В целом, применение искусственного интеллекта в промышленной робототехнике представляет собой важный шаг в развитии современной промышленности и может привести к значительным улучшениям в производственных процессах и повышению конкурентоспособности предприятий. Однако необходимо учитывать возможные риски и подходить к вопросу применения искусственного интеллекта ответственно и внимательно.

Работа выполнена под научным руководством к.т.н., доцента Палия А.В.

**Список литературы**

1. Accenture "Переработка революции" (отчёт). URL: https://www.accenture.com/_acnmedia/pdf-88/accenture-rework-the-revolution-2018.pdf.
2. Международный институт McKinsey "Искусственный интеллект: следующий рубеж?" (отчёт). URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.
3. Национальные академии наук, инженерии и медицины National Academies Press, 2017: "Роботы для продвинутого производства", URL : https://www.nap.edu/catalog/24676/robots-for-advanced-manufacturing.

4. "Искусственный интеллект в производстве: всеобъемлющее руководство", Altexsoft, 2020: https://www.altexsoft.com/blog/artificial-intelligence/ai-in-manufacturing-a-comprehensive-guide/</a>.
5. Отчет PwC "Определение размера приза: какова реальная ценность ИИ для вашего бизнеса и как вы можете извлечь выгоду?": 2017. URL : https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.

**References**

1. Accenture "Reworking the Revolution" (report). URL: https://www.accenture.com/_acnmedia/pdf-88/accenture-rework-the-revolution-2018.pdf. McKinsey International Institute "Artificial Intelligence: The Next Frontier?"
2. McKinsey International Institute "Artificial Intelligence: The Next Frontier?" (report). URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.
3. National Academies Press, 2017: "Robots for Advanced Manufacturing", URL: https://www.nap.edu/catalog/24676/robots-for-advanced-manufacturing.
4. "Artificial Intelligence in Manufacturing: A Comprehensive Guide", Altexsoft, 2020: https://www.altexsoft.com/blog/artificial-intelligence/ai-in-manufacturing-a-comprehensive-guide/</a>.
5. PwC report "Determining the size of the prize: what is the real value of AI for your business and how can you benefit?": 2017. URL : https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.

Здор Д.В., Савельева Е.В., Бондаренко Ю.Д. Реализация графических методов решения математических задач средствами электронных таблиц // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 5(31) ч.2. с. 140–144

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

# РЕАЛИЗАЦИЯ ГРАФИЧЕСКИХ МЕТОДОВ РЕШЕНИЯ МАТЕМАТИЧЕСКИХ ЗАДАЧ СРЕДСТВАМИ ЭЛЕКТРОННЫХ ТАБЛИЦ

**[1] Здор Д.В., Савельева Е.В., Бондаренко Ю.Д.**
*ФГБУО ВО «Приморская государственная сельскохозяйственная академия», Уссурийск, Россия (692510, Приморский край, город Уссурийск, пр-кт Блюхера, д.44), e-mail: [1] dmitriy.dv@inbox.ru,*

**Статья посвящена вопросу применения электронных таблиц в качестве средства реализации графических методов решения математических задач. Целью работы является изучение технологических приемов решения математических задач графическим методом с применением электронных таблиц. Технология реализации графического метода описана на примере ряда задач, выбранных произвольно, для которых применим графический метод решения. При описании технологии акцент был сделан на содержательных элементах, которые необходимо реализовать при применении электронных таблиц в качестве инструментального средства для решения рассматриваемых задач графическим методом. Описанная технология может быть использована для дальнейшей разработки вопросов, связанных с изучением методов и приемов решения математических задач средствами электронных таблиц.**

Ключевые слова: Электронная таблица, графический метод, технология решения.

# IMPLEMENTATION OF GRAPHICAL METHODS FOR SOLVING MATHEMATICAL PROBLEMS BY MEANS OF SPREADSHEETS

**[1] Zdor D.V., Savelyeva E.V., Bondarenko Yu.D.**
*Primorsky State Agricultural Academy, Ussuriysk, Russia (44 Blucher Ave., Ussuriysk, Primorsky Krai, 692510, Russian Federation), e-mail: [1] dmitriy.dv@inbox.ru*

**The article is devoted to the use of spreadsheets as a means of implementing graphical methods for solving mathematical problems. The aim of the work is to study technological methods for solving mathematical problems by a graphical method using spreadsheets. The technology for the implementation of the graphical method is described on the example of a number of problems, chosen arbitrarily, for which the graphical method of solution is applicable. When describing the technology, the emphasis was placed on the content elements that need to be implemented when using spreadsheets as a tool for solving the problems under consideration by a graphical method. The described technology can be used for further development of issues related to the study of methods and techniques for solving mathematical problems using spreadsheets.**

Keywords: Spreadsheet, graphic method, solution technology.

В настоящее время компьютеры широко используются для решения прикладных задач в различных областях деятельности человека. Среди всего многообразия прикладных программ очень широкое распространение при этом получили электронные таблицы.

