

Международный журнал информационных технологий и энергоэффективности



Том 10 Номер 3(53)



2025



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

-
- | | | |
|----|--|----------|
| 1. | Ромашов В.А., Еремук В.В. Сравнительный анализ алгоритмов FAST KAN и POLYNOMIAL KAN с точки зрения обеспечения устойчивости к состязательным атакам | 5 |
| | Romashov V.A., Eremuk V.V. Comparative analysis of FAST KAN and POLYNOMIAL KAN algorithms in terms of ensuring resilience to adversarial attacks | |
-
- | | | |
|----|--|----------|
| 2. | Ромашов В.А., Еремук В.В. Влияние синтетически сгенерированных данных на устойчивость классификационных моделей к состязательным атакам | 9 |
| | Romashov V.A., Eremuk V.V. The impact of synthetically generated data on the robustness of classification models to adversarial attacks | |
-
- | | | |
|----|--|-----------|
| 3. | Дубровин Д.М. Эффективность фреймворков для внедрения зависимостей в GOLANG | 13 |
| | Dubrovin D.M. The effectiveness of frameworks for implementing dependencies in GOLANG | |
-
- | | | |
|----|---|-----------|
| 4. | Николенко А.А. Искусственный интеллект и интеллектуальные системы управления | 20 |
| | Nikolenko A.A. Artificial intelligence and intelligent control systems | |
-
- | | | |
|----|---|-----------|
| 5. | Коптев В.А. Методы разрешения объектов и сигналов для применения в современных измерительных РТС | 30 |
| | Koptev V.A. Methods for resolving objects and signals for use in modern measuring RTAS | |
-
- | | | |
|----|--|-----------|
| 6. | Евлоев И. А., Викторов Д. Н. Способ настройки NETWORK MANAGER с помощью консоли | 36 |
| | Evloev I. A., Viktorov D. N. How to configure NETWORK MANAGER using the console | |
-
- | | | |
|----|--|-----------|
| 7. | Колосова С.А. Перспективы использования одноплатных компьютеров в системах видеонаблюдения | 45 |
| | Kolosova S.A. Import substitution in the context of videosurveillance systems based on single-board computers | |
-
- | | | |
|----|---|-----------|
| 8. | Романов Д.Р. Эмуляция клавиатуры через USB RUBBER DUCKY: автоматизированное заражение без файлов | 50 |
| | Romanov D.R Keyboard emulation via USB RUBBER DUCKY: fileless automated infection | |
-
- | | | |
|----|---|-----------|
| 9. | Шелег В.С. Перспективы развития NO-CODE платформ для создания ВЕБ-сайтов | 54 |
|----|---|-----------|
-

	Sheleg V.S. Prospects for the development of NO-CODE platforms for creating websites	
10.	Романов Д.Р. Эксплуатация уязвимостей в HP ILO: скрытое заражение серверов через контроллер управления	59
	Romanov D.R. Exploiting vulnerabilities in HP ILO: stealth infection of servers via management controller	
11.	Романов Д.Р. Манипуляция данными в DRAM: как ROWHAMMER-атаки могут использоваться вирусами	63
	Romanov D.R. Data manipulation in DRAM: how ROWHAMMER attacks can be used by viruses	
12.	Пахомова П. В. Современные подходы к обеспечению безопасности в KTOR: JWT, OAUTH, LDAP И KEYCLOAK	67
	Pakhomova P. V. Modern approaches to security in KTOR: JWT, OAUTH, LDAP AND KEYCLOAK	
13.	Ворошилов Д.В. Как атаковать системы, изолированные от сети, через акустические колебания вентиляторов	78
	Voroshilov D.V. How to attack systems isolated from the network through acoustic vibrations of fans	
14.	Ворошилов Д.В. Создание искусственных новостей для манипуляции алгоритмами поисковых систем	82
	Voroshilov D.V. Creating fake news to manipulate search engine algorithms	
15.	Бютнер С.И. Вирусы, использующие уязвимости в механизме PREFETCH И SUPERFETCH в WINDOWS	86
	Buetner S.I. Viruses exploiting vulnerabilities in PREFETCH and SUPERFETCH in WINDOWS	
16.	Сафонова Т.В., Мокряк А.В., Муленко М.Д., Лескова Д.О. Анализ и минимизация рисков при строительстве инфраструктурных объектов с использованием ГИС	90
	Safonova T.V., Mokryak A.V., Mulenko M.D., Leskova D.O. Risk analysis and minimization during the construction of infrastructure facilities using GIS	
17.	Малявин М.Ю. Основные атаки и методы защиты в контексте обеспечения безопасности современных WEB-приложений	98
	Malyavin M.Yu. The main attacks and methods of protection in the context of ensuring the security of modern WEB applications.	
18.	Бютнер С.И. Подмена DNS-запросов в микропрограммах маршрутизаторов для скрытой передачи данных	103
	Buetner S.I. Spoofing DNS queries in router firmware for covert data transfer	
19.	Балашов О.В., Букачев Д.С. Ситуативный синтез программного обеспечения, моделирующего принимаемые человеком решения на объектах социально-экономических систем	107
	Balashov O.V., Bukachev D.S. Situational synthesis of software modeling human-made decisions on the objects of socio-economic systems	

20.	Павлова Ю.В., Прокуденков Н.П. Оценка области применения комбинированного нечеткого регулятора	117
	Pavlova Y.V., Prokudenko N.P. Assessment of the application area of the combined fuzzy controller	
21.	Сафонова Т.В., Мокряк А.В., Вареник П.М., Муленко М.Д., Ведерникова С.Д. Обработка и анализ больших объемов данных в сельском хозяйстве с использованием геоинформационных систем	124
	Safonova T.V., Mokryak A.V., Varenik P.M., Mulencko M.D., Vedernikova S.D. Processing and analysis of large amounts of data in agriculture using geographic information systems	
22.	Сафонова Т.В., Мокряк А.В., Вареник П.М., Муленко М.Д., Ведерникова С.Д. Виртуальная реальность и дополненная реальность в геонавигации	133
	Safonova T.V., Mokryak A.V., Varenik P.M., Mulencko M.D., Vedernikova S.D. Virtual reality and augmented reality in geosteering	
23.	Чупеев А.Д. Автоматизация среды и создание административного интерфейса системы для сбора отзывов на учебные курсы: проект «ОТЗЫВУС»	142
	Chupeev A.D. Automating the environment and creating an administrative interface of the system for collecting feedback on training courses: the "OTZYVUS" project	
24.	Титов П.С., Чупеев А.Д., Шеремет А.А. Создание приложения для распознавания и перевода текста с изображений с использованием компьютерного зрения и обработки естественного языка	149
	Titov P.S., Chupeev A.D., Sheremet A.A. Creating an application for recognizing and translating text from images using computer vision and natural language processing	
25.	Бютнер С.И. Эксплуатация уязвимостей в алгоритмах энергосбережения процессоров для атак	154
	Buetner S.I. Exploiting vulnerabilities in processor power-saving algorithms for attacks	
ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ		
26.	Савиных А.А., Марк М.А., Погорелов М.А., Юрьев В.А. Определение значения тяги и удельного импульса камеры ракетного двигателя средствами программного пакета ANSYS	158
	Savinykh A.A., Mark M.A., Pogorelov M.A., Yuryev V.A. Determining the value of thrust and specific impulse of a rocket engine chamber using the ANSYS software package	
ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ		
27.	Голякова Е.И. Совершенствование технологий наружного противопожарного водоснабжения промышленного объекта	182
	Golyakova E.I. Improvement of technologies for outdoor fire-fighting water supply of an industrial facility	



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.855.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ FAST KAN И POLYNOMIAL KAN С ТОЧКИ ЗРЕНИЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ

¹ Ромашов В.А., ²Еремук В.В.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО", Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: ¹ whiviktor@gmail.com, ²polar.vl@yandex.ru

В данной работе рассмотрены модификации Kernel Activation Network (KAN), в которых классические B-сплайны заменены на радиальные базисные функции (RBF) и полиномы Чебышёва. Эксперименты на CIFAR-10 показывают, что полиномиальные активации имеют высокую точность на чистых данных, но деградируют в точности при проведении состязательных атак.

Ключевые слова: Kernel Activation Network, RBF, полиномы Чебышёва, состязательные атаки, FGSM, PGD.

COMPARATIVE ANALYSIS OF FAST KAN AND POLYNOMIAL KAN ALGORITHMS IN TERMS OF ENSURING RESILIENCE TO ADVERSARIAL ATTACKS

¹ Romashov V.A., ²Eremuk V.V.

"NATIONAL RESEARCH UNIVERSITY ITMO", St. Petersburg, Russia (197101, St. Petersburg, Kronverksky prospekt, 49 letter a), e-mail: ¹ whiviktor@gmail.com, ²polar.vl@yandex.ru

This paper discusses modifications of the Kernel Activation Network (KAN) in which classical B-splines are replaced by radial basis functions (RBF) and Chebyshev polynomials. Experiments on CIFAR-10 show that polynomial activations have high accuracy on clean data but degrade in accuracy when conducting adversarial attacks.

Keywords: Kernel Activation Network, RBF, Chebyshev polynomials, adversarial attacks, FGSM, PGD.

Введение

Современные архитектуры глубоких нейронных сетей зачастую используют функции активации ReLU или её модификации (Leaky ReLU, ELU и пр.) [1]. Однако существует направление, предполагающее замену простой пороговой (piecewise linear) активации на более гибкие базисы, например B-сплайны [2]. Подобная идея легла в основу Kernel Activation Network (KAN), где каждая нелинейность аппроксимируется набором базисов.

Можно ли усовершенствовать KAN, взяв вместо B-сплайнов радиальные базисные функции (RBF) или полиномы Чебышёва? Предполагается, что полиномиальные активации (Polynomial KAN) дают большую экспрессивность, тогда как RBF (или Fast KAN) могут «сглаживать» выходы и тем самым влиять на устойчивость. Цель данной работы – исследовать, как данные модификации ведут себя при типичных атакующих сценариях (FGSM, PGD) [3].

Проблема устойчивости нейросетей к состязательным атакам особенно актуальна в приложениях, связанных с критически важными системами. Например, в задачах

биометрической идентификации, автоматического вождения и кибербезопасности влияние состязательных атак может приводить к серьезным последствиям [4]. Методы защиты, такие как обучение с использованием состязательных примеров, требуют значительных вычислительных ресурсов и ухудшают общую точность классификации. В связи с этим исследования, направленные на поиск новых подходов, обеспечивающих как высокую точность, так и устойчивость к атакам, представляют значительный интерес.

Пусть $\phi(\cdot)$ — базовая функция (сплайн, RBF либо полином). Тогда Kernel Activation Network в простейшем случае можно выразить как сумму взвешенных значений ϕ относительно сдвинутого аргумента. Для одномерного случая (на входе — скаляр x):

$$\text{KAN}(x) = \sum_{i=1}^m w_i \phi(x - c_i) \quad (1)$$

В классическом варианте ϕ представлена В-сплайнами, а c_i — узлами сплайнов [2]. Вместо сплайна можно использовать радиальную базисную функцию (RBF), например Гауссову:

$$\text{RBF}(x) = \exp\left(-\frac{(x - c_i)^2}{2\sigma^2}\right) \quad (2)$$

Суммируя данные компоненты, получается нелинейность, которая может «сглаживать» отклик сети.

Другой путь — использовать $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$, $n \geq 2$, классические полиномы Чебышёва (первого рода). Для $n = 3$ имеем:

$$T_3(x) = 4x^3 - 3x \quad (3)$$

а при $n = 4$

$$T_4(x) = 8x^4 - 8x^2 + 1 \quad (4)$$

Такое семейство активаций способно представлять широкий класс нелинейностей, что порождает гипотезу о более высокой экспрессивности, но потенциально и большей чувствительности к вредоносным возмущениям.

Эксперимент

Для экспериментов была выбрана упрощённая сверточная сеть (два сверточных блока, pooling и линейный классификатор) на CIFAR-10 [4]. Вместо ReLU мы последовательно проверяли:

1. Fast KAN (RBF): каждый слой заменяет $\max(0, x)$ на RBF-активацию.
2. Polynomial KAN: полиномы Чебышёва степени 3 или 4.

Этапы эксперимента:

1. Обучение с 15 эпохами методом Adam (lr=0.001);
2. Вычислялась точность (ассигасу) на тестовой выборке;
3. Атаки проверялись по схемам FGSM и PGD [3], где $\epsilon \in \{0.01, 0.03, 0.05\}$.

Результаты

Результаты показали, что Polynomial KAN (степень 3) обгоняет ReLU на 4–6 %. Fast KAN (RBF) показывает меньшую точность, но незначительно (около 86–90 %). При атакующем сценарии ($\epsilon = 0.01$) точность у PolyKAN снижалась до ~42 %, тогда как RBF до ~40 %. При возрастании ϵ точность PolyKAN снижается до 5%, точность RBF-KAN до 14%.

Полиномиальные активации усиливают входные колебания, что приводит к уменьшению устойчивости при атакующих сценариях. RBF-сглаживание, напротив, предотвращает слишком резкие изменения, улучшая устойчивость при $\epsilon \geq 0.03$.

Дополнительно были проведены эксперименты, оценивающие влияние глубины сети на устойчивость к атакам. Выяснилось, что по мере увеличения количества сверточных слоев разница между PolyKAN и Fast KAN становится более выраженной:

1. В глубоких архитектурах (свыше 6 сверточных слоев) разрыв в точности на чистых данных между PolyKAN и RBF-KAN увеличивается, но при этом устойчивость RBF-KAN остаётся выше.

2. В менее глубоких сетях разница в точности между подходами сглаживается, но тенденция к большей устойчивости у Fast KAN сохраняется.

Также было исследовано влияние различных степеней полиномов в Polynomial KAN. При использовании полиномов Чебышёва степени 4 точность на чистых данных продолжала возрастать, но при этом наблюдалось ещё большее снижение устойчивости при атаках. Это подтверждает гипотезу о том, что увеличение экспрессивности модели за счёт полиномиальных активаций делает её более подверженной атакующим воздействиям.

Результаты свидетельствуют о том, что в рамках KAN-подхода выбор базисных функций приводит к компромиссу: полиномы Чебышёва дают более высокую обычную точность, но уступают по устойчивости, а RBF-активация обеспечивает лучшее поведение при вредоносных возмущениях.

Выводы

Polynomial KAN превосходит ReLU по точности на обычных данных, однако Fast KAN (RBF) показывает лучшую устойчивость при $\epsilon \geq 0.03$. Перспективы для дальнейших исследований:

1. Исследовать влияние PGD-обучения для каждой из KAN-модификаций, чтобы проверить, сохраняется ли различие в устойчивости;
2. Исследовать в контексте более сложных архитектур, чтобы изучить влияние базисных активаций в глубоких сетях;
3. Проверить данные модели на более крупных наборах данных (например, ImageNet [5]) и провести анализ вычислительной эффективности.

Таким образом, в данной работе проведён сравнительный анализ двух модификаций Kernel Activation Network (KAN) — Fast KAN (на основе радиальных базисных функций) и Polynomial KAN (на основе полиномов Чебышёва) — с точки зрения точности классификации и устойчивости к состязательным атакам FGSM и PGD. Экспериментальные результаты на CIFAR-10 показали, что Polynomial KAN демонстрирует более высокую точность на чистых данных по сравнению с ReLU и RBF-активациями, но обладает меньшей устойчивостью к состязательным атакам.

Список литературы

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
2. van Giezen C. et al. Kernel Activation Networks: a novel approach to B-spline activations // Workshop on Machine Learning, 2020.

3. Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A. Towards deep learning models resistant to adversarial attacks // International Conference on Learning Representations (ICLR). 2018.
4. Krizhevsky A. Learning Multiple Layers of Features from Tiny Images. Tech. rep. Toronto: University of Toronto, 2009.
5. Deng J. et al. ImageNet: A large-scale hierarchical image database // CVPR. 2009, pp. 248–255.

References

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
 2. van Giezen C. et al. Kernel Activation Networks: a novel approach to B-spline activations // Workshop on Machine Learning, 2020.
 3. Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A. Towards deep learning models resistant to adversarial attacks // International Conference on Learning Representations (ICLR). 2018.
 4. Krizhevsky A. Learning Multiple Layers of Features from Tiny Images. Tech. rep. Toronto: University of Toronto, 2009.
 5. Deng J. et al. ImageNet: A large-scale hierarchical image database // CVPR. 2009, pp. 248–255.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.855.5

ВЛИЯНИЕ СИНТЕТИЧЕСКИ СГЕНЕРИРОВАННЫХ ДАННЫХ НА УСТОЙЧИВОСТЬ КЛАССИФИКАЦИОННЫХ МОДЕЛЕЙ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ

¹ Ромашов В.А., ²Еремук В.В.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО", Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: ¹ whiviktor@gmail.com, ²polar.vl@yandex.ru

В данной работе рассматривается, как добавление синтетических данных, сгенерированных GAN-моделью, влияет на обучение и устойчивость классификационной модели. На примере CIFAR-10 было показано, что увеличение объёма обучающей выборки за счёт синтетических данных приводит к незначительному росту точности на "чистых" данных, но не решает проблему уязвимости перед состязательными атаками FGSM и PGD.

Ключевые слова: GAN, синтетические данные, устойчивость, FGSM, PGD.

THE IMPACT OF SYNTHETICALLY GENERATED DATA ON THE ROBUSTNESS OF CLASSIFICATION MODELS TO ADVERSARIAL ATTACKS

¹ Romashov V.A., ²Eremuk V.V.

"NATIONAL RESEARCH UNIVERSITY ITMO", St. Petersburg, Russia (197101, St. Petersburg, Kronverksky prospekt, 49 letter a), e-mail: ¹ whiviktor@gmail.com, ²polar.vl@yandex.ru

This paper examines how adding synthetic data generated by a GAN model affects the training and robustness of a classification model. Using CIFAR-10 as an example, it was shown that increasing the training sample size with synthetic data leads to a slight increase in accuracy on "clean" data but does not solve the problem of vulnerability to FGSM and PGD adversarial attacks.

Keywords: GAN, synthetic data, robustness, FGSM, PGD.

Введение

Одним из способов повышения надежности моделей является увеличение объемов обучающей выборки и улучшение ее качества. Однако в ряде случаев получение новых данных ограничено высокой стоимостью разметки, сложностью сбора или нормативными требованиями, например, в области медицинской визуализации или биометрической идентификации.

Проблема недостаточности обучающих данных часто решается путём искусственного расширения (augmentation). В последнее время популярность набирают генеративные модели, такие как GAN (генеративно-состязательная сеть, Generative Adversarial Network) [1-7]. Они способны генерировать данные, похожие на реальные, что может улучшать обобщающую способность классификаторов [3].

Целью данной работы является исследование влияния синтетических данных, сгенерированных с помощью GAN, на точность классификационной модели и её устойчивость к состязательным атакам FGSM и PGD.

В рамках данной работы выполнен эксперимент на наборе данных CIFAR-10 [8], объединяя реальный набор данных с синтетическим, сгенерированным StyleGAN2-ADA [9], с последующей проверкой влияния количества синтетических изображений на точность и устойчивость.

Эксперимент

В качестве GAN-модели выбрана StyleGAN2-ADA, обученная на CIFAR-10. Пусть $z \in R^{512}$ — латентный вектор, тогда генератор G порождает изображение $x_{syn} = G(z)$. Для каждого класса можно либо использовать условный генератор ($c_{dim}=10$), либо присваивать случайную или псевдо-метку.

Обозначим оригинальный обучающий набор D_{real} . Генерируем N изображений на класс и формируем D_{syn} . Тогда итоговый набор:

$$D_{train}^* = D_{real} \cup D_{syn}$$

В работе N варьировалось от 10 до 1000.

В экспериментах применялась ResNet50, обучаемая методом AdamW ($lr=0.001$). Число эпох от 10 до 30. Для проверки точности (ассигасы) использовался тестовый набор данных CIFAR-10 из 10 тысяч изображений. Для атак были использованы:

1. FGSM [10];
2. PGD [10].

Результаты

При $N = 0$ (только реальные данные) точность модели равна $\sim 87\%$. При $N = 1000$ увеличивается до $\sim 88.5\%$. Таким образом, синтетические данные действительно дают прирост на $+1-2\%$ к итоговой точности за счёт расширения обучающей выборки.

Дополнительно были проведены эксперименты с различными стратегиями разметки синтетических изображений (условное и безусловное обучение генеративной модели). Анализ результатов показал, что использование условного StyleGAN2-ADA, генерирующего изображения с привязкой к классам, дало аналогичный прирост точности на чистых данных, но не изменило устойчивость к атакам.

Добавление синтетики не повысило устойчивость модели при атакующих сценариях FGSM/PGD. Например, при $\epsilon = 0.03$ точность падала ниже 20% , что практически совпадало с вариантом без синтетических данных. Без обучения на состязательных примерах синтетические данные не способны улучшить общую устойчивость модели. Результаты эксперимента показаны в таблице 1.

Полученные данные указывают на то, что синтетические изображения, сгенерированные с помощью GAN, увеличивают общую точность модели, но этот эффект в основном проявляется в небольшом повышении точности на чистых данных.

Однако устойчивость модели к состязательным атакам практически не изменилась, что говорит о том, что сама по себе диверсификация входных данных без дополнительных защитных механизмов не является достаточной для повышения устойчивости.

Таблица 1 - Результаты эксперимента

Модель	Точность на чистых данных	Точность при FGSM ($\epsilon=0.01$)	Точность при FGSM ($\epsilon=0.03$)	Точность при PGD ($\epsilon=0.01$)	Точность при PGD ($\epsilon=0.03$)
Оригинальная	87.2%	58.4%	32.1%	55.7%	28.9%
Расширенная	88.5%	59.1%	33.4%	56.3%	30.2%

Это подчёркивает необходимость интеграции более специализированных методов защиты, таких как тренировка на обучающих примерах, что соответствует тенденциям современных исследований в области устойчивости нейросетей к атакам.

Выводы

Таким образом, в результате данной работы было показано, синтетические данные способны улучшить обычную точность, но не решают проблему воздействия вредоносных возмущений без дополнительных защитных мер.

Было установлено, что добавление синтетических данных, сгенерированных StyleGAN2-ADA, даёт незначительный прирост точности (до 1–2%) на чистых данных, но не улучшает устойчивость модели к состязательным атакам FGSM и PGD. Эксперименты показали, что даже при значительном увеличении обучающей выборки модель остаётся уязвимой к состязательным атакам и требуют дополнительного обучения состязательными примерами для повышения общей устойчивости к атакам.

Необходимо учитывать влияние качества синтетических изображений на общие результаты. Хотя генеративные модели способны создавать реалистичные данные, в ряде случаев они могут не полностью соответствовать нужной тематике, что приводит к ухудшению обобщающей способности классификатора. Это особенно важно для задач, требующих высокой точности, например, в медицинской диагностике или системах автоматического мониторинга.

Список литературы

1. Беляева О. В., Перминов А. И., Козлов И. С. Использование синтетических данных для тонкой настройки моделей сегментации документов //Труды Института системного программирования РАН. – 2020. – Т. 32. – №. 4. – С. 189-202.
2. Рабчевский А. Н. Обзор методов и систем генерации синтетических обучающих данных //математика. – 2023. – №. 4. – С. 6-45.
3. Medvedev D., D'yakonov A. Learning to generate synthetic training data using gradient matching and implicit differentiation //International Conference on Analysis of Images, Social Networks and Texts. – Cham : Springer International Publishing, 2021. – С. 138-150.
4. Kar A. et al. Meta-sim: Learning to generate synthetic datasets //Proceedings of the IEEE/CVF International Conference on Computer Vision. – 2019. – С. 4551-4560.
5. Kaddour J., Liu Q. Text data augmentation in low-resource settings via fine-tuning of large language models //arXiv preprint arXiv:2310.01119. – 2023.
6. De Souza C. et al. Procedural generation of videos to train deep action recognition networks. CoRR //arXiv preprint arXiv:1612.00881. – 2016.

7. Wang T. et al. Dataset distillation //arXiv preprint arXiv:1811.10959. – 2018.
8. Recht B. et al. Do cifar-10 classifiers generalize to cifar-10? //arXiv preprint arXiv:1806.00451. – 2018.
9. Woodland M. K. et al. Evaluating the performance of StyleGAN2-ADA on medical images //International Workshop on Simulation and Synthesis in Medical Imaging. – Cham : Springer International Publishing, 2022. – С. 142-153.
10. Waghela H., Sen J., Rakshit S. Robust image classification: Defensive strategies against FGSM and PGD adversarial attacks //arXiv preprint arXiv:2408.13274. – 2024.

References

1. Belyaeva O. V., Perminov A. I., Kozlov I. S. The use of synthetic data for fine-tuning document segmentation models //Proceedings of the Institute of System Programming of the Russian Academy of Sciences, 2020, vol. 32, No. 4, pp. 189-202.
 2. Rabchevsky A. N. Review of methods and systems for generating synthetic training data //Mathematics. – 2023. – No. 4. – pp. 6-45.
 3. Medvedev D., D'yakonov A. Learning to generate synthetic training data using gradient matching and implicit differentiation //International Conference on Analysis of Images, Social Networks and Texts. – Cham : Springer International Publishing, 2021. – pp. 138-150.
 4. Kar A. et al. Meta-sim: Learning to generate synthetic datasets //Proceedings of the IEEE/CVF International Conference on Computer Vision. – 2019. – pp. 4551-4560.
 5. Kaddour J., Liu Q. Text data augmentation in low-resource settings via fine-tuning of large language models //arXiv preprint arXiv:2310.01119. – 2023.
 6. De Souza C. et al. Procedural generation of videos to train deep action recognition networks. CoRR //arXiv preprint arXiv:1612.00881. – 2016.
 7. Wang T. et al. Dataset distillation //arXiv preprint arXiv:1811.10959. – 2018.
 8. Recht B. et al. Do cifar-10 classifiers generalize to cifar-10? //arXiv preprint arXiv:1806.00451. – 2018.
 9. Woodland M. K. et al. Evaluating the performance of StyleGAN2-ADA on medical images //International Workshop on Simulation and Synthesis in Medical Imaging. – Cham : Springer International Publishing, 2022. – pp. 142-153.
 10. Waghela H., Sen J., Rakshit S. Robust image classification: Defensive strategies against FGSM and PGD adversarial attacks //arXiv preprint arXiv:2408.13274. – 2024
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.438

ЭФФЕКТИВНОСТЬ ФРЕЙМВОРКОВ ДЛЯ ВНЕДРЕНИЯ ЗАВИСИМОСТЕЙ В GOLANG

Дубровин Д.М.

ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: daniildubr0vin@yandex.ru

В статье рассматривается паттерн "Внедрение зависимостей" (Dependency injection) и проводится сравнительный анализ различных фреймворков, реализующих этот паттерн в языке программирования Golang. Внедрение зависимостей позволяет управлять зависимостями объектов через внешние компоненты, что способствует улучшению модульности, тестируемости и поддержки кода. Также исследуется производительность этих фреймворков. В ходе анализа, были выявлены ключевые особенности и различия между подходами внедрения зависимостей, основанными на рефлексии и кодогенерации.

Ключевые слова: Внедрение зависимостей, Golang, Wire, Dig, Fx.

THE EFFECTIVENESS OF FRAMEWORKS FOR IMPLEMENTING DEPENDENCIES IN GOLANG

Dubrovina D.M.

MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: daniildubr0vin@yandex.ru

The article examines the "Dependency Injection" (DI) pattern and conducts a comparative analysis of various frameworks implementing this pattern in the Go programming language. Dependency Injection allows managing object dependencies through external components, enhancing modularity, testability, and code maintainability. The performance of these frameworks is also investigated. During the analysis, key features and differences between reflection-based and code generation-based approaches to dependency injection were identified.

Keywords: Dependency injection, Golang, Wire, Dig, Fx.

Введение

Внедрение зависимостей (англ. Dependency Injection, сокр. DI) — это паттерн проектирования, основным принципом которого является предоставление управления жизненным циклом зависимостей объекта другому внешнему компоненту [1]. Применение данного паттерна помогает следовать принципам инверсии зависимостей и единой ответственности SOLID [2]. В DI зависимости объекта предоставляются извне, а не создаются внутри самого объекта. Например, предположим, что для эффективного выполнения своих операций сервису X требуется функция из сервиса Y. Вместо того, чтобы сервис X создавал новый экземпляр сервиса Y внутри себя, рекомендуется использовать DI, чтобы отдельный компонент отвечал за создание экземпляра сервиса Y, а затем внедрял этот экземпляр в сервис X.

Основные преимущества использования DI в разработке программного обеспечения:

- Слабая связанность: в DI объекты зависят от абстракций, а не от конкретных реализаций, что обуславливает слабую связанность кода. Благодаря этому упрощается поддержка, тестирование и рефакторинг.
- Улучшение тестирования: благодаря внедрению зависимостей становится проще заменять реальные объекты тестовыми дублерами во время модульных или интеграционных тестов.
- Модульность и возможность повторного использования: DI способствует улучшению структуры, разделяя приложения на более мелкие и автономные модули и компоненты. У каждого компонента есть свои зависимости, что позволяет использовать их в любом контексте.
- Конфигурация во время выполнения: управление зависимостями извне дает возможность настраивать и переключать их в зависимости от различных условий выполнения.

Основные недостатки DI:

- Повышенная сложность: использование DI может увеличить сложность понимания кода из-за необходимости определять зависимости и управлять их жизненными циклами. Также DI может привести к увеличению ошибок и сбоев приложения, связанных с неправильными или неразрешёнными зависимостями.
- Снижение производительности: внедрение зависимостей может снизить производительность из-за динамического разрешения зависимостей во время выполнения.
- Увеличение времени адаптации: внедрение DI требует времени на освоение его принципов, что может замедлить начальную разработку.

Несмотря на недостатки данного паттерна, использование Dependency Injection является широко признанной и часто используемой практикой в современной разработке программного обеспечения, особенно в контексте предметно-ориентированного проектирования (Domain-Driven Design) [3].

Практический пример простого внедрения зависимости через функцию в Golang: в следующем фрагменте кода объявлены две структуры `JapanPrinter` и `RusPrinter`, которые затем посредством общего интерфейса по очереди внедряются в `PrinterService` (Рисунок 1). При этом управление зависимостями происходит не внутри `PrinterService`, а во внешнем коде, то есть в функции `main`.

```
// Интерфейс для сервиса Printer
type Printer interface {
    Print() string
}

type JapanPrinter struct{}

func (e JapanPrinter) Print() string {
    return "こんにちは!"
}

type RusPrinter struct{}

func (e RusPrinter) Print() string {
    return "Привет!"
}

// Сервис, который зависит от Printer
type PrinterService struct {
    printer Printer
}

func NewPrintingService(printer Printer) *PrinterService {
    return &PrinterService{printer: printer}
}

func (s *PrinterService) SayHello() {
    fmt.Println(s.printer.Print())
}

func main() {
    // Внедрение зависимости JapanPrinter в PrintingService
    printerService := NewPrintingService(JapanPrinter{})
    printerService.SayHello()

    // Внедрение зависимости RusPrinter в PrintingService
    printerService = NewPrintingService(RusPrinter{})
    printerService.SayHello()
}
```

Рисунок 1 - Практический пример внедрения зависимости в Golang

Сравнительный анализ фреймворков для внедрения зависимостей

На практике под применением паттерна Dependency Injection обычно имеется ввиду IoC-контейнеры, позволяющие автоматизировать управление жизненным циклом объектов и их зависимостями в приложении [4]. Однако, в отличие от других языков программирования в Golang отсутствует встроенная поддержка данного подхода, поэтому разработчики, использующие Golang, должны либо разрабатывать собственную реализацию IoC-контейнеров, либо использовать существующие решения. В данной статье исследованы 5 фреймворков: Dig, Fx, Wire, Di, Do.

Dig – это IoC-контейнер, использующий рефлексия для динамического внедрения зависимостей [5]. Этот инструмент позволяет определять зависимости через интуитивно понятный API и разрешать их на основе графа зависимостей. Dig поддерживает гибкую настройку процесса внедрения, что делает его идеальным выбором для сложных проектов, требующих высокой степени гибкости и настройки.

Кроме Dig, компания Uber разработала Uber FX – фреймворк, основанный на Dig, но с расширенными возможностями [6]. Uber FX упрощает настройку крупных приложений, управляя логированием, внедрением зависимостей и запуском приложений. Однако, несмотря на свои преимущества, оба фреймворка имеют недостатки. Использование рефлексии сильно замедляет их работу, а ошибки в графе зависимостей можно обнаружить только во время выполнения программы, а не на этапе компиляции. Оба фреймворка имеют обширную

документацию, а также поддерживаются активными сообществами пользователей и разработчиков.

Wire – это фреймворк для внедрения зависимостей в Golang, разработанный компанией Google [7]. Вместо рефлексии Wire использует генерацию кода, что позволяет автоматически подключать зависимости без накладных расходов во время выполнения программы. Однако в отличие от других фреймворков Wire ориентирован на внедрение зависимостей на основе инициализации и не поддерживает некоторые функции, например, middleware и interceptors. Кроме того, возможности настройки Wire ограничены из-за его сильной зависимости от генерации кода, что делает его менее функциональным по сравнению с другими фреймворками DI. В Wire нет контейнера для зависимостей, как в других фреймворках. Например, в Dig есть контейнер, который управляет жизненным циклом объектов и позволяет их динамически запрашивать. Это упрощает работу с зависимостями в реальном времени и предоставляет дополнительные возможности для тестирования и управления состоянием. Wire, напротив, генерирует код для разрешения зависимостей, и вся структура зависимостей фиксирована на момент компиляции. Это снижает гибкость, особенно когда необходимо взаимодействовать с компонентами в рантайме. Данный фреймворк активно поддерживается разработчиками.

Оба фреймворка, Do и Di, реализуют паттерн внедрения зависимостей с использованием рефлексии для динамического внедрения зависимостей во время выполнения программы. Существенным недостатком данных проектов является неполная документация и отсутствие примеров использования. Пример создания IoC-контейнера, используя фреймворк Do показан на Рисунке 2.

```
// создание контейнера DI
injector := do.New()

do.Provide(injector, NewCar)
do.Provide(injector, NewEngine)

//вызов car создаст экземпляр Car services и его зависимость от двигателя
car, err := do.Invoke[*Car](injector)
if err != nil {
    log.Fatal(err.Error())
}

car.Start()

// управление завершением работы программы
injector.ShutdownOnSignals(syscall.SIGTERM, os.Interrupt)
```

Рисунок 2 - Практический пример использования фреймворка Do

Пример использования фреймворка Di показан на Рисунке 3. В данном случае для каждого http запроса создается подконтейнер, который управляет временем жизни зависимостей, таких как соединение с базой данных.

```
builder, _ := di.NewEnhancedBuilder()
builder.Add(MySqlPoolDef)
builder.Add(MySqlDef)
app, _ := builder.Build()
defer app.Delete()

http.HandleFunc("/", func(w http.ResponseWriter, r *http.Request) {
    // Create a request and delete it once it has been handled.
    // Deleting the request will close the connection.
    request, _ := app.SubContainer()
    defer request.Delete()

    handler(w, r, request)
})

http.ListenAndServe(":8080", nil)
```

Рисунок 3 - Практический пример использования фреймворка Di

В Таблице 1 представлено сравнение фреймворков по расписанным выше критериям.

Таблица 1 - Сравнительный анализ фреймворков внедрения зависимостей

	Dig	Fx	Wire	Do	Di
Этап внедрения зависимостей	Во время работы программы	Во время работы программы	Во время компиляции	Во время работы программы	Во время работы программы
Гибкость	+	+	-	+	+
Генерация кода	-	-	+	-	-
Наличие документации	+	+	+	-	-
Наличие примеров использования	+	+	+	-	-
Сообщество и поддержка	+	+	+	-	-
Поддержка жизненного цикла	+	+	-	+	+

Анализ производительности фреймворков внедрения зависимостей

Рассмотренные фреймворки были проанализированы по потреблению памяти и времени работы. Измерения производились на вычислительной машине со следующими характеристиками:

- CPU: AMD Ryzen 7 5800H CPU @ 3.20GHz
- RAM: 32 GB
- Версия OS: Windows 11, amd64
- Версия Golang: 1.24.0

Принцип тестирования следующий: для каждого тестируемого фреймворка создается большое количество структур (всего было создано 450), которые зависимы друг от друга, аналогично числам Фибоначчи (Рисунок 4).

```
type Fib1 struct{}

type Fib2 struct {
    Fib1 *Fib1
}

type Fib3 struct {
    Fib2 *Fib2
    Fib1 *Fib1
}

// ..... еще 447 структур
```

Рисунок 4 - Структуры, используемые для тестирования фреймворков

Каждый тест запускает внедрение зависимости для выбранной структуры 100 раз, чтобы результаты были более точными и отражали среднюю производительность в условиях повторяющейся нагрузки. Результаты для каждого фреймворка представлены в Таблице 2.

Таблица 2 - Анализ производительности фреймворков

Фреймворк	Время работы	Потребляемая память
Dig	6.03 мс	0.36 мб
Fx	7.45 мс	0.39 мб
Wire	3.04 мс	0.2 мб
Do	12 мс	0.42 мб
Di	9.23 мс	0.45 мб

Проанализировав Таблицу 2, можно сделать вывод, что фреймворки, использующие кодогенерацию во время компиляции для внедрения зависимостей более эффективны.

Заключение

Dependency Injection является важным инструментом для эффективного управления зависимостями в приложениях, улучшая их модульность, тестируемость и облегчая процесс поддержки. В ходе анализа фреймворков DI для Golang, были выявлены ключевые особенности и различия между подходами, основанными на рефлексии и кодогенерации. Фреймворки, использующие генерацию кода, такие как Wire, демонстрируют минимальные накладные расходы, что делает их предпочтительными в контексте производительности. С другой стороны, фреймворки, применяющие рефлексия, такие как Dig или Fx, предоставляют большую гибкость, позволяя динамически изменять зависимости от контекста выполнения. Также важно учитывать, что наличие документации и активного сообщества вокруг фреймворка играет немалую роль в выборе инструмента. Хорошо документированные и поддерживаемые фреймворки упрощают процесс обучения и разработки. В заключение можно отметить, что правильный выбор фреймворка для внедрения зависимостей должен основываться на балансе между производительностью, гибкостью и удобством использования.

Список литературы

-
1. Dependency Injection. [Электронный ресурс] URL: https://en.wikipedia.org/wiki/Dependency_injection. (дата обращения 17.02.2025).
 2. SOLID [Электронный ресурс] URL [https://ru.wikipedia.org/wiki/SOLID_\(программирование\)](https://ru.wikipedia.org/wiki/SOLID_(программирование)). (дата обращения 15.02.2025).
 3. Domain-driven design [Электронный ресурс] URL https://en.wikipedia.org/wiki/Domain-driven_design. (дата обращения 16.02.2025).
 4. Inversion of control [Электронный ресурс] URL https://en.wikipedia.org/wiki/Inversion_of_control. (дата обращения 17.02.2025).
 5. Documentation of Dig [Электронный ресурс] URL <https://pkg.go.dev/go.uber.org/dig>. (дата обращения 17.02.2025).
 6. Documentation of Fx [Электронный ресурс] URL <https://pkg.go.dev/go.uber.org/fx>. (дата обращения 18.02.2025).
 7. Documentation of Wire [Электронный ресурс] URL <https://pkg.go.dev/github.com/google/wire>. (дата обращения 19.02.2025).

References

1. Dependency Injection. [Electronic resource] URL: https://en.wikipedia.org/wiki/Dependency_injection . (accessed 17.02.2025).
 2. SOLID [Electronic resource] URL [https://ru.wikipedia.org/wiki/SOLID_\(programming\)](https://ru.wikipedia.org/wiki/SOLID_(programming)). (accessed 02/15/2025).
 3. Domain-driven design [Electronic resource] URL https://en.wikipedia.org/wiki/Domain-driven_design . (accessed 02/16/2025).
 4. Inversion of control [Electronic resource] URL https://en.wikipedia.org/wiki/Inversion_of_control . (accessed 17.02.2025).
 5. Documentation of Dig [Electronic resource] URL <https://pkg.go.dev/go.uber.org/dig> . (accessed 17.02.2025).
 6. Documentation of Fx [Electronic resource] URL <https://pkg.go.dev/go.uber.org/fx> . (accessed 02/18/2025).
 7. Documentation of Wire [Electronic resource] URL <https://pkg.go.dev/github.com/google/wire> (accessed 02/19/2025).
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Николенко А.А.

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

В последние годы наблюдается значительное развитие искусственного интеллекта (ИИ) и интеллектуальных систем управления, что приводит к кардинальным изменениям в различных отраслях и сферах деятельности. Данная статья рассматривает современные тенденции и достижения в области ИИ, включая машинное обучение, обработку естественного языка, компьютерное зрение и многопрофильные интеллектуальные системы. Анализируется влияние ИИ на управление производственными процессами, транспортными системами, энергетическими сетями и другими критически важными секторами. Особое внимание уделено вопросам интеграции ИИ с традиционными системами управления и проблемам, связанным с безопасностью, этикой и правовыми аспектами использования ИИ. В заключение обсуждаются перспективы дальнейшего развития и применения интеллектуальных систем управления в условиях постоянно усложняющегося технологического ландшафта.

Ключевые слова: Искусственный интеллект, система управления, принятие решений, бизнес-стратегия, управление.