Данные в электронных таблицах могут быть связаны формульными зависимостями, при этом изменение хотя бы одного из данных приводит к мгновенному пересчету по формулам всех значений. В качестве характерной особенности электронных таблиц можно отметить возможность графической визуализации данных в интерактивном режиме. Это реализовано с помощью диаграмм и графиков. Отмеченные особенности электронных таблиц позволяют применять их в качестве средства решения математических задач графическим методом.

Объектом рассмотрения в данной работе выступают содержательные элементы технологических приемов решения математических задач графическим методом средствами электронных таблиц.

Можно отметить, что электронные таблицы относятся к широко распространенным программным продуктам, доступным пользователям, не обладающим навыками программирования [3, с. 196]. Это обстоятельство актуализирует необходимость изучения рассматриваемой проблемы как альтернативы методам и приемам решения математических задач на компьютере средствами программирования.

Описание технологических приемов решения математических задач графическим методом проведем на конкретных примерах. Это подробно иллюстрирует содержательные элементы рассматриваемых приемов и их непосредственную реализацию в электронных таблицах. В качестве программного средства избраны электронные таблицы Microsoft Excel. Выбор программного обеспечения обусловлен достаточно широким распространением среди пользователей данной программы по сравнению с другими табличными процессорами. При этом сами технологические приемы инвариантны, что позволит применять описанную технологию с другими программными средствами обработки электронных таблиц.

**Построение графиков функций.** Данная задача является наиболее простой в контексте рассматриваемой проблемы, так как она решается непосредственно путем применения встроенного инструмента электронных таблиц в виде диаграммы. При этом в электронных таблицах обычно имеется специальный встроенный тип диаграмм, предназначенный непосредственно для построения графика. В графических методах решения математических задач построение графика функции выступает основным элементом технологии.

Табулирование функции является первым необходимым элементом для построения графика с помощью диаграммы. При табулировании вычисляются значения функции на некотором промежутке с заданным шагом [4, с. 37].

Так как в электронных таблицах график функции получается как совокупность точек диаграммы, для достижения необходимой степени наглядности важным моментом становится выбор промежутка для табулирования функции и соответствующего шага изменения аргумента.

Итак, задача построения графика функции $y = f(x)$ сводится к построению диаграммы по предварительно полученной в ходе табулирования функции таблицы значений. В контексте решаемой задачи для функций, имеющих точки разрыва, будет более целесообразно использовать тип диаграммы «Точечная». Это объясняется тем, что в некоторых случаях при построении графика в диаграммах с типом диаграммы «График» автоматически соединяются и выделяются цветом все точки, включая и точки разрыва [1, с. 26].

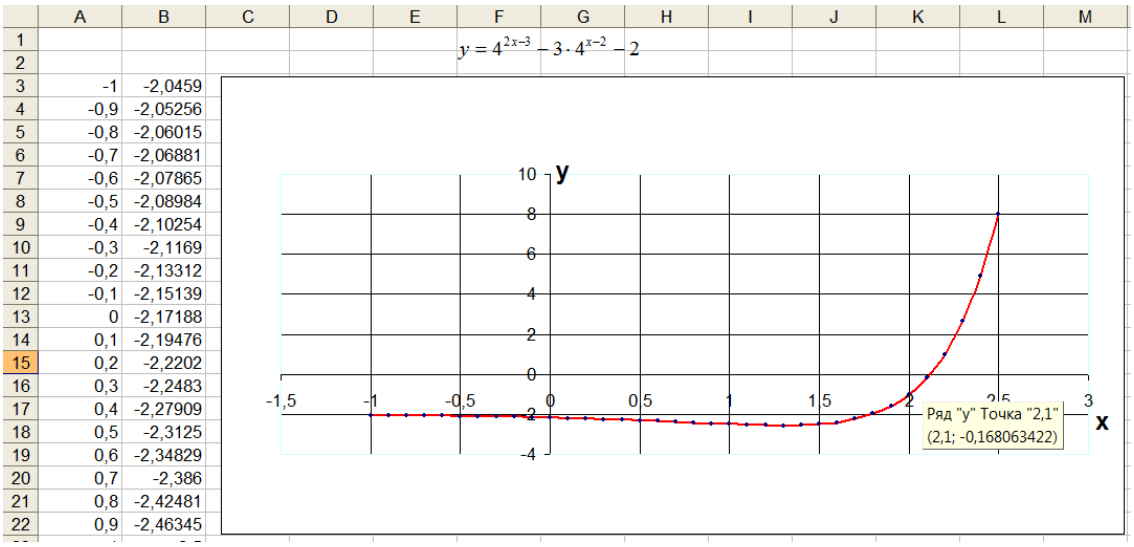
**Графические способы решения уравнений.** Графическим способом можно приближенно находить решение уравнения вида $f(x)=0$. Таким образом, уравнение, подлежащее решению, в первую очередь, должно быть преобразовано к этому виду. Графический метод решения данной задачи сводится к построению графика функции $y=f(x)$ и нахождению абсцисс точек пересечения графика с осью $x$ (числовых промежутков, содержащих корни уравнения). Каждое из полученных значений является приближенным значением корня уравнения $f(x)=0$.