ARTIFICIAL INTELLIGENCE AND INTELLIGENT CONTROL SYSTEMS

Nikolenko A.A.

"NATIONAL RESEARCH NUCLEAR UNIVERSITY "MEPHI", Moscow, Russia (115409, Moscow,
Kashirskoye sh., 31 e-mail: alexander.nikolenko.lawyer@gmail.com

In recent years, there has been a significant development of artificial intelligence (AI) and intelligent control systems, which leads to fundamental changes in various industries and fields of activity. This article examines current trends and advances in AI, including machine learning, natural language processing, computer vision, and multidisciplinary intelligent systems. The impact of AI on the management of production processes, transport systems, energy networks and other critical sectors is analyzed. Particular attention is paid to the integration of AI with traditional management systems and issues related to safety, ethics and legal aspects of the use of AI. Finally, the prospects for further development and application of intelligent control systems in an increasingly complex technological landscape are discussed.

Keywords: Artificial intelligence, management system, decision making, business strategy, management.

Введение

Интеграция искусственного интеллекта (ИИ) в процессы принятия решений является важнейшим событием в бизнесе и управлении, которое глубоко меняет бизнес-стратегии и операции. ИИ, с его способностью анализировать большие наборы данных, учиться на этой информации и принимать решения автономно или при поддержке лиц, принимающих решения, обеспечивает значительное конкурентное преимущество компаниям, которые его

внедряют. Однако это достижение также порождает этические и технические проблемы, требующие тщательного рассмотрения его ответственного использования при принятии бизнес-решений.

Потенциал ИИ для поддержки принятия решений огромен. Способность ИИ обрабатывать и анализировать огромные объемы данных обеспечивает беспрецедентную эффективность и точность. Несмотря на широко распространенное мнение, что основные стратегические решения являются исключительной прерогативой людей, всего через пять лет все важные бизнес-решения будут поддерживаться когнитивными технологиями, подчеркивая важность объединения когнитивных технологий.

Внедрение алгоритмов в процессах принятия решений менеджерами требует доверия к этим технологиям. Исследования показывают, что алгоритмы превосходят людей во многих ситуациях принятия решений, особенно когда дело касается задач долгосрочного планирования, но их внедрению по-прежнему препятствует ряд факторов, включая чрезмерную уверенность в собственных способностях менеджеров, страх перед заменой и проблемы конфиденциальности.

Алгоритмическое принятие решений, которое называют *«алгоритмическим управлением»*, меняет природу рутинных решений на рабочем месте. Работники, руководствуясь сложным алгоритмическим анализом, должны перемещаться по этой информации через упрощенные пользовательские интерфейсы, чтобы принимать обоснованные решения. Хотя алгоритмы приобретают все большее значение в принятии решений, функция алгоритмов при принятии решений сместилась от описательного к прогнозирующему и предписывающему режимам в оперативной и стратегической областях. Алгоритмы обучения, часто называемые искусственным интеллектом или *«когнитивными системами»*, находят свое место в принятии решений на рабочем месте, считаясь формой автоматизации анализа данных, где алгоритмы на основе машинного обучения улучшают процесс принятия решений. процессы с течением времени без вмешательства человека, что приводит к потере контроля над деятельностью человека. Однако крайне важно признать, что для достижения оптимальной эффективности эти алгоритмические модели должны обязательно интегрировать человеческий опыт, знания и эмоции, которые остаются неуловимыми для алгоритмов. Этот детальный подход напоминает о важности синергетического сотрудничества между алгоритмическими способностями и человеческой интуицией, тем самым признавая незаменимую ценность человеческого суждения в процессе принятия решений.

Вторя наблюдениям о важности управления данными в современной экономике, недавнее исследование подчеркивает широко распространенный оптимизм в отношении потенциальных преимуществ ИИ для организаций. По данным исследования, большинство респондентов верят, что ИИ принесет значительную выгоду их организации, будь то за счет создания новых возможностей для бизнеса или сокращения затрат. В частности, 84% участников считают, что ИИ позволит им получить или сохранить конкурентное преимущество. Столь высокий уровень уверенности в потенциале ИИ отражает растущее признание его стратегической роли в повышении операционной эффективности и совершенствовании процесса принятия решений в рамках различных организационных функций. Эти выводы подчеркивают необходимость того, чтобы организации стали ориентироваться на данные и использовать передовую аналитику, чтобы оставаться

конкурентоспособными в быстро меняющейся экономической ситуации [5].

Быстрое внедрение ИИ, демонстрируя его многочисленные количественные преимущества в обучении и прогнозировании, требует адекватного понимания его сильных и слабых сторон в процессе принятия организационных решений. Эта критическая перспектива создает основу для подчеркивания критической важности ИИ в совершенствовании процессов принятия бизнес-решений, одновременно подчеркивая необходимость сбалансированного подхода. Этот подход должен не только признать преимущества и проблемы ИИ, но и способствовать продуктивному синергизму между человеческим и искусственным интеллектом.

Методология исследования

Появление прорывных технологий глубоко изменило организационный ландшафт, катализируя радикальные изменения в том, как компании разрабатывают и реализуют свои стратегии принятия решений. Среди этих технологий искусственный интеллект выделяется как одна из наиболее влиятельных движущих сил, переопределяющих традиционные парадигмы управления и принятия решений. Последние годы были отмечены быстрым технологическим прогрессом, в частности появлением искусственного интеллекта и других современных технологий для информационных систем. Ряд исследователей подчеркивают растущую важность ИИ в управлении организациями, его возможность способствовать эффективному сотрудничеству между персоналом и автоматизированными системами для оптимизации процесса принятия решений [1, 3, 4].

Способность принимать обоснованные решения стала решающей для успеха организаций, особенно после того, как большинство организаций сейчас интегрируют ИИ в свои процессы принятия решений. Эта интеграция направлена на использование расширенных возможностей анализа данных и решения проблем, предлагаемых ИИ, для достижения беспрецедентного уровня точности и аккуратности принятия решений. Однако внедрение ИИ не всегда гарантирует повышение производительности. В некоторых случаях неспособность в полной мере воспользоваться преимуществами ИИ может быть связана с непониманием его механизмов и потенциального влияния на бизнес-операции руководителями.

Несмотря на эти проблемы, участие ИИ в процессах принятия решений продолжает набирать обороты, о чем свидетельствует исследование Института IBM *по оценке ценности бизнеса* совместно с *Oxford Economics*, показавшее, что 40% из 3000 опрошенных руководителей используют генеративный ИИ для совершенствования своих решений. процессы создания [4]. Столкнувшись со все более сложными и важными решениями, особенно по использованию искусственного интеллекта в своих структурах, бизнес-лидеры чувствуют повышенное давление, заставляющее их правильно делать свой выбор.

Затраты, связанные с неправильным принятием решений, значительны и составляют в среднем не менее 3% прибыли бизнеса. Последствия не ограничиваются финансовой сферой; плохое управление взаимодействием с клиентами или операционными инцидентами может привести к значительным репутационным и нормативным издержкам. В этом контексте компании все чаще обращаются к искусственному интеллекту, чтобы преодолеть разрыв между доступными данными и знаниями, необходимыми для улучшения процесса принятия решений в условиях высокого давления.

Эта эволюция приводит к центральному размышлению о реальном влиянии ИИ на

процессы принятия решений в различных секторах. Эта целенаправленная работа направлена на изучение того, как ИИ трансформирует механизмы принятия решений, влияет на глобальную стратегию, культуру и организационную структуру. Подчеркивая преимущества ИИ, такие как повышение эффективности и точности, важно учитывать проблемы, связанные с его интеграцией, включая этические вопросы, управление изменениями и развитие навыков. Посредством тематических исследований и экспертного анализа эта целенаправленная работа направлена на предоставление всестороннего обзора текущей практики и будущих тенденций использования ИИ в бизнес-решениях, руководствуясь следующим вопросом: как внедрение ИИ конкретно меняет процессы и стратегии принятия решений в компании из разных отраслей? Какие последствия цифровая трансформация имеет для эффективности и точности операций и какие проблемы она представляет?

Целью статьи является информирование лиц, принимающих решения, практиков и исследователей о возможностях оптимизации использования ИИ в бизнесе с учетом проблем, которые представляет такая эволюция.

Методология, принятая в этой направленной работе, основана на углубленном обзоре научной литературы, касающейся интеграции ИИ в процессы принятия стратегических и оперативных решений компаний. Чтобы структурировать обзор литературы, используется метод интегративного обзора литературы, который предлагает методологическую основу для систематического анализа и синтеза данных. Этот подход направлен на обеспечение целостного понимания изучаемого предмета, тем самым позволяя комплексную концептуализацию влияния ИИ на бизнес-решения.

Для подготовки обзора было изучено более шестидесяти статей и работ, опубликованных в период с 1991 по 2023 годы. Ссылки, цитируемые в этих публикациях, также были изучены для дальнейшего обогащения анализа.

Для поиска литературы использовались признанные академические базы данных, включая, помимо прочего, *Google Scholar*, *ScienceDirect*, *Cairn*, *ResearchGate*, *Semantic Scholar*, чтобы найти соответствующие публикации. Для обеспечения инклюзивности были использованы конкретные ключевые слова и фразы на английском и французском языках, имеющие непосредственное отношение к пересечению практики принятия решений и искусственного интеллекта (ИИ).

Обзор литературы

История и эволюция ИИ отмечены впечатляющими достижениями, периодами застоя и глубокими философскими и этическими дебатами. От своего теоретического происхождения до повсеместного распространения в современном обществе ИИ не только произвел революцию в том, как мы взаимодействуем с технологиями, но и поднял фундаментальные вопросы о том, что значит быть человеком.

Однако именно в XX веке ИИ по-настоящему начал формироваться как научная дисциплина. Алана Тьюринга, британского математика, часто называют отцом вычислений и искусственного интеллекта. В 1950 году Тьюринг опубликовал статью «*Вычислительная техника и интеллект*», в которой представил знаменитый тест Тьюринга — мысленный эксперимент, предназначенный для оценки способности машины имитировать человеческий интеллект [7].

1950-е и 1960-е годы ознаменовали начало ИИ как официальной области исследований.

Летняя конференция 1956 года в Дартмутском колледже считается отправной точкой для ИИ как формальной [1]. Эта конференция собрала исследователей, которые изучали возможность моделирования каждого аспекта обучения или любой другой характеристики интеллекта, чтобы можно было спроектировать машину, имитирующую его. Именно на этой конференции впервые был использован термин «искусственный интеллект» [3]. За этот период был достигнут значительный прогресс, особенно в разработке программ, способных решать логические задачи и учиться на опыте [2].

Начиная с конца 1990-х годов и особенно в начале XXI века, искусственный интеллект переживает период возрождения, обусловленный достижениями в алгоритмах машинного обучения, экспоненциальным увеличением вычислительной мощности и доступом к большим объемам данных. Глубокое обучение, отрасль машинного обучения, вдохновленная функционированием нейронных сетей в человеческом мозге, привела к значительному прогрессу в распознавании речи, компьютерном зрении и обработке естественного языка [5].

Сегодня искусственный интеллект интегрирован во многие аспекты повседневной жизни: от интеллектуальных личных помощников и систем рекомендаций на потоковых платформах до достижений в области автономного вождения и персонализированной медицины. Однако эта растущая интеграция поднимает важные этические и социальные вопросы, особенно в отношении конфиденциальности, безопасности, занятости и алгоритмической предвзятости [6].

Будущее ИИ обещает как невероятные инновации, так и сложные задачи. Поскольку технологии продолжают развиваться, обществу необходимо ориентироваться в потенциальных преимуществах ИИ и рисках, которые он представляет для социальных, экономических и политических структур. Продолжаются дебаты о том, как разработать этичный, прозрачный и ответственный ИИ, который улучшит общество, не принося в жертву человечность.

Область ИИ включает в себя широкий спектр концепций и методов. Понимание этих концепций необходимо для понимания функционирования и потенциала ИИ.

Машинное обучение — это важнейшая отрасль искусственного интеллекта, целью которой является предоставление машинам возможности учиться на основе данных, чтобы делать выводы, прогнозировать и выявлять ассоциации, которые могут определять решения [5]. В этой области основное внимание уделяется разработке методов, которые позволяют компьютерам обучаться на основе входных данных и обнаруженных закономерностей, используя алгоритмы для выявления закономерностей и обработки больших объемов данных (*большие данные*). Благодаря этому процессу машинное обучение создает среду самообучения, которая становится все более умной, автоматизируя повторяющиеся задачи на основе обучения ИИ и повторяя их по мере необходимости [5].

В основе машинного обучения лежит способность машины постоянно улучшать свою производительность, при этом людям не нужно точно объяснять, как выполнить все поставленные перед ней задачи. В последние годы эта возможность значительно улучшилась и демократизировалась, что позволило создавать системы, способные обучаться автономному выполнению задач. Машинное обучение применяется для выявления объяснительных механизмов, закономерностей и правил в больших наборах данных, обобщая методы, которые позволяют системам ИИ обучаться без явного программирования на такие результаты обучения [4]. Таким образом, хотя машинное обучение является фундаментальной частью ИИ,

оно является лишь его частью, поскольку ИИ также обладает способностью воспринимать данные посредством распознавания изображений и голоса или, например, обработки естественного языка. *«Глубокое обучение»*, часто используемое как синоним *«машинного обучения»*, представляет собой подотрасль, основанную на нейронных сетях, то есть компьютерных системах, имитирующих биологические нейронные сети, составляющие человеческий мозг.

Искусственные нейронные сети, вдохновленные функционированием человеческого мозга, представляют собой краеугольный камень в эволюции искусственного интеллекта и *машинного обучения*.

Технический прогресс заложил основу для множества практических приложений, продемонстрировав универсальность и способность нейронных сетей подходить и решать сложные проблемы в различных областях. Например, в робототехнике нейронные сети обеспечивают автономную навигацию и интеллектуальное взаимодействие с окружающей средой путем обработки сенсорных данных в реальном времени [4].

Эти примеры подчеркивают важность обратного распространения ошибки и искусственных нейронных сетей в развитии технологий искусственного интеллекта, открывая путь для дальнейших инноваций и исследования новых границ в практических исследованиях и применениях. Их способность учиться и обобщать данные делает эти модели особенно эффективными для обработки сложной информации, начиная от распознавания образов и сигналов и заканчивая прогнозным моделированием во множестве контекстов.

Результаты исследования: принятие решений с помощью искусственного интеллекта – концептуальная основа и организационный контекст

Сближение теории ограниченной рациональности с современными разработками в области искусственного интеллекта в процессе принятия организационных решений открывает богатые возможности для исследований [4-5]. Эти исследования показывают, как ИИ и ограниченная рациональность дополняют и противостоят друг другу при принятии решений.

Когнитивные ограничения относятся к внутренним ограничениям когнитивных способностей человека, таким как память, внимание и вычислительные навыки, которые ограничивают диапазон и глубину информации, которая может быть обработана. *Дефицит информации* относится к реальности лиц, принимающих решения, которым часто приходится работать с неполными или несовершенными данными. Такая ситуация усложняет поиск оптимальных решений. Кроме того, *нехватка времени* добавляет еще один уровень сложности, часто вынуждая отдельных лиц и организации выбирать удовлетворительные решения – достаточно хорошие, но не обязательно оптимальные.

Даже с учетом вклада ИИ эти ограничения сохраняются, подчеркивая, что рациональность решений, принимаемых с помощью ИИ, всегда ограничена человеческими и технологическими ограничениями.

С другой стороны, интеграция ИИ влияет на организационные структуры принятия решений. Ряд исследователей разрабатывают инновационную структуру для оптимального сочетания принятия решений человеком и искусственным интеллектом, подчеркивая взаимодополняемость человеческой интуиции и аналитической силы искусственного интеллекта [2-3]. С этой целью они описывают ключевые условия принятия решений в

организационном контексте с участием ИИ и людей.

Таблица 1 – Сравнение принятия решений на основе VIA и принятия решений человеком

Условия принятия решения	Принятие решений на основе искусственного интеллекта	Принятие решений человеком
Специфика пространства поиска решений	Требуется четко определенное пространство поиска решений с конкретными целями.	Адаптируется к гибко определяемому пространству поиска решений
Интерпретируемость процесса принятия решения и результата	Сложность функциональных форм может затруднить интерпретацию процесса принятия решения и его результатов.	Решения объяснимы и интерпретируемы, хотя и уязвимы для ретроспективного анализа.
Размер множества альтернатив	Может вместить большие наборы альтернатив	Ограниченная способность единообразно оценивать большой набор альтернатив.
Скорость принятия решений	Сравнительно быстро. Ограниченный компромисс между скоростью и точностью	Сравнительно медленный. Существенный компромисс между скоростью и
Воспроизводимость результатов	Процесс принятия решений и результаты имеют высокую воспроизводимость благодаря стандартизированной ИТ-процедуре.	Воспроизводимость уязвима к меж- и внутрииндивидуальным различиям, различиям во внимании, контексте и эмоциональном состоянии

Структура, предложенная автором, призвана проиллюстрировать, как оптимально сочетать решения, принимаемые человеком и искусственным интеллектом, для повышения качества принятия организационных решений. Они описывают три структурные категории, обеспечивающие такую комбинацию: полное делегирование от человека к ИИ, гибридное последовательное принятие решений (от человека к ИИ и от ИИ к человеку) и агрегированное принятие решений от человека к ИИ.

Объединение этих точек зрения раскрывает сложную картину, в которой ИИ, несмотря на свой потенциал расширения возможностей принятия решений, не устраняет присущие человеку ограничения принятия решений, примером которых является теория ограниченной рациональности. Поэтому интеграция ИИ в процессы принятия решений требует детального понимания его сильных и слабых сторон, понимания когнитивных и информационных ограничений, которые определяют человеческую рациональность, а также адаптированной организационной структуры принятия решений, с помощью которой люди и ИИ учатся сотрудничать для принятия оптимальных решений.

Анализ влияния ИИ на принятие решений в организациях не нов: Лоуренс (1991) предложил детальный анализ, который изучает взаимосвязь между технологиями ИИ и аспектами принятия решений, а также всесторонне исследует, как технологии ИИ влияют не только на них. сложность процессов принятия решений, но также их политическая природа и

динамика власти внутри организаций.

Говоря о сложности решений, Лоуренс (1991) признает, что ИИ может радикально изменить способ обработки информации и принятия решений, предоставляя инструменты, способные обрабатывать огромные объемы данных [6]. Эти инструменты могут снизить воспринимаемую сложность, упрощая анализ и интерпретацию данных, позволяя лицам, принимающим решения, более эффективно ориентироваться в ситуациях, которые ранее считались слишком сложными. Например, экспертные системы, объединяя специализированные знания и предоставляя конкретные рекомендации, могут упростить сложные проблемы и сделать процесс принятия решений менее трудным.

В то же время внедрение ИИ в процессы принятия решений может также усилить политизацию решений. Политизация относится к тому, как власть и влияние влияют на процесс принятия решений внутри организаций. ИИ может изменить существующий баланс сил, перераспределив доступ к информации и изменив способы оценки и использования знаний. Например, доступ к системам обработки естественного языка, которые позволяют извлекать и анализировать информацию из больших текстовых баз данных, может дать значительное преимущество определенным группам или отдельным лицам, тем самым влияя на внутреннюю политическую динамику.

Процессы принятия решений жизненно важны для эффективности и производительности организации, поэтому неудивительно, что многие исследования были направлены на улучшение качества принятия решений за счет использования технологий для расширения человеческих возможностей. Недавние разработки в области искусственного интеллекта сделали эту цель возможной в различных приложениях. Например, *интеллектуальные* системы поддержки принятия решений (IDSS) расширяют сферу применения и эффективность систем поддержки принятия решений (*DSS*) и постепенно используются для содействия процессу принятия решений в различных областях, таких как маркетинг и кибербезопасность [7]. Исследование признает принятие решений фундаментальной человеческой деятельностью и изучает, как ИИ может помогать или поддерживать людей в принятии «хороших» решений.

IDSS предназначены для интеграции ИИ в разработку альтернатив, тем самым улучшая процесс принятия решений, особенно в режиме реального времени и в сложных средах, особенно во время анализа: [...] приложения могут помочь лицу, принимающему решения, выбрать подходящее действие в режиме реального времени в стрессовых условиях, предоставляя доступ к актуальной информации, снижая информационную перегрузку и обеспечивая динамическое реагирование [2].

Можно сделать вывод, что следующие управленческие навыки будут иметь решающее значение для эффективного сотрудничества с ИИ:

- Понимание ИИ: базовые знания о принципах, возможностях и ограничениях ИИ.
- Навыки анализа данных: способность понимать и интерпретировать данные, генерируемые системами искусственного интеллекта, для принятия обоснованных решений.
- Управление изменениями: способность проводить организационные преобразования, необходимые для интеграции ИИ в повседневную деятельность.
- Лидерство в инновациях: способность продвигать культуру инноваций и поощрять внедрение новых технологий, таких как искусственный интеллект.

- Коммуникационные навыки: Эффективность информирования всех заинтересованных сторон о преимуществах и последствиях ИИ.
- Критическое и этическое мышление: способность оценивать этические последствия внедрения ИИ и принимать ответственные решения.
- Адаптивность и непрерывное обучение: открытость и готовность постоянно учиться, чтобы адаптироваться к разработкам в области искусственного интеллекта.
- Управление рисками: способность выявлять, оценивать и снижать риски, связанные с использованием ИИ в бизнес-процессах.

Эти навыки отражают необходимость для менеджеров не только понимать технологию искусственного интеллекта, но и управлять ее интеграцией в постоянно меняющуюся рабочую среду, уделяя особое внимание инновациям, этике и эффективному общению.

Заключение

ИИ оптимизирует обмен и распространение знаний, персонализируя процесс обучения сотрудников. Рекомендательные системы на базе искусственного интеллекта могут направлять пользователей к ресурсам, адаптированным к их индивидуальным потребностям и предпочтениям, способствуя непрерывному обучению и интеграции лучших практик. Платформы для совместной работы, обогащенные искусственным интеллектом, также способствуют обмену идеями и командной работе, укрепляя организационную культуру, основанную на обмене знаниями.

ИИ играет решающую роль в совершенствовании процесса принятия управленческих решений. С помощью прогнозной и предписывающей аналитики, основанной на накопленных знаниях, ИИ может предлагать сценарии будущего, оценивать риски и предлагать стратегии действий. Этот процесс существенно помогает лицам, принимающим решения, формулировать обоснованные решения, основанные на всестороннем понимании исторических данных и текущих тенденций бизнеса.

ИИ может служить мощным рычагом управления знаниями, тем самым стимулируя принятие более информированных и стратегических управленческих решений. Их работа подчеркивает необходимость срочного использования организациями потенциала искусственного интеллекта, чтобы успешно ориентироваться в эпоху постоянного информирования и инноваций.

Список литературы

1. Андреев В.К. Динамика правового регулирования применения искусственного интеллекта // Журнал российского права. – 2020. – N 3. – СПС ГАРАНТ
2. Емелин И.А. Глобальные тренды и ориентиры развития // Государственная служба. – 2019. – №1 (117). – URL: <https://cyberleninka.ru/article/n/globalnye-trendy-i-orientiry-razvitiya>
3. Карцхия А.А. Искусственный интеллект как средство управления в условиях глобальных рисков // Мониторинг правоприменения. – 2020. – №1 (34). – URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-kak-sredstvo-upravleniya-v-usloviyah-globalnyh-riskov>

4. Лаптев В.А. Перспективы применения технологии блокчейн в сфере корпоративных реестров для бизнеса в России // Предпринимательское право. – 2019. – N 3. – С. 23 - 28. – URL: Документ в СПС КонсультантПлюс
5. Попова Е.В. Российский опыт внедрения искусственного интеллекта в менеджмент предприятия // Инновации и инвестиции. – 2023. – №6. – URL: <https://cyberleninka.ru/article/n/rossiyskiy-opyt-vnedreniya-iskusstvennogo-intellekta-v-menedzhment-predpriyatiya>
6. Lawrence N. D. The atomic human: Understanding ourselves in the age of AI. – Random House, 2024.
7. McCollum T. audit in an age of intelligent machines. (cover story). Internal Auditor [Internet]. 2017 Dec [cited 2023 Oct 25];74(6):24–9. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=128494686&lang=ru>
8. Molloy BT. Project Governance for Defense Applications of Artificial Intelligence: An Ethics-Based Approach. PRISM Security Studies Journal [Internet]. 2021 Nov [cited 2023 Oct 25];9(3):106–20. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=155011456&lang=ru>

References

1. Andreev V.K. Dynamics of legal regulation of the use of artificial intelligence // Journal of Russian Law. – 2020. – N 3. – SPS GARANT
 2. Emelin I.A. Global trends and development guidelines // Public service. – 2019. – №1 (117). – URL: <https://cyberleninka.ru/article/n/globalnye-trendy-i-orientiry-razvitiya>
 3. Kartskhiya A.A. Artificial intelligence as a management tool in the context of global risks // Law enforcement monitoring. – 2020. – №1 (34). – URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-kak-sredstvo-upravleniya-v-usloviyah-globalnyh-riskov>
 4. Laptev V.A. Prospects for the use of blockchain technology in the field of corporate registries for business in Russia // Business law. – 2019. – N 3. – pp. 23-28. - URL: Document in the SPS ConsultantPlus
 5. Popova E.V. The Russian experience of introducing artificial intelligence into enterprise management // Innovation and investment. – 2023. – №6. – URL: <https://cyberleninka.ru/article/n/rossiyskiy-opyt-vnedreniya-iskusstvennogo-intellekta-v-menedzhment-predpriyatiya>
 6. Lawrence N. D. The atomic human: Understanding ourselves in the age of AI. – Random House, 2024.
 7. McCollum T. audit in an age of intelligent machines. (cover story). Internal Auditor [Internet]. 2017 Dec [cited 2023 Oct 25];74(6):24–9. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=128494686&lang=ru>
 8. Molloy BT. Project Governance for Defense Applications of Artificial Intelligence: An Ethics-Based Approach. PRISM Security Studies Journal [Internet]. 2021 Nov [cited 2023 Oct 25];9(3):106–20. Available from: <https://search.ebscohost.com/login.aspx?direct=true&db=lgs&AN=155011456&lang=ru>
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.38

МЕТОДЫ РАЗРЕШЕНИЯ ОБЪЕКТОВ И СИГНАЛОВ ДЛЯ ПРИМЕНЕНИЯ В СОВРЕМЕННЫХ ИЗМЕРИТЕЛЬНЫХ РТС

Коптев В.А.

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФГБОУ ВО "МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ", Москва, Россия, (111024, город Москва, Авиамоторная ул., д.8а), e-mail: yyy.xxx.98@bk.ru

В данной статье описываются классические методы определения углового направления на источник электромагнитного излучения. Определены их фундаментальные ограничения и недостатки. И сделано заключение, что в целях повышения разрешающей способности по угловым координатам необходимо использовать алгоритмы сверхразрешения.

Ключевые слова: разрешение Объектов, измерительные РТС, моноимпульсная радиолокация, сверхразрешение, разрешающая способность.

METHODS FOR RESOLVING OBJECTS AND SIGNALS FOR USE IN MODERN MEASURING RTAS

Koptev V.A.

OF THE ORDER OF THE RED BANNER OF LABOR OF THE MOSCOW TECHNICAL UNIVERSITY OF COMMUNICATIONS AND INFORMATICS, Moscow, Russia, (111024, Moscow, Aviamotornaya str., 8a), e-mail: yyy.xxx.98@bk.ru

This article describes classical methods for determining the angular direction of an electromagnetic radiation source. Their fundamental limitations and disadvantages are identified. And it is concluded that in order to increase the resolution in angular coordinates, it is necessary to use super-resolution algorithms.

Keywords: Object resolution, measuring RTDS, monopulse radar, super resolution, resolution.

Традиционные методы разрешения объектов и сигналов.

В современной обстановке обилия излучателей электромагнитных волн (ЭМВ) и разного рода помех, актуально стоит задача разделения радиотехническими системами сигналов от нескольких независимых источников [1-3]. Если взять за точку отсчёта приёмную систему – то видится несколько способ для решения данной проблемы [4-5]:

1. Разделение сигналов по физическим параметрам – мощность, амплитуда, частота, фаза, поляризация, тип модуляции.
2. Пространственное разделение сигналов – по угловому направлению прихода сигнала.

Разделение по первому признаку широко распространено в стандартах связи, например, временное и частотное разделение. Поляризационное разделение используется сверхвысокочастотных линий передачи. За разделение принятых сигналов по угловым

координатам, отвечают антенные системы и соответственно, они задают определённые ограничения по разрешению.

Разрешающая способность радиотехнической системы (РТС) по углу определяется способностью разделить два одинаковых источника излучения, с минимальным угловым расстоянием, находящихся на одинаковом удалении (1), рисунок 1. И определяется она шириной диаграммы направленности (ДН) антенны, поэтому, ДН стараются делать как можно уже, но при этом, возрастает время сканирования участка пространства. [6-7]

$$d \geq 2D * \sin\left(\frac{\theta}{2}\right)$$

Где, d – минимальное расстояние между целями, $\theta/2$ – половина угловой ширины ДН, D – дальность до цели.

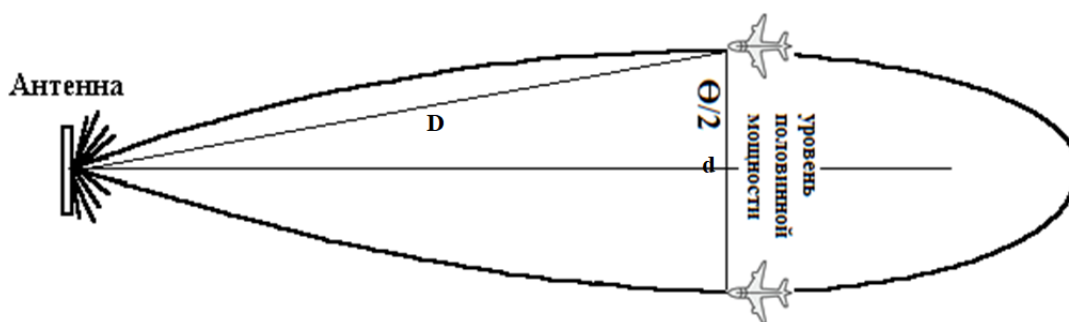


Рисунок 1 – Иллюстрация разрешающей способности антенны

Что бы улучшить определение координат цели, «внутри» ДН, используют определённые методы разрешения объектов и сигналов:

1. *Моноимпульсная радиолокация.* Этот метод основан на сравнении сигналов, одновременно принимаемых двумя антеннами или двумя каналами одной антенны. Для этого антенно-волноводный тракт должен быть специально построен определённым образом, чтобы снимать принятый сигнал с определённым смещением от нормали апертуры. Определение направления на источник определяется как направление, в котором разность амплитуд сигналов или их фаз минимальна – строятся разностные и суммарные диаграммы, что позволяет определить направление на источник сигнала за один импульс, рисунок 2.

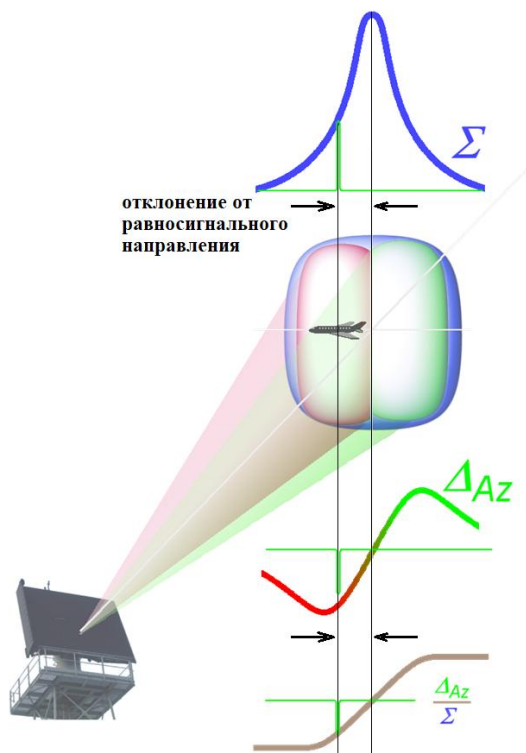


Рисунок 2 – Принцип моноимпульсной радиолокации

Но у этого метода есть весомые недостатки. Не может работать сразу по нескольким целям. Если источник сигнала находятся ближе друг к другу, чем ширина диаграммы направленности антенны, их сигналы сливаются, и определение направления становится невозможной. В условиях сложной радиочастотной обстановки, многолучевые сигналы искажают определение направления прихода. Также метод чувствителен к калибровки антенного тракта - любые отклонения в амплитудно-фазовых характеристиках антенны снижают точность. [5,7]

2. *Амплитудный методы.* Здесь используется зависимость уровня сигнала от угла прихода. Угол направления рассчитывается по амплитуде сигнала, измеренной на диаграмме направленности антенны, где угол определяется положением максимума сигнала, рисунок 3. Основной недостаток метода – низкая точность в условиях шумов и многолучевости. [5,7]

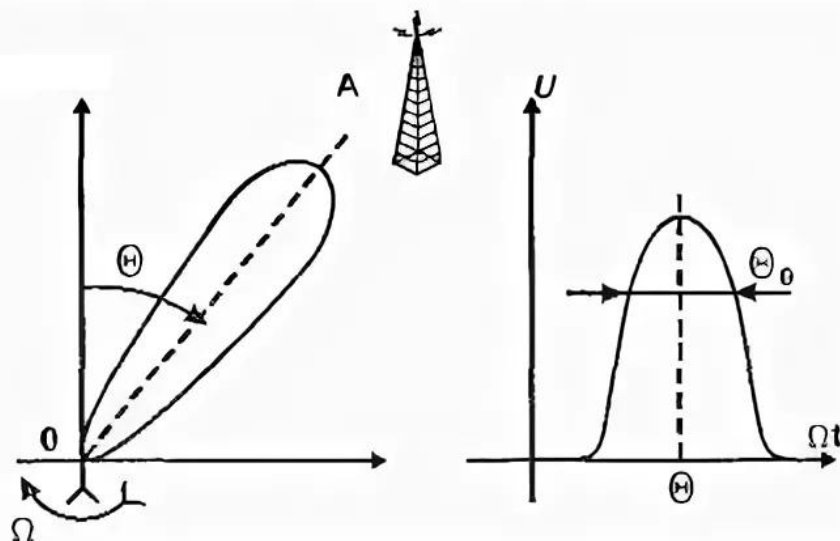


Рисунок 3 – Принцип работы амплитудного метода.

Эти методы демонстрируют ограниченные возможности при работе по нескольким целям и при наличии сильных помех, когда угловое расстояние между источниками меньше предела разрешения. Современные измерительные РТС сталкиваются с фундаментальным ограничением пространственного разрешения, установленным пределом Рэлея – это критерий, который определяет минимальное расстояние между двумя объектами, при котором они могут быть различимы как отдельные источники в системе с ограниченной апертурой (2).[8]

$$\frac{d}{D} > 1,22 \frac{\lambda}{A} \quad (2)$$

Где, d – расстояние между объектами, D – удалённость от наблюдателя, λ – длина волны, A – площадь апертуры, 1,22 – эмпирически найденный коэффициент, для круговой апертуры [8]. Два источника считаются различимыми, если центральный максимум одного совпадает с первым минимумом другого. Если расстояние между источниками меньше предела Рэлея, их дифракционные картины начинают перекрываться настолько, что становится трудно различить их как отдельные, рисунок 4.

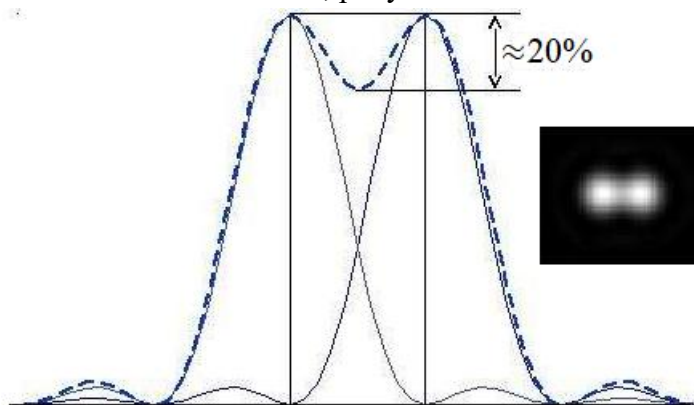


Рисунок 4 – Иллюстрация эффекта от предела Рэлея

Оба методов разрешения объектов и сигналов широко распространены и считаются классическими для радиолокации. Но для разделения источников ЭМВ в сложной радиочастотной среде не представляется возможным. Разрешающая способность продолжает

быть ограничена шириной ДН. Для преодоления этого ограничения разрабатываются методы сверхразрешения, которые позволяют разделять сигналы несмотря на то, что их угловое расстояние меньше необходимого.

Например, рассмотрим два известных метода сверхразрешения. MUSIC и NVDR (метод Кейпона). Их смысл заключается в том, чтобы провести дополнительную пост обработку сигнала, принятого отдельными элементами антенной системы. Следовательно, для работы этих алгоритмов требуется использовать фазированные антенные решётки с независимым подключением элементов решётки к приёмному тракту.

Выводы.

В данной работе были рассмотрены способы радения сигналов при помощи определения углового направления их прихода. Описаны области применения обычных методов разрешения сигналов и объектов и ограничения по разрешающей способности, которые с которыми они сталкиваются. Чтобы их преодолеть, требуется применять алгоритмы сверхразрешения.

Список литературы

1. Колесников Р.А. Зюзин В.Д. Воронцов А.И. Лопухов Р.С. Багажков Д.И. проблема электромагнитной совместимости. электромагнитная обстановка и анализ источников помех для оборудования связи // Инновации и инвестиции. - 2020. - №10. - С. 154-158.
2. Задорожная О.Н. Электромагнитная совместимость, электромагнитные помехи, радиоэлектронное оборудование, электромагнитная обстановка, экранирование, центральный узел связи.: автореф. дис. Инженерно-физический факультет наук: 03.03.02.. - Благовещенск, 2019. - 55 с.
3. Байкенов А.С., Ермекбаев М.М. Электромагнитная совместимость радиоэлектронных средств. - Алматы: Алматинский Университет энергетики и связи имени Гумарбека Даукеева, 2022. - 67 с.
4. Сергиенко А. Б. Цифровая обработка сигналов: учеб. пособие. — 3-е изд. — СПб.: БХВ-Петербург, 2011. — 768 с. — (Учебная литература для вузов)
5. Сперанский В.С. Радиолокация, радиолокационные системы и устройства. – М.: Брис-М, – 2011 – 257 с.,
6. Разрешающая способность по угловым координатам // radartutorial URL: <https://www.radartutorial.eu/01.basics/rb19.ru.html> (дата обращения: 05.01.2025).
7. Моноимпульсная антенна // radartutorial URL: <https://www.radartutorial.eu/06.antennas/an41.ru.html> (дата обращения: 05.01.2025).
8. Критерий Рэлея // Элементы URL: https://elementy.ru/trefil/33/Kriteriy_Releya?ysclid=m6b55i2wgy769205288 (дата обращения: 07.01.2025).
9. Capon, Jack. "High-resolution frequency-wavenumber spectrum analysis." Proceedings of the IEEE 57, no. 8 (1969): pp.1408-1418.
10. Schmidt R.O. Multiple Emitter Location and Signal Parameter Estimation // IEEE Transactions on Antennas and Propagation. — 1986. — Vol. 34, No. 3. — pp. 276–280.

References

1. Kolesnikov R.A. Zyuzin V.D. Vorontsov A.I. Lopukhov R.S. Baggage D.I. The problem of electromagnetic compatibility. electromagnetic environment and analysis of interference sources for communication equipment // Innovations and investments. 2020. No. 10. pp. 154-158.
 2. Zadorozhnaya O.N. Electromagnetic compatibility, electromagnetic interference, radioelectronic equipment, electromagnetic environment, shielding, central communications center.: abstract of the dissertation. Faculty of Engineering and Physics of Sciences: 03.03.02.-Blagoveshchensk, 2019. - p.55
 3. Baikenov A.S., Ermekbaev M.M. Electromagnetic compatibility of radioelectronic devices. Almaty: Gumarbek Daukeev Almaty University of Energy and Communications, 2022. 67 p.
 4. Sergienko A. B. Digital signal processing: textbook. stipend. — 3rd ed. — St. Petersburg: BHV-Petersburg, 2011. — p. 768— (Educational literature for universities)
 5. Speransky V.S. Radar, radar systems and devices. Moscow: Bris-M, 2011— p.257
 6. Angular resolution // radartutorial URL: <https://www.radartutorial.eu/01.basics/rb19.ru.html> (date of request: 05.01.2025).
 7. Monopulse antenna // radartutorial URL: <https://www.radartutorial.eu/06.antennas/an41.ru.html> (date of reference: 05.01.2025).
 8. Rayleigh's criterion // URL elements: https://elementy.ru/trefil/33/Kriteriy_Releya?ysclid=m6b55i2wgy769205288 (accessed: 01/07/2025).
 9. Capon, Jack. "High-resolution frequency-wavenumber spectrum analysis." Proceedings of the IEEE 57, no. 8 (1969): 1408-1418.
 10. Schmidt R.O. Multiple Emitter Location and Signal Parameter Estimation // IEEE Transactions on Antennas and Propagation. — 1986. — Vol. 34, No. 3. — pp. 276–280.
-



Международный журнал информационных технологий и
энергоэффективности

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



УДК 004.451

СПОСОБ НАСТРОЙКИ NETWORK MANAGER С ПОМОЩЬЮ КОНСОЛИ

¹ Евлоев И. А., ²Викторов Д. Н.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail: ¹evloev.islam.ink@gmail.com, ²daniilviktorov28@gmail.com

Статья посвящена руководству по настройке домашней сети компьютера в операционной системе Linux с помощью Network Manager и через консоль, для чего будет использована такая утилита, как nmcli. Настройка будет происходить на виртуальной машине и операционной системе РЕД ОС. В статье приведена небольшая информация о внутреннем устройстве Network Manager. Для примера настройки будут рассмотрены возможности использования DHCP, DNS, Wi-Fi и базовое управление различными подключениями.