Рассмотрим пример. Решить уравнение графически $4^{2x-3}-3\cdot 4^{x-2}=2$.

Решение. Преобразуем уравнение к виду $4^{2x-3}-3\cdot 4^{x-2}-2=0$.

Построим график функции $y=4^{2x-3}-3\cdot 4^{x-2}-2$

Найдем абсциссы точек пересечения графика с осью $x$ (Рисунок 1).




| | A | B |
|---|---|---|
| 3 | -1 | -2,0459 |
| 4 | -0,9 | -2,05256 |
| 5 | -0,8 | -2,06015 |
| 6 | -0,7 | -2,06881 |
| 7 | -0,6 | -2,07865 |
| 8 | -0,5 | -2,08984 |
| 9 | -0,4 | -2,10254 |
| 10 | -0,3 | -2,1169 |
| 11 | -0,2 | -2,13312 |
| 12 | -0,1 | -2,15139 |
| 13 | 0 | -2,17188 |
| 14 | 0,1 | -2,19476 |
| 15 | 0,2 | -2,2202 |
| 16 | 0,3 | -2,2483 |
| 17 | 0,4 | -2,27909 |
| 18 | 0,5 | -2,3125 |
| 19 | 0,6 | -2,34829 |
| 20 | 0,7 | -2,386 |
| 21 | 0,8 | -2,42481 |
| 22 | 0,9 | -2,46345 |

Рисунок 1 – Графический способ решения уравнения

Ответ: $x\approx 2{,}1$.

**Графические способы решения систем уравнений.** Для нахождения решения системы двух уравнений с двумя неизвестными систему необходимо привести к виду $\begin{cases} y=f_1(x) \\ y=f_2(x) \end{cases}$. Затем на одной диаграмме построить графики функций $y=f_1(x)$ и $y=f_2(x)$. Координаты точек пересечений графиков будут приближенным решением системы уравнений.

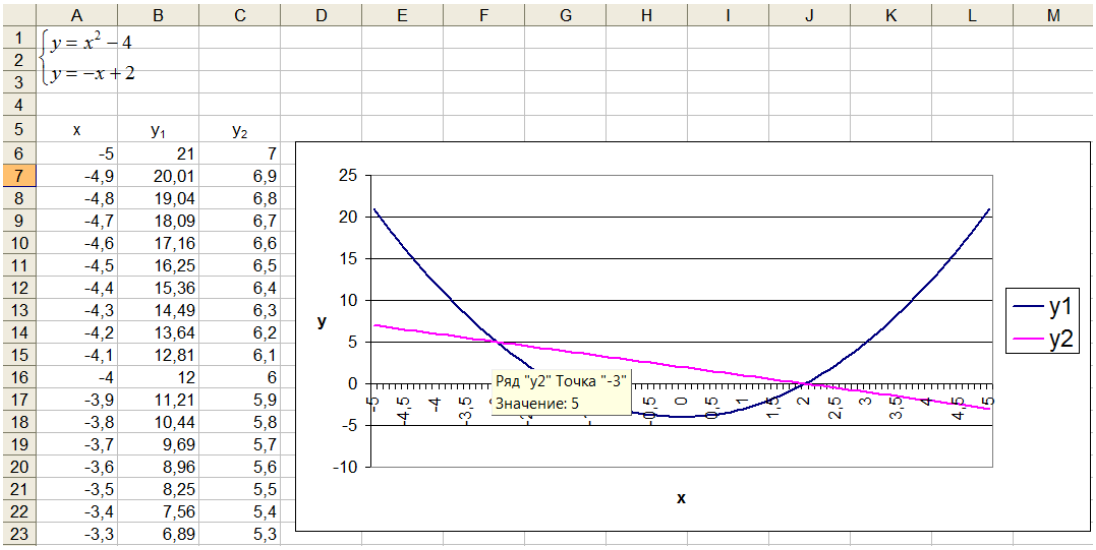
Рассмотрим пример. Решить систему уравнений графическим методом.

$$\begin{cases} y=x^2-4 \\ x+y=2 \end{cases}$$

Решение. Преобразуем систему к виду $\begin{cases} y=x^2-4 \\ y=-x+2 \end{cases}$

Построим на одной диаграмме графики функций $y = x^2 - 4$ и $y = -x + 2$.

Найдем координаты точек пересечения графиков функций (Рисунок 2).




| | x | $y_1$ | $y_2$ |
|---|---|---|---|
| 6 | -5 | 21 | 7 |
| 7 | -4,9 | 20,01 | 6,9 |
| 8 | -4,8 | 19,04 | 6,8 |
| 9 | -4,7 | 18,09 | 6,7 |
| 10 | -4,6 | 17,16 | 6,6 |
| 11 | -4,5 | 16,25 | 6,5 |
| 12 | -4,4 | 15,36 | 6,4 |
| 13 | -4,3 | 14,49 | 6,3 |
| 14 | -4,2 | 13,64 | 6,2 |
| 15 | -4,1 | 12,81 | 6,1 |
| 16 | -4 | 12 | 6 |
| 17 | -3,9 | 11,21 | 5,9 |
| 18 | -3,8 | 10,44 | 5,8 |
| 19 | -3,7 | 9,69 | 5,7 |
| 20 | -3,6 | 8,96 | 5,6 |
| 21 | -3,5 | 8,25 | 5,5 |
| 22 | -3,4 | 7,56 | 5,4 |
| 23 | -3,3 | 6,89 | 5,3 |

Рисунок 2 – Графический способ решения системы уравнений

Ответ: приближенное решение (-3;5) ; (2;0).

Приведенное описание технологических приемов математических задач графическим методом с применением электронных таблиц не может претендовать на завершенность, так как рассмотрен небольшой круг таких задач и рассмотрено недостаточное количество соответствующих примеров. Вместе с тем описание содержательных элементов рассматриваемой технологии позволяет получить общее представление о возможностях применения электронных таблиц для реализации графического метода, и может быть использована для дальнейшей разработки вопросов, связанных с изучением методов и приемов решения математических задач средствами электронных таблиц.

**Список литературы**

1. Здор Д.В. Решение задач на ЭВМ как способ реализации компьютерного практикума в вузовском курсе информатики // Объединенный научный журнал. – 2011. – № 5-6 – С. 26-29.
2. Информатика: Практикум по технологии работы на компьютере / Под ред. Н.В. Макаровой. – М.: Финансы и статистика, 2005. – 256 с.
3. Могилев А.В., Пак Н.И., Хеннер Е.К. Информатика: учебное пособие / Под ред. Е.К. Хеннера. – М.: Академия, 2003. – 816 с.
4. Сайков Б.П. Excel: построение диаграмм // Информатика и образование. – 2001. – № 3. – С. 37-44.
5. Ефимова О.В. Microsoft Excel 2003. Электронные таблицы. – М.: Интеллект-Центр, 2006. – 112 с.

Здор Д.В., Савельева Е.В., Бондаренко Ю.Д. Реализация графических методов решения математических задач средствами электронных таблиц // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2. с. 140–144

**References**

1. Zdorov D.V. Solving problems on a computer as a way to implement a computer workshop in a university course of computer science // United Scientific Journal. – 2011. – № 5-6 – pp. 26-29.
2. Computer science: A workshop on computer technology / Edited by N.V. Makarova. – M.: Finance and Statistics, 2005. – 256 p.
3. Mogilev A.V., Pak N.I., Henner E.K. Computer science: textbook / Edited by E.K. Henner. – M.: Academy, 2003. – p.816
4. Saikov B.P. Excel: diagramming // Informatics and education. - 2001. – No. 3. – pp. 37-44.
5. Efimova O.V. Microsoft Excel 2003. Spreadsheets. – M.: Intellect Center, 2006. – p.112

Хмелёв И.С. Разработка методики расчёта тепловой сети по алгоритму Дейкстры на PYTHON // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 145–150

Международный журнал информационных технологий и энергоэффективности

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

УДК 697.343

# РАЗРАБОТКА МЕТОДИКИ РАСЧЁТА ТЕПЛОВОЙ СЕТИ ПО АЛГОРИТМУ ДЕЙКСТРЫ НА PYTHON

**Хмелёв И.С.**
*ФГБОУ ВО "Самарский Государственный Технический Университет", Самара, Россия (443100, г. Самара, Молодогвардейская ул., д.244),* e-mail: *igori111@mail.ru*

**Рассмотрен алгоритм расчёта потерь давления на вводах потребителей, подключенных к тепловой сети. Методика расчёта разработана на основе пошагового алгоритма Дейкстры и написана на языке программирования Python.**

Ключевые слова: Тепловая сеть, потери давления, алгоритм Дейкстры, Python

# DEVELOPMENT OF A METHOD FOR CALCULATING THE HEAT NETWORK USING DIJKSTRA'S ALGORITHM IN PYTHON

**Khmelev I.S.**
*Samara State Technical University, Samara, Russia (443100, Samara, Molodogvardeyskaya St., 244),* e-mail: *igori111@mail.ru*

**An algorithm for calculating pressure losses at the inputs of consumers connected to the heating network is considered. The calculation method is based on Dijkstra's step-by-step algorithm and is written in the Python programming language.**

Keywords: Heat network, pressure loss, Dijkstra algorithm, Python.