Ключевые слова: Linux, Network Manager, nmcli, настройка сети.

HOW TO CONFIGURE NETWORK MANAGER USING THE CONSOLE

¹ Evloev I. A., ²Viktorov D. N.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: ¹evloev.islam.ink@gmail.com, ²daniilviktorov28@gmail.com

The article is devoted to a guide on how to set up a computer's home network in the Linux operating system using Network Manager and through the console, for which a utility such as nmcli will be used. The configuration will take place on the virtual machine and the RED OS operating system. The article provides a little information about the internals of Network Manager. For an example of configuration, we will look at the possibilities of using DHCP, DNS, Wi-Fi, and basic management of various connections.

Keywords: Linux, Network Manager, nmcli, network configuration.

ВВЕДЕНИЕ

Network Manager — это популярный инструмент для управления сетевыми подключениями в операционных системах на базе Linux. Он предоставляет удобный интерфейс для настройки различных сетевых параметров, но бывают ситуации, когда окружение рабочего стола не запускается, и нужно поднимать сеть из консоли, или нужно настроить сеть на сервере, где не установлено рабочее окружение [1].

Соответственно, настройка Network Manager через консоль может быть полезна в случаях серверных и облачных решений, а также этот способ позволяет использовать скрипты для автоматической настройки и устранения неисправностей.

Сам проект по Network Manager был инициирован компанией Red Hat, а сейчас активно поддерживается различными Linux-дистрибутивами и имеет официальный проект в GitHub. Над его созданием участвовали такие люди, как Дэн Уильямс — ведущий разработчик и один

из основателей, и Роберт Маккуин — человек, работавший над созданием интерфейсов и инструментов для взаимодействия с сетевыми настройками через командную строку, включая такие утилиты, как `nmcli`.

Network Manager помог решить несколько важных научных и технических проблем в области настройки сетевых подключений в Linux. Среди решённых проблем можно выделить автоматизацию настройки сетевых соединений, поддержку множества типов сетевых интерфейсов и повышение безопасности. В результате использования Network Manager значительно улучшилась как удобство для пользователей, так и возможности для системных администраторов, что сделало Linux более удобной и безопасной операционной системой для работы с сетью.

Сетевые технологии развиваются с огромной скоростью. Появляются новые протоколы и стандарты, такие как Wi-Fi 7, 5G, IPv6, а также новые методы шифрования и аутентификации, которые требуют соответствующей поддержки со стороны инструментов управления сетью. Вопрос заключается в том, насколько Network Manager сможет оперативно интегрировать новые технологии и стандарты.

В условиях растущих угроз безопасности и повышенных требований к конфиденциальности, настройка безопасных сетевых соединений остается одной из самых важных проблем. Network Manager поддерживает большинство методов и протоколов сетевой безопасности, включая WPA/WPA2/WPA3 (персональные и корпоративные), проводной 802.1x, MACsec и VPN. Network Manager также хранит сетевые секреты, такие как ключи шифрования и информацию для входа в систему, в безопасном хранилище: в связке ключей пользователя для пользовательских подключений или в защищённом хранилище с обычными правами системного администратора (например, `root`) для подключений на уровне системы [2]. Несмотря на широкую поддержку шифрования, важным вопросом остается возможность интеграции новых стандартов безопасности и адаптации к меняющимся условиям угроз.

Объектом исследования является *процесс настройки и управления сетевыми соединениями в операционных системах на базе Linux*.

Предметом исследования является тот самый *процесс настройки и управления через командную строку с использованием инструментов Network Manager*.

Цель данного исследования — рассмотреть способ настройки Network Manager в Linux через консоль.

Литературный обзор

Известно, что Network Manager состоит из двух компонентов:

- демон NetworkManager, собственно программное обеспечение, которое управляет подключениями и сообщает об изменениях в сети;
- несколько графических интерфейсов для различных графических сред рабочего стола, таких как GNOME Shell, GNOME Panel, KDE Plasma Workspaces, Cinnamon и др [3].

Компоненты взаимодействуют через D-Bus. NetworkManager работает с ним, чтобы обнаруживать и настраивать сетевые интерфейсы, когда они подключены к компьютеру с Linux [4].

D-Bus — это промежуточное программное обеспечение, ориентированное на передачу сообщений, механизм, который обеспечивает связь между несколькими процессами, запущенными одновременно на одном компьютере [5].

Архитектура Network Manager также включает три слоя:

- Сетевой слой. Взаимодействует непосредственно с сетью. Содержит функции обнаружения сети и опроса [6].
- Уровень данных. Хранит данные топологии, полученные при обнаружении сети, и данные событий, полученные при опросе сети [6].
- Уровень визуализации. Предоставляет инструменты, которые нужны операторам и администраторам для просмотра топологии, событий и запуска инструментов устранения неполадок в сети [6].

Утилита `nmcli` — многофункциональный и гибкий инструмент командной строки для настройки сети с помощью Network Manager из консоли. Её синтаксис состоит из: «`nmcli` опции объект команда».

В `nmcli` чаще всего используются такие объекты:

- `device` — управление сетевыми интерфейсами;
- `connection` — управление соединениями;
- `networking` — управление сетью в целом;
- `general` — показывает состояние всех сетевых протоколов и NetworkManager в целом;
- `radio` — управление сетевыми протоколами, `wifi`, `ethernet` и т. д.

Среди используемых определений в статье можно встретить:

Таблица маршрутизации — электронная таблица, хранящаяся на маршрутизаторе, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора.

DHCP соединение — сетевой протокол, который позволяет автоматически назначать подключаемым к сети устройствам IP-адреса.

DNS сервер — специальный сервер, на котором хранятся и кэшируются записи с информацией о IP-адресах сайтов.

Wi-Fi — технология беспроводной локальной сети, позволяющая устройствам обмениваться данными по радиоволнам.

Шлюз — устройство, позволяющее коммуницировать между собой сетям, построенным на основе разных протоколов и технологий.

По ходу статьи следует убедиться, действительно ли настройка Network Manager через консоль способна быть удобной и полезной.

Методы исследования

Тип исследования статьи — описательно-аналитическое руководство. Она направлена на описание способа настройки Network Manager в консоли.

К методам сбора данных можно отнести изучение документации и анализ статей с схожей тематикой.

Вся процедура проведения исследования будет построена на использовании РЕД ОС и виртуальной машины. Также будут последовательно выполнены и разобраны команды по настройке различных систем сети через командную строку в Network Manager.

Его можно установить с помощью пакета networkmanager, который содержит демон, интерфейс командной строки nmcli и графический интерфейс nmtui [7].

После установки следует запустить NetworkManager.service. Как только демон NetworkManager будет запущен, он автоматически подключится ко всем доступным подключениям, которые уже были настроены [7].

Состав используемого пакета:

- Версия: 1.44.2.
- Выпуск: 1.red80.
- Архитектура: x86_64.

Результаты исследования

Чтобы получить информацию обо всех установленных в системе сетевых интерфейсах используется команда: «ip addr show».

```
[user@vbox ~]$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fe:79:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86367sec preferred_lft 86367sec
    inet6 fd00::a00:27ff:fe79:0e/64 scope global dynamic noprefixroute
        valid_lft 86369sec preferred_lft 14369sec
    inet6 fe80::a00:27ff:fe79:0e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Рисунок 1 - Сетевые интерфейсы

Для просмотра статистики переданных и полученных пакетов для интерфейса, например, enp0s3: «ip -s link show enp0s3».

```
[user@vbox ~]$ ip -s link show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:fe:79:0e brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped missed mcast
         3842      31      0      0      0      1
    TX:  bytes packets errors dropped carrier collsns
         8215      73      0      0      0      0
```

Рисунок 2 - Статистика интерфейса

Чтобы посмотреть таблицу маршрутизации: «ip route show match 0/0».

```
[user@vbox ~]$ ip route show match 0/0  
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
```

Рисунок 3 - Таблица маршрутизации

Запуск Network Manager из консоли: «sudo systemctl start NetworkManager».

```
[user@vbox ~]$ sudo systemctl start NetworkManager  
[sudo] пароль для user:
```

Рисунок 4 - Запуск Network Manager

Посмотреть общий статус Network Manager помощью nmcli: «nmcli general status».

```
[user@vbox ~]$ nmcli general status  
STATE      CONNECTIVITY  WIFI-HW      WIFI      WWAN-HW      WWAN  
подключено полностью  отсутствует включено  отсутствует включено
```

Рисунок 5 - Состояние Network Manager

Посмотреть имя хоста: «nmcli general hostname».

```
[user@vbox ~]$ nmcli general hostname
```

Рисунок 6 - Имя хоста

Получить состояние интерфейсов: «nmcli device status».

```
[user@vbox ~]$ nmcli device status  
DEVICE  TYPE      STATE              CONNECTION  
enp0s3  ethernet  подключено        enp0s3  
lo      loopback  подключено (внешнее) lo
```

Рисунок 7 - Состояние интерфейсов

Посмотреть список доступных подключений: «nmcli connection show».

```
[user@vbox ~]$ nmcli connection show  
NAME      UUID                                  TYPE      DEVICE  
enp0s3    e02c9414-6829-315f-872c-e7c55c92b7c7 ethernet  enp0s3  
lo        e977e6ba-d0f5-4812-a37a-88a504fdfb1d loopback   lo
```

Рисунок 8 - Список подключений

С помощью следующей команды можно посмотреть информацию о подключении: «nmcli connection show "enp0s3"».


```
[user@vbox ~]$ nmcli connection show "enp0s3"
connection.id:                enp0s3
connection.uuid:              e02c9414-6829-315f-872c-e7c55c92b7c7
connection.stable-id:         --
connection.type:              802-3-ethernet
connection.interface-name:    enp0s3
connection.autoconnect:       да
connection.autoconnect-priority: -999
connection.autoconnect-retries: -1 (default)
connection.multi-connect:      0 (default)
connection.auth-retries:       -1
connection.timestamp:          1734383549
connection.permissions:        --
connection.zone:               --
connection.master:             --
connection.slave-type:         --
connection.autoconnect-slaves: -1 (default)
connection.secondaries:        --
connection.gateway-ping-timeout: 0
connection.metered:            неизвестно
```

Рисунок 9 - Информация о подключении

Чтобы подключиться к сети с помощью нужного подключения используется команда `up`: «`nmcli connection up "enp0s3"`».

```
[user@vbox ~]$ nmcli connection up "enp0s3"
Подключение успешно активировано (активный путь D-Bus: /org/freedesktop/NetworkManager/ActiveConnection/3)
```

Рисунок 10 - Подключение к сети

А для деактивации подключения используется команда `down`: «`nmcli conn down "enp0s3"`».

```
[user@vbox ~]$ nmcli conn down "enp0s3"
Подключение «enp0s3» успешно отключено (активный путь D-Bus: /org/freedesktop/NetworkManager/ActiveConnection/3)
```

Рисунок 11 - Отключение от сети

Чтобы создать новое подключение используется команда `add`. Например, можно создать новое подключение с именем `dhcp`: «`nmcli connection add con-name "dhcp" type ethernet ifname enp0s3`»

```
[user@vbox ~]$ nmcli connection add con-name "dhcp" type ethernet ifname enp0s3
Подключение «dhcp» (7575da8d-3ebb-4190-8494-849b559ed9f1) успешно добавлено.
```

Рисунок 12 - Создание dhcp подключения

Команде передаётся параметр «`type`» —тип устройства, а также «`ifname`» — название сетевого интерфейса. По умолчанию используется тип подключения DHCP, поэтому больше ничего настраивать не надо.

Для статического подключения настроек необходимо передать команде `add` IP-адрес, который будет использоваться в качестве основного в параметре «`ip4`», а также шлюз с

помощью параметра «gw4»: «nmcli connection add con-name "static" ifname enp2s0 autoconnect no type ethernet ip4 192.168.0.210 gw4 192.168.0.1».

```
[user@vbox ~]$ nmcli connection add con-name "static" ifname enp0s3 autoconnect  
no type ethernet ip4 192.168.0.210 gw4 192.168.0.1  
Предупреждение: есть ещё 1 подключение с именем 'static'. Ссылайтесь на подклю  
чение по его uuid '74ecb532-941e-4044-ad3b-67511847e042'  
Подключение «static» (74ecb532-941e-4044-ad3b-67511847e042) успешно добавлено.
```

Рисунок 13 - Создание статического подключения

Для добавления DNS-сервера используется команда modify: «nmcli conn modify "static" ipv4.dns 8.8.8.8».

И ещё один DNS сервер с помощью оператора «+»: «nmcli conn modify "static" +ipv4.dns 8.8.4.4».

Для добавления дополнительной информации в поле используется символ «+». Например, добавление еще одного IP-адреса: «nmcli conn modify "static" +ipv4.addresses 192.168.0.240/24».

Важно, что IP-адрес должен быть из той же подсети, что и шлюз, а иначе может ничего не работать. Можно активировать подключение: «nmcli connection up static».

```
[user@vbox ~]$ nmcli conn modify "static" ipv4.dns 8.8.8.8  
[user@vbox ~]$ nmcli conn modify "static" +ipv4.addresses 192.168.0.240/24  
[user@vbox ~]$ nmcli connection up static  
Подключение успешно активировано (активный путь D-Bus: /org/freedesktop/NetworkM  
anager/ActiveConnection/5)
```

Рисунок 14 - Статическое подключение

Посмотреть состояние Wi-Fi: «nmcli radio wifi».

Включить Wi-Fi: «nmcli radio wifi on».

Отключить Wi-Fi: «nmcli radio wifi off».

```
[user@vbox ~]$ nmcli radio wifi  
enabled  
[user@vbox ~]$ nmcli radio wifi on  
[user@vbox ~]$ nmcli radio wifi off  
[user@vbox ~]$ nmcli radio wifi  
disabled
```

Рисунок 15 - Работа с Wi-Fi

Посмотреть список доступных сетей Wi-Fi: «nmcli device wifi list».

Подключение к новой сети Wi-Fi, например, подключения к сети TP-Link с паролем 12345678: «nmcli device wifi connect "TP-Link" password 12345678 name "TP-Link Wifi"».

```
[user@vbox ~]$ nmcli device wifi list  
[user@vbox ~]$ nmcli device wifi connect "TP-Link" password 12345678 name "TP-Li  
nk Wifi"  
Ошибка: устройство Wi-Fi не найдено.
```

Рисунок 16 - Подключение к Wi-Fi

Заключение

В результате получилось рассмотреть основные принципы работы с консольной утилитой nmcli для настройки Network Manager. Были проделаны действия по просмотру, управлению, созданию и изменению проводных и беспроводных подключений. Рассмотрены как автоматические (DHCP), так и ручные (статический) варианты настройки IP, а также настройка Wi-Fi.

Примеры настройки показали, что данный метод может быть полезным и удобным при использовании и необходимости.

В дальнейшем также есть возможность изучения настройки технологии VLAN с помощью консоли, объединения нескольких сетевых интерфейсов в один логический канал, настройки сетевого моста или же написания bash-скриптов для настройки сети.

Список литературы

1. Настройка Network Manager в консоли [Электронный ресурс]. URL: <https://losst.pro/upravlenie-networkmanager-iz-konsoli#toc-6-nastroyka-podklyucheniya> (дата доступа 14.01.2025).
2. NetworkManager for administrators [Электронный ресурс]. URL: <https://networkmanager.dev/docs/admins>
3. NetworkManager [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/NetworkManager>
4. Get started with NetworkManager on Linux [Электронный ресурс]. URL: <https://opensource.com/article/22/4/networkmanager-linux>
5. D-Bus [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/D-Bus>
6. Network Manager architecture [Электронный ресурс]. URL: <https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=manager-network-architecture>
7. NetworkManager [Электронный ресурс]. URL: <https://wiki.archlinux.org/title/NetworkManager>
8. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург: Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ

References

1. Configuring the Network Manager in the console [Electronic resource]. URL: <https://losst.pro/upravlenie-networkmanager-iz-konsoli#toc-6-nastroyka-podklyucheniya> (accessed 14.01.2025).
2. NetworkManager for administrators [Electronic resource]. URL: <https://networkmanager.dev/docs/admins>
3. NetworkManager [Electronic resource]. URL: <https://en.wikipedia.org/wiki/NetworkManager>
4. Get started with NetworkManager on Linux [Electronic resource]. URL: <https://opensource.com/article/22/4/networkmanager-linux>
5. D-Bus [Electronic resource]. URL: <https://en.wikipedia.org/wiki/D-Bus>

6. Network Manager architecture [Electronic resource]. URL: <https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=manager-network-architecture>
 7. NetworkManager [Electronic resource]. URL: <https://wiki.archlinux.org/title/NetworkManager>
 8. Uimin, A. G. Basic level demonstration exam. Network and System Administration: A practical course. Textbook for universities / A. G. Uimin. Saint Petersburg: Lan Publishing House, 2024. p. 116 (Higher education). – ISBN 978-5-507-48647-2. – EDN BZJRIQ
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОДНОПЛАТНЫХ КОМПЬЮТЕРОВ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Колосова С.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: kolosovasvetlana2005@icloud.com

В данной статье рассматриваются перспективы применения одноплатных компьютеров в системах видеонаблюдения. Анализируются преимущества данных устройств, их технические возможности и потенциал для реализации интеллектуальных систем безопасности. Также внимание уделено сравнительному анализу популярных моделей по ключевым параметрам, описаны методы интеграции современных технологий искусственного интеллекта в видеосистемы. Представленный материал демонстрирует, как применение одноплатных компьютеров позволяет существенно сократить затраты на оборудование, снизить энергопотребление и повысить отказоустойчивость систем видеонаблюдения за счёт локальной обработки данных.

Ключевые слова: Одноплатные компьютеры, видеонаблюдение, Raspberry Pi, Jetson Nano, искусственный интеллект, видеоаналитика.

IMPORT SUBSTITUTION IN THE CONTEXT OF VIDEO SURVEILLANCE SYSTEMS BASED ON SINGLE-BOARD COMPUTERS

Kolosova S.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: kolosovasvetlana2005@icloud.com

The article discusses the prospects of applying single-board computers (SBCs) in video surveillance systems. The advantages of these devices, their technical capabilities, and their potential for implementing intelligent security systems are analyzed. Special attention is given to the comparative analysis of popular SBC models based on key parameters, as well as to methods of integrating modern artificial intelligence technologies into video systems. The presented material demonstrates how the use of SBCs can significantly reduce equipment costs, lower energy consumption, and increase the fault tolerance of surveillance systems through local data processing.

Keywords: Single-board computers, video surveillance, Raspberry Pi, Jetson Nano, artificial intelligence, video analytics.

Введение

Системы видеонаблюдения сегодня требуют высокопроизводительных решений для обработки и анализа видеоданных в режиме реального времени. Традиционные архитектуры, основанные на использовании серверных комплексов, зачастую сопряжены с высокими затратами на оборудование и энергопотребление. В последние годы всё большую популярность набирают одноплатные компьютеры, которые благодаря своим компактным размерам и достаточной вычислительной мощности способны эффективно решать задачи по сбору, обработке и анализу видеопотоков. Применение таких устройств позволяет организовывать локальную обработку данных, что способствует снижению задержек и повышению отказоустойчивости систем безопасности.[1]

Преимущество использования одноплатных компьютеров в видеонаблюдении

- Низкая стоимость. Одноплатные компьютеры, такие как Raspberry Pi и Orange Pi, существенно дешевле традиционных серверов, что делает их привлекательным решением для развертывания систем видеонаблюдения даже при ограниченном бюджете.
- Компактность и энергоэффективность. Малые размеры и низкое энергопотребление позволяют устанавливать устройства непосредственно в точках сбора данных, что уменьшает задержки при передаче информации и снижает общие затраты на эксплуатацию системы.
- Гибкость и масштабируемость. Поддержка различных операционных систем (например, Raspbian, Ubuntu MATE) и программных платформ, а также использование стандартизированных интерфейсов (RTSP, ONVIF) позволяют адаптировать одноплатные компьютеры под специфические требования проекта и легко интегрировать их в существующие системы безопасности.[2]
- Интеграция с технологиями искусственного интеллекта. Современные устройства, такие как NVIDIA Jetson Nano, оснащены специализированными графическими ускорителями, что позволяет использовать фреймворки типа TensorFlow Lite и NVIDIA DeepStream для реализации алгоритмов машинного обучения непосредственно на устройстве. Это значительно расширяет функциональные возможности систем видеонаблюдения, позволяя осуществлять распознавание лиц, детекцию объектов и анализ поведения в режиме реального времени.

Технические возможности одноплатных компьютеров

Современные одноплатные компьютеры обладают высокопроизводительными процессорами, достаточным объёмом оперативной памяти и множеством интерфейсов для подключения периферийных устройств. Приведённая ниже таблица (Таблица 1) демонстрирует сравнение популярных и особенных моделей по основным параметрам.

Таблица 1 - Сравнение современных SBC

Модель	Процессор	Оперативная память	Графический процессор	Интерфейсы
Raspberry Pi 5	Quad-core Cortex-A76 2.4 GHz	2GB/4GB/8GB/16 GB	VideoCore VII	2xUSB 3.0, 2xUSB 2.0, PCIe 2.0, HDMI
NVIDIA Jetson Nano	Quad-core ARM A57 1.43 GHz	4GB	128-core Maxwell	4xUSB 3.0, HDMI, DisplayPort

Модель	Процессор	Оперативная память	Графический процессор	Интерфейсы
Repka Pi 4 Optimal	Quad-core Cortex-A53 2.0 GHz	2GB	Mali-T720 MP2	USB 3.0, 3xUSB 2.0, HDMI
OrangePi RV	Quad-core StarFive JH7110 1.5 GHz	2GB/4GB/8GB	RISC-V architecture	4xUSB 3.0, HDMI

Источник: анализ автора

Применение одноплатных компьютеров в системах видеонаблюдения

Одноплатные компьютеры находят широкое применение в системах видеонаблюдения благодаря своей способности обрабатывать видеопотоки и выполнять видеоаналитику непосредственно на местах установки. Такой подход снижает нагрузку на центральные серверы, повышает отказоустойчивость системы.

Интеллектуальная видеоаналитика

Устройства с высокопроизводительными графическими ускорителями, например, NVIDIA Jetson Nano, открывают возможности для реализации интеллектуальной видеоаналитики. Для достижения этой цели используются следующие методы и технологии:

- Классификация и обнаружение объектов. Применение сверточных нейронных сетей (CNN) с использованием TensorFlow Lite и NVIDIA DeepStream SDK позволяет точно распознавать лица, транспортные средства и фиксировать подозрительное поведение.
- Алгоритм трекинга. Методы SORT (Simple Online and Realtime Tracking) и алгоритмы на базе Kalman Filter обеспечивают стабильное отслеживание объектов в видеопотоке при низкой вычислительной нагрузке.[3]
- Обнаружение аномалий. Применение автоэнкодеров и рекуррентных нейронных сетей позволяет анализировать временные ряды видеоданных, выявляя нестандартные события и снижая число ложных срабатываний.
- Интеграция с системами управления. Использование OpenCV в связке с Python или C++ обеспечивает оперативное взаимодействие между видеосистемой и средствами управления, а также позволяет проводить настройку системы через веб-интерфейсы.

Мобильные системы видеонаблюдения

Компактные и энергоэффективные одноплатные компьютеры являются идеальной платформой для разработки мобильных систем видеонаблюдения. Такие решения находят применение в правоохранительных органах, на транспорте и при организации временного

мониторинга на массовых мероприятиях. В мобильных системах одноплатные компьютеры могут работать в автономном режиме с подключением к аккумуляторным блокам и мобильным сетям (4G/5G), что обеспечивает передачу видеопотока в режиме реального времени как на центральные серверы, так и на мобильные устройства операторов.[4]

Актуальность и перспективы

Современные требования к системам безопасности и мониторинга диктуют необходимость использования распределённых вычислительных платформ, способных обрабатывать большие объёмы видеоданных в реальном времени. Применение одноплатных компьютеров позволяет организовать локальную обработку видеопотоков, что сокращает задержки, связанные с передачей данных на удалённые серверы, и повышает общую отказоустойчивость системы. Среди конкретных технологий, способствующих развитию систем видеонаблюдения, можно выделить следующие направления:

- Edge Computing. Платформы, такие как NVIDIA Jetson Nano и Google Coral, позволяют реализовывать сложные алгоритмы обработки данных непосредственно на периферии сети, что ускоряет реакцию системы на инциденты и снижает затраты на передачу данных.
- Беспроводные технологии и IoT. Использование стандартов Wi-Fi, LoRaWAN и мобильных сетей 4G/5G обеспечивает надёжную передачу данных даже при отсутствии проводного подключения.
- Модульность и стандартизация. Применение протоколов ONVIF для IP-камер и RTSP для потоковой передачи видео облегчает интеграцию одноплатных компьютеров в существующие системы безопасности.

Заключение

Одноплатные компьютеры демонстрируют высокий потенциал для применения в системах видеонаблюдения. Их использование позволяет создавать экономичные, масштабируемые и интеллектуальные решения, способные значительно повысить уровень безопасности в различных сферах. Внедрение таких устройств, особенно в сочетании с современными технологиями искусственного интеллекта, облачными вычислениями и IoT, открывает перспективы для создания эффективных систем мониторинга с оперативным реагированием на инциденты.

Список литературы

1. Добровольский Н.С. Применение одноплатных компьютеров в системах мониторинга параметров окружающей среды / Проблемы автоматики и управления. 2015. № 1. – С. 171-174.
2. Тельминов О.А., Горнев Е.С., Теплов Г.С, Процессоры, память и программное обеспечение для эффективной реализации нейронных сетей / НАНОИНДУСТРИЯ. 2020. № S96-2 – С. 580-584.
3. Raspberry Pi Documentation [Электронный ресурс] / raspberrypi.org: website – URL: <https://www.raspberrypi.org/documentation/>

4. ONVIF – Standard for IP-based Video Surveillance [Электронный ресурс] / onvif.org: website – URL: <https://www.onvif.org>

References

1. Dobrovolsky N.S. The use of single-board computers in environmental parameter monitoring systems / Problems of automation and control. 2015. No. 1. pp. 171-174.
 2. Telminov O.A., Gornev E.S., Teplov G.S., Processors, memory and software for effective implementation of neural networks / NANOINDUSTRIA. 2020. No. S96-2 – pp. 580-584.
 3. Raspberry Pi Documentation [Electronic resource] / raspberrypi.org: website – URL: <https://www.raspberrypi.org/documentation/>
 4. ONVIF – Standard for IP-based Video Surveillance [Electronic resource] / onvif.org : website – URL: <https://www.onvif.org>
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

ЭМУЛЯЦИЯ КЛАВИАТУРЫ ЧЕРЕЗ USB RUBBER DUCKY: АВТОМАТИЗИРОВАННОЕ ЗАРАЖЕНИЕ БЕЗ ФАЙЛОВ

Романов Д.Р.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: danilio2003.dr@gmail.com

USB Rubber Ducky — это специализированное устройство, которое использует эмуляцию клавиатуры для выполнения вредоносных команд на целевой системе без необходимости установки файлов. В статье рассматривается принцип работы Rubber Ducky, механизмы автоматизированных атак, сценарии эксплуатации в реальной среде и методы защиты от подобных угроз. Особое внимание уделяется концепции fileless-атак, которые позволяют злоумышленникам обходить традиционные антивирусные решения и системы обнаружения вторжений.

Ключевые слова: USB Rubber Ducky, эмуляция клавиатуры, fileless-атака, автоматизированное заражение, безопасность, USB-угрозы, защита информации.

KEYBOARD EMULATION VIA USB RUBBER DUCKY: FILELESS AUTOMATED INFECTION

Romanov D.R.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: danilio2003.dr@gmail.com

USB Rubber Ducky is a specialized device that uses keyboard emulation to execute malicious commands on a target system without requiring file installation. This article explores the working principle of Rubber Ducky, mechanisms of automated attacks, real-world exploitation scenarios, and protection methods against such threats. Special attention is given to the concept of fileless attacks, which allow attackers to bypass traditional antivirus solutions and intrusion detection systems.

Keywords: USB Rubber Ducky, keyboard emulation, fileless attack, automated infection, cybersecurity, USB threats, information security.

Введение

В современном мире угрозы информационной безопасности становятся всё более изощрёнными, а методы атаки — сложнее и эффективнее. Одним из таких методов является использование устройств, эмулирующих клавиатуру, среди которых особенно выделяется USB Rubber Ducky. Этот инструмент, внешне напоминающий обычную флешку, позволяет злоумышленникам незаметно выполнять вредоносные команды на атакуемой системе. В отличие от традиционных вредоносных программ, USB Rubber Ducky не требует установки файлов на диск, а использует механизмы эмуляции клавиатуры для быстрого ввода команд, что делает атаку практически незаметной для антивирусных систем.

Концепция атаки на основе эмуляции клавиатуры основана на простом, но эффективном подходе: операционная система доверяет физическим устройствам ввода, таким как клавиатура, и практически не проверяет их на наличие вредоносных действий. Это позволяет Rubber Ducky автоматически вводить команды так, как если бы их печатал сам пользователь, но с гораздо большей скоростью и точностью. Такие атаки могут использоваться для кражи данных, установки бэкдоров, скачивания вредоносного ПО или даже отключения системной защиты.

С ростом популярности USB Rubber Ducky и аналогичных устройств актуальность защиты от подобных атак возрастает. Несмотря на опасность этой угрозы, многие организации и пользователи недооценивают риски, связанные с подключением незнакомых USB-устройств. В данной статье подробно рассматривается принцип работы USB Rubber Ducky, примеры его использования в атаках, а также методы защиты от подобных угроз.

Эмуляция клавиатуры через USB Rubber Ducky: автоматизированное заражение без файлов

USB Rubber Ducky — это устройство, созданное для автоматизированного выполнения команд на целевой машине. Оно использует эмуляцию клавиатуры, что позволяет выполнять любые команды с привилегиями пользователя, который в данный момент авторизован в системе. Устройство программируется с помощью специального языка сценариев Ducky Script, который позволяет задать последовательность команд, вводимых в систему. В отличие от обычной флешки, Rubber Ducky определяется компьютером не как USB-накопитель, а как HID (Human Interface Device), что делает его невидимым для стандартных систем безопасности[1].

Принцип работы Rubber Ducky довольно прост. Как только устройство подключается к компьютеру, оно мгновенно начинает вводить заранее подготовленные команды. Например, атакующий может запрограммировать Rubber Ducky на открытие командной строки (cmd.exe) и выполнение PowerShell-скрипта, который загружает вредоносный код из сети и выполняет его в памяти без записи на диск. Этот метод позволяет обходить большинство традиционных антивирусных решений, которые отслеживают файлы, но не анализируют ввод с клавиатуры[2].

Одним из самых популярных сценариев атаки является получение удалённого доступа через обратное подключение (reverse shell). Rubber Ducky может быстро ввести команду, которая подключает целевую машину к серверу атакующего, позволяя ему выполнять команды удалённо. Этот метод используется не только хакерами, но и тестировщиками на проникновение (pentesters) для оценки уровня безопасности организаций[3].

Другой вариант использования Rubber Ducky — кража паролей. Устройство может быстро открыть диспетчер учетных данных Windows или извлечь сохранённые пароли из браузеров, сохранив их в скрытом файле или отправив на сервер злоумышленника. Также возможны атаки на двухфакторную аутентификацию, когда Rubber Ducky перехватывает временные коды или автоматически вводит скомпрометированные данные на веб-сайтах[4].

Популярность Rubber Ducky объясняется не только его эффективностью, но и доступностью. Сценарии атак можно найти в открытых репозиториях, таких как GitHub, а само устройство легко купить или даже создать самостоятельно, используя

микроконтроллеры, такие как Digispark. Это делает подобные атаки потенциально опасными даже для обычных пользователей, не обладающих глубокими техническими знаниями.

Несмотря на высокую угрозу, существует ряд методов защиты от атак с использованием USB Rubber Ducky. Во-первых, рекомендуется ограничить использование USB-устройств с помощью групповых политик Windows или специализированных решений для контроля подключаемых периферийных устройств. Организации могут использовать программное обеспечение для мониторинга HID-устройств и отключения несанкционированных клавиатур[5].

Во-вторых, стоит настроить систему таким образом, чтобы любая новая клавиатура требовала ручного подтверждения перед активацией. Например, в некоторых Linux-дистрибутивах уже существуют механизмы, позволяющие блокировать автоматическое определение HID-устройств.

Третий важный аспект защиты — это осведомлённость пользователей. Часто атака начинается с физического доступа к устройству, когда злоумышленник незаметно подключает Rubber Ducky к компьютеру жертвы. Поэтому важно обучать сотрудников и пользователей не подключать неизвестные USB-устройства, даже если они выглядят как обычные флешки.

Дополнительно можно использовать специализированное программное обеспечение, такое как USBKill, которое отслеживает появление новых HID-устройств и может автоматически блокировать их, если они не были заранее одобрены пользователем. Также эффективным методом защиты является отключение PowerShell или ограничение его функций через групповые политики, что затруднит выполнение вредоносных команд.

Таким образом, атаки с использованием USB Rubber Ducky представляют серьёзную угрозу, так как позволяют автоматизировать выполнение команд без необходимости установки вредоносных файлов. Однако при правильной настройке систем безопасности и повышении осведомлённости пользователей можно значительно снизить риск успешной эксплуатации данной технологии.

Заключение

Эмуляция клавиатуры через USB Rubber Ducky является одним из наиболее эффективных методов атак, позволяющих обойти традиционные средства защиты и автоматизировать выполнение вредоносных команд. Этот инструмент активно используется как в целях тестирования безопасности, так и в реальных атаках, нацеленных на корпоративные сети и персональные компьютеры.

Главная опасность Rubber Ducky заключается в том, что он не требует установки вредоносных файлов и способен обходить традиционные антивирусные решения. Подобные атаки становятся всё более популярными, особенно с учётом доступности устройства и большого количества готовых сценариев в открытых источниках.

Для защиты от атак через USB Rubber Ducky необходимо применять комплексный подход: ограничение доступа к USB-портам, мониторинг HID-устройств, блокировка PowerShell и повышение осведомлённости пользователей. В условиях постоянно развивающихся угроз информационной безопасности осознание рисков и внедрение эффективных защитных механизмов являются ключевыми мерами для предотвращения подобных атак.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

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



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.738.5:004.42

ПЕРСПЕКТИВЫ РАЗВИТИЯ NO-CODE ПЛАТФОРМ ДЛЯ СОЗДАНИЯ ВЕБ-САЙТОВ

Шелег В.С.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "ВЫСШАЯ ШКОЛА ЭКОНОМИКИ" (САНКТ-ПЕТЕРБУРГСКИЙ ФИЛИАЛ), Санкт-Петербург, Россия (190121, город Санкт-Петербург, ул. Союза Печатников, д.16), e-mail: varsheleg@mail.ru

В данной статье рассматриваются преимущества и недостатки no-code платформ для создания сайтов. Анализируются их различия с традиционным способом создания сайтов с помощью написания кодов HTML и CSS. Исследуются тенденции развития конструкторов для создания сайтов и их влияние на рынок веб-разработки.

Ключевые слова: Создание сайта, no-code, конструктор сайтов, сайт, no-code платформа, Tilda, веб-дизайн.

PROSPECTS FOR THE DEVELOPMENT OF NO-CODE PLATFORMS FOR CREATING WEBSITES

Sheleg V.S.

NATIONAL RESEARCH UNIVERSITY HIGHER SCHOOL OF ECONOMICS (ST. PETERSBURG BRANCH), St. Petersburg, Russia (190121, St. Petersburg, Soyuza Pechatnikov st., 16), e-mail: varsheleg@mail.ru

This article discusses the advantages and disadvantages of no-code platforms for creating websites. Their differences with the traditional way of creating websites by writing HTML and CSS codes are analyzed. The article examines the trends in the development of designers for creating websites and their impact on the web development market.

Keywords: Website creation, no-code, website builder, website, no-code platform, Tilda, web design.

Введение

В современном мире практически невозможно представить свою жизнь без ежедневного использования интернета и поиска информации на различных веб-сайтах. Люди ищут информацию о необходимой им услуге, стоимости товаров или графике работы той или иной компании. Ежедневно среднестатистический пользователь интернета проводит онлайн 6 часов 40 минут в день [3]. В связи с этим, спрос на создание сайта компании растет, и все больше предпринимателей понимают важность наличия собственного сайта, который не только расскажет всю информацию о компании, но и приблизит предполагаемого клиента к совершению целевого действия. Целевым действием может являться не только покупка услуги или товара, но и, например, заполнение формы на сайте. В данном случае сайт является местом первого касания с клиентом и способствует увеличению продаж.

Так как спрос на создание сайтов растет, возрастает и спрос на относительно недорогие способы создания веб-страниц, а именно, с использованием no-code технологий.

Цель исследования

Так как в настоящее время популярность использования относительно простых решений для создания сайтов возрастает, данная статья посвящена анализу текущего состояния No-Code платформ, оценки их преимуществ и выявлению недостатков. Также, важно оценить перспективы развития конструкторов для создания веб-сайтов и их влияние на рынок веб-разработки.

Проблема исследования

В сравнении с классическим способом создания сайта, а именно, с помощью языка программирования HTML, кажется, что использование no-code платформ – это примитивный и ненадежный подход, функционал которого очень ограничен. Скептическое отношение к конструкторам сайтов наблюдается в России, а также недостаточный уровень знаний о no-code среди тех, кому он мог бы быть полезен [5].

Метод исследования

Исследование строится на анализе существующей литературы и статей по теме, обзоре основных преимуществ и недостатков no-code платформ, изучение тенденций в развитии и применении конструкторов сайтов.

Преимущества использования No-Code

Самый первый сайт был создан в 1991 году Тимом Бернерсом-Ли на языке HTML5 [6]. С тех пор ситуация на рынке создания сайтов сильно изменилась и, с развитием новых технологий, появились no-code платформы, которые позволяют создать сайт без знаний языков программирования. Их бурный рост начался в 2020 году. На текущий момент известно более 600 платформ, с помощью которых можно создать сайт без написания кода. К самым популярным платформам для создания сайта относят платформы Tilda, Webflow, WIX и другие.

No-Code платформы работают по принципу drag-and-drop на основе визуального интерфейса. В основе создания сайтов лежат шаблоны, которые можно кастомизировать и настраивать под нужды клиента, добавляя уникальные тексты, иконки и изображения.

Ранее для того, чтобы создать сайт, необходимо было собрать команду разработчиков и архитектором, а срок создания сайта начинался от 2 месяцев и более. С появлением no-code платформ сроки создания сайтов сократились значительно. При сжатых сроках можно собрать сайт буквально за 2-3 дня, а процесс создания сайта «под ключ» занимает в среднем от 2 до 4 недель. В создание сайта «под ключ» входит аналитика конкурентов и целевой аудитории, разработка дизайн-концепции, прототипа и дизайна, а также перенос сайта на платформу и его полная настройка. Существенное сокращение сроков разработки сайта связано с простотой переноса сайта на платформу и отсутствием необходимости иметь глубокие знания программирования. Сайт, созданный на шаблонах, можно сверстать за 1 день, при использовании уникальных zero-блоков этот процесс увеличивается до 2-3 дней, что в любом случае, существенно меньше, чем написание кода традиционным способом.

По данным исследований компании Forrester, скорость разработки программного обеспечения с использованием конструкторов увеличивается в среднем в 10 раз [5].

Более того, стоимость разработки сайта на no-code платформах существенно ниже, чем при написании кода, потому что складывается из стоимости работы веб-дизайнера и цены пользования платформой. Средняя стоимость одностраничного сайта составляет в 2025 году 50 000 рублей в то время, как стоимость сайта, написанного на языке программирования, начинается от 100 000 рублей.

Сайт, собранный на конструкторе, — это отличный способ для быстрой проверки гипотез и оценке жизнеспособности продукта. Стартапы, которые только планируют выходить на рынок и не имеют времени и средств на большую разработку сайта, могут проверить, насколько их продукт актуален и протестировать идею [4].

Несмотря на то, что многие считают, что сайт, собранный на конструкторе, – это шаблонное решение, стандартизация блоков, шрифтов и анимации [4], разработчики no-code платформ доказывают обратное. На текущий момент, например Tilda, предлагает большое количество возможностей для кастомизации сайта. На этой платформе можно как кастомизировать уже готовые стандартные блоки, которых более 400, меняя их под необходимую стилистику сайта, так и создавать уникальный дизайн на Zero-блоках. Zero-блок – это как «чистый лист», профессиональный редактор, на который можно добавить любой элемент. Он позволяет добавлять различные текстовые и графические элементы в блок, располагать их любым способом и добавлять различные эффекты, реализовывая любую задумку.

No-code платформы не только просты в использовании, но и предлагают большое количество сервисов, с которыми можно интегрировать ваш сайт. Интеграция возможна с сервисами доставки и оплаты, модулями бронирования или оставления отзывов, с сервисами для автоматизации бизнес-процессов и многими другими. Более того, при использовании связующего звена, например Albato, между конструктором и другими сервисами можно интегрировать более 700 различных систем [1].

Недостатки использования No-Code

К существенным недостаткам no-code можно отнести невозможность внесения изменения в исходный код страницы, так как серверная часть сайта для пользователей закрыта [6]. В связи с этим, создание сайта на конструкторе может не подойти тем, кто хочет внедрить в свой проект сложное, инновационное решение. Веб-дизайнер не сможет реализовать сложную по логике идею, если она не предусмотрена платформой. Так, например, при создании интернет-магазина на Тильде, невозможно прописать гибкую систему скидок, которые будут применять к отдельным товарам, а не ко всем сразу. Также невозможно без интеграции со сторонними сервисами реализовать модуль доставки по адресу пользователя для расчёта итоговой суммы заказа.

Еще один недостаток, — это зависимость от площадки. Таким образом, если на сервере no-code платформы произойдет какой-то сбой, то вы никак не сможете повлиять на работоспособность сайта. Потеря доступа к сайту, даже на короткое время, – это серьезная проблема для крупных компаний, где 10 минут простоя сайта могут стоить десятки и сотни тысяч рублей.

Перспективы развития No-Code

На текущий момент no-code платформы активно развиваются и с каждым годом добавляют новые стандартные блоки, новые возможности для кастомизации уникальных

блоков и новые интеграции со сторонними сервисами. В связи с этим, количество пользователей данных платформ постоянно растет.

По прогнозам агентства IDC (International Data Corporation), к 2026 году более 40 % компаний будут использовать в основе своих сервисов low-code/no-code [4]. По прогнозам Research and Markets, за 2020–2030 годы рынок low-code/no-code увеличится с \$10,3 млрд до \$187 млрд со среднегодовым темпом роста 31,1% [5].

Уже сейчас, no-code платформы внедряют в свой функционал искусственный интеллект, что значительно упрощает процесс разработки сайта. ИИ-помощник может сгенерировать текст как для отдельного блока, так и для всего сайта. Для использования искусственного интеллекта достаточно указать краткую информацию о компании, и нужный текст будет сгенерирован [2].

Использование возможностей искусственного интеллекта неограниченно, поэтому можно предположить, что в ближайшем будущем мы увидим, как с помощью простого запроса можно будет значительно ускорить процесс создания сайта и его настройки.

Заключение

Таким образом, no-code платформы – это отличная возможность для создания сайта, который будет отвечать всем требованиям современного веб-дизайна и привлекать клиентов. Конструкторы сайтов предлагают относительно недорогие и быстрые решения для бизнесов, которым не нужны инновационные решения. Рынок создания сайтов на no-code платформах стремительно растет и развивается с каждым годом, что позволяет предлагать все более актуальные решения в создании сайтов.

Список литературы

1. Интеграции с Tilda Api — связать Tilda с сервисами и приложениями. – URL: <https://albato.ru/app-tilda> (дата обращения: 04.02.2025). – Текст : электронный.
2. Конструктор сайтов с AI. – URL: <http://tilda.cc/ai> (дата обращения: 04.02.2025). – Текст : электронный.
3. Connecting The Dots: 2025 Consumer Trends | GWI. – URL: <https://www.gwi.com/connecting-the-dots> (дата обращения: 04.02.2025). – Текст : электронный.
4. Новичихина, А. А. Применение No-Code И Low-Code Инструментов Для Разработки Программных Средств / А. А. Новичихина. – Текст : электронный. – Хакасский государственный университет им. Н.Ф. Катанова, 2023. – С. 187-189. – URL: <https://www.elibrary.ru/item.asp?id=54074576> (дата обращения: 04.02.2025).
5. Тренд на low-code/no-code: как разработка без кода влияет на рынок, и почему она не заменит опытных программистов. – URL: <https://habr.com/ru/companies/netologyru/articles/710728/> (дата обращения: 04.02.2025). – Текст : электронный.
6. Ягодкин, Д. А. Сравнительный Анализ Бесплатных Конструкторов Сайта / Д. А. Ягодкин, К. В. Закутаева, Н. А. Череватенко. – Текст : электронный. – Общество с ограниченной ответственностью «Агентство международных исследований», 2018. – С. 111-116. – URL: <https://www.elibrary.ru/item.asp?id=36593704> (дата обращения: 04.02.2025).

References:

1. Integration with Tilda Api — connect Tilda with services and applications. – URL: <https://albato.ru/app-tilda> (date of request: 02/04/2025). – Text : electronic.
 2. Website builder with AI. – URL: <http://tilda.cc/ai> (date of request: 02/04/2025). – Text : electronic.
 3. Connecting The Dots: 2025 Consumer Trends | GWI. – URL: <https://www.gwi.com/connecting-the-dots> (date of request: 02/04/2025). – Text : electronic.
 4. Novichikhina, A. A. Application Of No-Code And Low-Code Tools For Software Development / A. A. Novichikhina. – Text : electronic. – N.F. Katanov Khakass State University, 2023. – pp. 187-189. – URL: <https://www.elibrary.ru/item.asp?id=54074576> (date of issue: 02/04/2025).
 5. Low-code/no-code trend: how code-free development affects the market, and why it won't replace experienced programmers. – URL: <https://habr.com/ru/companies/netologyru/articles/710728/> / (date of access: 02/04/2025). – Text : electronic.
 6. Yagodkin, D. A. Comparative Analysis Of Free Website Designers / D. A. Yagodkin, K. V. Zakutaeva, N. A. Cherevatenko. – Text : electronic. – Limited Liability Company "Agency for International Studies", 2018. – pp. 111-116. – URL: <https://www.elibrary.ru/item.asp?id=36593704> (date of request: 02/04/2025).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ В HP iLO: СКРЫТОЕ ЗАРАЖЕНИЕ СЕРВЕРОВ ЧЕРЕЗ КОНТРОЛЛЕР УПРАВЛЕНИЯ

Романов Д.Р.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: danilio2003.dr@gmail.com

Контроллер управления HP Integrated Lights-Out (iLO) широко используется для удалённого администрирования серверов, но его уязвимости могут представлять серьёзную угрозу безопасности. Эксплуатация таких уязвимостей позволяет злоумышленникам получить скрытый доступ к серверу, выполнять вредоносный код, а также устанавливать бэкдоры, которые трудно обнаружить и удалить. В статье рассматриваются основные атаки на HP iLO, их последствия и методы защиты, включая обновления прошивки, изоляцию сетевого доступа и мониторинг аномальной активности.

Ключевые слова: HP iLO, уязвимости, скрытые атаки, удалённое управление, бэкдор, серверная безопасность, эксплуатация уязвимостей.

EXPLOITING VULNERABILITIES IN HP iLO: STEALTH INFECTION OF SERVERS VIA MANAGEMENT CONTROLLER

Romanov D.R.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: danilio2003.dr@gmail.com

The HP Integrated Lights-Out (iLO) management controller is widely used for remote server administration, but its vulnerabilities pose a serious security threat. Exploiting these vulnerabilities allows attackers to gain stealth access to servers, execute malicious code, and install backdoors that are difficult to detect and remove. This article examines key attacks on HP iLO, their impact, and protection methods, including firmware updates, network isolation, and monitoring for anomalous activity.

Keywords: HP iLO, vulnerabilities, stealth attacks, remote management, backdoor, server security, exploitation.

Введение

Современные серверные инфраструктуры активно используют контроллеры удалённого управления, такие как HP Integrated Lights-Out (iLO), которые предоставляют администраторам возможность контролировать и управлять серверами даже при выключенной основной операционной системе. Эта функциональность значительно упрощает администрирование, особенно в крупных дата-центрах и корпоративных средах. Однако уязвимости в iLO представляют собой критический вектор атаки, позволяя злоумышленникам получить полный доступ к серверу, обходя традиционные механизмы защиты операционной системы.

Одна из главных проблем безопасности iLO заключается в его низкоуровневом уровне доступа. Контроллер встроен непосредственно в аппаратное обеспечение сервера и работает независимо от основной ОС. Это означает, что атака на iLO может остаться незамеченной традиционными средствами защиты, такими как антивирусы или системы обнаружения вторжений. В результате злоумышленники могут устанавливать бэкдоры, удалённо управлять сервером и даже стирать следы своего присутствия, что делает такие атаки особенно опасными.

За последние годы было обнаружено несколько критических уязвимостей в HP iLO, включая CVE-2017-12542 и другие аналогичные проблемы, позволяющие злоумышленникам выполнить удалённое выполнение кода, перехватить аутентификационные данные или полностью скомпрометировать систему. В данной статье рассматриваются способы эксплуатации уязвимостей в HP iLO, примеры атак и рекомендации по защите серверов от подобных угроз.

Эксплуатация уязвимостей в HP iLO: скрытое заражение серверов через контроллер управления

HP iLO предоставляет администраторам широкие возможности для удалённого управления серверами, включая доступ к консоли, загрузку образов операционных систем, мониторинг аппаратных параметров и автоматизированное администрирование. Однако такие широкие привилегии превращают iLO в привлекательную цель для хакеров, которые могут использовать его уязвимости для скрытого проникновения на сервер[1].

Одной из наиболее известных уязвимостей является CVE-2017-12542, которая позволяет удалённо выполнить код на сервере без необходимости аутентификации. Эксплуатируя ошибки в механизме обработки HTTP-запросов, злоумышленники могут отправить специально сформированный пакет, который позволяет им получить полный контроль над контроллером. Это даёт возможность загружать вредоносные прошивки, устанавливать бэкдоры и выполнять команды с максимальными привилегиями[2].

Использование уязвимостей iLO позволяет атакующим выполнять несколько видов атак:

Поскольку iLO работает независимо от основной ОС, вредоносный код, загруженный в контроллер, не исчезает даже после переустановки операционной системы. Это делает атаку крайне стойкой и сложной для обнаружения.

Вредоносное ПО может модифицировать данные о состоянии сервера, скрывать факт вторжения или даже подменять команды администратора.

Если злоумышленник получает доступ к одному серверу, он может использовать встроенные механизмы iLO для поиска других серверов в сети и автоматического заражения их аналогичным образом.

Такие атаки особенно опасны в корпоративных сетях и дата-центрах, где компрометация одного узла может привести к цепной реакции и захвату множества серверов. Использование уязвимостей iLO позволяет атакующим практически полностью скрыть своё присутствие, а отсутствие видимого вредоносного процесса в ОС затрудняет обнаружение атаки[3].

Для защиты от атак на HP iLO рекомендуется применять комплексный подход, включающий несколько ключевых мер:

Производитель выпускает исправления для обнаруженных уязвимостей, поэтому своевременное обновление iLO является обязательным шагом для предотвращения атак[4].

Если удалённое управление сервером через iLO не требуется, рекомендуется отключить внешний доступ к контроллеру или ограничить его использованием VPN и защищённых сетей.

Анализ сетевого трафика, поиск аномальных соединений и неожиданных запросов к iLO помогут обнаружить подозрительные действия на ранних этапах.

Использование уникальных паролей и двухфакторной аутентификации. Простые или стандартные пароли значительно облегчают атаку, поэтому необходимо использовать сложные комбинации и дополнительные уровни защиты.

В некоторых критических средах рекомендуется использовать отдельные сетевые сегменты или даже выделенные устройства для управления серверами, что снижает вероятность взлома через общие сети[5].

Несмотря на все меры безопасности, iLO остаётся привлекательной целью для атак, особенно в корпоративных средах, где злоумышленники могут использовать уязвимости для скрытого присутствия в инфраструктуре на протяжении длительного времени. Это подчёркивает важность постоянного контроля за безопасностью серверов и применения передовых методов защиты.

Заключение

Эксплуатация уязвимостей в HP iLO представляет собой серьёзную угрозу для корпоративных серверов, поскольку позволяет злоумышленникам обходить традиционные механизмы защиты и скрыто управлять системой на аппаратном уровне. Из-за своей независимости от операционной системы iLO может использоваться для установки устойчивых бэкдоров, перехвата данных и распространения атак внутри корпоративных сетей.

Атаки на HP iLO особенно опасны, потому что традиционные антивирусные программы и системы обнаружения вторжений часто не могут зафиксировать активность вредоносного кода в контроллере. Это делает такие атаки трудно обнаруживаемыми и устойчивыми к традиционным методам очистки системы.

Для защиты серверов от подобных угроз необходим комплексный подход, включающий регулярные обновления прошивки, ограничение доступа к iLO, мониторинг сетевого трафика и использование надёжных механизмов аутентификации. Понимание угроз, связанных с эксплуатацией уязвимостей iLO, и применение передовых стратегий защиты поможет организациям минимизировать риски и предотвратить скрытые атаки на серверную инфраструктуру.

Список литературы

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределённых информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. – 2004.

4. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
5. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //Офтальмохирургия. – 2022. – №. 4с. – С. 92-101.

References

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruевич, 1996.
 2. Minyaev A. A. Method for evaluating the effectiveness of information security systems of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020). 2020. pp. 716-719.
 3. Dushin S. E. et al. Synthesis of structurally complex nonlinear control systems. – 2004.
 4. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
 5. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology //Ophthalmosurgery. – 2022. – No. 4s. – pp. 92-101.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

МАНИПУЛЯЦИЯ ДАННЫМИ В DRAM: КАК ROWHAMMER-АТАКИ МОГУТ ИСПОЛЬЗОВАТЬСЯ ВИРУСАМИ

Романов Д.Р.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: danilio2003.dr@gmail.com

Rowhammer-атака — это серьёзная уязвимость в современных модулях DRAM, позволяющая изменять содержимое памяти без прямого доступа к ней. Эта атака использует быстрые повторяющиеся обращения к определённым строкам памяти, что вызывает сбои в соседних ячейках, приводя к несанкционированному изменению данных. Вирусы и вредоносное ПО могут эксплуатировать этот механизм для повышения привилегий, обхода защитных механизмов и нарушения работы системы. В статье рассматриваются принципы работы Rowhammer-атак, реальные примеры их использования и методы защиты, такие как коррекция ошибок, аппаратные и программные контрмеры.

Ключевые слова: Rowhammer, DRAM, манипуляция данными, битовые сбои, кибератаки, повышение привилегий, защита памяти.

DATA MANIPULATION IN DRAM: HOW ROWHAMMER ATTACKS CAN BE USED BY VIRUSES

Romanov D.R.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: danilio2003.dr@gmail.com

The Rowhammer attack is a serious vulnerability in modern DRAM modules that allows changing the contents of memory without direct access to it. This attack uses fast repetitive accesses to certain memory lines, which causes failures in neighboring cells, leading to unauthorized data modification. Viruses and malware can exploit this mechanism to elevate privileges, bypass security mechanisms, and disrupt the system. The article discusses the principles of Rowhammer attacks, real-world examples of their use, and protection methods such as error correction, hardware and software countermeasures.

Keywords: Rowhammer, DRAM, data manipulation, bit failures, cyber attacks, privilege escalation, memory protection.

Введение

С развитием технологий безопасности операционных систем и процессоров злоумышленникам становится всё сложнее находить уязвимости для выполнения атак. Однако аппаратные уязвимости, такие как Rowhammer, представляют особую опасность, поскольку они воздействуют на саму структуру памяти, выходя за рамки традиционных методов защиты. Rowhammer-атака была впервые обнаружена исследователями в 2014 году и до сих пор остаётся актуальной угрозой для современных компьютеров, серверов и мобильных устройств.

Суть уязвимости заключается в том, что частый доступ к одной и той же строке памяти может привести к изменению данных в соседних строках из-за электромагнитных помех. Это явление, известное как "битовые сбои" (bit flips), можно использовать для изменения привилегий пользователя, обхода механизмов защиты и выполнения вредоносного кода. Более того, Rowhammer является уникальным типом атаки, который не требует традиционного программного эксплойта или уязвимости в операционной системе, а использует фундаментальные физические свойства компьютерной памяти.

Исследования показали, что Rowhammer может быть использована в реальных атаках. Например, злоумышленники могут эксплуатировать этот механизм для повышения прав доступа в системе, выполняя вредоносный код с привилегиями администратора. Вирусы, использующие Rowhammer, могут обходить песочницы и другие методы изоляции процессов, что делает их особенно опасными в многопользовательских средах и виртуальных машинах. Несмотря на предпринимаемые меры защиты, Rowhammer остаётся активной угрозой, требующей комплексного подхода к её нейтрализации.

Манипуляция данными в DRAM: как Rowhammer-атаки могут использоваться вирусами

Rowhammer-атака основана на особенностях работы современных чипов DRAM. В отличие от процессорной памяти (кэша), DRAM-хранилище использует конденсаторы для хранения битов информации. Эти конденсаторы расположены в ячейках памяти, сгруппированных в строки, которые хранят данные. Однако по мере увеличения плотности размещения транзисторов в современных чипах DRAM их чувствительность к электромагнитным помехам возросла. Это привело к тому, что частые обращения к определённой строке могут повлиять на данные в соседних строках, вызывая случайные изменения битов[1].

Для успешного выполнения Rowhammer-атаки злоумышленники используют специальный программный код, который быстро и многократно активирует определённые строки памяти, добиваясь появления битовых сбоев в соседних ячейках. Вредоносное ПО, использующее этот метод, может изменять критически важные данные, например, таблицы доступа пользователей или ключи аутентификации, что позволяет обходить стандартные механизмы безопасности[2].

В 2015 году исследователи Google показали, что Rowhammer можно использовать для получения root-доступа в операционной системе Linux. Они создали Proof-of-Concept эксплойт, который позволял обычному пользователю с низкими привилегиями изменять критически важные области памяти ядра, что приводило к захвату системы. В дальнейшем появилось множество вариаций атак, в том числе атаки через JavaScript, которые позволяли злоумышленникам использовать Rowhammer даже в браузере без необходимости локального доступа к устройству[3].

Опасность Rowhammer-атак заключается в том, что они могут применяться в различных сценариях. Например, вредоносные программы могут использовать эту уязвимость для выхода из песочницы, что представляет угрозу для виртуальных сред, браузеров и мобильных приложений. В случае с облачными сервисами Rowhammer-атака может быть использована для выхода за пределы виртуальной машины и компрометации других клиентов, работающих на той же аппаратной платформе[4].

Для защиты от Rowhammer-атак разработчики аппаратного и программного обеспечения внедряют различные методы защиты. Один из наиболее эффективных способов — использование механизмов коррекции ошибок (ECC, Error-Correcting Code), которые позволяют обнаруживать и исправлять случайные изменения битов в памяти. Однако не все системы поддерживают ECC, а его реализация увеличивает стоимость оборудования.

Другим способом защиты является программное ограничение доступа к памяти с высокой частотой. Например, современные версии операционных систем включают специальные алгоритмы, которые обнаруживают аномально частые обращения к памяти и блокируют потенциально вредоносные процессы. Также исследуются аппаратные решения, такие как увеличение физического расстояния между строками памяти или использование новых материалов, менее подверженных помехам[5].

Несмотря на эти меры, Rowhammer остаётся актуальной угрозой, поскольку новые исследования показывают способы обхода существующих механизмов защиты. Например, некоторые атаки позволяют обойти ECC-коррекцию за счёт одновременного изменения нескольких битов, а программные контрмеры могут быть нейтрализованы вредоносным кодом, имитирующим легитимные процессы.

С развитием технологий искусственного интеллекта и машинного обучения Rowhammer может стать ещё более опасной. Автоматизированные системы анализа уязвимостей способны находить оптимальные способы эксплуатации битовых сбоях, делая атаки более эффективными и труднообнаруживаемыми. Это создаёт дополнительные вызовы для специалистов по кибербезопасности, требуя постоянного совершенствования методов защиты.

Заключение

Rowhammer-атаки представляют собой уникальную угрозу в сфере информационной безопасности, так как они воздействуют непосредственно на аппаратное обеспечение, обходя традиционные программные механизмы защиты. Их особенность заключается в том, что они используют физические свойства компьютерной памяти, что делает их особенно сложными для обнаружения и предотвращения.

Несмотря на то, что исследователи предлагают различные методы защиты, включая коррекцию ошибок, программные контрмеры и аппаратные решения, Rowhammer остаётся активной угрозой, которая продолжает развиваться. Злоумышленники находят новые способы обхода защитных механизмов, а развитие облачных технологий и виртуализации делает возможным использование Rowhammer-атак в масштабных сценариях.

Для эффективной защиты систем необходимо использовать комплексный подход: внедрение ECC, постоянное обновление программного обеспечения, мониторинг активности памяти и повышение осведомлённости пользователей о рисках. Только комбинированные меры могут снизить вероятность успешной атаки и защитить критически важные данные от манипуляции с помощью Rowhammer.

Список литературы

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

2. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
3. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Научные технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.

References

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruевич, 1996.
 2. Chmutov M. V. et al. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture // Information security of the regions of Russia (IBRD-2017). Conference proceedings, 2017, pp. 535-537.
 3. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
 4. Lesnova E. M., Pestov I. E. Method development error detection and correction for a distributed information network based on big data // Regional Informatics and information Security. - 2018. – pp. 236-240.
 5. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS // Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056:004.438

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В KTOR: JWT, OAUTH, LDAP И KEYCLOAK

Пахомова П. В.

ФГБОУ ВО "ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Воронеж, Россия
(394018, Воронежская область, город Воронеж, Университетская пл., д. 1), e-mail:
polinapahomova12@mail.ru

Безопасность программных приложений является важнейшей проблемой в современной разработке программного обеспечения, особенно в условиях преобладания распределённых систем и микросервисов. Ktor выделяется как набирающий популярность фреймворк разработки с поддержкой экосистемы Java, которая предлагает широкий спектр возможностей для реализации надёжных механизмов безопасности. В этой статье основное внимание уделено изучению современных передовых подходов обеспечения безопасности корпоративных сред с использованием Ktor; в частности, будут обсуждаться такие темы, как веб-токен JSON (JWT), OAuth 2.0, облегчённый протокол доступа к каталогам (LDAP) и решения на основе Keycloak. Использование JWT позволяет реализовать аутентификацию без состояния (stateless authentication), что особенно важно в контексте распределённых систем. OAuth 2.0 служит стандартом авторизации, который предоставляет пользователям доступ к общим ресурсам, одновременно защищая конфиденциальные учётные данные пользователя от ненужного раскрытия. LDAP находит практическое применение, облегчая централизованное управление идентификационными данными и привилегированными доступами, что особенно выгодно при работе со сложными организационными структурами большого масштаба. Являясь платформенным решением с открытым исходным кодом, специально разработанным для распознавания личности и управляемой авторизации, Keycloak предоставляет службы поддержки, соответствующие общепринятым протоколам, таким как OpenID Connect или SAML; надёжные решения, необходимые для обеспечения чётко регламентированных конфиденциальных взаимодействий, например, в ситуациях, требующих надёжной проверки, вызванных как внутренними потребностями, так и внешними партнёрами по сети. В рамках Ktor данные механизмы интегрируются с помощью существующих библиотек. В этой статье в рамках Ktor исследовано, каким образом передовые технологии могут быть надлежащим образом использованы для создания безопасных и масштабируемых приложений. В ходе анализа подробно рассматривается каждый из этих механизмов, описываются их преимущества и проблемы, а также предложения по их решению и интеграции при возникновении сложных бизнес-сценариев. В конечном счёте, это исследование предназначено для улучшения понимания прогрессивных мер безопасности, тем самым предоставляя разработчикам расширенные возможности для создания более устойчивых прикладных решений.

Ключевые слова: Кибербезопасность, Ktor, Ktor Authentication, JWT, OAuth, LDAP, Keycloak.

MODERN APPROACHES TO SECURITY IN KTOR: JWT, OAUTH, LDAP AND KEYCLOAK

Pakhomova P. V.

VORONEZH STATE UNIVERSITY, Voronezh, Russia (394018, Voronezh region, Voronezh city,
Universitetskaya square, 1), e-mail: polinapahomova12@mail.ru

Software application security is a critical issue in modern software development, especially with the prevalence of distributed systems and microservices. Ktor stands out as a gaining popularity as a development framework with support for the Java ecosystem, which offers a wide range of options for implementing robust security mechanisms. This paper focuses on exploring current best practices for securing enterprise environments using Ktor; in particular, topics such as JSON Web Token (JWT), OAuth 2.0, Lightweight Directory Access Protocol (LDAP),

and Keycloak-based solutions will be discussed. The use of JWT enables stateful authentication, which is especially important in the context of distributed systems. OAuth 2.0 serves as an authorization standard that gives users access to shared resources while protecting sensitive user credentials from unnecessary disclosure. LDAP finds practical applications by facilitating centralized identity and privileged access management, which is especially beneficial when dealing with complex, large-scale organizational structures. As an open source platform solution specifically designed for identity recognition and managed authorization, Keycloak provides support services that are compliant with common protocols such as OpenID Connect or SAML; robust solutions necessary to ensure highly regulated sensitive interactions, such as those requiring strong verification, whether driven by internal needs or external network partners. The Ktor framework integrates these mechanisms using existing libraries. In this paper, the Ktor framework explores how advanced technologies can be appropriately utilized to create secure and scalable applications. The analysis examines each of these mechanisms in detail, describing their benefits and challenges, as well as suggestions for addressing and integrating them when complex business scenarios arise. Ultimately, this research is intended to improve the understanding of progressive security measures, thereby providing developers with enhanced capabilities to create more resilient application solutions.

Keywords: Cybersecurity, Ktor, Ktor Authentication, JWT, OAuth, LDAP, Keycloak.

Введение

Платформа Ktor становится наиболее популярным компонентом в разработке современных приложений. Впервые она была представлена в 2018 году и значительно улучшила развитие Kotlin как языка программирования для серверной разработки. В отличие от более традиционного подхода на основе Spring, Ktor предоставляет более легковесную архитектуру, которая может быть особенно полезна для приложений с высокой нагрузкой, требующих быстрого отклика. Одним из его главных преимуществ является его способность интегрироваться с фреймворком Spring и Java.

Если говорить о безопасности, то ключевой функцией в рамках этой платформы является Ktor Authentication; влиятельная и персонализированная система аутентификации и контроля доступа, которая играет решающую роль в защите приложений от распространенных угроз безопасности.

JSON Web Token (JWT) представляет а широко распространённую и устоявшуюся среду для безопасного обмена информацией в виде объектов JSON, эти токены выделяются своей компактностью, совместимостью с URL-адресами, поддержкой цифровой подписи, что приводит к улучшенным функциям безопасности, следовательно, является идеальным вариантом в контексте аутентификации без состояния в современных веб-приложениях [1] [10]. JWT обеспечивают бесперебойные механизмы, совместимые с общим решением для обеспечения безопасности несессионных функциональных возможностей, разработанных на основе методологии программирования Spring.

Платформа OAuth 2.0 служит средством авторизации, которое позволяет приложениям получать ограниченный доступ к учётным записям пользователей в службе HTTP. Этот процесс включает делегирование задач аутентификации пользователя службе хостинга [12]. Что касается Ktor Authentication, OAuth 2.0 представляет собой мощный метод защиты RESTful-сервисов и API-интерфейсов за счёт передачи функций аутентификации пользователей на аутсорсинг внешнему серверу авторизации.

Облегчённый протокол доступа к каталогам (LDAP) - широко используемый протокол для доступа к распределённым информационным службам каталогов и их обслуживания по сети Internet Protocol (IP). В Ktor Authentication LDAP играет ключевую роль в управлении идентификациями пользователей и контроле доступа, особенно в обширных корпоративных средах.

Keycloak - это решение с открытым исходным кодом для управления идентификацией и

доступом, которое обслуживает современные приложения и службы. Он обладает широким спектром функций, включая единый вход (SSO), посредничество при идентификации личности, а также возможности входа в систему через социальные сети. Keycloak эффективно интегрируется с платформами, предоставляя разработчикам беспрепятственный доступ к различным механизмам аутентификации наряду с протоколами авторизации, которые повышают параметры безопасности в среде их приложений.

Включение сложных механизмов безопасности, а именно JWT, OAuth, LDAP и Keycloak, в Ktor с помощью Ktor Authentication олицетворяет значительный прогресс в создании безопасных приложений на Kotlin. Такое объединение не только упрощает процесс внедрения сложных требований безопасности, но и гарантирует устойчивость этих приложений к широкому спектру атак.

1. JWT

Использование JWT приобрело значительное значение в современных практиках веб-безопасности, поскольку оно обеспечивает краткий и автономный подход к передаче информации между участниками через объект JSON, который обеспечивает конфиденциальность высокого уровня. JWT предназначены для включения механизмов подписи, что может быть достигнуто путём использования либо криптографии с секретным ключом с использованием алгоритма HMAC, либо публично-частного шифрования с использованием алгоритмов RSA или ECDSA, тем самым обеспечивая целостность данных во время передачи. При наличии таких протоколов аутентификации, которые не зависят от хранилища состояний сеанса, JWT обслуживает подходящие сценарии, такие как RESTful API [1].

JWT обычно состоит из трёх компонентов: заголовок, полезной нагрузки и подписи. Заголовок обычно состоит из двух частей, которые включают тип токена - то есть JWT - и оптимизируемый алгоритм подписи. Полезная нагрузка включает в себя утверждения относительно объекта (обычно пользователя) наряду с дополнительными данными. Наконец, чтобы гарантировать, что после проверки не было внесено никаких изменений, используются подписи для обеспечения подлинности с течением времени.

Ktor Authentication предлагает всестороннюю поддержку JWT. Его включение предоставляет разработчикам возможность решать проблемы аутентификации пользователей и авторизации с помощью непостоянного подхода, что оказывается существенно выгодным для RESTful-приложений. С помощью Ktor Authentication процедуры проверки JWT становятся доступными; они гарантируют, что JWT имеют правильное формирование, проверяют их подпись, а также достоверность. При внедрении JWT в приложение Ktor разработчики обычно полагаются на такие известные библиотеки, такие как `io.ktor:ktor-auth:2.x.x` или `io.ktor:ktor-auth-jwt:2.x.x`, они содержат основные ресурсы, необходимые для эффективного создания, анализа и аутентификации JWT. Процесс реализации включает в себя настройку `JwtTokenStore` и `JwtAccessTokenConverter` с одновременным предоставлением дополнительного `TokenEnhancer` для дополнения информации в токене. Кроме того, крайне важно, чтобы разработчики настроили менеджер аутентификации в дополнение к описанию ограничений безопасности, налагаемых на конечные точки (endpoints), используемые приложением.

Протокол JWT особенно полезен в ситуациях, когда важно установить подлинность

пользователя и необходимые доступы к определённым ресурсам. Это служит дополнительным преимуществом в архитектуре микросервисов, где безопасная межсервисная коммуникация становится обязательной. Для оптимального использования JWT с Ktor установленные рекомендации включают развёртывание HTTPS для защиты токенов от угроз перехвата, установление реалистичных сроков истечения срока действия токенов и разумное управление информацией, относящейся к разделам полезной нагрузки, чтобы конфиденциальные данные не могли быть случайно раскрыты.

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0dEBnbWFpbC5jb20iLCJpc3N1ZWREYXR1IjoimjAyNS0wMS0wNFQxMjoxNjowOC4yNDAYOTI3MDAiLCJpYXQiOiJlZ3MzU5OTI5Njh9.v2ESSXy6V6fRX_HBw9rT2w3vbF7RqDsBMuj0uF9EE34
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "HS256",  "typ": "JWT"}
```

PAYLOAD: DATA

```
{  "sub": "tt@gmail.com",  "issuedDate": "2025-01-04T12:16:08.240292700",  "iat": 1735992968}
```