В настоящее время существуют различные методы и способы расчёта тепловых сетей от «классической» реализации алгоритма в таблицах Excel до использования специализированного программного обеспечения, например, системы ZuluThermo.

Рассмотрим методику, разработанную на основе алгоритма Дейкстры и реализованную с помощью языка программирования Python. Данная методика предназначена для расчёта потерь давления в тепловой сети на вводах подключенных к ней потребителей. Для начала вкратце разберём, что из себя представляет сам алгоритм Дейкстры.

Алгоритм Дейкстры – это пошаговый метод, который находит кратчайший путь от одной вершины графа до другой [1]. Граф – это некоторая структура, состоящая из узлов, соединенных гранями каждая из которых имеет свой весовой коэффициент – в данном случае потери давления.

На этапе инициализации задается начальный узел графа, и расстояние до всех узлов приравнивается к бесконечности. Далее на первом шаге выбирается узел ближайший к

начальному, расстояние до него приравнивается к весовому коэффициенту пройденной грани. На всех последующих шагах сравниваются узлы-соседи текущего узла графа. К расстоянию, пройденному от начального узла до текущего прибавляется расстояние от текущего узла до каждого его «соседа». После чего выбирается узел с наименьшим расстоянием и аналогичные действия проделываются с его «соседями». Расчёт завершается после того как все узлы были посещены.

В качестве исходных данных используются две таблицы, реализованные в виде Pandas DataFrame. В первой содержится информация об узлах тепловой сети: наименование узла, порядковый номер узла и тип (источник или потребитель). Во второй таблице хранится информация об участках тепловой сети: наименование начального и конечного узла, диаметр трубопровода и длина участка.

| Наименование | Номер | Тип |
|---|---|---|
| **ТЭЦ-1** | 0 | Источник |
| **ТК6-19** | 1 | NaN |
| **ПРК-1** | 2 | NaN |
| **ПРК-2** | 3 | NaN |
| **СВК-1** | 4 | NaN |
| **...** | ... | ... |
| **ул. Труда,15** | 249 | Потребитель |
| **ул. Труда,39** | 250 | Потребитель |
| **ул. Труда,37а** | 251 | Потребитель |
| **ул. Чехова,2** | 252 | Потребитель |
| **ул. Чехова,8** | 253 | Потребитель |

254 rows × 2 columns

| | Начало линии | Конец линии | Диаметр | Длина |
|---|---|---|---|---|
| **0** | ТК6-19 | ПРК-1 | 0.225 | 61.875 |
| **1** | ПРК-1 | ПРК-2 | 0.225 | 38.750 |
| **2** | ПРК-2 | СВК-1 | 0.225 | 56.087 |
| **3** | СВК-1 | СВК-2 | 0.225 | 14.375 |
| **4** | СВК-2 | СВК-2а | 0.225 | 37.500 |
| **...** | ... | ... | ... | ... |
| **258** | ТРК-24 | ул. Труда,15 | 0.050 | 27.900 |
| **259** | ТРК-16 | ул. Труда,39 | 0.050 | 67.067 |
| **260** | ТРК-16 | ул. Труда,37а | 0.050 | 54.374 |
| **261** | СВК-3б | ул. Чехова,2 | 0.050 | 17.288 |
| **262** | ТК-1 Чехова,8 | ул. Чехова,8 | 0.050 | 18.728 |

263 rows × 5 columns

Рисунок 1 – Таблицы исходных данных

Приступим к реализации алгоритма Дейкстры на языке Python. Для начала создадим класс для нашего графа и методы необходимые для заполнения его данными (Рисунок 1).

```
class Graph:
    def __init__(self):
        self.v = num_of_nodes
        self.edges = [[-1 for i in range(num_of_nodes)] for j in range(num_of_nodes)]
        self.visited = []

    def add_line(self, begin_line, end_line, diametr, lenght):
        self.diametr = diametr
        self.lenght = lenght
        self.hydro = hydro_by_d[diametr]*lenght
        self.num_beginline = NameNodes_num.loc[begin_line, 'Номер']
        self.num_endline = NameNodes_num.loc[end_line, 'Номер']
        self.edges[self.num_beginline][self.num_endline] = self.hydro
```

Рисунок 2 – *Класс Graph*

Внутри метода init находится три переменные:

- v – определяет количество узлов в созданном графе;
- edges – представляет собой матрицу, в которую будут заноситься значения потерь давления;
- visited – это список посещенных узлов.

Далее разберём метод add_line, он используется для заполнения графа исходными данными. В этом методе прописаны следующие переменные:

- diametr – диаметр участка трубопровода;
- lenght – длина участка;
- hydro – абсолютные потери давления, по значению диаметра из словаря подтягиваются удельные потери давления и умножаются на длину участка;
- num_beginline – номер начального узла, определяется из Pandas DataFrame по наименованию узла и столбцу, где NameNodes_num – название DataFrame;
- num_endline – номер конечного узла, определяется аналогично начальному узлу;
- edges – заполнение матрицы граней значениями абсолютных потерь давления, каждый элемент матрицы соответствует комбинации номеров начального и конечного узлов.

Теперь импортируем класс PriorityQueue и создадим новую функцию, которая будет описывать непосредственно алгоритм расчёта (Рисунок 2).

```
from queue import PriorityQueue

def dijkstra(graph, start_vertex):
    D = {v:float('inf') for v in range(graph.v)}
    D[start_vertex] = 0

    pq = PriorityQueue()
    pq.put((0, start_vertex))

    while not pq.empty():
        (dist, current_vertex) = pq.get()
        graph.visited.append(current_vertex)

        for neighbor in range(graph.v):
            if graph.edges[current_vertex][neighbor] != -1:
                distance = graph.edges[current_vertex][neighbor]
                if neighbor not in graph.visited:
                    old_cost = D[neighbor]
                    new_cost = D[current_vertex] + distance
                    if new_cost < old_cost:
                        pq.put((new_cost, neighbor))
                        D[neighbor] = new_cost
    return D
```

Рисунок 3 – Функция Дейкстра

В функции Дейкстра вводится несколько новых переменных:

- graph – переменная присвоенная созданному графу;
- start_vertex – номер начального узла;
- D – словарь с результатами расчёта;
- dist – значение весового коэффициента (потери давления);
- current_vertex – номер текущего узла;
- neighbor – номер узла-соседа;
- distance - значение потерь давления, берётся из матрицы граней;
- old_cost – старое значение потерь давления узла-соседа, берётся из словаря D;
- new_cost – новое значение потерь давления узла-соседа, определяется суммой значения текущего узла из словаря D и переменной distance.

Следующим этапом является создание цикла, который передаст все исходные данные в метод add_line и функцию Дейкстра, а также настроим алгоритм добавления результатов расчёта вТаблицу.

```
# Расчёт
  g = Graph()
  for i in range(0, num_of_line):
    g.add_line(line_info.iloc[i, 0], line_info.iloc[i, 1],
               line_info.iloc[i, 2], line_info.iloc[i, 3])
  D = dijkstra(g, 0)
#Создание таблицы с результатами
for vertex in range(len(D)):
  new_row = { 'Наименование': num_NameNodes.iloc[vertex, 0],
              'Тип': num_NameNodes.iloc[vertex, 2],
              'Потери давления, Па': D[vertex],}
  All_results = All_results.append(new_row, ignore_index=True)

mask_user = (All_results['Тип'] == 'Потребитель')
User_results = All_results[mask_user]
```

Рисунок 4 – Запуск расчёта и вывод результатов

Как результат выполнения описанного алгоритма получаем таблицу в которой сведена информация по всем потребителям подключенным к тепловой сети: их наименования и суммарные потери давления на абонентских вводах каждого из них.

| | Наименование | Тип | Потери давления, Па |
|---|---|---|---|
| **110** | пер. Дерендяева,19 | Потребитель | 68002.35 |
| **122** | ул. Володарского,46 | Потребитель | 47792.95 |
| **126** | ул. К.Маркса,35 | Потребитель | 32076.89 |
| **133** | ул. Р.Люксембург,33 | Потребитель | 53861.00 |
| **136** | ул. Р.Люксембург,68 | Потребитель | 36963.67 |
| **...** | ... | ... | ... |
| **249** | ул. Труда,15 | Потребитель | 74363.65 |
| **250** | ул. Труда,39 | Потребитель | 63764.19 |
| **251** | ул. Труда,37а | Потребитель | 61077.84 |
| **252** | ул. Чехова,2 | Потребитель | 49644.61 |
| **253** | ул. Чехова,8 | Потребитель | 49255.30 |

118 rows × 3 columns

Рисунок 5 – Таблица результатов расчёта

**Список литературы**

1. Skillfactory media [Электронный ресурс] – Электрон. Текстовые дан. – Москва – Режим доступа: https://blog.skillfactory.ru/glossary/algoritm-dejkstry/

2. Помощник Python [Электронный ресурс] – Электрон. Текстовые дан. – Режим доступа: https://pythonpip.ru/examples/ochered-python
3. Академия Яндекса [Электронный ресурс] – Электрон. Текстовые дан. – Москва – Режим доступа: https://academy.yandex.ru/handbook/python/article/obuektnaya-model-python-klassy-polya-i-metody

**References**

1. Skillfactory media [Electronic resource] – Electron. Text data. – Moscow – Access mode: https://blog.skillfactory.ru/glossary/algoritm-dejkstry/
2. Python Assistant [Electronic resource] – Electron. Text data. – Access mode: https://pythonpip.ru/examples/ochered-python
3. Yandex Academy [Electronic resource] – Electron. Text data. – Moscow – Access mode: https://academy .yandex.ru/handbook/python/article/obuektnaya-model-python-klassy-polya-i-metody