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  your-256-bit-secret)
```

☐ secret base64 encoded

Рисунок 1 - Структура JWT в формате JSON.

Включение JSON в Ktor Authentication обеспечивает надёжный и эффективный подход к управлению аутентификацией и авторизацией в неизменяемом интерфейсе. Его универсальность в сочетании с удобством в использовании делают его оптимальной альтернативой для защиты приложений, основанных на Ktor, особенно тех, которые структурированы вокруг микросервисов, а также услуг RESTful.

2. OAuth 2.0

OAuth 2.0 - это платформа авторизации, которая предоставляет сторонним приложениям ограниченный доступ к HTTP-сервису, будь то через владельца ресурса или автономное получение доступа. Его отличие от аутентификации делает его незаменимым в ситуациях, когда пользовательские данные должны запрашиваться у других служб без ущерба для их соответствующих учётных данных [3].

OAuth 2.0 вводит несколько ролей:

- владелец: Пользователь, который разрешает приложению доступ к своей учётной записи;
- сервер ресурсов: На нём хранятся защищённые пользовательские данные;
- клиент: Приложение, запрашивающее доступ к учётной записи пользователя;

Сервер авторизации проверяет личность владельца ресурса и выдаёт токены доступа.

OAuth 2.0 определяет четыре основных типа грантов, подходящих для различных типов

приложений:

- предоставление кода авторизации: Идеально подходит для клиентов, которые могут безопасно хранить клиентские секреты;
- неявное предоставление: Предназначено для клиентов, которые не могут безопасно хранить клиентские секреты;
- предоставление учётных данных с паролем владельца ресурса: Подходит для клиентов с высоким уровнем доверия;
- предоставление учётных данных клиента: Используется для доступа приложений к их собственным ресурсам.

Поддержка OAuth 2.0 в Ktor Authentication упрощает реализацию этих типов грантов:

- конфигурация серверов авторизации и ресурсов: В Ktor для настройки аутентификации через OAuth 2.0 можно использовать установку обработчиков, например, через Authentication с использованием обработчиков типа oauth (используются `authorizeUrl`, `accessTokenUrl`, `clientId`, `clientSecret` и области доступа);
- ведения о клиенте: Можно настроить клиентские данные, такие как `client_id`, `client_secret`, и области доступа (`scopes`), с помощью параметров в конфигурации OAuth 2.0. Эти данные необходимы для успешной аутентификации и получения токенов от сервера авторизации;
- управление токенами: Внедрение хранилища токенов и службы токенов для управления генерацией, сроком действия и обновлением токенов;
- конфигурация безопасности: Определение ограничения безопасности для различных конечных точек, какие из них защищены, а какие общедоступны.

Так же Ktor Authentication OAuth 2.0 предоставляет несколько расширенных функций, среди них - усилители пользовательских токенов, которые позволяют добавлять дополнительные данные к токенам OAuth, а также обработчики утверждений, предназначенные для управления утверждениями пользователей при выдаче токенов. Доступны конечные точки (`endpoints`) для обработки перенаправлений пользователя после аутентификации и для предоставления информации о пользователе клиентам. Эти функции значительно расширяют возможности аутентификации и позволяют гибко настраивать процессы безопасности в приложениях.

К числу передовых практик, которые способствуют повышению уровня безопасности, относятся защита клиентских секретов, что требует их безопасного хранения и недопущения раскрытия в клиентском коде. Важно также проверять URI перенаправления, чтобы все перенаправления были предварительно зарегистрированы и проверены, что исключает риск несанкционированных редиректов. Для обеспечения безопасности токенов необходимо использовать HTTPS во всех коммуникациях, связанных с токенами и учетными данными, а также внедрять стратегии отзыва и ротации токенов для предотвращения утечек и атак [16].

Благодаря стратегическому использованию возможностей конфигурации и автоматизации Ktor разработчики имеют возможность адаптировать реализацию OAuth 2.0 для различных требований приложений, обеспечивая при этом оптимальную функциональность и соблюдение мер безопасности.

3. LDAP

Облегченный протокол доступа к каталогам (LDAP) - широко используемый протокол, предназначенный для доступа к распределенным информационным службам каталогов и поддержания их функциональности в сети по интернет-протоколу (IP). LDAP служит для различных целей, включая, но не ограничиваясь, поиск по электронной почте, процессы аутентификации, а также организацию данных компании. Это оказалось особенно выгодным с точки зрения облегчения управления пользовательской информацией наряду с обеспечением возможностей аутентификации и авторизации в обширных корпоративных средах [4] [13].

В Ktor LDAP функционирует как фундаментальный источник как пользовательских данных, так и аутентификации. Благодаря широкой поддержке он эффективно облегчает бесшовную интеграцию с уже существующими серверами LDAP. Следовательно, эта синергия предоставляет приложениям возможность проверять пользователей, одновременно извлекая соответствующую информацию о роли пользователя, которая была сохранена в независимом каталоге в базе данных LDAP.

Реализация аутентификации LDAP в приложении Ktor обычно включает в себя несколько этапов:

- зависимости: Включите в свой проект зависимости Ktor LDAP;
- конфигурация источника LDAP Context: Настройте `LdapContextSource` для указания URL-адреса и базового суффикса сервера LDAP;
- провайдер аутентификации: Настройте `LdapAuthenticationProvider` для обработки всех запросов аутентификации. Это включает в себя указание базы поиска пользователя, фильтра поиска пользователя и, при необходимости, базы группового поиска и фильтра группового поиска;
- сопоставление сведений о пользователе: Это может включать использование собственных классов для сопоставления данных из LDAP с объектами пользователя в Ktor, а также настройку ролей и прав доступа, что можно сделать с помощью специализированных популяторов ролей и мапперов данных;
- конфигурация безопасности: Определите ограничения безопасности в конфигурации Ktor, указав, какие конечные точки (endpoints) защищены, а какие общедоступны.

Так же интеграция с LDAP может включать расширенные функции, такие как реализация службы для более сложного поиска пользовательской информации. Это позволяет улучшить работу с пользовательскими данными, а также внедрить механизмы для настройки политик паролей и обработки исключений, связанных с безопасностью паролей. Дополнительно, использование LDAP-операций может быть реализовано через специализированные шаблоны, такие как `LdapTemplate`, которые предоставляют более гибкие и сложные возможности для работы с LDAP, помимо базовой аутентификации.

При внедрении LDAP в Ktor важно следовать лучшим практикам безопасности. Это включает использование защищенного канала связи с сервером LDAP (например, через LDAP с SSL), чтобы обеспечить безопасность передаваемых данных. Кроме того, критически важно правильно обрабатывать пароли, избегая их небезопасного хранения или регистрации. Также необходимо защищать приложение от атак с использованием LDAP-инъекций, что достигается проверкой и очисткой входных данных для предотвращения несанкционированных попыток доступа [4].

Включение LDAP в приложение Ktor представляет собой высокоэффективный подход к

управлению аутентификацией пользователей и авторизацией в корпоративных приложениях. Благодаря выгодному использованию встроенной поддержки LDAP в Ktor - разработчики программного обеспечения смогут устанавливать бесперебойную связь с каталогами LDAP, одновременно повышая безопасность и масштабируемость в рамках соответствующих прикладных задач.

4. Keycloak

Keycloak - это современное решение для управления идентификацией и доступом, разработанное Red Hat в виде программного обеспечения с открытым исходным кодом. Его основная цель заключается в упрощении интеграции стандартных протоколов, таких как OpenID Connect и SAML 2.0, в процессы аутентификации при одновременном упрощении процедур авторизации. В дополнение к возможностям централизованной консоли управления, касающимся идентификации пользователей, Keycloak предоставляет функции, обеспечивающие эффективную поддержку единого входа, двухфакторной аутентификации и функций социального входа. Эти расширенные возможности безопасности делают его особенно подходящим для обеспечения целостности современных приложений в различных сервисных средах, где высоко ценятся индивидуальные решения по управлению идентификацией [5] [11].

В контексте Ktor Authentication - Keycloak даёт приложениям Ktor возможность делегировать свои протоколы аутентификации пользователей и авторизации непосредственно Keycloak-динамике, которая впоследствии упрощает усилия по управлению безопасностью. Кроме того, эта интеграция предоставляет указанным приложениям доступ к расширенным функциям, эксклюзивным для Keycloak; примеры включают единый вход, меры аутентификации на основе токенов в дополнение к возможностям объединения пользователей.

Внедрение Keycloak в приложение Ktor обычно включает в себя несколько этапов:

- зависимости: Включите зависимость Keycloak в свой проект;
- настройка сервера перехвата ключей: Настройте сервер перехвата ключей, определив области, клиентов, роли и пользователей;
- конфигурация приложения: Настройте приложение Ktor на использование Keycloak для аутентификации и авторизации. Это включает в себя настройку свойств скрытия ключей в `application.conf` или `application.yml` файле;
- конфигурация безопасности: Настройте Ktor на использование адаптера Keycloak для аутентификации. Это включает в себя определение ограничений безопасности и указание защищенных ресурсов в приложении;
- управление пользователями и ролями: Используйте консоль администрирования Keycloak для управления пользователями и ролями, которые могут быть сопоставлены с полномочиями Ktor Authentication.

Так же Keycloak предоставляет расширенные возможности настройки, такие как добавление и управление пользовательскими атрибутами, что позволяет гибко управлять данными пользователей. Можно настроить посредничество при идентификации, чтобы Keycloak выполнял роль промежуточного звена для аутентификации между различными поставщиками идентификационных данных, обеспечивая единую точку входа. Вдобавок, существует возможность настройки темы для Keycloak, это позволит персонализировать внешний вид страниц входа и электронных писем, улучшая пользовательский интерфейс и

опыт.

При интеграции следует придерживаться ряда рекомендаций для обеспечения безопасности. В первую очередь, необходимо обеспечить безопасную коммуникацию между приложением Ktor и сервером Keycloak, используя HTTPS для защиты данных. Также важно безопасно управлять клиентскими секретами, избегая их утечек и несанкционированного доступа. Наконец, следует внедрить надёжную проверку токенов, чтобы убедиться, что доступ к защищенным ресурсам имеет только авторизованный пользователь, предотвращая возможность несанкционированного доступа [18].

Такая интеграция предлагает мощное и гибкое решение для управления аутентификацией и авторизацией в приложениях. Используя Keycloak, разработчики могут повысить безопасность своих приложений, используя преимущества таких функций, как единый вход, аутентификация на основе токенов и федерация пользователей.

5. Обзор литературы

JSON Web Tokens (JWT) остаются важнейшим инструментом в обеспечении безопасности веб-приложений. В статье, опубликованной в 2020 году, подчёркивается, что использование JWT для аутентификации и авторизации позволяет значительно повысить защиту от атак, таких как фальсификация токенов и их повторное использование. В частности, исследование указывает на важность использования JWT вместе с механизмами мониторинга активности пользователей, что улучшает защиту путём обнаружения аномальных действий, таких как попытки несанкционированного доступа. Это, в свою очередь, повышает общую безопасность системы [1].

В научной статье 2023 года обсуждается использование JSON Web Token (JWT) для аутентификации между сервисами в микросервисных приложениях. Отмечается, что JWT позволяет реализовать безсессионный механизм аутентификации, что особенно важно для высоконагруженных систем, требующих масштабируемости и эффективности. Авторы также рассматривают преимущества использования JWT в таких сценариях и приводят примеры его применения [2].

Другим важным аспектом является интеграция OAuth 2.0 в микросервисные архитектуры. Согласно статье 2023 года, использование OAuth 2.0 в таких приложениях позволяет обеспечить высокий уровень безопасности, а также гарантировать контроль над доступом через различные типы грантов. Предлагается модель управления доступом на основе атрибутов для кросс-доменных API, включающая архитектурные решения и принципы ABAC и OAuth. ABAC-сервис авторизации рассматривается как микросервис или набор микросервисов, что обеспечивает совместимость с приложениями, построенными на микросервисной архитектуре. Системы, использующие Ktor Authentication, могут гибко адаптировать авторизацию в зависимости от нужд приложения и пользователя. В этом контексте важно отметить, что OAuth 2.0 помогает интегрировать токенизацию и права доступа на уровне отдельных микросервисов, что особенно полезно для распределённых систем [3].

Параллельно с OAuth 2.0 стоит рассмотреть и возможности LDAP (Lightweight Directory Access Protocol) для управления аутентификацией и авторизацией пользователей. Статья 2023 года показала, что LDAP интегрируется с различными веб-фреймворками, в том числе с Ktor, для обеспечения централизованного управления учётными записями в крупных организациях

[4]. Важной деталью является возможность интеграции LDAP с другими системами безопасности, такими как SAML и OpenID Connect, что расширяет возможности для настройки гибкой и безопасной авторизации в многослойных инфраструктурах [17].

Для более сложных сценариев аутентификации и авторизации в корпоративных системах, Keycloak становится ключевым компонентом. В статьях 2023 года утверждается, что Keycloak позволяет обеспечить управление пользователями, автоматическое распределение ролей и реализацию политики безопасности в реальном времени, что делает его отличным выбором для предприятий, которым необходимы надёжные механизмы защиты API и пользовательских данных [5] [11].

Наконец, использование JWT в легковесных протоколах обмена сообщениями, таких как MQTT, подтверждается исследованием 2019 года, в котором анализировались возможности аутентификации и авторизации для устройств в IoT-средах. JWT, будучи компактным и быстрым для обработки, идеально подходит для работы с протоколами с ограниченными ресурсами, такими как MQTT, и может использоваться для безопасного обмена сообщениями в реальном времени. Исследование показало, что использование JWT совместно с MQTT позволяет создавать высокозащищенные IoT-системы, что актуально для приложений, работающих в облачных и распределённых средах [6].

Заключение

Благодаря своей модульной архитектуре и возможностям настройки, Ktor позволяет разработчикам интегрировать различные механизмы безопасности, при этом каждый компонент обладает своими преимуществами и недостатками. В частности, JWT может похвастаться функциональностью без сохранения состояния, а также возможностью масштабирования, что делает его подходящим для современных веб-приложений; однако тщательный мониторинг безопасности токенов имеет решающее значение для предотвращения любой потенциальной уязвимости или риска кражи. OAuth 2.0 служит обширной, но способной к адаптации структурой авторизации, подходящей для различных типов приложений; тем не менее сложность может представлять проблемы во время внедрения, в то время как строгое соблюдение рекомендаций по передовой практике должно постоянно поддерживаться на протяжении всей работы. LDAP превосходен в управлении идентификациями пользователей в обширных операционных средах с помощью централизованных механизмов аутентификации, но настройка может создавать значительные логистические препятствия, особенно когда сталкиваются с быстро меняющимися наборами данных, требующими постоянной корректировки по сравнению с имеющимися альтернативными решениями. Наконец, интеграция Keycloak в микросервисные архитектуры позволяет проще обрабатывать комплексные функции управления доступом к идентификаторам, значительно сокращая потребности в администрировании, хотя одновременно предъявляет дополнительные требования к конфигурации сервера, возможно, приводя к проблемам снижения производительности, без уделения тщательного внимания оптимизации и определения эффективных компромиссов относительно требуемых конкретных ограничений пропускной способности инфраструктуры. Keycloak, предоставляемый посредством интеграции, позволяет эффективно запускать все эти методы с использованием Ktor Authentication, обеспечивает надёжную общую защиту системы, обеспечивающую максимальное снижение негативных уязвимостей, возникающих в

результате оптимального развертывания, следуя исчерпывающему пониманию фундаментальных принципов, определяющих надежное безопасное управление операциями экосистемы, широко применимых во многих отраслевых вертикалях, извлекающих из этого немалую выгоду после успешного завершения внедрения, достижения стратегических бизнес-целей, нацеливания бизнеса на получение прибыльных результатов, получения конкурентного преимущества перед аналогами, не использующими инновационные подходы для соответствующей защиты своих информационных технологических систем в будущем.

Список литературы

1. Pooja M., Uma P. Insights of JSON Web Token. 2020.
2. Зими́на К.И. и Лапо́нина О.Р. Механизмы межсервисной аутентификации в приложениях с микросервисной архитектурой. 2023.
3. А.В. Беловодов, О.Р. Лапонина Использование управления доступом на основе атрибутов в протоколе OAuth 2.0. 2023.
4. Balaji V. Andres S. Advanced Spring LDAP. 2023.
5. Danso S. D., Yin C. API Security: Protecting APIs With Keycloak. 2023.
6. Krishna S. JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT). 2019.
7. Ж. Стоянов, И. Христоский Направления будущих исследований и рекомендации по развитию микросервисной архитектуры. 2024.
8. Ł. Wyciślik, Ł. Latusik, A. M. Kamińska A comparative assessment of jvm frameworks to develop microservices. 2023.
9. R. Hat Keycloak-open source identity and access management. 2021.
10. A. Bucko, K. Vishi, B. Krasniqi, B. Rexha, Enhancing JWT Authentication and Authorization in Web Applications. 2023.
11. A. Chatterjee, A. Prinz Applying Spring Security Framework with Keycloak-based OAuth2. 2022.
12. D. Hardt The OAuth 2.0 Authorization Framework. 2012.
13. M. Rouse LDAP (Lightweight Directory Access Protocol). 2019.
14. M. G. de Almeida, E. D. Canedo Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. 2022.
15. T. Sylla, L. Mendiboure, M. A. Chalouf, F. Krief Blockchain-based Context-Aware Authorization Management as a Service in IoT. 2021.
16. A. Hoffman Web Application Security: Exploitation and Countermeasures for Modern Web Applications. 2020.
17. S.Thorgersen, P. I. Silva Keycloak - Identity and Access Management for Modern Applications: Harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications. 2021.

References

1. Pooja M., Uma P. Insights of JSON Web Token. 2020.
2. K.I. Zimina, O.R. Laponina Cross-Service Authentication Mechanisms in Applications with Microservice Architecture. 2023.
3. A.V. Belovodov, O.R. Laponina Using attribute-based access control in OAuth 2.0. 2023.

4. Balaji V. Andres S. Advanced Spring LDAP. 2023.
 5. Danso S. D., Yin C. API Security: Protecting APIs With Keycloak. 2023.
 6. Krishna S. JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT). 2019.
 7. Z. Stojanov, I. Hristoski Research Trends and Recommendations for Future Microservices Research. 2024.
 8. Ł. Wyciślik, Ł. Latusik, A. M. Kamińska A comparative assessment of jvm frameworks to develop microservices. 2023.
 9. R. Hat Keycloak-open source identity and access management. 2021.
 10. A. Bucko, K. Vishi, B. Krasniqi, B. Rexha, Enhancing JWT Authentication and Authorization in Web Applications. 2023.
 11. A. Chatterjee, A. Prinz Applying Spring Security Framework with Keycloak-based OAuth2. 2022.
 12. D. Hardt The OAuth 2.0 Authorization Framework. 2012.
 13. M. Rouse LDAP (Lightweight Directory Access Protocol). 2019.
 14. M. G. de Almeida, E. D. Canedo Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. 2022.
 15. T. Sylla, L. Mendiboure, M. A. Chalouf, F. Krief Blockchain-based Context-Aware Authorization Management as a Service in IoT. 2021.
 16. A. Hoffman Web Application Security: Exploitation and Countermeasures for Modern Web Applications. 2020.
 17. S.Thorgersen, P.I.Silva Keycloak - Identity and Access Management for Modern Applications: Harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications. 2021.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

КАК АТАКОВАТЬ СИСТЕМЫ, ИЗОЛИРОВАННЫЕ ОТ СЕТИ, ЧЕРЕЗ АКУСТИЧЕСКИЕ КОЛЕБАНИЯ ВЕНТИЛЯТОРОВ

Ворошилов Д.В.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
superdaniil2002@yandex.ru

Системы, изолированные от сети (air-gapped systems), традиционно считаются одними из самых защищённых, поскольку они физически отключены от интернета и корпоративных сетей. Однако исследователи в области кибербезопасности разработали методы атак, использующие акустические колебания компьютерных компонентов, таких как вентиляторы, для передачи данных. В данной статье рассматривается принцип работы такого метода, его техническая реализация, потенциальные риски и способы защиты, включая мониторинг акустических аномалий и физическую изоляцию критически важных систем.

Ключевые слова: Изолированные системы, air-gap, атака через акустику, утечка данных, вентиляторы, вибрации, инфосек, кибербезопасность.

HOW TO ATTACK SYSTEMS ISOLATED FROM THE NETWORK THROUGH ACOUSTIC VIBRATIONS OF FANS

Voroshilov D.V.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: superdaniil2002@yandex.ru

Air-gapped systems are traditionally considered among the most secure because they are physically disconnected from the internet and corporate networks. However, cybersecurity researchers have developed attack methods that utilize acoustic vibrations of computer components, such as fans, to transmit data. This article explores the working principle of this method, its technical implementation, potential risks, and protection strategies, including acoustic anomaly monitoring and physical isolation of critical systems.

Keywords: Isolated systems, air-gap, acoustic attack, data leakage, fans, vibrations, infosec, cybersecurity.

Введение

В современном мире информационной безопасности одной из самых надёжных стратегий защиты является изоляция систем от сети. Air-gapped системы широко применяются в государственных учреждениях, военной сфере, ядерной энергетике и других критически важных инфраструктурах для предотвращения кибератак и утечек данных. Такие системы не подключены к интернету и корпоративным сетям, что делает невозможными традиционные методы атак через удалённый доступ или вредоносное ПО, распространяемое по сети.

Однако даже изолированные системы не являются абсолютно безопасными. Исследования в области кибербезопасности показывают, что злоумышленники могут

использовать нетрадиционные методы атак, в том числе побочные каналы передачи данных. Одним из таких методов является эксплуатация акустических колебаний вентиляторов компьютера. Этот способ позволяет передавать информацию из изолированной системы в контролируемую злоумышленником среду с использованием изменения скорости вращения вентиляторов, создающих различающиеся акустические сигналы.

В данной статье рассматривается принцип работы атак через акустические колебания вентиляторов, механизм их реализации, возможные сценарии применения и методы защиты. Несмотря на сложность подобных атак, они демонстрируют, что даже физическая изоляция системы не является гарантией полной безопасности.

Как атаковать системы, изолированные от сети, через акустические колебания вентиляторов

Изолированные системы (air-gapped systems) применяются для защиты особо важных данных, поскольку их физическое отключение от внешних сетей делает невозможными традиционные кибератаки, основанные на удалённом доступе. Однако современные исследования в области безопасности демонстрируют, что даже такие системы не являются абсолютно защищёнными. Одним из самых необычных и сложных методов атак на изолированные компьютеры является использование акустических колебаний их внутренних компонентов, в частности вентиляторов, для передачи данных в контролируемую злоумышленником среду[1].

Этот метод основан на том, что скорость вращения вентиляторов в компьютерах и серверах может изменяться программно, а изменение скорости создаёт характерные акустические колебания. Эти колебания могут быть зафиксированы микрофонами, находящимися в непосредственной близости от атакуемой системы, включая смартфоны, умные колонки или даже специализированные устройства для перехвата ультразвуковых сигналов. Код, управляющий атакой, может модифицировать скорость вращения вентиляторов таким образом, чтобы создать закодированную последовательность звуковых сигналов, содержащих полезную нагрузку[2].

Для успешного осуществления такой атаки злоумышленникам требуется несколько ключевых условий. Во-первых, вредоносное ПО должно быть предварительно установлено на изолированной системе. Это может быть достигнуто через заражённые USB-носители, компрометацию обновлений ПО или физический доступ к машине. Во-вторых, вблизи атакуемой системы должен находиться приёмник, способный зафиксировать звуковые сигналы. В качестве такого приёмника могут выступать смартфоны сотрудников, умные устройства или даже устройства IoT, которые имеют встроенные микрофоны и соединение с интернетом[3].

Принцип передачи данных через акустические колебания заключается в модуляции частоты звука, создаваемого вентиляторами. Например, изменение скорости вращения вентилятора может быть использовано для кодирования двоичных данных, где определённая частота означает "0", а другая — "1". Это позволяет передавать небольшие объёмы информации, такие как пароли, криптографические ключи или другие конфиденциальные данные[4].

Преимущества такого метода атаки заключаются в том, что он не требует традиционных каналов передачи данных и сложно обнаруживается стандартными средствами защиты.

Антивирусное ПО, межсетевые экраны и даже системы обнаружения вторжений не способны предотвратить утечку информации через акустические каналы. Однако у этой атаки есть и ограничения: скорость передачи данных остаётся крайне низкой, обычно в диапазоне 10-50 бит в секунду, что делает невозможной передачу больших объёмов информации.

Защита от подобных атак требует комплексного подхода. Один из основных способов защиты — это контроль над возможными точками утечки данных. Например, можно запрещать или ограничивать использование мобильных устройств вблизи критически важных систем, а также изолировать атакуемые машины в звуконепроницаемых помещениях. Ещё один эффективный метод — это мониторинг аномального поведения вентиляторов и акустической активности в серверных комнатах. Если скорость вращения вентиляторов изменяется без видимой причины, это может свидетельствовать о попытке передачи данных[5].

Дополнительно можно применять физические методы защиты, такие как использование систем шумоподавления или генераторов белого шума, которые маскируют акустические сигналы, предотвращая их фиксацию приёмными устройствами. Некоторые организации уже используют такие методы для защиты от атак через ультразвуковые каналы, применяя акустические глушители и экранированные серверные помещения.

Заключение

Современные методы атак на информационные системы выходят далеко за рамки традиционных хакерских инструментов. Эксплуатация акустических колебаний вентиляторов для утечки данных показывает, насколько изощрёнными могут быть способы компрометации даже самых защищённых систем. Изолированные от сети системы долгое время считались практически неуязвимыми, однако исследования в области кибербезопасности доказывают, что ни одна защита не является абсолютной.

Хотя атаки такого типа пока остаются редкостью, они представляют серьёзную угрозу для организаций, работающих с критически важными данными. Учитывая сложность их обнаружения, традиционные антивирусные средства и системы мониторинга сетевого трафика неэффективны против таких атак. Поэтому защита от них требует комплексных мер, включая физическую изоляцию, мониторинг акустических сигналов, использование белого шума и программные ограничения на управление аппаратными компонентами.

С развитием технологий безопасность информационных систем требует всё более продвинутых решений. В мире, где даже вентиляторы могут стать инструментом утечки данных, кибербезопасность перестаёт быть вопросом только программных барьеров.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
4. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
5. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 107-110.

References

1. Gelfand A.M. et al. Development of a self-modifying code distribution model in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. No. 8. pp. 91-97.
 2. Orlov G. A., Krasov A.V., Gelfand A.M. Application of Big Data in the analysis of big data in computer networks //High-tech technologies in space exploration of the Earth. 2020. – Vol. 12. – No. 4. – pp. 76-84.
 3. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelec communications in science and education (APINO 2019). – 2019. – pp. 262-266.
 4. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: actual aspects of the "National Research Institute of National Development". July 2018. – 2018. – pp. 31-35.
 5. Birikh E. V. and others. Research of issues of increasing the level of protection of executive authorities //Actual problems of infotelec communications in science and education (APINO 2018), 2018, pp. 107-110.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.9

СОЗДАНИЕ ИСКУССТВЕННЫХ НОВОСТЕЙ ДЛЯ МАНИПУЛЯЦИИ АЛГОРИТМАМИ ПОИСКОВЫХ СИСТЕМ

Ворошилов Д.В.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большеви́ков, 22, корп. 1), e-mail: superdaniil2002@yandex.ru

В эпоху цифровой информации манипуляция алгоритмами поисковых систем стала инструментом влияния на общественное мнение. Создание искусственных новостей позволяет недобросовестным источникам продвигать ложные или искажённые сведения, влияя на информационную повестку. В статье рассматриваются методы создания и распространения фейковых новостей, их влияние на алгоритмы поисковых систем и механизмы борьбы с подобными манипуляциями, включая совершенствование алгоритмов ранжирования и развитие методов выявления недостоверного контента.

Ключевые слова: Фейковые новости, манипуляция поисковыми системами, алгоритмы ранжирования, информационная безопасность, дезинформация, SEO-манипуляции.

CREATING FAKE NEWS TO MANIPULATE SEARCH ENGINE ALGORITHMS

Voroshilov D.V.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: superdaniil2002@yandex.ru

The manipulation of search engine algorithms has become a powerful tool for influencing public opinion in the digital age. The creation of fake news allows unreliable sources to promote false or distorted information, shaping the information landscape. This article explores the methods of creating and distributing fake news, their impact on search engine algorithms, and mechanisms for combating such manipulations, including improvements in ranking algorithms and the development of methods for detecting unreliable content.

Keywords: Fake news, search engine manipulation, ranking algorithms, information security, disinformation, SEO manipulation.

Введение

В современном мире интернет является основным источником информации для большинства людей, а поисковые системы играют ключевую роль в её распространении. Алгоритмы ранжирования, используемые такими системами, как Google и Yandex, определяют, какие страницы попадут в топ выдачи, а значит, какие сведения будут восприняты пользователями как наиболее достоверные. Однако эти алгоритмы не всегда способны отличить правдивый контент от фейкового, чем активно пользуются злоумышленники, создавая искусственные новости для продвижения определённых идей, манипуляции общественным мнением или даже для коммерческих целей.

Распространение фейковых новостей стало острой проблемой, поскольку дезинформация способна влиять на политические процессы, финансовые рынки и общественные настроения. Применяя различные SEO-техники, злоумышленники могут вывести ложную информацию в топ поисковой выдачи, тем самым увеличивая её доверие среди пользователей. Это делает проблему не просто актуальной, но и угрожающей информационной безопасности как отдельных пользователей, так и целых государств.

Создание искусственных новостей для манипуляции алгоритмами поисковых систем

Фейковые новости создаются с целью влияния на общественное мнение или продвижения определённых интересов. Основной принцип заключается в том, чтобы подстроить контент под алгоритмы поисковых систем, обеспечив его видимость в топе поисковой выдачи. Для этого используются несколько методов, каждый из которых играет важную роль в процессе распространения ложной информации[1].

Один из ключевых инструментов для продвижения фейковых новостей — это SEO-оптимизация. Злоумышленники анализируют, какие ключевые слова и фразы чаще всего ищут пользователи, и включают их в текст, заголовки и метаописания своих материалов. Это позволяет обойти алгоритмы фильтрации и сделать ложную информацию максимально релевантной для поисковых систем. Кроме того, активно используются так называемые "контентные фермы" — сети сайтов, публикующие однотипные или переписанные статьи, увеличивающие индексруемость ложных сведений[2].

Ещё одним способом продвижения дезинформации является использование ботов и сетей фейковых аккаунтов в социальных сетях. Автоматизированные системы генерируют репосты, комментарии и лайки, создавая видимость популярности фейковой новости. В результате поисковые алгоритмы воспринимают материал как "актуальный" и поднимают его выше в результатах выдачи[3].

Кроме того, злоумышленники могут использовать взломанные или специально созданные сайты с высоким уровнем доверия, чтобы размещать там фейковый контент. Такие ресурсы, уже имея репутацию надёжных источников, способствуют распространению ложных сведений через поисковики, поскольку их материалы воспринимаются как заслуживающие доверия[4].

Одним из самых изощрённых методов является "петля подтверждения", когда несколько фейковых сайтов ссылаются друг на друга, создавая иллюзию достоверности информации. Поисковые алгоритмы, основанные на оценке ссылочной массы, могут принять такую информацию за правду, что приводит к её массовому распространению.

Чтобы бороться с подобными манипуляциями, поисковые системы разрабатывают всё более сложные алгоритмы проверки достоверности контента. Google, например, внедрил технологию E-E-A-T (Experience, Expertise, Authoritativeness, Trustworthiness — опыт, экспертиза, авторитетность, надёжность), которая оценивает не только содержание статьи, но и авторитетность источника. Однако злоумышленники находят способы обхода таких проверок, создавая псевдонаучные публикации или ссылаясь на якобы экспертные мнения[5].

Несмотря на все усилия поисковых систем, проблема фейковых новостей остаётся актуальной. Манипуляции алгоритмами могут оказывать влияние не только на общественное

мнение, но и на важные экономические и политические процессы. В связи с этим возникает необходимость в более жёстких мерах контроля за распространяемой информацией.

Заключение

Создание искусственных новостей с целью манипуляции алгоритмами поисковых систем является серьёзной угрозой для информационной безопасности. Используя методы SEO, ботовые сети и поддельные источники, злоумышленники способны продвигать ложную информацию, создавая у пользователей ложное представление о реальности.

Поисковые системы, такие как Google и Yandex, активно разрабатывают механизмы борьбы с фейковыми новостями, внедряя алгоритмы, оценивающие достоверность источников и анализирующие поведенческие факторы пользователей. Однако борьба с дезинформацией остаётся сложной задачей, так как злоумышленники постоянно находят новые способы обхода фильтров.

Для эффективного противодействия распространению фейковых новостей необходим комплексный подход, включающий развитие технологий анализа контента, усиление контроля над источниками информации и повышение цифровой грамотности пользователей. В условиях стремительного роста цифровой информации осведомлённость о методах манипуляции данными становится ключевым фактором защиты от дезинформации.

Список литературы

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределённых информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. – 2004.
4. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
5. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 92-101.

References

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
2. Minyaev A. A. Method for evaluating the effectiveness of information security systems of geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020). 2020. pp. 716-719.
3. Dushin S. E. et al. Synthesis of structurally complex nonlinear control systems. – 2004.

4. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
 5. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology // Ophthalmosurgery. – 2022. – No. 4s. – pp. 92-101.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.736

ВИРУСЫ, ИСПОЛЬЗУЮЩИЕ УЯЗВИМОСТИ В МЕХАНИЗМЕ PREFETCH И SUPERFETCH В WINDOWS

Бютнер С.И.

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

Механизмы Prefetch и Superfetch в операционных системах Windows предназначены для ускорения работы приложений за счет предварительной загрузки часто используемых данных в память. Однако, эти функции также могут быть использованы злоумышленниками для распространения вирусов и выполнения произвольного кода. В статье рассматриваются уязвимости, связанные с этими механизмами, способы их эксплуатации вредоносными программами, а также методы защиты, такие как обновления системы, настройка безопасности и ограничение прав доступа.

Ключевые слова: Вирусы, Prefetch, Superfetch, уязвимости, Windows, безопасность, защита, эксплуатация, обновления.

VIRUSES EXPLOITING VULNERABILITIES IN PREFETCH AND SUPERFETCH IN WINDOWS

Buetner S.I.

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

The Prefetch and Superfetch mechanisms in Windows operating systems are designed to speed up application performance by preloading frequently used data into memory. However, these features can also be exploited by attackers to spread viruses and execute arbitrary code. The article discusses vulnerabilities related to these mechanisms, how malicious software exploits them, and protection methods such as system updates, security configuration, and access control restrictions.

Keywords: Viruses, Prefetch, Superfetch, vulnerabilities, Windows, security, protection, exploitation, updates.

Введение

Механизмы Prefetch и Superfetch в операционных системах Windows играют ключевую роль в оптимизации производительности системы. Эти функции позволяют ускорить загрузку приложений, предзагружая в память файлы и данные, которые наиболее часто используются пользователем. Однако, несмотря на их пользу, в этих механизмах были обнаружены уязвимости, которые могут быть использованы злоумышленниками для выполнения вредоносного кода. В последние годы возникли случаи эксплуатации этих уязвимостей вирусами и другими вредоносными программами, что делает их важной темой для обсуждения в контексте информационной безопасности.

Суть проблемы заключается в том, что механизм Prefetch, предназначенный для ускорения запуска программ, хранит в себе информацию о том, какие файлы и компоненты использовались при запуске приложений. Эта информация сохраняется в специальных файлах с расширением .pf, что делает систему уязвимой к атакам, которые могут создать вредоносный файл, использующий такую же структуру данных. Механизм Superfetch, в свою очередь, пытается предсказать, какие данные будут использоваться в будущем, и заранее загружает их в память. Злоумышленники могут использовать эти механизмы для внедрения вредоносных программ, которые могут скрыться от традиционных методов обнаружения или использовать их для выполнения кода на уязвимых системах.

Вирусы, использующие уязвимости в механизме Prefetch и Superfetch в Windows

Механизм Prefetch в Windows был разработан для того, чтобы повысить производительность системы за счет кэширования и загрузки в память часто используемых файлов и компонентов. Однако его структура хранит важную информацию о процессе запуска приложений. Эти файлы с расширением .pf, в которых содержатся записи о запуске программ, также могут быть использованы для хранения данных, которые злоумышленники могут эксплуатировать. Вредоносное ПО может воспользоваться этими записями и внедрить свой код в файлы, которые обычно не проверяются антивирусными программами. Такой подход позволяет вирусам скрываться в системе, не привлекая внимания[1].

Кроме того, механизм Superfetch, который анализирует поведение пользователя и заранее подготавливает данные для более быстрого их использования, может быть использован для распространения вредоносных программ. Когда пользователи запускают приложение, которое было подготовлено Superfetch, возможно, что приложение будет пытаться загрузить данные или файлы, созданные злоумышленниками. В результате вирус может быть загружен на систему, если она подвержена уязвимостям, связанным с управлением памятью или с другими компонентами операционной системы[2].

Эксплуатация этих механизмов вирусами чаще всего происходит через социальную инженерию, когда злоумышленники подготавливают вредоносные файлы, которые имитируют нормальные операционные процессы. Например, вирус может сгенерировать файл Prefetch, который будет выглядеть как запись о запуске популярной программы, и при этом содержать скрытый вредоносный код. Когда система запускает этот файл, вирус может активироваться, что позволяет ему получить доступ к системным файлам или даже установить дополнительные компоненты, которые могут быть использованы для дальнейших атак[3].