Шишкина Д.Е. Содержание и сущность стратегии энергетической безопасности и ее правовое регулирование // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 151–154

Международный журнал информационных технологий и энергоэффективности

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

УДК 620.9

# СОДЕРЖАНИЕ И СУЩНОСТЬ СТРАТЕГИИ ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ И ЕЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ

**Шишкина Д.Е.**
*ФГБОУ ВО "Санкт-Петербургский государственный экономический университет", Санкт-Петербург, Россия (191023, город Санкт-Петербург, наб. Канала Грибоедова, д. 30-32 литер а), e-mail: solnce_2410@mail.ru*

**В работе подробно раскрыто значение стратегии энергетической безопасности России. Обозначен правовой механизм регулирования и обеспечения энергетической безопасности.**

Ключевые слова: Энергетическая безопасность, стратегия, государство.

# THE CONTENT AND ESSENCE OF THE ENERGY SECURITY STRATEGY AND ITS LEGAL REGULATION

**Shishkina D.E.**
*"St. Petersburg State University of Economics", St. Petersburg, Russia (191023, St. Petersburg, Griboyedov Canal Embankment, 30-32 letter a), e-mail: solnce_2410@mail.ru*

**The paper reveals in detail the importance of Russia's energy security strategy. The legal mechanism for regulating and ensuring energy security is outlined.**

Keywords: Energy security, strategy, state.

Эффективно функционирующий энергетический комплекс страны – один из ключевых факторов, от которого зависит уровень экономического развития страны.

Стратегия энергетической безопасности должна определять приоритетные направления для обеспечения защищенности жизненно важных интересов как отдельной личности, так и общества в целом. Рассматривая содержание стратегии энергетической безопасности, необходимо в первую очередь определить основные понятия и термины, которые будут использоваться в данном исследовании.

Энергетическая безопасность — это определенное состояние страны, при котором отсутствуют внутренние и внешние угрозы энергетическим интересам, как и государству, так и отдельным потребителям, которые могут возникнуть в процессе добычи, транспортировки, переработки и использования природных энергоресурсов и получаемых видов энергии. В процессе обеспечения энергетической безопасности поддерживаются условия для стабильного функционирования и развития энергетики, промышленности и всего топливно-энергетического комплекса страны, а также для достойной жизни общества.

Обеспечение энергетической безопасности является неотъемлемым фактором для поддержания экономической безопасности, поскольку формирует национальную безопасность в совокупности с политической, социальной, оборонной и поддерживает общую защищенность как государства, так и населения.

Угрозами энергетической безопасности – являются факторы, создающие возможность нанесения ущерба энергетики страны. Стратегия — это общий план, разработанный на длительный период времени, определяющий основные цели и способы их достижения.

Таким образом, стратегия энергетической безопасности – это совокупность правил и мер, которые определяют задачи и цели долгосрочного энергетического развития России.

Стратегия представляет собой систему мер, основной целью которых является обеспечение охраны и защита энергетических интересов, с целью нейтрализации возможных угроз, возникающих в функционировании этой отрасли [1-3].

Условиями реализации энергетической безопасности, будут являться:

1. создание и поддержание конкурентного рынка топливно-энергетических ресурсов;
2. сохранение единой энергетической системы для надежного энергообеспечения;
3. слаженная политика регулирования цен на продукты отрасли;
4. обеспечение административными, нормативно-правовыми и организационными мерами деятельность объектов энергетики.

Стратегия энергетической безопасности заключается в одновременном повышении доступности и эффективности рационального использования энергоресурсов для конечных пользователей, то есть для всех жителей страны.

Важнейшими принципами стратегии обеспечения энергетической безопасности является:

1. гарантированность поставки энергообеспечения до конечного потребителя;
2. соответствие требованиям экологической безопасности, для минимизации техногенного воздействия;
3. создание условий для развития энергетической отрасли и инвестирование;
4. минимизация ущерба в результате функционирования комплекса;
5. достижение рационального уровня использования энергоресурсов;
6. повышение энергетической эффективности экономики России.

Правовой механизм реализации стратегии обеспечения энергетической безопасности России Процесс обеспечения энергетической безопасности страны, на данный момент, регламентирует Энергетическая стратегия Российской Федерации на период до 2035 года (Утверждена Правительством РФ от 09.06.2020 г.).

Основной целью развития энергетического комплекса является поддержание социально-экономического роста страны и укрепление позиций энергетического блока на период на 2035 года. Стратегия предполагает цифровое и интеллектуальное развитие энергетического комплекса, с целью повышения качества всех процессов в этой сфере и появления новых возможностей для потребителей продукции и услуг топливно-энергетической сферы [4].

Также особое внимание уделено повышению конкурентоспособности, технологической независимости, совершенствованию государственного управления и развитию международных отношений энергетической сфере.