Одной из угроз, связанных с использованием уязвимостей Prefetch и Superfetch, является возможность распространения вирусов через локальные и удаленные сети. Вредоносные файлы, связанные с этими механизмами, могут быть размещены в сети, и при доступе к ним на других устройствах система может заражаться. Сложность заключается в том, что такой вирус может быть трудно обнаружить, поскольку он не требует явного взаимодействия с пользователем и может активно использовать функции операционной системы для скрытности[4].

Существует несколько методов защиты от уязвимостей в механизмах Prefetch и Superfetch, которые можно внедрить на уровне настройки операционной системы и безопасности. Одним из самых простых и эффективных способов защиты является регулярное обновление операционной системы. Microsoft активно устраняет уязвимости в различных

компонентах Windows, и установление последних патчей является важной мерой профилактики.

Другим важным шагом является настройка безопасности с использованием групповых политик и ограничение доступа к определённым системным файлам и папкам. Например, можно отключить функции Prefetch и Superfetch, если они не являются критически важными для производительности системы. Это можно сделать через настройки реестра или с помощью инструментов администрирования Windows, что поможет минимизировать риски, связанные с использованием уязвимостей.

Кроме того, важно использовать антивирусные программы с поддержкой анализа поведения, которые способны обнаружить подозрительные активности в процессе работы системы. Такие программы могут отслеживать действия вредоносных файлов, которые пытаются внедрить код в систему через Prefetch или Superfetch, и заблокировать их до того, как они смогут нанести вред[5].

Для защиты от вирусов, использующих уязвимости в этих механизмах, следует также применять сегментацию сети и минимизацию прав доступа. Вредоносные программы чаще всего нацелены на слабые места, связанные с высокими правами доступа. Путём ограничения прав пользователей можно предотвратить заражение системы даже в случае эксплуатации уязвимости.

Заключение

Механизмы Prefetch и Superfetch в Windows являются полезными функциями для повышения производительности системы, но они также представляют собой уязвимости, которые могут быть использованы для распространения вирусов и выполнения произвольного кода. Злоумышленники могут эксплуатировать эти уязвимости для внедрения вредоносных программ в систему, что ставит под угрозу безопасность как индивидуальных пользователей, так и организаций.

Для защиты от таких угроз важно регулярно обновлять операционную систему, отключать ненужные функции, использовать антивирусное ПО с поддержкой анализа поведения и настраивать правильные параметры безопасности в системе. Эти меры помогут минимизировать риски и защитить систему от вирусов, которые используют уязвимости в Prefetch и Superfetch.

Список литературы

1. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
2. Волкогонов В. Н. и др. Применение физически неклонированных функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.

4. Кушнир Д. В., Шемякин С. Н., Орлов Г. А. Представление некоторых аспектов отсеивания составных чисел для криптографических приложений //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 1. – С. 25-28.
5. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения //Интеллектуальные технологии на транспорте. – 2018. – №. 3 (15). – С. 47-54.

References

1. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
 2. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.
 3. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in the class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2020. No. 4. pp. 61-65.
 4. Kushnir D. V., Shemyakin S. N., Orlov G. A. Presentation of some aspects of screening composite numbers for cryptographic applications //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 1. – pp. 25-28.
 5. Kalinin M. O., Shterenberg S. I. Analysis of information security of an enterprise based on monitoring of information resources using machine learning //Intelligent technologies in transport. – 2018. – №. 3 (15). – pp. 47-54.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.92

АНАЛИЗ И МИНИМИЗАЦИЯ РИСКОВ ПРИ СТРОИТЕЛЬСТВЕ ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ГИС

¹Сафонова Т.В., ²Мокряк А.В., ³Муленко М.Д., ⁴Лескова Д.О.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: ¹tatyana.vsafonova@gmail.com, ³mariyamouse@mail.com, ⁴das21t5ehek@gmail.com;

²ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г. Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

Статья фокусируется на анализе и снижении рисков, возникающих при возведении инфраструктурных объектов, уделяя особое внимание использованию геоинформационных систем (ГИС). Описываются основные категории рисков, подходы к их выявлению и оценке, а также стратегии минимизации. ГИС представлены как действенный инструмент для визуализации данных и анализа пространственных связей, что способствует оптимизации управления проектами. В завершение отмечается значимость внедрения ГИС в процесс управления рисками для укрепления устойчивости инфраструктуры.

Ключевые слова: ГИС, инфраструктурные объекты, риск-менеджмент, климатические риски, экологические риски.

RISK ANALYSIS AND MINIMIZATION DURING THE CONSTRUCTION OF INFRASTRUCTURE FACILITIES USING GIS

¹Safonova T.V., ²Mokryak A.V., ³Mulenko M.D., ⁴Leskova D.O.

RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: ¹tatyana.vsafonova@gmail.com, ³mariyamouse@mail.com, ⁴das21t5ehek@gmail.com;

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

The article focuses on the analysis and reduction of risks arising from the construction of infrastructure facilities, paying special attention to the use of geographic information systems (GIS). The main categories of risks, approaches to their identification and assessment, as well as minimization strategies are described. GIS is presented as an effective tool for data visualization and spatial relationship analysis, which helps optimize project management. In conclusion, the importance of GIS implementation in the risk management process for strengthening infrastructure sustainability is noted.

Keywords: GIS, infrastructure facilities, risk management, climate risks, environmental risks.

Введение

Анализ и снижение рисков при возведении инфраструктурных объектов играют важную роль в качественном управлении проектами. Учитывая стремительный рост городов, изменения климата и повышенные требования к надежности и безопасности инфраструктуры, потребность в действенных способах оценки и контроля рисков становится всё актуальнее. Такие инфраструктурные задачи, как строительство дорог, мостов, зданий и энергетических систем, требуют крупных вложений и продолжительного времени на выполнение, что делает их особенно подверженными разнообразным угрозам.

Управление рисками в строительстве подразумевает выявление, оценку и разработку мер противодействия возможным угрозам, которые способны оказать негативное влияние на проект. Данные угрозы могут возникать как внутри организации — например, ошибки в проектировании или нехватка средств, так и извне — такие как стихийные бедствия, изменения в нормативных актах или общественные протесты. Грамотный подход к управлению рисками не только сокращает потенциальные убытки, но и усиливает общую устойчивость проектов.

Геоинформационные системы (ГИС) представляют собой универсальный инструмент для анализа данных и визуализации рисков, так как они позволяют интегрировать пространственные данные с информацией о рисках, что обеспечивает многопараметрический анализ доступности инфраструктуры и выявление потенциальных угроз [1]. ГИС помогают строителям и проектировщикам принимать обоснованные решения на всех этапах проекта — от планирования до эксплуатации. Цель предоставленной работы заключается в исследовании методов анализа и минимизации рисков при строительстве инфраструктурных объектов с использованием ГИС.

Риски в строительстве инфраструктурных объектов

Возведение инфраструктурных объектов сопряжено с различными рисками, которые могут существенно сказаться на успехе проекта. Подобные риски можно разделить на несколько ключевых категорий, каждая из которых обладает определенными характеристиками и возможными последствиями.

Естественные риски охватывают природные катаклизмы, такие как землетрясения, наводнения, ураганы и прочие погодные аномалии. Такие факторы могут нанести ущерб объектам, вызвать задержки в строительстве и увеличить расходы. К примеру, в России, где климат колеблется от субтропического до тундрового, важно учитывать региональные особенности при планировании и возведении объектов.

Технические риски обусловлены вероятными трудностями на этапах проектирования и возведения. Сюда входят ошибки в расчётах, конструктивные недостатки или применение низкокачественных материалов, что может повлечь за собой доработки, увеличение сроков выполнения работ и дополнительные финансовые траты. Например, пренебрежение строительными нормами способно создать серьёзные проблемы с безопасностью объекта.

Финансовые риски появляются вследствие колебаний цен на стройматериалы и услуги, а также незапланированных трат. Даже незначительные изменения в стоимости материалов могут заметно увеличить общие затраты на проект. Помимо этого, задержки в ходе работ могут привести к дополнительным расходам и снижению прибыльности.

Юридические риски возникают из-за возможного нарушения контрактных обязательств, претензий со стороны клиентов или надзорных инстанций. Невыполнение страховых условий может обернуться судебными спорами и значительными финансовыми убытками. Например, если подрядная организация не уложится в сроки или допустит отклонения по качеству работы, это может иметь серьёзные последствия.

Социальные риски проявляются через общественное мнение и протесты местных жителей против строительства. Негодование общества может затянуть реализацию проекта или вовсе остановить его. Привлечение жителей к обсуждению проектов поможет уменьшить подобные риски.

Экологические риски обусловлены влиянием строительства на природу, что может выражаться в загрязнении атмосферы и водоёмов, уничтожении экосистем и негативном воздействии на здоровье людей. Учитывая актуальные стандарты экологической безопасности, проведение экологической экспертизы на каждом этапе проекта крайне важно [2-4].

Для эффективного управления рисками при строительстве инфраструктурных объектов необходим всесторонний подход и внедрение передовых технологий, таких как ГИС, которые позволяют объединить данные о разнообразных рисках и наглядно продемонстрировать их влияние на проект, что способствует более взвешенному принятию решений. Грамотное управление рисками не только сводит к минимуму возможные убытки, но и увеличивает общую сопротивляемость проектов внешним угрозам.

Итак, осознание разных типов рисков и использование соответствующих методик для их оценки и управления являются основополагающими элементами успешного осуществления инфраструктурных проектов в России.

Идентификация и оценка рисков с помощью ГИС

Выявление рисков предполагает формирование перечня возможных угроз, что служит ключевым элементом управления проектами. Оценка рисков может проводиться качественно или количественно, используя такие методы, как анализ методом Монте-Карло для численной оценки вероятности возникновения событий и их последствий.

Основные методы применения ГИС для определения и оценки рисков при строительстве инфраструктурных объектов заключаются в следующем: анализ природных условий; объединение пространственных данных; моделирование различных сценариев развития событий; мониторинг состояния строительных площадок; оценка влияния на окружающую среду; визуализация полученных результатов. Давайте рассмотрим каждый из них подробнее [5, 6]. ГИС дают возможность анализировать природные факторы, принимая во внимание особенности территории, такие как рельеф, гидрогеологию, структуру почв и климатические показатели, что помогает оценивать риски, связанные с землетрясениями, наводнениями, оползнями и прочими природными катастрофами. Например, изучение зон подтопления позволяет определить самое безопасное место для расположения объекта.

Объединение пространственных данных в ГИС осуществляется путем наложения различных информационных слоев: топографических карт, спутниковых снимков, кадастровых планов, схем инженерных коммуникаций и других. Данный процесс позволяет

провести всесторонний анализ участка под строительство, выявить уже имеющиеся объекты инфраструктуры и сократить риски, связанные с их взаимным влиянием.

ГИС позволяют смоделировать разнообразные сценарии развития событий, такие как колебания уровня грунтовых вод, последствия техногенных аварий или влияние климатических изменений, что помогает предвидеть возможные трудности заранее и подготовить упреждающие меры [7].

Кроме того, современные ГИС используются для мониторинга состояния возводимых объектов в реальном времени, что охватывает слежение за перемещением грунтов, контроль состояния инженерных сооружений и быстрое выявление отклонений от проектных значений.

Оценка экологических рисков представляет собой обязательный этап любого масштабного инфраструктурного проекта. ГИС способствуют анализу воздействия строительства на окружающую среду, включая изменения в экосистемах, загрязнение атмосферного воздуха и водоемов, уничтожение лесных массивов и другие факторы [8]. Полученная информация позволяет сформировать программы по уменьшению неблагоприятных последствий и возмещению причиненного вреда.

Одной из значимых функций ГИС является генерация понятных карт и схем, облегчающих восприятие итогов проведенного анализа, что особенно полезно при презентациях проектов клиентам, инвесторам и государственным органам, так как позволяет оперативно и доходчиво изложить потенциальные риски и предлагаемые способы их нейтрализации.

Минимизация рисков

Чтобы успешно свести к минимуму риски, нужно формировать стратегии, включающие следующие элементы:

- планирование, т.е. создание подробных планов управления рисками на каждом этапе проекта, что помогает заранее выявить потенциальные угрозы и предусмотреть меры по их предотвращению;
- мониторинг за ходом проекта и изменениями в окружающей среде с применением ГИС, который позволит обеспечить быструю реакцию на любые изменения условий;
- применение новейших технологий и методов для усиления устойчивости инфраструктуры к рискам;
- подготовка и повышение квалификации сотрудников в области управления рисками, что позволит более эффективно справляться с возникающими проблемами;
- создание резервов бюджета для покрытия непредвиденных расходов, что поможет предотвратить финансовые сложности в случае возникновения кризисных ситуаций;
- сотрудничество с местными сообществами для снижения социальных рисков и улучшения общественного восприятия проекта [9].

Методы оценки и управления рисками

Оценка и управление рисками при возведении инфраструктурных объектов подразумевает использование нескольких важных методов для выявления, анализа и снижения возможных угроз. Давайте рассмотрим ключевые подходы к оценке и управлению рисками.

Самым распространенным методом является метод экспертных оценок, который основан на сборе мнений экспертов для определения вероятности появления разных рисков. Эксперты анализируют возможные убытки, опираясь на свой опыт и знания о проекте. Достоинство данного подхода заключается в том, что он позволяет учитывать сложные аспекты, которые сложно учесть с использованием статистических моделей.

Следующий подход к оценке и управлению рисками — это моделирование Монте-Карло. Данный метод является вероятностным и предусматривает многократное моделирование различных сценариев развития проекта для оценки воздействия разнообразных факторов риска, что особенно полезно при анализе больших объемов данных и сложных систем.

Еще один метод – это дерево решений, который представляет собой графическую схему, отображающую варианты решения проблемы или анализ возможных результатов различных действий. Дерево решений помогает систематизировать размышления о потенциальных рисках и определить самый надежный способ осуществления проекта.

Следующим методом является кумулятивный подход, который предполагает включение уровня риска в расчеты экономических показателей проекта (таких как NPV и IRR) посредством ставки дисконтирования [10].

Управление рисками охватывает не только их идентификацию и анализ, но и создание стратегий для минимизации или полного устранения этих рисков. Такой комплексный подход обеспечивает более эффективное управление инфраструктурными проектами на всех этапах их реализации — начиная с планирования и заканчивая завершением строительства.

Примеры использования ГИС при строительстве инфраструктурных объектов

ГИС приобретают всё большее значение как инструмент для обеспечения устойчивого развития городских территорий за счет комплексного анализа пространственных данных.

Данная технология активно используется в строительстве для выполнения множества задач, таких как проектирование, управление и контроль над инфраструктурными проектами. Ознакомимся с примерами успешного применения ГИС в данной сфере, представленными в Таблице 1.

Таблица 1. Известные проекты ГИС в строительстве

Проект	Регион	Инициатор/ Инвестор	Срок реали- зации	Объем инвест иций (млрд руб.)	Описание
Строительство мостового перехода через Керченский пролив	Краснодарский край	ОАО «Крымская железная дорога»	2015-2018	50	Проект включает строительство моста протяженностью 19 км, который соединяет Крым с материковой частью России
Создание всесезонного горного курорта	Сочи	Группа компаний «Альпика»	2021-2025	30	Проект включает создание горнолыжных трасс и гостиничной инфраструктуры

«Долина Васта»					
Строительство обхода Аксая	Ростовская область	ГК «Автодор»	2019-2023	15	Обход города Аксая включит в себя новые дороги и развязки для улучшения транспортной доступности
Модернизация и создание инфраструктуры трамвая в Ростове-на-Дону	Ростовская область	Администрация города	2023-2048	25	Проект направлен на обновление трамвайной сети и создание новых маршрутов
Строительство Дальнего западного обхода Краснодара	Краснодарский край	ГК «Автодор», АО «Донаэродорстрой»	2020-2023	41.5	Обход протяженностью более 51 км включает четыре полосы движения, три развязки и несколько мостов
Создание всесезонного курорта «Лагонаки»	Республика Адыгея	НАО «Красная Поляна»	2022-2025	35	Проект включает в себя горнолыжные трассы и гостиничные комплексы
Строительство Западной хорды	Ростовская область	ГК «Регион»	2022-2025	30	Западная хорда строится в два этапа, включая эстакады и развязки
Создание и эксплуатация объектов транспортной инфраструктуры наземного городского электрического транспорта	Краснодарский край	ООО «Синара-ГТР Краснодар»	2022-2026	28.425	Проект включает создание новой транспортной инфраструктуры с современными технологиями
Строительство нового аэровокзального комплекса в Геленджике	Краснодарский край	Банк ВТБ, ООО «Аэропорт «Геленджик»»	2019-2034	5.4	Новый терминал будет иметь площадь более 16,7 тыс. кв. м и пропускную способность более 890 пассажиров в час
Строительство объектов теплоснабжения в Краснодаре	Краснодарский край	ООО «Тепловая энергетическая компания «Знаменская»»	2022-2025	3.5	Проект включает строительство объектов теплоснабжения для нового микрорайона

Примеры показывают, насколько универсальны ГИС в решении разнообразных задач строительной сферы — от этапа планирования до управления выполнением проектов, что

помогает улучшить эффективность процессов благодаря точному анализу пространственных данных, подчеркивая важность использования современных технологий [11, 12].

Выводы

Использование ГИС представляет собой эффективный метод анализа и снижения рисков при строительстве инфраструктуры, поскольку они позволяют обрабатывать пространственные данные и проводить всесторонний анализ окружающей среды вокруг возводимого объекта. Комбинирование методов экспертной оценки с данными спутникового мониторинга помогает точнее предсказывать возможные трудности еще на этапе проектирования. В результате, ГИС становятся ключевым инструментом современного управления рисками и играют важную роль в стратегии крупных строительных компаний.

Список литературы

1. Астафьева О.Е., Моисеенко Н.А., Козловский А.В., Шемякина Т.Ю., Серов В.М. Риск-менеджмент в строительстве: монография. – Москва: ИНФРА-М, 2022. – 183 с. ISBN 978-5-16-017320-7.
2. Рогов В.А., Чудаков А.Д. Управление рисками. – Москва: ТНТ, 2020. – 200 с. ISBN 978-5-94178-287-1.
3. Воронцовский А.В. Управление рисками. – Москва: Юрайт, 2020. – 256 с. ISBN 978-5-534-07137-4.
4. Борзов В.В., Кочемасов К.С. Рынок международного строительства: проблемы и перспективы транснациональных компаний, управление рисками. – Сметно-нормативная документация, 2021.
5. Мельчаков А.П. Управление риском и конструкционная безопасность строительных объектов. – Москва: Литрес, 2023. – 150 с. ISBN 978-5-532-12345-6.
6. Кузнецов С.И., Федоров В.А. Геоинформационные технологии в управлении проектами строительства. – Санкт-Петербург: Питер, 2023.
7. Смирнов П.Н., Ефимова Т.С. Анализ рисков в инвестиционно-строительных проектах. Журнал "Строительство", 2022, №4(12), с. 45–50.
8. Сидоров А.Г., Петрова Л.В. Управление проектами и рисками в строительстве: учебное пособие. – Москва: Академический проект, 2020.
9. Сафонова Т.В., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. ГИС для мониторинга и оценки сельскохозяйственных угодий Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 19-27.
10. Попов В.Н., Сафонова Т.В., Кирспуу К.А. Анализ технологии сенсорного мониторинга Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 24-28.
11. Ковалев А.Н., Тихомиров И.Г. Инновационные подходы к управлению рисками в строительстве. Журнал "Управление проектами", 2021, №3(15), с. 30–35.
12. Зенин С.А., Кузеванов Д.В. Развитие системы управления риском при обследованиях и оценке технического состояния строительных объектов. Журнал "Строительные технологии", 2023, №2(10), с. 15–20.

References

1. Astafieva O.E., Moiseenko N.A., Kozlovsky A.V., Shemyakina T.Yu., Serov V.M. Risk management in construction: monograph. - Moscow: INFRA-M, 2022. - 183 p. ISBN 978-5-16-017320-7.
 2. Rogov V.A., Chudakov A.D. Risk management. - Moscow: TNT, 2020. - 200 p. ISBN 978-5-94178-287-1.
 3. Vorontsovsky A.V. Risk management. - Moscow: Yurait, 2020. - 256 p. ISBN 978-5-534-07137-4.
 4. Borzov V.V., Kochemasov K.S. The international construction market: problems and prospects of transnational companies, risk management. - Estimate and regulatory documentation, 2021.
 5. Melchakov A.P. Risk management and structural safety of construction projects. - Moscow: Litres, 2023. - 150 p. ISBN 978-5-532-12345-6.
 6. Kuznetsov S.I., Fedorov V.A. Geoinformation technologies in construction project management. - St. Petersburg: Piter, 2023.
 7. Smimov P.N., Efimova T.S. Risk analysis in investment and construction projects. Magazine "Construction", 2022, No. 4 (12), pp. 45-50.
 8. Sidorov A.G., Petrova L.V. Project and risk management in construction: a tutorial. – Moscow: Akademicheskiiy proekt, 2020.
 9. Safonova T.V., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. GIS for monitoring and assessing agricultural land Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). P. 19-27.
 10. Popov V.N., Safonova T.V., Kirspuu K.A. Analysis of sensor monitoring technology Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). P. 24-28.
 11. Kovalev A.N., Tikhomirov I.G. Innovative approaches to risk management in construction. Project Management Journal, 2021, No. 3 (15), pp. 30–35.
 12. Zenin S.A., Kuzevanov D.V. Development of a risk management system for inspections and assessment of the technical condition of construction projects. Journal "Construction Technologies", 2023, No. 2 (10), pp. 15–20.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.056

ОСНОВНЫЕ АТАКИ И МЕТОДЫ ЗАЩИТЫ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ WEB-ПРИЛОЖЕНИЙ

Малявин М.Ю.

АНО ВО "МОСКОВСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ - МОСКОВСКИЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ ИНСТИТУТ", Москва, Россия (109316, город Москва, Волгоградский пр-кт, д. 32 к. 11) e-mail: max-malyavin@bk.ru

В условиях стремительного развития веб-технологий и роста киберугроз обеспечение безопасности современных веб-приложений становится одной из приоритетных задач в сфере информационной безопасности. Цель данной статьи заключается в анализе и систематизации актуальных видов атак на веб-приложения, а также методов их предотвращения. В рамках исследования рассмотрены наиболее распространенные угрозы, а также систематизированы эффективные методы защиты. Ценность материалов работы заключается в возможности разработчикам и специалистам по информационной безопасности выбрать оптимальные стратегии и методы защиты веб-приложений. Предложенные в статье рекомендации могут быть использованы как основа для повышения уровня безопасности веб-систем и разработки более надежных приложений в условиях современных киберугроз.

Ключевые слова: Веб-разработка, веб-технологии, киберугроза, информационная безопасность.

THE MAIN ATTACKS AND METHODS OF PROTECTION IN THE CONTEXT OF ENSURING THE SECURITY OF MODERN WEB APPLICATIONS

Malyavin M.Yu.

MOSCOW UNIVERSITY OF HUMANITIES AND TECHNOLOGY - MOSCOW INSTITUTE OF ARCHITECTURE AND CIVIL ENGINEERING, Moscow, Russia (109316, Moscow, Volgogradsky prospekt, 32, bld. 11) e-mail: max-malyavin@bk.ru

In the context of the rapid development of web technologies and the growth of cyber threats, ensuring the security of modern web applications is becoming one of the priorities in the field of information security. The purpose of this article is to analyze and systematize current types of attacks on web applications, as well as methods to prevent them. The study examines the most common threats, as well as systematizes effective methods of protection. The value of the materials of the work lies in the opportunity for developers and information security specialists to choose the best strategies and methods for protecting web applications. The recommendations proposed in the article can be used as a basis for improving the security of web systems and developing more reliable applications in the face of modern cyber threats.

Keywords: Web development, web technologies, cyber threat, information security.

В последние годы веб-приложения становятся неотъемлемой частью цифровой экономики, обеспечивая работу множества сервисов, от электронной коммерции до государственных платформ. По данным аналитиков Market Research Future, по итогам 2024 года затраты на глобальном рынке веб-разработки достигли \$57,31 млрд, что примерно на 5% больше, чем в 2023 году [1]. Такой рост свидетельствует о непрерывном развитии веб-технологий и расширении их функциональности. Однако стремительное увеличение числа

веб-приложений неизбежно приводит к росту киберугроз и делает информационную безопасность одним из ключевых вызовов. По результатам исследования BI.Zone, около 25% веб-уязвимостей, выявляемых ежемесячно, представляют высокий риск для кибербезопасности [2]. При этом, согласно их же отчетам, ежемесячно в мире обнаруживается порядка 1000 новых веб-уязвимостей, что демонстрирует сложность и динамичность угроз, с которыми сталкиваются разработчики и специалисты по информационной безопасности. В данных условиях эффективные методы защиты веб-приложений становятся критически важными. Организациям необходимо внедрять комплексные стратегии безопасности, учитывая актуальные виды атак и разрабатывая соответствующие защитные механизмы. Рассмотрение этих аспектов в рамках статьи позволит систематизировать угрозы и предложить наиболее действенные подходы к обеспечению надежной защиты современных веб-систем.

Итак, на фоне стремительного роста цифровизации и увеличения числа веб-приложений актуальность кибератак продолжает возрастать. Как отмечают П. Байраммырадов, Ш. Довлетназаров Ш. и Г. Гарягдыева, злоумышленники совершенствуют свои методы, используя уязвимости в веб-инфраструктуре для компрометации данных, финансовых потерь и нарушения работы сервисов [3]. Среди наиболее актуальных атак в 2025 году автором настоящей статьи выделяются следующие:

- SQL-инъекции (SQLi) – один из старейших, но по-прежнему эффективных способов атаки, позволяющий злоумышленникам получить несанкционированный доступ к базе данных через уязвимые запросы;
- XSS (межсайтовый скриптинг) – позволяет внедрять вредоносный код на веб-страницы, что ведет к краже данных пользователей или компрометации учетных записей;
- CSRF (межсайтовая подделка запросов) – эксплуатирует доверие веб-приложения к аутентифицированным пользователям, заставляя их неосознанно выполнять вредоносные действия;
- Credential Stuffing – атака, основанная на переборе украденных учетных данных с целью компрометации аккаунтов;
- Server-Side Request Forgery (SSRF) – позволяет атакующим отправлять произвольные запросы от имени веб-сервера, получая доступ к внутренним системам;
- Zero-Day-атаки – использование неизвестных уязвимостей до выпуска соответствующих исправлений, что делает их крайне опасными;
- DDoS-атаки – перегрузка серверов веб-приложения огромным количеством запросов, приводящая к отказу в обслуживании. Согласно Cloud Networks, в 2024 году количество DDoS-атак в России увеличилось на 32% по сравнению с 2023 годом, что подчеркивает их возрастающую угрозу [4].

С учетом постоянно меняющихся угроз и усложняющихся методов атак для защиты веб-приложений необходимо применять комплексный подход. Основные методы защиты включают: Web Application Firewall (WAF – фильтрация трафика для блокировки вредоносных запросов); контроль ввода данных (строгая валидация и экранирование пользовательского ввода для предотвращения SQL-инъекций и XSS-атак); многофакторная аутентификация (MFA – защита от атак на учетные записи); защита от ботов и CAPTCHA (предотвращение

автоматизированных атак, таких как Credential Stuffing); Rate Limiting и защита от DDoS (ограничение количества запросов для снижения нагрузки); журналирование и мониторинг (выявление подозрительной активности и предотвращение атак); обновление и патчинг ПО (минимизация риска эксплуатации уязвимостей Zero-Day).

С учетом представленных данных автором разработана Таблица 1, в которой систематизированы основные атаки на веб-приложения, соответствующие методы защиты, особенности их реализации и потенциальная эффективность. Данный анализ позволяет определить оптимальные стратегии безопасности в зависимости от типа угроз. Также в последнем столбце автором отражена потенциальная оценка эффективности каждого метода защиты при его корректном внедрении, основанная на экспертных данных, результатах тестирований и статистике выявленных атак. При этом, как отмечают М.М. Путятю, А.С. Макарян, В.В. Лещенко и В.О. Немчинова, применение данных методов защиты в комплексе позволит значительно повысить уровень безопасности современных веб-приложений, снижая риски атак и сводя к абсолютному минимуму их последствия [5].

Таблица 1 - Рекомендации по применению методов защиты

№ п\п	Атака	Метод защиты	Особенности реализации	Эффективность
1.	SQL-инъекция (SQLi)	Контроль ввода данных, WAF	Использование параметризованных запросов	95%
2.	XSS	Валидация и экранирование данных	Применение Content Security Policy (CSP)	90%
3.	CSRF	CSRF-токены, SameSite cookies	Генерация уникальных токенов для запросов	88%
4.	Credential Stuffing	MFA, защита от ботов	Ограничение количества неудачных входов	92%
5.	SSRF	Ограничение исходящих запросов	Использование allow/deny-листов адресов	85%
6.	Zero-Day-атаки	Обновления и мониторинг	Автоматизированное сканирование уязвимостей	80%
7.	DDoS-атака	Rate Limiting, WAF, защита на уровне CDN	Использование облачных решений для фильтрации трафика	93%

В результате проведенного исследования установлено, что обеспечение безопасности веб-приложений в 2025 году требует комплексного подхода, учитывающего не только известные угрозы, но и динамически изменяющийся ландшафт кибератак. Анализ актуальных данных и статистики показал, что увеличение числа веб-уязвимостей и рост атак, таких как SQL-инъекции, XSS, CSRF, а также усиление DDoS-атак, создают серьезные вызовы для разработчиков и специалистов по информационной безопасности. Систематизация методов защиты позволяет определить наиболее эффективные стратегии противодействия различным

видам атак. Так, например, использование параметризованных запросов практически полностью исключает риск SQL-инъекций, а CSP в сочетании с валидацией входных данных значительно снижает вероятность XSS-атак. Однако даже высокая эффективность отдельных решений не отменяет необходимости комплексного подхода, включающего постоянное обновление систем, мониторинг угроз и применение проактивных механизмов защиты.

По мнению автора настоящей статьи, наибольшую опасность представляют атаки, направленные на эксплуатацию уязвимостей нулевого дня, а также автоматизированные атаки, такие как подбор учетных данных (Credential Stuffing). В этих условиях повышается значимость таких механизмов, как многофакторная аутентификация, защита API и использование искусственного интеллекта для обнаружения аномального поведения. В перспективе киберугрозы будут становиться более сложными, что потребует не только технологических решений, но и повышения осведомленности разработчиков, пользователей и специалистов по информационной безопасности [6]. Исходя из этого, защита веб-приложений должна рассматриваться как непрерывный процесс, включающий анализ новых угроз, адаптацию существующих механизмов безопасности и использование интегрированных решений для минимизации рисков.

Список литературы

1. Веб-разработка (мировой рынок). Электронный ресурс. Режим доступа: [https://www.tadviser.ru/index.php/Статья:Веб-разработка_\(мировой_рынок\)](https://www.tadviser.ru/index.php/Статья:Веб-разработка_(мировой_рынок)) (дата обращения 17.02.2025 г.).
2. Безопасность веб-приложений. Электронный ресурс. Режим доступа: https://www.tadviser.ru/index.php/Статья:Безопасность_веб-приложений (дата обращения 17.02.2025 г.).
3. Байраммырадов П., Довлетназаров Ш., Гарягдыева Г. Атаки на веб-приложения: уязвимости и способы защиты // Вестник науки. 2024. №10 (79). С. 835-838.
4. Обзор крупнейших киберинцидентов 2024 года. Электронный ресурс. Режим доступа: <https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/> (дата обращения 17.02.2025 г.).
5. Пулято М.М., Макарян А.С., Лещенко В.В., Немчинова В.О. Анализ типовых уязвимостей при построении веб-приложений // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. №3 (306). С. 77-85.
6. Шутько Н. А. Теоретические понятия защиты web-приложений от уязвимостей // Вестник науки. 2022. №11 (56). С. 253-269.

References

1. Web development (global market). An electronic resource. Access mode: [https://www.tadviser.ru/index.php/Статья:Web_development_\(global_market\)](https://www.tadviser.ru/index.php/Статья:Web_development_(global_market)) (date of issue 17.02.2025).
2. Web application security. An electronic resource. Access mode: https://www.tadviser.ru/index.php/Статья:Security_of_web_applications (accessed 17.02.2025).

3. Bayrammyradov P., Dovetnazarov Sh., Garyagdieva G. Attacks on web applications: vulnerabilities and protection methods // Bulletin of Science. 2024. No. 10 (79). pp. 835-838.
 4. An overview of the largest cyber incidents in 2024. An electronic resource. Access mode: <https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda> / (accessed 17.02.2025).
 5. Putyato M.M., Makaryan A.S., Leshchenko V.V., Nemchinova V.O. Analysis of typical vulnerabilities in building web applications // Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences. 2022. No. 3 (306). pp. 77-85.
 6. Shutko N. A. Theoretical concepts of web application vulnerability protection // Bulletin of Science. 2022. No. 11 (56). pp. 253-269.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056

ПОДМЕНА DNS-ЗАПРОСОВ В МИКРОПРОГРАММАХ МАРШРУТИЗАТОРОВ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ

Бютнер С.И.

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

Подмена DNS-запросов в прошивках маршрутизаторов представляет собой один из современных методов скрытой передачи данных, который может использоваться злоумышленниками для кражи информации, обхода сетевых фильтров или создания каналов для удалённого управления заражёнными устройствами. В данной статье рассматриваются принципы работы этой атаки, её последствия для пользователей и организаций, а также способы защиты, включая мониторинг сетевого трафика, использование безопасных DNS-серверов и регулярное обновление прошивок маршрутизаторов.

Ключевые слова: Подмена DNS, маршрутизаторы, скрытая передача данных, компрометация прошивки, безопасность сети, утечка данных.

SPOOFING DNS QUERIES IN ROUTER FIRMWARE FOR COVERT DATA TRANSFER

Buetner S.I.

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

DNS query spoofing in router firmware is a modern method of covert data transmission that can be used by attackers to steal information, bypass network filters, or create channels for remote control of compromised devices. This article explores the principles behind this attack, its consequences for users and organizations, and protection methods, including network traffic monitoring, using secure DNS servers, and regularly updating router firmware.

Keywords: DNS spoofing, routers, covert data transmission, firmware compromise, network security, data leakage.

Введение

Современные маршрутизаторы являются не только ключевыми элементами сетевой инфраструктуры, но и потенциальными целями для атак, направленных на компрометацию их прошивок. Одной из таких атак является подмена DNS-запросов на уровне микропрограммного обеспечения маршрутизатора с целью скрытой передачи данных. Этот метод представляет собой серьёзную угрозу для безопасности как частных пользователей, так и корпоративных сетей, так как позволяет злоумышленникам манипулировать трафиком без непосредственного вмешательства на уровне конечных устройств.

DNS (Domain Name System) играет критическую роль в работе Интернета, переводя доменные имена в IP-адреса. Если злоумышленник получает контроль над DNS-запросами, он

может перенаправлять пользователей на вредоносные сайты, перехватывать передаваемую информацию или использовать DNS-запросы для создания скрытых каналов передачи данных. Особую опасность представляет подмена DNS-запросов, встроенная в прошивку маршрутизатора, так как этот метод позволяет атакам оставаться незаметными для стандартных антивирусных решений и систем мониторинга безопасности.

Подмена DNS-запросов в микропрограммах маршрутизаторов для скрытой передачи данных

Одним из наиболее изощрённых методов манипуляции сетевым трафиком является внедрение вредоносного кода в микропрограммы маршрутизаторов с целью подмены DNS-запросов. Эта техника позволяет злоумышленникам скрытно контролировать сетевые соединения пользователей, модифицировать маршрутизацию трафика и даже передавать данные в обход традиционных систем обнаружения[1].

Атака начинается с компрометации маршрутизатора, которая может происходить через использование уязвимостей в прошивке, слабых паролей администратора или поддельных обновлений программного обеспечения. После получения доступа злоумышленник внедряет вредоносный код в прошивку маршрутизатора, который изменяет обработку DNS-запросов. В результате при попытке пользователя обратиться к определённому домену маршрутизатор может подменять ответ DNS-сервера, направляя трафик на контролируемый злоумышленниками ресурс[2].

Однако возможности данной атаки не ограничиваются простым перенаправлением пользователей на фишинговые сайты. Более сложные схемы позволяют использовать DNS-запросы в качестве скрытого канала передачи данных. Вредоносное ПО на компрометированном устройстве может кодировать информацию в специфические DNS-запросы, которые маршрутизатор затем отправляет на сервер атакующего. Этот метод делает передачу данных практически незаметной для традиционных средств обнаружения, поскольку DNS-запросы считаются стандартной частью сетевого взаимодействия и редко подвергаются детальному анализу[3].

Одним из известных примеров использования подобных техник является применение DNS-туннелирования для обхода межсетевых экранов и фильтрации трафика. Вредоносные программы могут встраивать конфиденциальную информацию в поддельные DNS-запросы, а атакующий сервер, получая их, расшифровывает переданные данные. Такой подход позволяет злоумышленникам скрытно извлекать данные из корпоративных сетей, передавать команды заражённым устройствам или организовывать удалённое управление ботнетами[4].

Использование подмены DNS-запросов в прошивках маршрутизаторов также делает обнаружение атаки значительно сложнее. В отличие от вредоносного ПО на компьютере, которое можно выявить с помощью антивирусных решений, вредоносные изменения в микропрограмме маршрутизатора остаются незамеченными до тех пор, пока администратор сети не проведёт детальный анализ трафика или не заменит прошивку на официальную версию.

Защита от данной атаки требует комплексного подхода. В первую очередь пользователи должны регулярно обновлять прошивки маршрутизаторов, так как производители периодически выпускают патчи для устранения уязвимостей. Кроме того, рекомендуется

отключить удалённое управление маршрутизатором, если оно не используется, и сменить стандартные пароли администратора на более сложные[5].

Одним из эффективных методов защиты является использование безопасных DNS-серверов с поддержкой DNS over HTTPS (DoH) или DNS over TLS (DoT). Эти протоколы обеспечивают шифрование DNS-запросов, что затрудняет их перехват и подмену. Также следует использовать системы мониторинга трафика, которые могут выявлять аномальные DNS-запросы, указывающие на возможное наличие скрытого канала передачи данных.

Корпоративным пользователям рекомендуется применять сегментацию сети, ограничивая доступ маршрутизаторов к критически важным системам, а также использовать инструменты анализа трафика и детектирования аномалий. Внедрение правил брандмауэра для фильтрации подозрительных DNS-запросов и запрет использования нестандартных DNS-серверов также может помочь в предотвращении атак.

Современные маршрутизаторы играют важную роль в обеспечении безопасности сети, и их компрометация может привести к серьёзным последствиям, включая утечку конфиденциальной информации и потерю контроля над устройствами. Подмена DNS-запросов в прошивках маршрутизаторов остаётся одной из наиболее сложных для обнаружения угроз, требующей как технических мер защиты, так и осведомлённости пользователей о рисках, связанных с использованием устаревшего и неподдерживаемого сетевого оборудования.

Заключение

Подмена DNS-запросов в микропрограммах маршрутизаторов представляет собой опасный вектор атаки, который позволяет злоумышленникам скрыто управлять трафиком, организовывать скрытые каналы передачи данных и компрометировать сетевую инфраструктуру. Данная угроза особенно опасна тем, что остаётся незамеченной при стандартных методах защиты, поскольку изменения в прошивке маршрутизатора трудно обнаружить без специализированного анализа трафика и оборудования.

Защита от подобных атак требует регулярного обновления прошивок, использования безопасных DNS-серверов и мониторинга сетевого трафика для выявления аномалий. В условиях растущей киберугрозы пользователи и компании должны уделять особое внимание безопасности маршрутизаторов, так как их компрометация может стать первым шагом к более масштабной атаке на всю сеть. Только комплексный подход к обеспечению безопасности сетевых устройств может минимизировать риски и защитить критически важные данные от несанкционированного доступа.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей. – 2018.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределённых информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

References

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



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.89:004.94

СИТУАТИВНЫЙ СИНТЕЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, МОДЕЛИРУЮЩЕГО ПРИНИМАЕМЫЕ ЧЕЛОВЕКОМ РЕШЕНИЯ НА ОБЪЕКТАХ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМ

¹Балашов О.В., ²Букачев Д.С.

¹АО «РАДИОЗАВОД» (НИО-4), Смоленск, Россия, (214027, г. Смоленск, улица Котовского, 2), e-mail: smradio@mail.ru

²ФГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Смоленск, Россия (214000, г. Смоленск, ул. Пржевальского, 4), e-mail: dsbuka@yandex.ru

В статье рассматривается ситуативный синтез программного обеспечения, моделирующего процесс принятия решений человеком в контексте социально-экономических систем (СЭС). Предлагается новый подход к формализации процесса принятия решений в условиях нестатистической неопределенности, включающий классификацию действий и мероприятий, а также методы их оценки и визуализации. Введена классификация действий, основанная на логико-лингвистической шкале (ЛЛШ), которая позволяет оценивать реализуемость мероприятий. Разработан механизм построения систем поддержки принятия решений (СППР), включающий использование модели имитации, визуализации и оценки реализуемости решений. Особое внимание уделено использованию теории возможностей и нечеткой логики для оценки реализуемости действий. Статья также описывает процесс формирования интерфейсов для моделей и их интеграцию с объектной базой данных (ОБД). Предложенный подход позволяет автоматизировать процессы планирования и оперативного управления в СЭС, обеспечивая более точную и оперативную оценку реализуемости принимаемых решений.

Ключевые слова: Программное обеспечение, ситуативный синтез, социально-экономическая система, нестатистическая неопределенность, классификация действий, оценка реализуемости, теория возможностей, нечеткая логика, принятие решений.

SITUATIONAL SYNTHESIS OF SOFTWARE MODELING HUMAN-MADE DECISIONS ON THE OBJECTS OF SOCIO-ECONOMIC SYSTEMS

¹Balashov O.V., ²Bukachev D.S.

¹JOINT-STOCK COMPANY "RADIO FACTORY" (RESEARCH DEPARTMENT 4), Smolensk, Russia, (214027, Smolensk, street Kotovskogo, 2), e-mail: smradio@mail.ru

²SMOLENSK STATE UNIVERSITY, Smolensk, Russia (214000, Smolensk, street Przewalski, 4), e-mail: dsbuka@yandex.ru

The article deals with the situational synthesis of software modeling the process of human decision-making in the context of socio-economic systems (SES). A new approach to the formalization of the decision-making process under non-statistical uncertainty is proposed, including the classification of actions and measures, as well as methods of their evaluation and visualization. The classification of actions based on the logical-linguistic scale (LLS) is introduced, which makes it possible to evaluate the realizability of actions. The mechanism of building decision support systems (DSS) including the use of simulation model, visualization and evaluation of feasibility of decisions is developed. Special attention is paid to the use of possibility theory and fuzzy logic to assess the realizability of actions. The paper also describes the process of forming interfaces for the models and their integration with the object database (OBD). The proposed approach allows to automate the processes of planning

and operational management in the SES, providing a more accurate and rapid assessment of the feasibility of decisions.

Keywords: Software, situational synthesis, socio-economic system, non-statistical uncertainty, classification of actions, feasibility assessment, possibility theory, fuzzy logic, decision making.

В настоящее время функционирование любой организации или предприятия как объекта социально-экономической системы (СЭС) осуществляется с применением компьютерных информационных технологий, которые позволяют автоматизировать процессы управления. Ключевыми функциями управления являются планирование и оперативное управление.

На сегодняшний день отсутствует сформировавшийся теоретический подход к формализации процесса принятия решений о выполнении мероприятий плана в условиях нестатистической неопределенности. В Таблице 1 приводится предлагаемая классификация мероприятий (действий), лежащая в основе этого подхода.

Таблица 1 – Предлагаемая классификация действий (мероприятий)

Наименование	Определения	Меры неопределенности, используемые для оценки	Особенности
<i>Действие</i>	Последовательность технологических операций, направленных на реализацию одной из множества функций, которые может выполнять объект системы, исходя из своего предназначения.	П, U, N	Результат выполнения определяется условиями обстановки.
Группа А	Оценка реализуемости производится по логико-лингвистической шкале (ЛЛШ).		Границы ЛЛШ: левая граница равна нулю, а правая - максимальному значению данного показателя. Правая граница характеризует потенциальные возможности подразделения по выполнению действия в идеальных условиях обстановки.
Группа Б	Оценка реализуемости производится по ЛЛШ.		Границы ЛЛШ: левая граница теоретически равна $+\infty$, а правая граница равна минимальному его значению и является константой.
Группа В	Оценка реализуемости производится по ЛЛШ.		Границы ЛЛШ: левая граница теоретически равна $+\infty$, а правая граница равна минимальному значению этого показателя,

			соответствующего содержанию действия.
<i>Мероприятие</i>	Совокупность действий, направленных на реализацию мероприятий, выполняемых несколькими подразделениями одного отдела.	П, U, N	Результат выполнения определяется рыночными условиями.
<i>Общая задача</i>	Совокупность мероприятий, выполняемых разнородными подразделениями организации (цехи, отделы, секторы и др.)	П, U, N	Результат выполнения определяется рыночными условиями.

Примечание: П - возможность, U- полезность, N – необходимость [9].

Под управленческим решением (УР) понимаются указания руководителя на выполнение совокупности мероприятий (действий) некоторым объектом СЭС с целью получения конкретного результата. Суть предлагаемого подхода состоит в выделении действий, структура которых постоянна, и задач, структура которых определяется условиями обстановки (ситуативна).

Толчком к разработке предлагаемой классификации явилась классификация, данная Клыковым Ю.И. в работе [4]. Недостатком подхода, предложенного Клыковым Ю.И., является отсутствие в нем средств оценки реализуемости мероприятий плана (общих задач, действий).

В статье предлагается подход к построению системы поддержки принятия решений (СППР), обеспечивающей ситуативный синтез программного обеспечения, моделирующего принимаемые ЛПР решения. В качестве программного обеспечения рассматриваются следующие модели:

- имитации мероприятий (действий);
- визуализации мероприятий (действий);
- оценки реализуемости принимаемых решений на выполнение мероприятий (действий);
- управляющие программы, обеспечивающие реализацию этих мероприятий (действий).

Имитация процессов выполнения мероприятий (действий) необходима в процессе формирования управленческого решения, в технологию выполнения которого входит рассматриваемое мероприятие (действие). Под моделями имитации рассматривается ПО, имитирующее процессы выполнения действий. В качестве таких моделей могут рассматриваться как аналитические модели, так и детерминированные стохастические модели. В качестве основных рассматриваются детерминированные стохастические модели, что дает возможность производить имитацию процессов выполнения действий в различном временном масштабе. В зависимости от содержания модель имитации действия может представлять собой совокупность моделей, имитирующих процессы элементарных операций (бизнес-операций), входящих в технологию его выполнения, или аналитическую модель, имитирующую процесс выполнения действия в общем виде. Каждому действию ставится в

соответствие интерфейс, содержащий в себе необходимые исходные данные для исполнения моделей, а также языковые конструкции, определяющие место расположения этих моделей в памяти ЭВМ и порядок их активизации. В интерфейсах действий определяется режим выполнения рассматриваемого решения (имитация, визуализация, оценка реализуемости и реализация) и в зависимости от выбранного режима активизируются те или иные модели.

Модель имитации выполнения одного и того же действия может быть различной для объектов системы. Модель имитации может быть полунатурной, а может быть математической. Модель имитации выполнения мероприятия представляет собой некоторые языковые конструкции, определяющие порядок активизации моделей, имитирующих процессы выполнения действий, входящих в технологию выполнения рассматриваемого мероприятия. Причем в силу ситуативности мероприятий данные языковые конструкции должны формироваться непосредственно в процессе вывода этого мероприятия. Множество языковых конструкций, определяющих порядок имитации действий, входящих в технологию выполнения мероприятия, образует интерфейс этого мероприятия. В зависимости от содержания мероприятия может имитироваться последовательное, параллельное или смешанное выполнение действий, входящих в технологию выполнения этого мероприятия. Модель имитации общего решения представляет собой набор языковых конструкций, активизирующих соответствующие модели мероприятий для подразделений, выполняющих эти мероприятия.

Процесс имитации выполнения мероприятий (действий) не имеет смысла без представления ЛПР возможностей по наблюдению за ходом имитации выполнения этих мероприятий (действий) и общих задач. Для наблюдения за ходом имитации необходимо предоставить ЛПР различного рода мультимедийные, графические и текстовые данные, отображающие и характеризующие процесс имитации. Для синхронизации вывода этих данных с процессом имитации необходимо использование соответствующих моделей визуализации. Модель визуализации должна соответствовать каждому действию. Процесс визуализации имитируемого процесса должен быть синхронизирован с ним по времени. Модели визуализации мероприятий и общих задач создаются таким же образом, как и модели имитации этих процессов. Визуализация необходима ЛПР для структуризации мероприятий и общих задач плана.

Автоматизация процессов планирования и оперативного управления СЭС требует решения проблемы оценки реализуемости принимаемых решений по выполнению мероприятий (действий). Сложность решения этой проблемы состоит в том, что для большинства СЭС решения, принимаемые ЛПР на объектах этих систем, являются уникальными. Следовательно, отсутствует возможность накопить и обработать соответствующую статистическую информацию. Отсутствие статистики делает невозможным использование вероятностных статистических методов (определения объективной вероятности) при разработке моделей оценки реализуемости планируемых мероприятий (действий) [5, 6, 8]. Для оценки реализуемости мероприятий и формализованного представления данных могут быть использованы методы извлечения и обработки экспертной информации [1].

Уникальность мероприятий (действий) проявляется в заранее неизвестной их структуре. Под последней целесообразно рассматривать набор определенных действий, выполняемых объектом СЭС с целью получения конкретного результата.

Нестатистичность структуры мероприятия может быть вызвана незнанием или неполнотой данных о предстоящих действиях конкурирующих и взаимодействующих систем, а также условий актуальной внешней среды. Задача оценки реализуемости мероприятий тесно связана с необходимостью их формализованного представления. На сегодняшний день отсутствует сформировавшийся подход к формализованному представлению мероприятий, планируемых в условиях нестатистической неопределенности.

Необходимо отметить, что уникальность имеет место не только для мероприятий, но и в целом для плана предстоящих действий, содержание которого образуют эти мероприятия. Отсутствие на сегодняшний день подхода к оценке реализуемости мероприятий, включаемых в план действий в условиях нестатистической неопределенности, а также подхода к их формализованному представлению, делает невозможным автоматизацию процессов разработки и оценки хода реализуемости плана предстоящих действий.

Наиболее развитыми средствами оценки мероприятий в современной теории принятия решений являются средства теории вероятностей и теории полезности. Рассмотрим возможности по использованию данных теорий при решении задачи оценки реализуемости принимаемых решений. Использование для оценки реализуемости принимаемых решений методов оценки субъективной вероятности [5, 9] не корректно в силу ряда следующих причин:

Во-первых, необходимо оценивать реализуемость принимаемого человеком решения непосредственно в процессе его формирования. В то же время методы оценки субъективной вероятности требуют получения и обработки экспертных оценок, что является довольно длительным процессом и может не соответствовать требуемому времени реакции СЭС.

Во-вторых, в субъективную вероятность человек вкладывает степень своей уверенности в получении требуемого результата, при этом реализуемость этого результата оценивается человеком весьма приближенно. Последнее утверждение вызвано тем, что ЛПР не в состоянии полностью учитывать технологию выполнения принимаемого им решения на выполнение задачи, рассматриваемым объектом СЭС, а также оценивать степень влияния на реализуемость этого решения различных внутренних и внешних факторов обстановки.

Использование для оценки реализуемости решений методов теории полезности не корректно в силу того, что функция полезности характеризует желательность результата для ЛПР, не оценивая при этом его реализуемость [6, 7]. В качестве одного из подходов к оценке реализуемости решений предлагается использовать подход, в основе которого лежат положения теории возможностей и нечеткой логики [2, 3]. Исходя из определения, действия, в отличие от мероприятий и общих задач, имеют жесткую структуру, но исходные данные для них определяются условиями обстановки и заранее неизвестны.

Действиям ставятся в соответствие модели оценки реализуемости, разработанные на этапе проектирования СППР. В основе разработки моделей оценки реализуемости действий лежит использование моделей оценки возможностей объекта СЭС по выполнению этих действий. В основе рассматриваемых моделей лежит процесс определения текущего значения некоторого объективного показателя, характеризующего процесс выполнения соответствующего действия. Отношение текущего значения данного показателя к его

идеальному значению рассматривается как количественная оценка, характеризующая возможность выполнения рассматриваемого действия. Идеальное значение объективного показателя является правой границей логико-лингвистической шкалы (ЛЛШ), отображающей распределение возможностей объекта СЭС по выполнению соответствующего действия. Помимо количественной оценки возможностей объекта по выполнению действия, существует качественная оценка, которая может принимать одно из множества лингвистических значений, характеризующих качество выполнения рассматриваемого действия. Определение интервалов значений количественной оценки между лингвистическими значениями производится в результате обработки мнений экспертов в рассматриваемой предметной области. Формирование ЛЛШ осуществляется на этапе проектирования модели объекта СЭС. В ходе жизненного цикла объекта ЛЛШ постоянно корректируется.

Таким образом, для каждого объекта СЭС разрабатывается программное обеспечение, позволяющее оценить реализуемость действий, которые он способен выполнять исходя из своего функционального предназначения.

Синтез моделей оценки реализуемости мероприятий и общих задач плана представляет собой последовательную, параллельную или смешанную свертку оценок, характеризующих реализуемость действий (мероприятий), входящих в технологию их выполнения, и производится непосредственно в процессе вывода этих мероприятий и общих задач.

Модели имитации, визуализации и оценки реализуемости действий, а также их интерфейсы создаются на этапе проектирования интеллектуальной системы и вместе с ОБД образуют предметную область этой системы. Синтез рассматриваемых моделей мероприятий и общих задач производится в процессе формирования этих решений, а сами модели представляют собой ссылки на интерфейсы моделей, соответствующих действий. С практической точки зрения моделей имитации, визуализации и оценки реализуемости мероприятий и общих задач реально не существует. В памяти ЭВМ существуют только лишь интерфейсы этих мероприятий и общих задач, в которых отражен порядок выполнения тех или иных моделей.

Формирование интерфейсов производится планировщиком СППР на языке обработки логики управления. Планировщик СППР предназначен для решения следующих задач: формирование интерфейсов (программных модулей) общих задач, мероприятий и действий (Таблица 1) в виде исходного кода на языке определения интерфейсов; определяет логическую последовательность, приоритетность и глубину трансляции программных модулей; формирует объектные запросы в объектную базу данных. Необходимо отметить разницу в формировании интерфейсов общих задач, мероприятий и действий. Формирование интерфейсов действий состоит в копировании нового интерфейса из имеющегося шаблона и определение значений его атрибутов. Интерфейсы мероприятий плана и общих задач синтезируются по соответствующим правилам. В задачу планировщика входит также присваивание мероприятиям (общим задачам) соответствующих идентификаторов. На Рисунках 1-4 показаны примеры интерфейсов общих задач, мероприятий и действий.

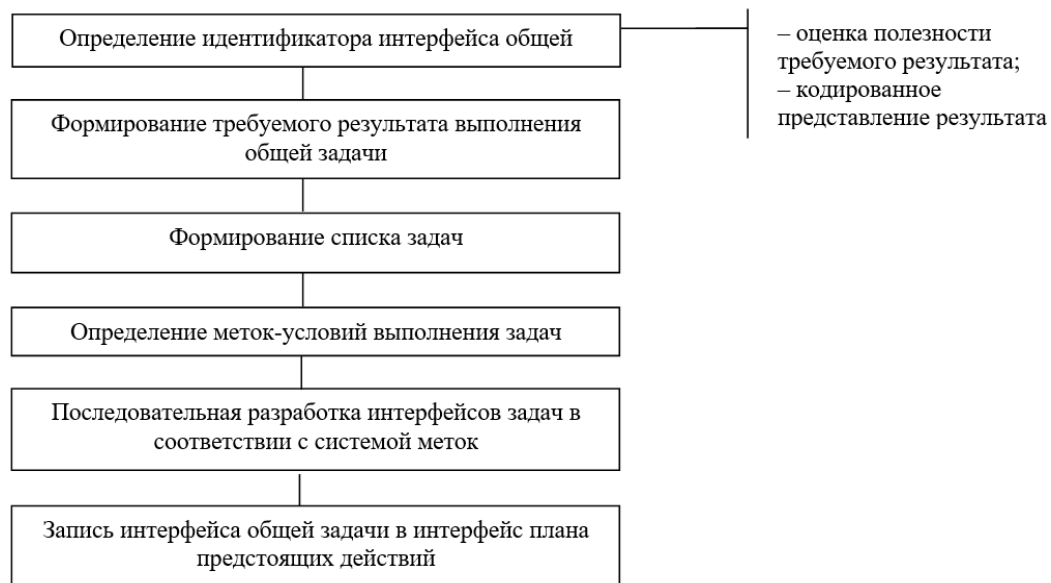


Рисунок 1 – Синтез интерфейса общей задачи

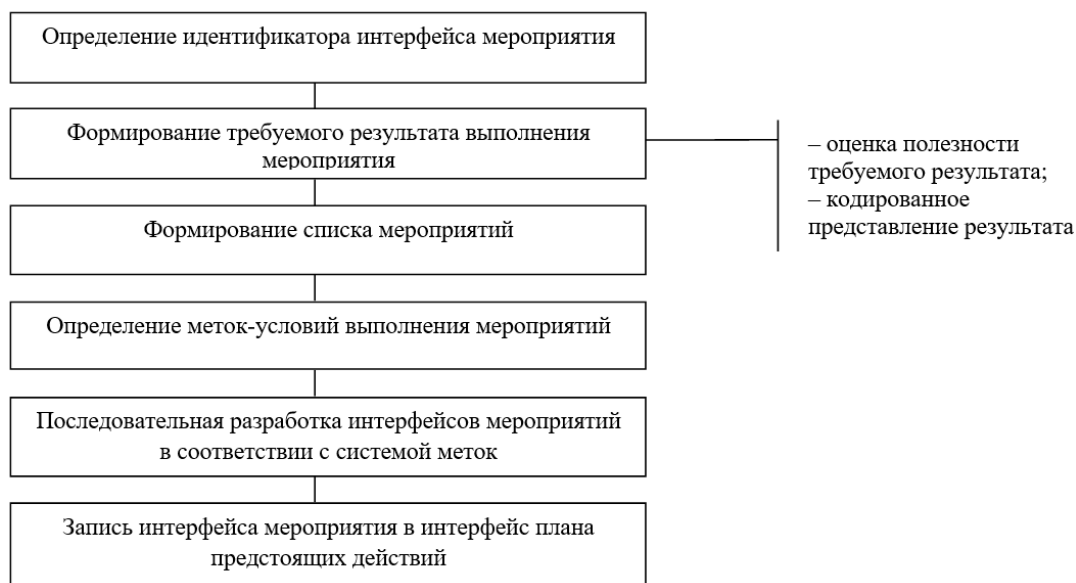


Рисунок 2 – Синтез интерфейса мероприятия

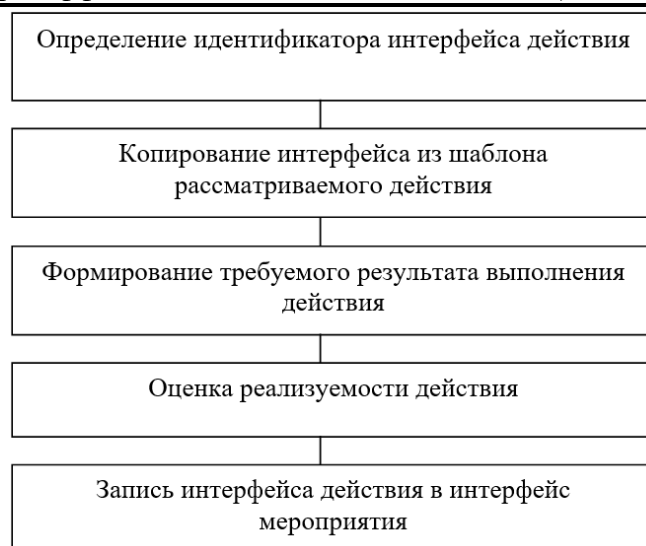


Рисунок 3 – Синтез интерфейса действия

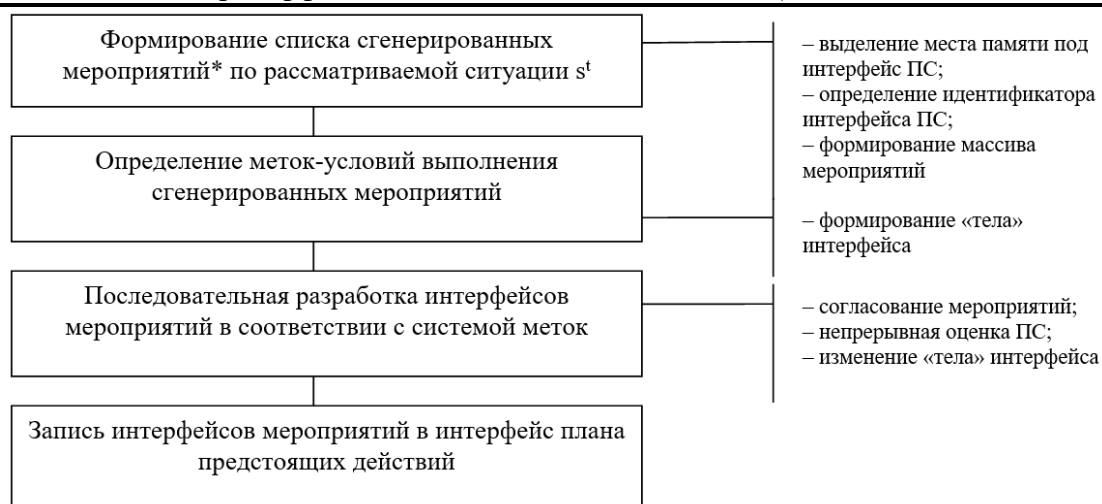
Формирование объектных запросов к объектной базе данных (ОБД) должно проводиться на языке определения запросов автоматически, в соответствии с семантикой формируемых мероприятий (общих задач). Решение данной задачи возможно посредством включения синтаксических и семантических правил формирования объектных запросов в соответствующие правила языка определения интерфейсов.

Необходимость использования ОБД вызвана следующими причинами:

- формализованное представление данных в виде, адекватном действительности;
- устранение необходимости в использовании «шлюзов», обеспечивающих согласование объектно-ориентированного представления данных в жестком программном обеспечении с представлением данных, используемым в реляционных базах данных;
- возможность компактного размещения в ОБД данных о свойствах и ресурсах объекта (системы), его (ее) текущем и прогнозируемых состояниях (план предстоящих действий), а также данных из области управления (целевая ситуация, стратегия управления, мероприятия, задачи и другие).

План предстоящих действий представляет собой совокупность планов перехода системы из ситуации в ситуацию. Каждый из этих планов представляется в виде интерфейса, определяющего порядок выполнения общих задач (мероприятий), обеспечивающих переход из одной ситуации в другую. Порядок формирования этих интерфейсов должен быть аналогичен порядку формирования мероприятий и общих задач. В свою очередь, план предстоящих действий также представляет собой интерфейс, определяющий порядок активизации планов перехода из одной ситуации в другую (Рисунок 4).

Результаты разработки плана предстоящих действий записываются в ОБД, а в интерфейсе плана отображается порядок активизации планов перехода системы из ситуации в ситуацию, а также те области ОБД, в которых хранится информация, соответствующая этим планам.



* - вместо мероприятий, в зависимости от масштаба плана, могут рассматриваться общие задачи

Рисунок 4 – Синтез плана предстоящих действий (ПС)

Таким образом, ситуативный синтез ПО, моделирующего принимаемые человеком решения, сводится к формированию интерфейсов. Практическое выполнение решений производится посредством трансляции интерфейсов в исполняемый код и исполнение этого кода процессором ЭВМ.

Список литературы

1. Балашов О.В, Букачев Д.С. Выбор методов извлечения и обработки экспертной информации для базы знаний систем поддержки принятия решений // Международный журнал информационных технологий и энергоэффективности. – 2018. – Т. 3, № 4(10). – С. 28-35.
2. Балашов О.В, Букачев Д.С. Подход к оценке качества управленческих решений на основе нечёткой логики // Международный журнал информационных технологий и энергоэффективности. – 2020. – Т. 5, № 1(15). – С. 3-7.
3. Балашов О.В, Букачев Д.С. Методический аппарат разработки математических моделей для систем поддержки принятия решений // Международный журнал информационных технологий и энергоэффективности. – 2021. – Т. 6, № 2(20). – С. 25-33.
4. Клыков Ю.И. Ситуационное управление большими системами. М., «Энергия», 1974.
5. Наумов Г.Е., Подиновский В.В., Подиновский В.В. Субъективная вероятность: способы представления и методы получения. // Техническая кибернетика. 1991. № 5.
6. Трахтенгерц Э. А. Компьютерная поддержка принятия решений. М., СИНТЕГ, 1998.
7. Фишберн П.С. Теория полезности для принятия решений. М., Наука, 1972.
8. Экономико-математические методы и прикладные модели: / В.В. Федосеев, А.Н. Гармаш, Д.М. Дайитбегов и др.; Под ред. В.В. Федосеева. - М.: ЮНИТИ, 2001.
9. Ягер Р.Р. Нечеткие множества и теория возможностей. Последние достижения /Пер. с англ., Радио и связь, 1986.

References

1. Balashov O.V, Bukachev D.S. Vybora metodov izvlecheniya i obrabotki ekspertnoj informacii dlya bazy znaniy sistem podderzhki prinyatiya reshenij // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2018. – Т. 3, № 4(10). – pp. 28-35.
 2. Balashov O.V, Bukachev D.S. Podhod k ocenke kachestva upravlencheskih reshenij na osnove nechyotkoj logiki // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2020. – Т. 5, № 1(15). – pp. 3-7.
 3. Balashov O.V, Bukachev D.S. Metodicheskij apparat razrabotki matematicheskikh modelej dlya sistem podderzhki prinyatiya reshenij // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2021. – Т. 6, № 2(20). – pp. 25-33.
 4. Klykov Yu.I. Situacionnoe upravlenie bol'shimi sistemami. М., «Energija», 1974.
 5. Naumov G.E., Podinovskij V.V., Podinovskij V.V. Sub"ektivnaya veroyatnost': sposoby predstavleniya i metody polucheniya. // Tekhnicheskaya kibernetika. 1991. № 5.
 6. Trahtengerc E. A. Komp'yuternaya podderzhka prinyatiya reshenij. М., SINTEG, 1998.
 7. Fishbern P.S. Teoriya poleznosti dlya prinyatiya reshenij. М., Nauka, 1972.
 8. Ekonomiko-matematicheskie metody i prikladnye modeli: / V.V. Fedoseev, A.N. Garmash, D.M. Dajitbegov i dr.; Pod red. V.V. Fedoseeva. - М.: YuNITI, 2001.
 9. Yager R.R. Nechetkie mnozhestva i teoriya vozmozhnostej. Poslednie dostizheniya /Per. s angl., Radio i svyaz', 1986.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.434

ОЦЕНКА ОБЛАСТИ ПРИМЕНЕНИЯ КОМБИНИРОВАННОГО НЕЧЕТКОГО РЕГУЛЯТОРА

Павлова Ю.В.,¹ Прокуденков Н.П.

ФГБОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МЭИ" (ФИЛИАЛ В ГОРОДЕ СМОЛЕНСКЕ), Смоленск, Россия, (, (214013, РФ, г. Смоленск, Энергетический проезд, дом 1), e-mail: ¹nik.prok54@mail.ru

В данной статье рассматривается применение комбинированных ПИД-регуляторов с нечеткой логикой для автоматического регулирования технологических процессов. Исследуется эффективность таких регуляторов в сравнении с классическими ПИД-регуляторами. В частности, проводится моделирование систем с различными типами объектов управления, такими как звенья первого и второго порядка с и без запаздывания. Результаты моделирования показали, что в некоторых случаях комбинированные регуляторы с нечеткой логикой могут улучшить параметры регулирования, такие как время регулирования и перерегулирование, по сравнению с традиционными ПИД-регуляторами. Однако, в системах с объектами первого порядка с запаздыванием и без него, использование нечеткой логики не дает значительных преимуществ, и применение таких регуляторов нецелесообразно.

Ключевые слова: ПИД-регулятор, нечеткое регулирование, комбинированный регулятор, Matlab Simulink, автоматическое регулирование, технологические процессы.

ASSESSMENT OF THE APPLICATION AREA OF THE COMBINED FUZZY CONTROLLER

Pavlova Y.V.,¹ Prokudnikov N.P.

"NATIONAL RESEARCH UNIVERSITY "MPEI" (BRANCH IN THE CITY OF SMOLENSK), Smolensk, Russia, (214013, Smolensk, Energeticheskiiy proezd, 1), E-MAIL: ¹nik.prok54@mail.ru

This article examines the application of combined PID controllers with fuzzy logic for automatic control of technological processes. The effectiveness of such controllers is compared with traditional PID controllers. Specifically, systems with different types of controlled objects, such as first- and second-order systems with and without time delay, are modeled. The simulation results showed that in some cases, combined controllers with fuzzy logic can improve control parameters such as settling time and overshoot, compared to traditional PID controllers. However, in systems with first-order objects with and without time delay, the use of fuzzy logic does not provide significant advantages, making the application of such controllers undesirable.

Keywords: PID controller, fuzzy control, combined controller, Matlab Simulink, automatic control, technological processes.

Среди находящихся в эксплуатации регуляторов более 90% приходится на ПИД-регуляторы. Такое широкое распространение данный вид регуляторов получил благодаря простоте построения, низкой стоимости, возможности решить большинство практических задач, а также простоте промышленного использования.

Однако при неизвестных возмущениях и недостаточных сведениях о параметрах объекта при учете транспортной задержки, не всегда удастся достичь требуемого качества регулирования.

Решить проблемы такого типа позволяет нечеткое регулирование, которое является одним из перспективнейших направлений в интеллектуальном управлении. Преимуществом использования нечеткого управления является возможность настройки при недостаточном знании о параметрах объекта, в случае если идентификация слишком трудоемка или для настройки требуются знания эксперта.

Комбинация данных методов регулирования позволяет повысить качество управления технологическими объектами, но при этом повышается сложность настройки и затраты ресурсов на управление такими системами.

В среде Matlab Simulink было проведено экспериментальное моделирование систем автоматического регулирования (САР) как с четким ПИД-регулятором, так и с комбинированным нечетким регулятором, с целью выявления области применения комбинированных регуляторов.

В промышленных системах управления объект регулирования с точки зрения теории управления может быть описан звеном первого или второго порядка как с запаздыванием, так и без него. Исходя из этого рассмотрим модели с указанными типовыми объектами регулирования.

На Рисунке 1 представлена общая модель системы для исследования с объектом управления – звеном первого порядка.

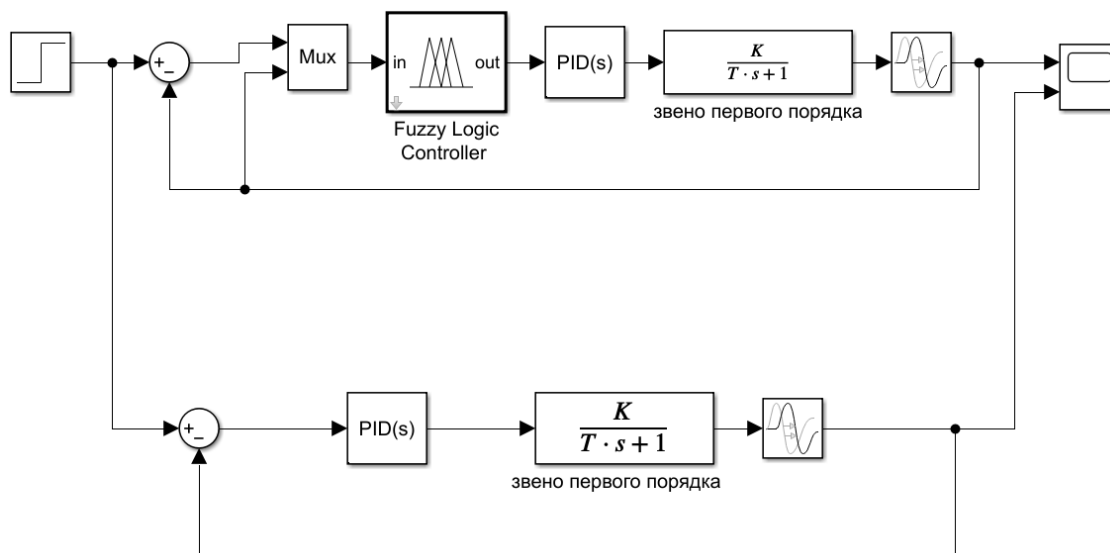


Рисунок 1 – Модель системы в общем виде

Возьмем в качестве объекта управления звено первого порядка с запаздыванием. Ниже приведена передаточная функция данного объекта управления в общем виде:

$$W(p) = \frac{K}{Tp + 1} e^{-\tau p}. \quad (1)$$

Проведем моделирование при $K=5$, $T=5$ и изменяющемся значении $\tau = \{0,5; 0,75; 1\}$. Результаты моделирования системы со звеном первого порядка с запаздыванием представлены в Таблице 1.

Оценка полученных результатов проводилась на основе переходного процесса, результаты сравнивались по критериям таким, как перерегулирование и время регулирования при точности регулирования равной 5%.

Таблица 1 – Результаты моделирования системы со звеном первого порядка при изменении времени запаздывания

	С модулем нечеткой логики		
	$\tau = 0,5$	$\tau = 0,75$	$\tau = 1$
Перерегулирование, %	21	44,9	77,6
Время регулирования, с	18,293	18,293	18,798
	Без модуля нечеткой логики		
Перерегулирование, %	7	9	11,5
Время регулирования, с	9,758	9,758	9,356

По полученным значениям времени регулирования и перерегулирования можно сделать вывод, о том, что в данной системе обычный ПИД-регулятор дает лучшие результаты управления.

Возьмем в качестве объекта управления звено второго порядка и выясним влияние изменения коэффициента передачи объекта на параметры переходного процесса. Модель системы аналогична модели на рисунке 1, с объектом управления – звеном второго порядка. Ниже приведена передаточная функция данного объекта управления в общем виде:

$$W(p) = \frac{K}{(T_1 p + 1)(T_2 p + 1)} e^{-\tau p}. \quad (2)$$

Проведем моделирование при $\tau = 0$, $T_1 = 0.5$, $T_2 = 1$ и изменяющемся значении $K = \{2; 5, 10\}$. Результаты моделирования системы со звеном второго порядка без запаздывания представлены в Таблице 2.

Таблица 2 – Результаты моделирования при изменении коэффициента усиления и временем запаздывания $\tau = 0$

	С модулем нечеткой логики		
	$K = 2$	$K = 5$	$K = 10$
Перерегулирование, %	5,8	5,3	0
Время регулирования, с	2,6	1,7	1,5
	Без модуля нечеткой логики		
Перерегулирование, %	6,7	9,2	8,6
Время регулирования, с	3,9	2,9	2,26

По полученным значениям времени регулирования и перерегулирования можно сделать вывод, о том, что в данной системе комбинированный ПИД-регулятор дает лучшие результаты управления.

Проведем моделирование на том же объекте управления при $\tau = 0$, $T_2 = 1$, $K = 2$ и изменяющемся значении $T_1 = \{0.5; 1.5; 2\}$. Результаты моделирования системы со звеном второго порядка без запаздывания представлены в Таблице 3.

Таблица 3 – Результаты моделирования при изменении постоянной времени

	С модулем нечеткой логики		
	$T_1 = 0,5$	$T_1 = 1,5$	$T_1 = 2$
Перерегулирование, %	5,8	26	32,5
Время регулирования, с	2,6	5,8	6,8
	Без модуля нечеткой логики		
Перерегулирование, %	6,7	28	34
Время регулирования, с	3,9	8,3	9,5

По результатам моделирования нечеткий ПИД-регулятор продолжает показывать лучшие результаты.

Возьмем в качестве объекта управления звено второго порядка с запаздыванием и выясним влияние изменения времени запаздывания на параметры переходного процесса.

Проведем моделирование при $K=5$, $T_1 = 0.5$, $T_2 = 1$ и изменяющемся значении $\tau = \{0,1; 0,15; 0,2\}$.

Результаты моделирования системы со звеном первого порядка с запаздыванием представлены в Таблице 4.

Таблица 4 – Результаты моделирования звена второго порядка с запаздыванием при изменении времени запаздывания

	С модулем нечеткой логики		
	$\tau = 0,1$	$\tau = 0,15$	$\tau = 0,2$
Перерегулирование, %	5,2	21	23
Время регулирования, с	2,1	2,25	2.9
	Без модуля нечеткой логики		
Перерегулирование, %	5	22	32
Время регулирования, с	3,5	4,45	3.8

Полученные результаты говорят о том, что в системах, которые можно смоделировать с помощью звена второго порядка с запаздыванием целесообразно использовать комбинированный регулятор.

Для более наглядного сравнения двух видов регулирования на Рисунке 2 приведен график переходного процесса для звена второго порядка с запаздыванием равным $\tau = 0.1$, на рисунке 3 соответствующий ему график ошибки.

По графику переходного процесса видно, что время регулирования системы с нечетким ПИД-регулятором меньше, а также по графику ошибки можно определить, что и интегральный квадратичный показатель меньше, чем у обычного регулятора.

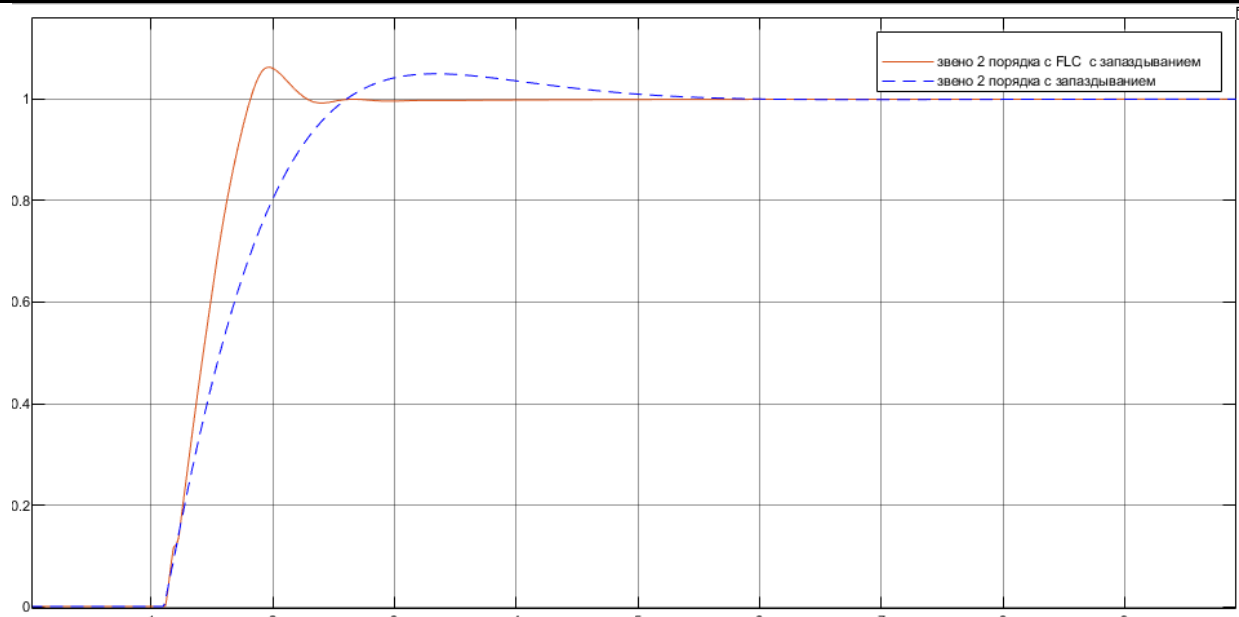


Рисунок 2 – График переходного процесса системы. при времени запаздывания $\tau = 0,1$

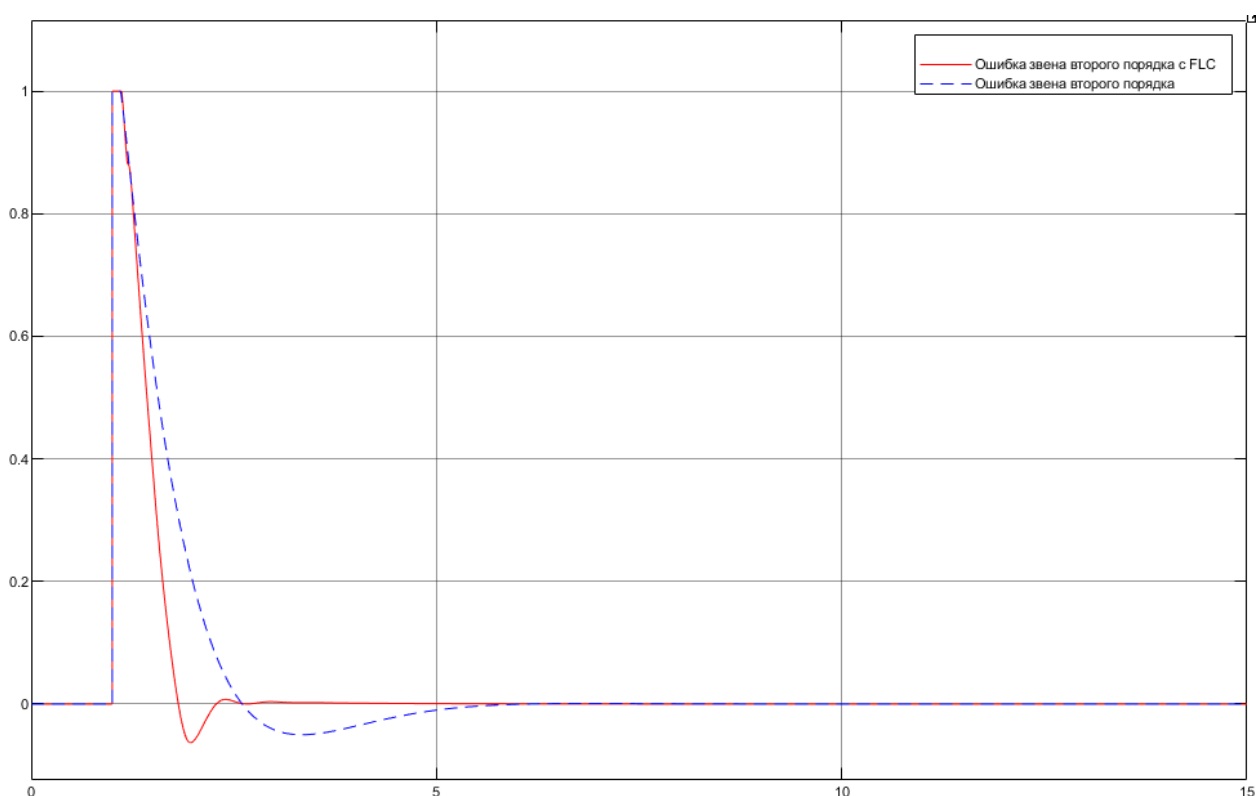


Рисунок 3 – График ошибки регулирования

Таким образом исследование показало, что для технологических систем, в которых объект управления моделируется звеном первого порядка с запаздыванием и без него использование комбинированного регулятора не приносит выигрыша в качестве регулирования. Следовательно, в таких системах нецелесообразно использование сложно регулятора с модулем нечеткой логики.

Для случая, когда объект управления описывается звеном второго порядка как с запаздыванием, так и без него, использование комбинированного ПИД- регулятора с нечеткой

логикой значительно повышает качество регулирования, а именно время регулирования и перерегулирование уменьшаются по отношению к классическому ПИД-регулятору.

В результате моделирования систем автоматического управления с различным объектом управления можно сделать вывод что комбинированный регулятор имеет смысл использовать в системах начиная со второго порядка.

Список литературы

1. Макаров И.М., В.М. Лохин Интеллектуальные системы автоматического управления /И.М. Макаров, В.М. Лохин. – М.: ФИЗМАЛИТ, 2001. – 576 с.
2. Куленко М.С., Буренин С.В. Исследование применения нечетких регуляторов в системах управления технологическими процессами // Вестник ИГЭУ. 2010. №2. С. 10 – 15.
3. Усков А.А. Системы с нечеткими моделями объектов управления: Монография. – Смоленск: СФРУК, 2013. – 153 с.
4. Павлова Ю.В., Прокуденков Н.П. Сравнительный анализ регуляторов для настройки САР. В сборнике: Информационные технологии, энергетика и экономика. 2023. С. 75-78.
5. Никитенко Е.В., Айрих И.А. Системы автоматического регулирования: Учебное пособие для студентов направления "Информатика и вычислительная техника". - Изд, 2-е. / Рубцовский индустриальный институт. – Рубионск, 2016. – 73 с.
6. Лазарева Т.Я., Мартемьянов Ю. Ф. Основы теории автоматического управления: Учебное пособие. 2-е изд., перераб. И доп. Тамбов: Изд-во Тамб. Гос. Техн. Ун-та, 2004. 352 с
7. Николаев Е.В. Технологические объекты второго порядка с запаздыванием // Молодой ученый. 2017. №23. С. 149-152.
8. Чернодуб А.Н., Дзюба Д.А. Обзор методов нейроуправления // Проблемы программирования. 2011. №2. С. 79-94.

References

1. Makarov I.M., Lokhin, V.M. *Intelligent Automatic Control Systems* / I.M. Makarov, V.M. Lokhin. – Moscow: FIZMALIT, 2001. – p.576.
2. Kulenko M.S., Burenin, S.V. *Study of the Application of Fuzzy Controllers in Technological Process Control Systems* // Bulletin of the IGEU. 2010. No. 2. pp. 10–15.
3. Uskov A.A. *Systems with Fuzzy Models of Control Objects: Monograph* – Smolensk: SFROK, 2013. – p.153.
4. Pavlova Yu.V., Prokudencov N.P. *Comparative Analysis of Controllers for Setting up Automatic Control Systems* in the collection: *Information Technologies, Energy, and Economics*. 2023. pp. 75-78.
5. Nikitenko E.V., Airikh I.A. *Automatic Control Systems: A Textbook for Students of the "Informatics and Computer Engineering" Program*. 2nd ed. / Rubtsov Industrial Institute. – Rubtsovsk, 2016. – p.73.
6. Lazareva T.Y., Martemyanov Yu.F. *Fundamentals of Automatic Control Theory: A Textbook*. 2nd ed., revised and supplemented. Tambov: Publishing House of Tambov State Technical University, 2004. – p.352.
7. Nikolaev E.V. *Technological Second-Order Objects with Time Delay* // Young Scientist. 2017. No. 23. pp. 149-152.

8. Chernodub A.N., Dzyuba D.A. *Review of Neurocontrol Methods* // *Programming Problems*. 2011. No. 2. pp. 79-94.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.8

ОБРАБОТКА И АНАЛИЗ БОЛЬШИХ ОБЪЕМОВ ДАННЫХ В СЕЛЬСКОМ ХОЗЯЙСТВЕ С ИСПОЛЬЗОВАНИЕМ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

¹Сафонова Т.В., ²Мокряк А.В., ³Вареник П.М., ⁴Муленко М.Д., ⁵Ведерникова С.Д.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская
ул., д. 79) e-mail: ¹tatyana.vsafonova@gmail.com, ³pvarenik1810@gmail.com,

⁴mariyamouse@mail.com, ⁵vettrai@yandex.ru

²ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ
ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО
ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ
ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-
Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

В статье исследуется использование технологий анализа больших данных и геоинформационных систем (ГИС) в сельском хозяйстве. Основное внимание уделяется преимуществам объединения этих технологий для увеличения продуктивности агропроизводства, рационального использования ресурсов и совершенствования процедур принятия решений. Представлены примеры успешной реализации таких подходов в разных регионах, а также обсуждается потенциал их дальнейшего развития в рамках цифровизации аграрной отрасли.

Ключевые слова: Большие данные, ГИС, агропроизводство, прогнозирование урожайности.

PROCESSING AND ANALYSIS OF LARGE AMOUNTS OF DATA IN AGRICULTURE USING GEOGRAPHIC INFORMATION SYSTEMS

¹Safonova T.V., ²Mokryak A.V., ³Varenik P.M., ⁴Mulenko M.D., ⁵Vedernikova S.D.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St.
Petersburg, Voronezhskaya str., 79), e-mail: ¹tatyana.vsafonova@gmail.com,
³pvarenik1810@gmail.com, ⁴mariyamouse@mail.com, ⁵vettrai@yandex.ru;

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

The article examines the use of big data analysis technologies and geographic information systems (GIS) in agriculture. The main focus is on the benefits of combining these technologies to increase agricultural productivity, rational use of resources and improve decision-making procedures. Examples of successful implementation of such approaches in different regions are presented, and the potential for their further development within the framework of digitalization of the agricultural sector is discussed.

Keywords: Big data, GIS, agricultural production, yield forecasting.

Введение

Анализ больших данных и использование геоинформационных систем (ГИС) превращаются в основные инструменты современного сельского хозяйства, предоставляющие аграриям и фермерам новые способы повышения эффективности и устойчивости агропроизводства. В условиях роста мировой популяции, изменения климата и уменьшения природных ресурсов необходимость в инновационных методах управления сельским хозяйством становится все более важной. Главная цель настоящего исследования заключается в изучении возможностей применения анализа больших данных и ГИС для оптимизации сельскохозяйственных процессов и обеспечения стабильности производства. Следует отметить, что интеграция данных технологий может кардинально изменить подходы к агрономии, способствуя принятию более точных и обоснованных решений на всех этапах агропроизводства [1].

Актуальность проблемы и преимущества использования больших данных и ГИС

Современное сельское хозяйство сталкивается с серьезными проблемами, такими как климатические изменения, рост спроса на продукты питания и необходимость повышения производительности при минимальном воздействии на природу. Согласно данным Продовольственной и сельскохозяйственной организации ООН (ФАО), к 2050 году численность населения мира достигнет 9,7 миллиардов человек, что потребует увеличения объема производимой пищи на 70%, что диктует необходимость внедрения новых технологий и методов управления со стороны аграриев [2, 3].

Технологии анализа больших данных позволяют собирать, обрабатывать и анализировать большие массивы информации из разнообразных источников, что предоставляет возможность фермерам получить полную картину состояния своих полей, спрогнозировать урожайность и оптимально использовать ресурсы. Например, анализ данных о влажности почвы помогает выбрать наилучшие сроки для полива, снижая расход воды и повышая урожайность.

ГИС играют важную роль в визуализации пространственных данных, которые помогают агрономам детально изучать состояние почв, распределение ресурсов и контролировать здоровье растений. Использование ГИС позволяет выявить проблемные зоны на полях, оперативно реагировать на изменения и предпринимать шаги для улучшения состояния посевов [4].

Значение больших данных в сельском хозяйстве

Большие данные в сельском хозяйстве представляют собой обширные массивы информации, собранные с применением различных технологий, таких как сенсоры, спутники и дроны. Такая информация включает сведения о погоде, характеристиках почвы, урожайности и прочих аспектах, оказывающих влияние на производство сельхозпродукции. Применение аналитических инструментов для работы с большими данными позволяет прогнозировать урожайность, так как на основании исторических данных и текущих условий фермеры могут точнее предсказывать результаты своей деятельности. Например, анализ метеорологической информации помогает определить оптимальное время для посева [5].

Также использование аналитических технологий дает возможность оптимизировать использование ресурсов за счет снижения затрат на удобрения и воду, способствуя более устойчивому ведению хозяйства. Методология точного земледелия позволяет эффективно применять ресурсы лишь там, где они действительно необходимы.