Основными направлениями стратегии Энергетической безопасности до 2030 года определены следующие факторы:

1. эффективное удовлетворение внутреннего спроса на энергоресурсы;
2. реализация запланированного объема продукции и услуг топливно-энергетического комплекса для экспорта;
3. реализация национальных программ и проектов для эффективного развития энергетических отраслей;
4. трансформация энергетической инфраструктуры с учетом экономических и политических изменений на международном рынке;
5. повышение конкурентоспособности топливно-энергетического комплекса России.

Правовой основой стратегического планирования в сфере обеспечения энергетической Российской Федерации является Указ Президента РФ от 13 мая 2019 г. № 216 “Об утверждении Доктрины энергетической безопасности Российской Федерации”. Документ определяет структуру топливно-энергетического комплекса России, в которую входят следующие отрасли: 8 электроэнергетика, нефтяная, газовая и угольная промышленность, теплоснабжение.

Энергетический комплекс имеет первостепенное значение в формировании доходов бюджета России и вносит существенный вклад в обеспечение международной энергетической безопасности. Согласно правовому акту, Правительство Российской федерации должно проводить единую государственную политику в обеспечении энергетической безопасности, организовывать, организовывать систему управления рисками, контролировать деятельность федеральных органов по обеспечению энергетической безопасности, представлять доклад о состоянии энергетической безопасности президенту Российской Федерации [5].

Рассматриваемый законодательный акт определяет задачи государственного управления в реализации стратегии энергетической безопасности и определяет следующие направления:

1. совершенствование правовой базы, регулирующей инфраструктуру отраслей ТЭК;
2. введение мероприятий по оптимизации налоговой политики;
3. профилактика противоправных действий на объектах топливно-энергетического комплекса и центрах управления;
4. охрана труда и обеспечение безопасности работников предприятий ТЭК;
5. совершенствование внешнеэкономического взаимодействия между партнерами и международными организациями по вопросам обеспечения энергоресурсами.

Вопросы безопасности объектов энергетического комплекса должны быть строго регламентированы законодательством, поскольку это опасная промышленность, в функционировании которой имеется большое количество угроз и рисков. Федеральный закон от 21.07.2011 № 256-ФЗ (ред. от 06.07.2016) «О безопасности объектов топливно-энергетического комплекса» регулирует механизмы защиты охраны труда персонала на предприятии определяет принципы обеспечения пожарной, техносферной и экологической безопасности для защиты населения от чрезвычайных ситуаций. В законодательном акте отражены требования к персоналу на объектах ТЭК. Особое внимание уделено процессу финансирования мероприятий по обеспечению безопасности комплекса [6].

**Список литературы**

1. Горяинов, М.В. Современное состояние и перспективы развития топливно-энергетического комплекса страны. Монография / М.В. Горяинов. - М.: Русайнс, 2017г.
2. Кулагина В. А. Макарова А. А. Митрова Т. А. Прогноз развития энергетики мира и России 2019 /А. А. Макарова, Т. А. Митрова, В. А. Кулагина //ИНЭИ РАН–Московская школа управления СКОЛКОВО – Москва, 2019. – С. 26– 59. 5
3. Кулагина В. А. Перспективы развития мировой энергетики с учетом влияния технологического прогресса / В. А. Кулагина // М.: ИНЭИ РАН, 2020. – С. 5– 37
4. «О безопасности объектов топливно-энергетического комплекса»: Федеральный закон от 21.07.2011 № 256-ФЗ (ред. от 06.07.2016).
5. «Об утверждении Доктрины энергетической безопасности Российской Федерации»: указ Президента РФ от 13 мая 2019 г. № 216.
6. Постовалов А. И. Стратегия и политика энергосбережения/А. И. Постовалов // Вестник Московского университета имени С. Ю. Витте. - 2029. - №4. - С. 3–6.

**References**

1. Goryainov, M.V. The current state and prospects of development of the fuel and energy complex of the country. Monograph / M.V. Goryainov. - M.: Rusains, 2017.
2. Kulagina V. A. Makarova A. A. Mitrova T. A. Forecast of the development of energy in the world and Russia 2019 /A. A. Makarova, T. A. Mitrova, V. A. Kulagina //INEI RAS–Moscow School of Management SKOLKOVO – Moscow, 2019. – pp. 26-59. 5
3. Kulagina V. A. Prospects for the development of world energy taking into account the impact of technological progress / V. A. Kulagina // Moscow: INEI RAS, 2020. – pp. 5– 37
4. "On the safety of fuel and energy complex facilities": Federal Law No. 256-FZ dated 21.07.2011 (ed. dated 06.07.2016).
5. "On approval of the Energy Security Doctrine of the Russian Federation": Decree of the President of the Russian Federation dated May 13, 2019 No. 216.
6. Postovalov A. I. Strategy and Policy of energy saving/A. I. Postovalov // Bulletin of the S. Y. Witte Moscow University. - 2029. - No. 4. - pp. 3-6.