Технологии анализа больших данных способны предсказывать возможные угрозы, такие как засуха или болезни растений, что позволяет заблаговременно принять защитные меры. Также большие данные используются для изучения рыночных трендов, помогая фермерам принимать взвешенные решения относительно того, какие культуры следует выращивать [6, 7].

Роль ГИС в сельском хозяйстве с использованием больших данных

ГИС играют важную роль в сборе, обработке и визуализации пространственных данных. Они предоставляют агрономам и фермерам возможности сбора и обработки картографической информации, что позволяет создавать карты урожайности и определять менее продуктивные участки. Спутниковые снимки и дроны, в свою очередь, помогают следить за здоровьем растений и своевременно выявлять проблемы, что обеспечивает быструю реакцию на изменения в состоянии полей.

ГИС дает возможность оптимизировать маршруты транспортировки продукции, сокращая транспортные расходы фермерских хозяйств, занимающих значительные площади. С помощью ГИС можно оценить последствия климатических изменений на продуктивность сельского хозяйства, разрабатывая стратегии адаптации.

Объединение технологий анализа больших данных с ГИС создаёт мощнейший инструмент для аграриев. Такое сочетание дает возможность анализировать большие объёмы пространственных данных. Например, фермер может узнать актуальную информацию о состоянии своего поля непосредственно во время выполнения полевых работ [8-10].

Алгоритмы машинного обучения позволяют прогнозировать изменения в урожайности или потребности в ресурсах на основе пространственных данных, что помогает фермерам строить планы на будущее, опираясь на точные прогнозы. Также данные из ГИС могут быть использованы для формирования комплексных отчётов и визуализаций, облегчая понимание сложных взаимодействий внутри агросистем. Примеры практического применения больших данных и ГИС в сельском хозяйстве представлены в таблице 1 [11-13].

Таблица 1 - Примеры использования ГИС и больших данных в сельском хозяйстве

Регион	Название проекта	Описание
Россия	Цифровое сельское хозяйство	Проект Минсельхоза России, направленный на цифровую трансформацию аграрного сектора с созданием «озер» данных
	Геоинформационная система Удмуртской Республики	Система на базе РусГИС для мониторинга сельскохозяйственных угодий, контроля состояния растений и пастбищ
	Система мониторинга полей и животных	Внедрение датчиков для контроля состояния растений и цифровых бирок для мониторинга здоровья скота
	Проект Agrarium	Автоматизированная платформа для синхронизации цифровых данных и

Регион	Название проекта	Описание
		управления активами сельхозпроизводителей
США	Precision Agriculture	Технологии точного земледелия с использованием данных дронов и спутников для мониторинга состояния полей
	FarmLogs	Платформа для отслеживания урожайности, планирования посевов и управления ресурсами на основе анализа больших данных
Великобритания	Agri-Tech East	Инициатива по развитию агрономических технологий через сотрудничество между учеными, бизнесом и фермерами
Нидерланды	Smart Farming	Внедрение технологий умного сельского хозяйства, включая автоматизацию процессов в теплицах с помощью датчиков и ИИ

Технологический аспект функционирования ГИС и больших данных для отрасли сельского хозяйства

ГИС и большие данные становятся важным инструментом для повышения эффективности и устойчивости агропроизводства. Давайте рассмотрим, каким образом функционирует ГИС с использованием больших данных для отрасли сельского хозяйства.

- Шаг 1 - сбор данных.

Первым этапом работы ГИС является сбор данных из различных источников. Этими источниками могут быть датчики, сенсоры, спутниковые снимки, аэрофотосъемка и метеорологические данные, которые применяются для различного рода мониторинга показателей.

- Шаг 2 - хранение и обработка данных

Собранные данные интегрируются в системы управления базами данных (СУБД). Часто используются реляционные базы данных, такие как PostgreSQL с расширением PostGIS, а также NoSQL-базы данных. После сохранения данные подвергаются обработке, которая включает: анализ временных рядов для прогнозирования агроклиматических условий, урожайности и распределения водных ресурсов; пространственный анализ, который включает расчет состояний, определение площадей и выявление пространственных закономерностей; моделирование процессов для оценки влияния различных факторов на показатель урожайности культур и здоровье растений.

- Шаг 3 - визуализация данных

На этом этапе информация представляется в виде интерактивных карт и графиков. ГИС позволяет создавать многослойные карты, которые помогают фермерам увидеть различные

аспекты своих полей, а именно: картирование урожайности для определения участков с низкой продуктивностью и выявления проблем; температурные карты для отслеживания температурных изменений в разных частях поля; картирование влажности почвы для оптимизации орошения и использования удобрений.

- Шаг 4 - принятие решений

Основываясь на анализе и визуализации данных, принимаются обоснованные решения по оптимизации использования ресурсов, а именно удобрений и средств защиты растений, что поможет снизить затраты и минимизировать негативное воздействие на окружающую среду. Также на данном этапе на основе прогнозных данных и анализе состояния полей реализуется планирование сельскохозяйственных работ, а именно: посевы, уборка урожая и прочие операции.

Для корректного принятия решения проводится мониторинг состояния посевов, который позволяет отслеживать состояние растений в реальном времени и быстро реагировать на изменения и предотвращать убытки.

- Шаг 5 - применение технологий больших данных

За счет интеграции технологий больших данных в ГИС существенно увеличивается аналитический потенциал, позволяя прогнозировать урожайность, что может привести к росту урожайности зерновых культур более чем на 30%.

Автоматизация процессов функционирования ГИС предоставляет возможность формировать цифровую карту сельскохозяйственных угодий для отслеживания и управления показателями в режиме реального времени.

На Рисунке 1 представлена диаграмма последовательности действий, демонстрирующая очередность шагов пользователя в ГИС, которые связаны с обработкой и анализом данных для рационального управления сельскохозяйственными работами [14].

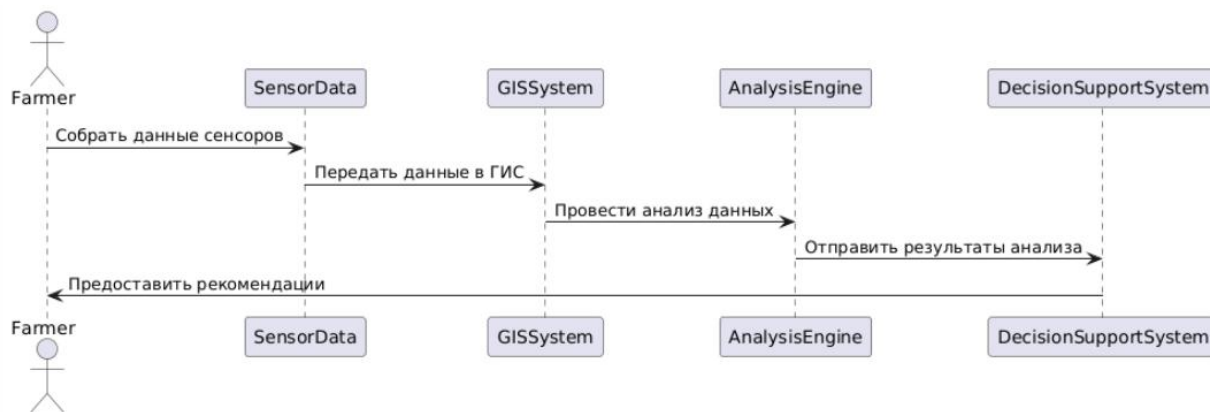


Рисунок 1 - Диаграмма последовательности действий пользователя в ГИС

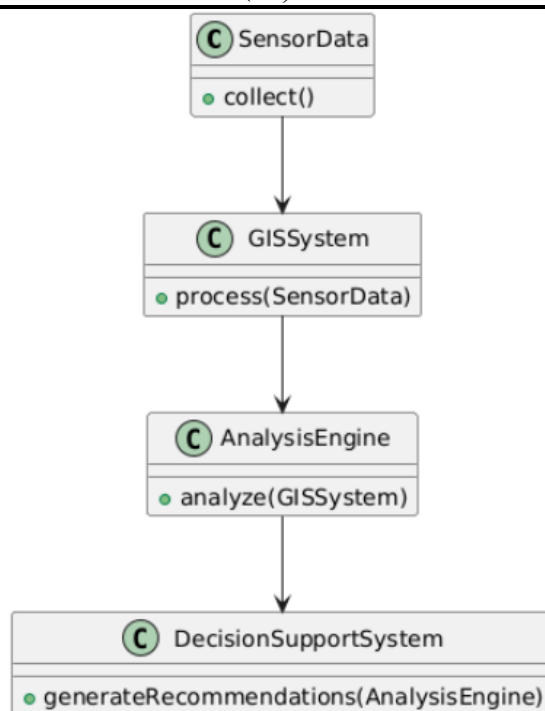


Рисунок 2 - Диаграмма классов ГИС для сельского хозяйства

На Рисунке 2 представлена диаграмма классов, которая показывает структуру ГИС, включая классы и отношения.

Выводы

Анализ больших данных и использование ГИС в сельском хозяйстве представляют собой значимые этапы цифровой трансформации аграрного сектора. Данные технологии не только увеличивают эффективность производства, но и способствуют устойчивому развитию агросферы, что особенно важно в условиях глобального изменения климата и роста численности населения.

Внедрение технологий анализа больших данных позволяет фермерам точнее оценивать состояние своих полей, прогнозировать урожайность и оптимизировать использование ресурсов, что ведет к снижению расходов на удобрения и воду, уменьшению потерь и увеличению общей продуктивности. Так, точное земледелие позволяет фермерам применять удобрения и средства защиты растений исключительно там, где это действительно нужно, что не только экономит средства, но и уменьшает вредное воздействие на окружающую среду.

Использование ГИС вместе с большими данными помогает агрономам и фермерам принимать более обоснованные решения на основе пространственного анализа. Сюда входит мониторинг состояния почвы, управление водными ресурсами и оценка последствий климатических изменений на сельскохозяйственную продукцию. Такой подход способствует формированию более устойчивых агросистем, способных адаптироваться к меняющимся условиям.

Несмотря на явные преимущества, внедрение технологий больших данных и ГИС сталкивается с определенными трудностями. Среди них — высокие затраты на внедрение

технологий, нехватка квалифицированного персонала для работы с данными, а также сложности с получением качественных данных из-за слабого уровня инфраструктуры в отдельных регионах.

Перспективы дальнейшего развития технологий Big Data и ГИС в сельском хозяйстве весьма обнадеживающие. Ожидается, что благодаря развитию облачных технологий и искусственного интеллекта возможности для анализа данных будут значительно расширяться, что позволит создавать более сложные прогнозирующие модели, учитывающие множество факторов одновременно.

Кроме того, интеграция Интернета вещей (IoT) с большими данными и ГИС открывает новые возможности для автоматизации процессов в сельском хозяйстве. Например, использование сенсоров для мониторинга состояния почвы и растений в реальном времени даст фермерам возможность оперативно реагировать на изменения условий и принимать решения на основе актуальных данных.

Список литературы

1. Баранов, А. В. Технологии Big Data в сельском хозяйстве / А. В. Баранов // Научные исследования и разработки. – 2019. – Т. 1, № 2. – С. 45-50.
2. Демичев, В. В. Понятие, основные характеристики и источники больших данных в сельском хозяйстве / В. В. Демичев // РГАУ-МСХА имени К. А. Тимирязева. – 2022.
3. Кузнецов, И. А. Применение геоинформационных систем в сельском хозяйстве / И. А. Кузнецов, Е. С. Петрова // Агроинженерия и технологии. – 2020. – Т. 3, № 1. – С. 12-20.
4. Лебедев, С. А. Применение технологий больших данных в агрономии: Перспективы и вызовы / С. А. Лебедев, О. В. Кузьмина // Научный журнал АГРОТЕХ. – 2020. – Т. 2, № 3. – С. 15-22.
5. Иванов, Д. С. Геоинформационные системы в аграрном секторе: Технологии и приложения / Д. С. Иванов, А. П. Михайлов // NextGIS. – 2021.
6. Григорьев, П. Инновационные технологии в аграрном секторе: Роль больших данных / П. Григорьев, Т. Орлова // Вестник агрономии. – 2019. – Т. I(1). – С. 50-58.
7. Сидоров, В. Н. Геоинформационные системы как инструмент повышения эффективности сельского хозяйства в России: Обзор и анализ практики / В. Н. Сидоров, Е. А. Васильева // Сельское хозяйство России. – 2023. – Т. I(2). – С. 18-25.
8. Frolov, A. N. Использование геоинформационных технологий для мониторинга состояния сельскохозяйственных угодий: Практические аспекты и результаты исследований / A. N. Frolov, I. V. Shevchenko // Агроэкология и устойчивое развитие. – 2021. – Т. I(3). – С. 29-37.
9. Ковальев, Р. И. ГИС-технологии для управления сельским хозяйством: Современные подходы и инструменты / Р. И. Ковальев, Н. В. Федорова // Аграрная наука. – 2022. – Т. I(4). – С. 34-42.
10. Яковлев, С. А. Применение больших данных для повышения эффективности агропроизводства: Анализ современных тенденций и практик в России и за рубежом / С. А. Яковлев, А. В. Кузнецова // Журнал агрономических наук. – 2023. – Т. I(1). – С. 12-19.

11. Спутниковый мониторинг лесных пожаров Логинов И.С., Мошуров В.М., Сафонова Т.В., Вершинин А.К., Ясников А.И. Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 4-10.
12. Анализ технологии сенсорного мониторинга Попов В.Н., Сафонова Т.В., Кирспуу К.А. Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 24-28.
13. Использование БПЛА в сельском хозяйстве Русскин В.Д., Мошуров В.М., Ясников А.И., Вершинин А.К., Сафонова Т.В. Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 4-10.
14. ГИС для мониторинга и оценки сельскохозяйственных угодий Сафонова Т.В., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 19-27.

References

1. Baranov, A.V. Big Data technologies in agriculture / A.V. Baranov // Scientific research and development. 2019. Vol. 1, No. 2. pp. 45-50.
2. Demichev, V. V. The concept, main characteristics and sources of big data in agriculture / V. V. Demichev // RGAU-MSHA named after K. A. Timiryazev. – 2022.
3. Kuznetsov, I. A. Application of geoinformation systems in agriculture / I. A. Kuznetsov, E. S. Petrova // Agroengineering and technology. – 2020. – Vol. 3, No. 1. – pp. 12-20.
4. Lebedev, S. A. Application of big data technologies in agronomy: Prospects and challenges / S. A. Lebedev, O. V. Kuzmina // Scientific journal AGROTECH. 2020. Vol. 2, No. 3. pp. 15-22.
5. Ivanov, D. S. Geoinformation systems in the agricultural sector: Technologies and applications / D. S. Ivanov, A. P. Mikhailov // NextGIS. – 2021.
6. Grigoriev, P. Innovative technologies in the agricultural sector: The role of big data / P. Grigoriev, T. Orlova // Bulletin of Agronomy. – 2019. – Vol. I(1). – pp. 50-58.
7. Sidorov, V. N. Geoinformation systems as a tool for improving agricultural efficiency in Russia: Review and analysis of practice / V. N. Sidorov, E. A. Vasilyeva // Agriculture in Russia. – 2023. – Vol. I(2). – pp. 18-25.
8. Frolov, A. N. The use of geoinformation technologies for monitoring the condition of agricultural land: Practical aspects and research results / A. N. Frolov, I. V. Shevchenko // Agroecology and sustainable development. – 2021. – Vol. I(3). – pp. 29-37.
9. Kovalev, R. I. GIS technologies for agricultural management: Modern approaches and tools / R. I. Kovalev, N. V. Fedorova // Agrarian Science. – 2022. – Vol. I(4). – pp. 34-42.
10. Yakovlev, S. A. The use of big data to improve the efficiency of agricultural production: Analysis of modern trends and practices in Russia and abroad / S. A. Yakovlev, A.V. Kuznetsova // Journal of Agronomic Sciences. – 2023. – Vol. I(1). – pp. 12-19.
11. Satellite monitoring of forest fires Loginov I.S., Moshurov V.M., Safonova T.V., Vershinin A.K., Yasnikov A.I. Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 4-10.
12. Analysis of sensor monitoring technology Popov V.N., Safonova T.V., Kirspuu K.A. Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 24-28.

13. The use of UAVs in agriculture Ruskin V.D., Moshurov V.M., Yasnikov A.I., Vershinin A.K., Safonova T.V. Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 4-10.
 14. GIS for monitoring and evaluation of agricultural lands Safonova T.V., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 19-27.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.925

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ И ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ В ГЕОНАВИГАЦИИ

¹Сафонова Т.В., ²Мокряк А.В., ³Вареник П.М., ⁴Муленко М.Д., ⁵Ведерникова С.Д.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79) e-mail: ¹tatyana.vsafonova@gmail.com, ³pvarenik1810@gmail.com,

⁴mariyamouse@mail.com, ⁵vettrai@yandex.ru

²ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

В данной статье изучаются технологии виртуальной реальности (VR) и дополненной реальности (AR) и их применение в геонавигации. Рассматриваются базовые принципы работы этих технологий, их общие черты и отличия, а также примеры использования в таких областях, как транспорт, туризм и образование. Обсуждается, каким образом VR и AR влияют на улучшение навигационных систем и пользовательского опыта. Также в работе рассматриваются перспективы развития этих технологий в контексте геонавигации.

Ключевые слова: Виртуальная реальность (VR), дополненная реальность (AR), геонавигация, иммерсивные технологии.

VIRTUAL REALITY AND AUGMENTED REALITY IN GEOSTEERING

¹Safonova T.V., ²Mokryak A.V., ³Varenik P.M., ⁴Mulenko M.D., ⁵Vedernikova S.D.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79), e-mail: ¹tatyana.vsafonova@gmail.com, ³pvarenik1810@gmail.com, ⁴mariyamouse@mail.com, ⁵vettrai@yandex.ru;

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

This paper examines virtual reality (VR) and augmented reality (AR) technologies and their application in geosteering. It discusses the basic principles of operation of these technologies, their similarities and differences, and examples of use in areas such as transportation, tourism, and education. It discusses how VR and AR affect the improvement of navigation systems and user experience. The paper also considers the prospects for the development of these technologies in the context of geosteering.

Keywords: Virtual reality (VR), augmented reality (AR), geonavigation, immersive technologies.

Введение

Развитие технологий виртуальной реальности (VR) и дополненной реальности (AR) приносит значительные изменения в подходы к навигации и ориентации в пространстве. Геонавигация, основывающаяся на глобальных навигационных спутниковых системах (GNSS), таких как GPS, получает дополнительные возможности благодаря интеграции VR и AR. Данные технологии не только улучшают точность навигации, но и обогащают пользовательский опыт за счёт интерактивной визуализации информации. Целью данной статьи является исследование возможностей применения технологий виртуальной и дополненной реальности в геонавигации для повышения эффективности навигационных систем и улучшения пользовательского опыта.

Актуальность выбранной области исследования обусловлена возрастающим интересом к VR и AR в различных сферах жизнедеятельности. Согласно прогнозам аналитических компаний, в 2025 году рынок VR и AR технологий увеличится до 200 миллиардов долларов США, что открывает новые горизонты для их применения в таких областях, как транспорт, строительство, образование, медицина и туризм [1, 2]. В контексте геонавигации использование VR и AR может значительно повысить эффективность маршрутизации, уменьшить количество ошибок при ориентировании и улучшить взаимодействие пользователей с окружающей средой. Основные задачи данной статьи заключаются в изучении основных принципов работы технологий VR и AR, анализе текущего состояния применения VR и AR в геонавигации и оценке преимуществ и недостатков использования VR и AR в навигационных системах.

Принципы работы виртуальной и дополненной реальности

Виртуальная реальность (VR) создает полностью погруженную среду, которая замещает физический мир компьютерным пространством. Для входа в VR пользователи нуждаются в специальных устройствах, таких как шлемы виртуальной реальности (например, Oculus Rift или HTC Vive). Данные устройства обеспечивают глубокое погружение, позволяя пользователям взаимодействовать с виртуальными объектами через контроллеры или жесты.

Дополненная реальность (AR) накладывает виртуальные объекты на реальный мир, давая пользователям возможность взаимодействовать с физическим окружением, получая дополнительную информацию. AR чаще всего реализуется через мобильные устройства или специализированные очки (например, Microsoft HoloLens или Google Glass). Данная технология позволяет пользователям видеть как реальные объекты, так и их цифровые дополнения одновременно. Рассмотрим более подробно примеры применения VR и AR в геонавигации [3].

- Туризм

В туристической сфере VR и AR широко используются для создания интерактивных карт и навигационных приложений. Путешественникам доступны AR-приложения, которые предоставляют информацию о достопримечательностях в режиме реального времени. Пользователи могут не только читать тексты, но и видеть трехмерные модели объектов.

- Транспорт

В автомобильной промышленности AR применяется для создания навигационных систем, которые проецируют маршруты на лобовое стекло автомобиля (Head-Up Display, HUD), что позволяет водителям следить за дорогой, не отвлекаясь от руля. Такие системы также могут предупреждать об опасных ситуациях на дорогах.

- **Образование**

В учебных заведениях VR активно внедряется для создания симуляторов, которые помогают студентам изучать географию и картографию. Учащиеся могут «посетить» различные уголки мира, исследуя их особенности в интерактивном формате, что делает обучение более интересным и результативным.

- **Экстренные службы**

VR-тренинги используются для подготовки сотрудников служб быстрого реагирования. Они позволяют моделировать сложные ситуации спасения людей в условиях плотной городской застройки, что улучшает подготовку специалистов к реальным вызовам.

- **Военные**

Вооруженные силы применяют VR для тренировок солдат в экстремальных условиях боя. Симуляторы позволяют отрабатывать тактические навыки без риска для жизни военнослужащих [4-7].

Таблица 1 - Отечественные и зарубежные проекты и практики применения AR и VR

Регион	Название проекта	Описание
Россия	Образовательная метавселенная НЕЙМАР	Платформа для обучения с использованием VR, позволяющая студентам погружаться в учебный процесс через интерактивные сценарии
	VR-проект «В трех измерениях: Гончарова и Малевич»	Проект Третьяковской галереи, создающий атмосферу мастерских художников, где зрители могут взаимодействовать с виртуальными объектами
	Платформа «Перспектива»	Помогает школьникам выбирать профессию через VR-тренажеры, позволяя попробовать себя в роли различных специалистов
	ATLAS VR	Проект, создающий виртуальный мир на основе космических снимков для моделирования сложных явлений и обучения основам безопасности
	Программа «VR Школа» в Нижнем Новгороде	Цифровой курс ОБЖ с использованием VR-тренажеров, отрабатывающих эвакуацию из зданий при пожаре и действия в экстренных ситуациях
	Дополненная реальность в образовании	Программный комплекс для создания сценариев учебных демонстраций с использованием AR-технологий, повышающий качество усвоения материала

Регион	Название проекта	Описание
За рубежом	Pilgrim — AR-парки Outdoor	Стартап, создавший парки дополненной реальности в Европе, позволяющий туристам видеть исторические памятники в их первоначальном виде
	Arcona	Глобальный проект по созданию слоя AR, охватывающего всю планету, позволяющий пользователям взаимодействовать с контентом через мобильные приложения
	Pokemon GO	Мобильное приложение, использующее AR для создания игрового опыта, где игроки ловят покемонов в реальном мире
	IKEA Place	Приложение от IKEA для визуализации мебели в доме с помощью AR-технологий перед покупкой
	Google Maps — Live View	Функция AR для отображения направлений на улицах города через камеру смартфона, упрощающая навигацию для пользователей

Технология применения виртуальной и дополненной реальности в геонавигации

Процесс функционирования VR и AR в контексте геонавигации включает несколько этапов:

- Сбор данных

Первый шаг заключается в сборе необходимой информации, такой как геоданные, сенсорные данные, спутниковые снимки и другие источники, что может включать использование глобальных навигационных систем (GPS, GLONASS и др.), а также данные с датчиков и камер [6].

- Обработка данных

После сбора данные обрабатываются с использованием мощных вычислительных ресурсов и специализированного ПО. Данный этап включает в себя: обработку геоданных, а именно преобразование пространственных данных в удобные для использования формы, такие как карты и 3D-модели; моделирование, включая создание трёхмерных моделей местности или объектов, которые могут затем использоваться в виртуальных средах; анализ данных в реальном времени (обработка большого объёма информации в облачной инфраструктуре для обновления информации о положении объектов и их состоянии); визуализация данных (преобразование результатов обработки в форму, удобную для восприятия пользователем) [7]. VR создаёт иммерсивные 3D-среды, а дополненная реальность накладывает цифровые элементы на реальные объекты, что позволяет показать маршруты и подсказки прямо на лобовое стекло автомобиля или на экран мобильного устройства, создавать интерактивные карты (карты достопримечательностей, исторических мест и

природных объектов) в режиме реального времени и предоставлять дополнительную информацию.

- Интерактивность и управление

Виртуальные интерфейсы позволяют пользователям управлять навигационными системами с помощью жестов или голосовых команд [8].

VR моделирование используется для создания симуляторов, которые помогают обученным навыкам навигации и ориентирования, что особенно полезно для служб экстренной помощи или военных подразделений, где навыки ориентирования имеют решающую роль.

Проектирование работы системы геонавигации по предоставлению данных в формате виртуальной и дополненной реальности

Для наглядного представления работы VR и AR в области геонавигации рассмотрим проекты функционирования геонавигационной системы посредством использования унифицированного языка моделирования UML. На Рисунке 1 представлена диаграмма последовательности, которая демонстрирует взаимодействие между пользователем, системой AR и VR, а также геонавигационными данными [9].

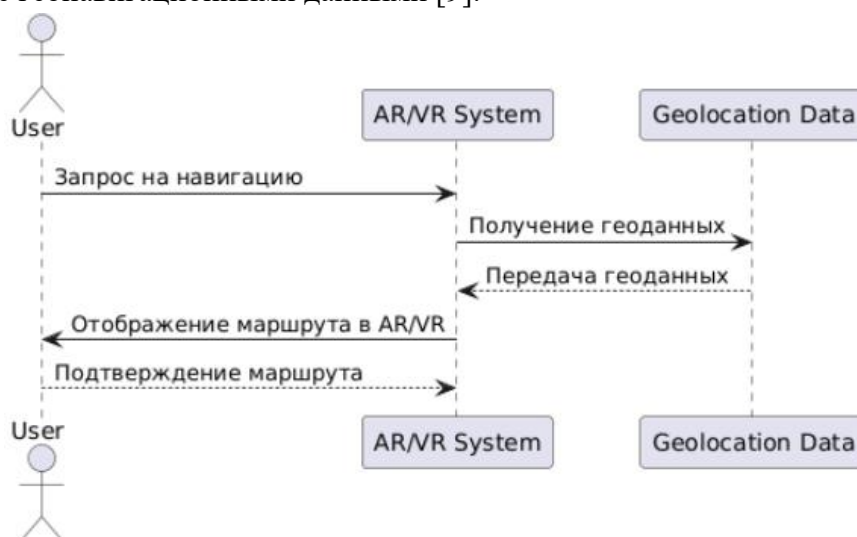


Рисунок 1 - Диаграмма последовательности

- Пользователь инициирует взаимодействие с системой AR/VR, например, через мобильное устройство или шлем виртуальной реальности.
- Система AR/VR собирает данные о местоположении пользователя, его действиях и окружающей среде.
- Геонавигационные данные поступают в систему AR/VR, включая информацию о карте, маршрутах, погодных условиях и т.д.
- Система AR/VR обрабатывает полученные данные и генерирует интерактивные карты, маршруты и подсказки для пользователя.
- Пользователь взаимодействует с системой AR/VR, выбирая маршруты, используя ее подсказки и навигационную поддержку [10-12].

На Рисунке 2 представлена диаграмма компонентов, которая демонстрирует структуру системы, включающей VR и AR, применяемую для целей геонавигации.

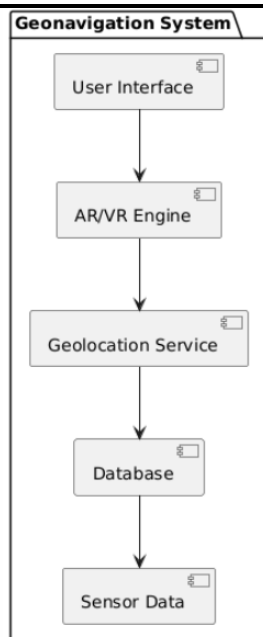


Рисунок 2 - Диаграмма компонентов

На Рисунке 3 диаграмма классов, которая описывает основные классы и их взаимосвязи в системе геонавигации с использованием VR и AR [13-17].

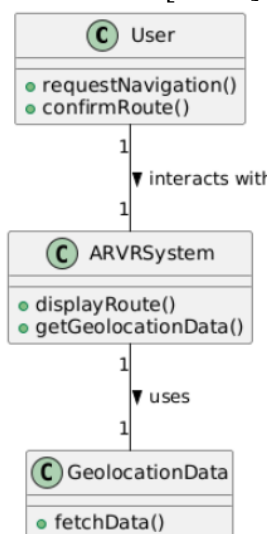


Рисунок 3 - Диаграмма классов

Выводы

VR и AR представляют собой прорывные технологии, которые могут радикально изменить подходы к геонавигации и ориентированию в пространстве. Данные технологии не только улучшают точность навигационных систем, но и обогащают пользовательский опыт, предоставляя интерактивные и визуально привлекательные интерфейсы.

Преимущества применения VR и AR в геонавигации заключаются в повышении точности навигации, а именно: AR позволяет отображать маршруты и подсказки непосредственно на реальных объектах, что значительно снижает вероятность ошибок при

ориентировании. Например, автомобильные системы Head-Up Display (HUD) помогают водителям сохранять фокус на дороге, избегая отвлечения.

VR и AR создают иммерсивные среды, которые делают процесс навигации более увлекательным. Пользователи могут взаимодействовать с виртуальными объектами, что способствует лучшему запоминанию информации о маршрутах и достопримечательностях.

AR-технологии позволяют пользователям получать данные о реальном мире в режиме реального времени. Например, туристы могут направить устройство на исторический объект и получить подробную информацию о его происхождении, дате строительства и других аспектах.

VR используется для создания симуляторов, которые помогают обучаемым осваивать различные аспекты навигации и ориентирования, что особенно полезно для служб экстренного реагирования и армии, где от навыков ориентирования зависят жизнь и работа.

Учитывая прогнозируемый рост рынка VR и AR, можно ожидать дальнейшего распространения этих технологий в геонавигации. Повышение доступности оборудования (например, более доступные шлемы VR и AR-очки) может сделать технологии более популярными среди широких масс.

Интеграция искусственного интеллекта (AI) в системы VR и AR также имеет большой потенциал. AI может способствовать персонализации пользовательского опыта, адаптируя контент под индивидуальные предпочтения и поведение пользователей. Например, системы могут анализировать маршруты пользователя и предлагать оптимальные варианты на основе его привычек.

Несмотря на многочисленные преимущества, внедрение VR и AR сталкивается с некоторыми вызовами из-за высокой стоимости оборудования VR и AR и трудностей освоения новых технологий, что требует разработки интуитивно понятных интерфейсов. Также могут возникать проблемы с доступом к данным, так как требуется наличие высококачественных геоданных, что может стать препятствием в определенных регионах.

Список литературы

1. Кичеев, В. Г., Макаренко, Н. Н. Геоинформационное пространство: реальный мир и дополненная реальность // Сибирский государственный университет геосистем и технологий. – 2020. – URL: <https://cyberleninka.ru/article/n/geoinformatsionnoe-prostranstvo-realnyy-mir-i-dopolnennaya-realnost> (Дата обращения: 01.01.2025).
2. Виртуальная реальность: разбираемся в терминологии // Habr. – 2021. – URL: <https://habr.com/ru/companies/puzzleenglish/articles/370977/> (Дата обращения: 01.01.2025).
3. Виртуальная реальность (VR) // Sber Developer. – 2022. – URL: <https://developers.sber.ru/help/ar-vr/virtual-augmented-reality> (Дата обращения: 01.01.2025).
4. Дополненная реальность (AR) // Big dream lab. – 2023. – URL: <https://bigdreamlab.kz/blog/dopolnennaya-i-virtualnaya-realnosti> (Дата обращения: 02.01.2025).
5. Технологии виртуальной реальности // IT Week. – 2022. – URL: <https://www.itweek.ru/mobile/article/detail.php?ID=224416> (Дата обращения: 02.01.2025).
6. Google Maps Live View // Google Support. – 2023. – URL: <https://support.google.com/maps/answer/10000000?hl=ru> (Дата обращения: 06.01.2025).

7. Arcona — проект по созданию слоя дополненной реальности // Arcona. – 2023. – URL: <https://arcona.io/> (дата обращения: 06.01.2025).
8. Piligrim — AR-парки Outdoor // Piligrim. – 2023. – URL: <https://piligrim.app/> (Дата обращения: 06.01.2025).
9. Бошков, И. И., Крутикова, А. А. Системы дополненной реальности для морской навигации // СИМВОЛ НАУКИ, 2018, №8, С. 1-5.
10. Иванова, Н. А., Петрова, А. В. Виртуальная и дополненная реальность в образовании // Научный журнал «Образование и наука», 2019, №4, С. 23-30.
11. Сидоров, С. В. AR и VR в туризме // Туризм и отдых, 2020, Т.1(3), С. 45-50.
12. Демидова, Е. Н. Влияние технологий VR и AR на эффективность обучения в вузах // Высшее образование в России, 2019, №6, С. 67-75.
13. Кузнецов, А. В., Максимов, И. Н. Применение AR в навигационных системах // Научные исследования и разработки, 2019, Т.1(1), С. 12-18.
14. Муленко М.Д., Лескова Д.О., Сафонова Т.В., Мокряк А.В. Расширенная реальность // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 5 (43). С. 85-91.
15. Лескова Д.О., Сафонова Т.В., Муленко М.Д., Мокряк А.В. Геймификация в образовании: влияние на мотивацию и результаты обучающихся // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 7 (45). С. 187-194.
16. Ясников А.И., Сафонова Т.В., Рускин В.Д., Логинов И.С., Мошуров В.М. Использование технологий виртуальной реальности в обучении // Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 60-69.
17. Субботина В.В., Назаренко М.Д., Сафонова Т.В., Мокряк А.В. Применение облачных технологий для цифровизации отраслей промышленности // Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 4 (48). С. 92-98.

References

1. Kicheev, V. G., Makarenko, N. N. Geoinformation space: the real world and augmented reality // Siberian State University of Geosystems and Technologies. – 2020. – URL: <https://cyberleninka.ru/article/n/geoinformatsionnoe-prostranstvo-realnyy-mir-i-dopolnennaya-realnost> (Date of access: 01.01.2025).
2. Virtual reality: understanding terminology // Habr. – 2021. – URL: <https://habr.com/ru/companies/puzzleenglish/articles/370977/> (Date of access: 01.01.2025).
3. Virtual Reality (VR) // Sber Developer. - 2022. – URL: <https://developers.sber.ru/help/ar-vr/virtual-augmented-reality> (Accessed: 01.01.2025).
4. Augmented Reality (AR) // Big dream lab. – 2023. – URL: <https://bigdreamlab.kz/blog/dopolnennaya-i-virtualnaya-realnosti> (Date of access: 02.01.2025).
5. Virtual reality technologies // IT Week. - 2022. – URL: <https://www.itweek.ru/mobile/article/detail.php?ID=224416> (Date of request: 02.01.2025).

6. Google Maps Live View // Google Support. – 2023. – URL: <https://support.google.com/maps/answer/10000000?hl=ru> (Accessed: 01/06/2025).
 7. Arcona — a project to create an augmented reality layer // Arcona. – 2023. – URL: <https://arcona.io/> (accessed: 01/06/2025).
 8. Pilgrim — AR-parks Outdoor // Pilgrim. – 2023. – URL: <https://pilgrim.app/> (Date of access: 01/06/2025).
 9. Boshkov, I. I., Krutikova, A. A. Augmented reality systems for marine navigation // SYMBOL OF SCIENCE, 2018, No. 8, pp. 1-5.
 10. Ivanova, N. A., Petrova, A.V. Virtual and augmented reality in education // Scientific journal "Education and Science", 2019, No. 4, pp. 23-30.
 11. Sidorov, S. V. AR and VR in tourism // Tourism and Recreation, 2020, Vol. I(3), pp. 45-50.
 12. Demidova, E. N. The impact of VR and AR technologies on the effectiveness of higher education // Higher Education in Russia, 2019, No. 6, pp. 67-75.
 13. Kuznetsov, A.V., Maksimov, I. N. Application of AR in navigation systems // Scientific Research and Development, 2019, Vol. I(1), pp. 12-18.
 14. Mulyenko M.D., Leskova D.O., Safonova T.V., Mokryak A.V. Augmented reality International Journal of Information Technology and Energy Efficiency. 2024. Vol. 9. No. 5 (43). pp. 85-91.
 15. Leskova D.O., Safonova T.V., Mulyenko M.D., Mokryak A.V. Gamification in education: influence on motivation and results of students International Journal of Information Technology and Energy Efficiency. 2024. Vol. 9. No. 7 (45). pp. 187-194.
 16. Yasnikov A.I., Safonova T.V., Ruskin V.D., Loginov I.S., Moshurov V.M. The use of virtual reality technologies in teaching Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 60-69.
 17. Subbotina V.V., Nazarenko M.D., Safonova T.V., Mokryak A.V. Application of cloud technologies for the digitalization of industries Information technologies and systems: management, economics, transport, law. 2023. No. 4 (48). pp. 92-98.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 004.3:37

АВТОМАТИЗАЦИЯ СРЕДЫ И СОЗДАНИЕ АДМИНИСТРАТИВНОГО ИНТЕРФЕЙСА СИСТЕМЫ ДЛЯ СБОРА ОТЗЫВОВ НА УЧЕБНЫЕ КУРСЫ: ПРОЕКТ «ОТЗЫВУС»

Чупеев А.Д.

ФГБОУ ВО "ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ", Тюмень, Россия
(625000, Тюменская область, город Тюмень, ул. Володарского, д. 38), e-mail:
cenzi217@gmail.com

В статье рассматривается модернизация информационной системы «Отзывус», направленной на сбор и анализ отзывов студентов на элективные и основные учебные курсы. Основной задачей проекта было расширение функционала системы для автоматического обновления данных о курсах и повышения удобства взаимодействия пользователей с системой. Проведена, автоматизация среды разработки с использованием Docker, а также разработан административный интерфейс для управления учебными подразделениями и курсами. В результате данных изменений удалось существенно повысить функциональность системы, улучшить её производительность и удобство использования.

Ключевые слова: Информационная система, учебные курсы, обратная связь, автоматизация.

AUTOMATING THE ENVIRONMENT AND CREATING AN ADMINISTRATIVE INTERFACE OF THE SYSTEM FOR COLLECTING FEEDBACK ON TRAINING COURSES: THE "OTZYVUS" PROJECT

Chupeev A.D.

TYUMEN INDUSTRIAL UNIVERSITY, Tyumen, Russia (625000, Tyumen Region, Tyumen,
Volodarskogo St., 38), e-mail: cenzi217@gmail.com

The article deals with the modernization of the information system "Otzavus", aimed at collecting and analyzing student feedback on elective and core courses. The main task of the project was to expand the functionality of the system to automatically update the data on courses and improve the convenience of user interaction with the system. The development environment was automated using Docker, and an administrative interface was developed for managing academic departments and courses. As a result of these changes it was possible to significantly increase the functionality of the system, improve its performance and usability.

Keywords: Information system, educational courses, feedback, automation.

Введение

Информационные системы для сбора отзывов студентов играют важную роль в совершенствовании образовательных программ и повышении качества преподавания. Проект «Отзывус» изначально был разработан для сбора отзывов на элективные курсы, но возникла необходимость расширения функциональности системы для обработки отзывов как по элективным, так и по основным курсам. Это расширение привело к модернизации архитектуры базы данных и внедрению новых возможностей для автоматизации процесса обновления данных о курсах.

Задачи проекта включали:

1. Внедрение автоматизированной среды разработки и тестирования с использованием Docker.
2. Создание административного интерфейса для управления учебными подразделениями и курсами.

Создание конфигурации автоматизированной среды разработки и тестирования

Изначально проект не включал в себя использование Docker. Чтобы развернуть проект локально, требовалось настраивать конфигурационные файлы PHP, прописывать 14 команд для установки зависимостей, настраивать .env файл, создавать базу данных и прописывать команду миграций. При осуществлении этого процесса заказчик принял решение заказать интегра

цию Docker [1,7]. Цель заключается в настройке автоматизированной среды разработки и тестирования с использованием Docker [1,7]. Главной задачей является создание среды для эффективной разработки и реализации тестов, направленных на проверку успешной загрузки страниц, стабильности сортировок и корректной работы пагинации в разделах "Элективы" и "Отзывы".

Для конфигурации Docker-среды были разработаны Docker-контейнеры, включающий в себя все необходимые зависимости, библиотеки и сервисы для успешного локального развертывания и тестирования веб-приложения. Эти контейнеры могут быть воспроизведены на любой совместимой с Docker платформе. Кроме того, были предусмотрены задокументированные инструкции по настройке и запуску Docker-контейнеров, что обеспечивает ясность воспроизведения окружения для разработчиков. Конфигурация Docker-среды включала создание основного образа с поддержкой PHP и необходимых расширений, а также для веб-приложения с настроенным веб-сервером и базой данных. Это обеспечило легкость воспроизведения окружения на различных платформах и стабильность в процессе разработки и тестирования. Дополнительно был создан контейнер в котором был механизм логирования для регистрации ошибок, предупреждений и других событий в CI/CD логах.

Реализация Dockerfile.dev:

Таблица 1 - Реализация Dockerfile.dev

Шаг	Описание
FROM php:8.2-cli-alpine AS final	Использует официальный образ PHP версии 8.2 с Alpine Linux в качестве базового образа для конечного образа.
RUN apk --no-cache add ...	Устанавливает необходимые зависимости, такие как git, zip, unzip, libpng-dev, и другие, используя apk.
RUN docker-php-ext-install ...	Устанавливает расширения PHP, такие как mbstring, exif, pcntl, bcmath, gd.
RUN curl -sS https://getcomposer.org/installer ...	Устанавливает Composer глобально.
WORKDIR /otzyvus/web/	Копирует все файлы из текущего контекста

	(локальной папки) в /otzyvus/web/ внутри контейнера.
RUN composer install --ignore-platform-reqs	Устанавливает зависимости Composer, игнорируя платформенные требования.
RUN npm install	Устанавливает зависимости Node.js с помощью npm.
RUN php artisan key:generate	Генерирует ключ приложения для Laravel.
RUN php artisan migrate	Выполняет миграции базы данных.
CMD npm run dev -- --host=0.0.0.0 --port=5173 & php artisan serve --host=0.0.0.0 --port=8000	Команда для запуска npm и веб-сервера с приложением внутри контейнера.

Реализация docker-compose.dev.yml:

Таблица 2 - Реализация docker-compose.dev.yml

Сервис	Описание
app	Контейнер с веб-приложением otzyvus-app и настроенным веб-сервером и базой данных
build	Контекст: ./web, Dockerfile: Dockerfile.dev
ports	Порты: 8000 для веб-приложения, 5173 для механизма логирования
volumes	Привязка локальной папки ./web к контейнеру
environment	Переменные окружения: APP_ENV=local, DB_CONNECTION=sqlite

Аспект тестирования включал написание тестов на PHP, охватывающих успешную загрузку страниц, обработку ошибок и предупреждений, а также проверку стабильности сортировок и пагинаций для элективов и отзывов. Тесты были интегрированы в автоматизированный режим в рамках процесса CI/CD, обеспечивая регулярное тестирование функциональности приложения.

Тестирование автоматизированной среды разработки:

Таблица 3 - Тестирование автоматизированной среды разработки

Название теста	Описание
testCallback	Тестирование обработчика обратного вызова, проверяющего создание и сохранение пользователя
testEditFeedback	Тестирование редактирования отзыва, проверяющее существование и отсутствие отзывов
testUpdateFeedback	Тестирование обновления отзыва, проверяющее существование и отсутствие отзывов
testDeleteFeedback	Тестирование удаления отзыва, проверяющее существование и отсутствие отзывов
testRestoreFeedback	Тестирование восстановления отзыва, проверяющее существование и отсутствие отзывов

Документационная работа включала в себя описание постановки задачи, используемых технологий и результатов разработки. Также предоставлено подробное руководство по конфигурации Docker-среды с описанием созданных тестов. Это позволило ясно представить контекст разработки и облегчило интеграцию компонентов в проект.

Разработка интерфейса для конфигурации подразделений университета

Администратор “Отзывус” может изменить информацию об подразделений ВУЗа только импортируя файл в котором содержится данные о подразделениях, при этом информация которая есть в БД удаляется и заменяется данными из файла, это увеличивает потенциальный риск удаления данных, что не удовлетворяет заказчика. Поэтому необходимо спроектировать и разработать пользовательский интерфейс для страницы конфигурации подразделений университета. Интерфейс должен обеспечивать функциональность поиска, добавления, редактирования и удаления подразделений. Также должна быть предоставлена функция импорта данных подразделений из файла. Выбор технологий обусловлен стеком разработки “Отзывус”: Laravel – фреймворк PHP [3,4], Blade - шаблонизатор, встроенный в Laravel [3,4] , Livewire – инструмент для создания интерактивных пользовательских интерфейсов на основе PHP [3,4].

В админ-панели администратор имеет возможность управлять подразделениями. Он может добавить новое подразделение, предоставив полное и краткое название. При необходимости пользователь может отредактировать название подразделения, нажав на кнопку "редактировать". В случае удаления подразделения пользователю будет предложено выбрать, куда перевести всех привязанных к этому подразделению пользователей, что обеспечивает более гибкое и безопасное удаление. Кроме того, оставлена возможность импорта подразделений через файл (Рисунок 1).

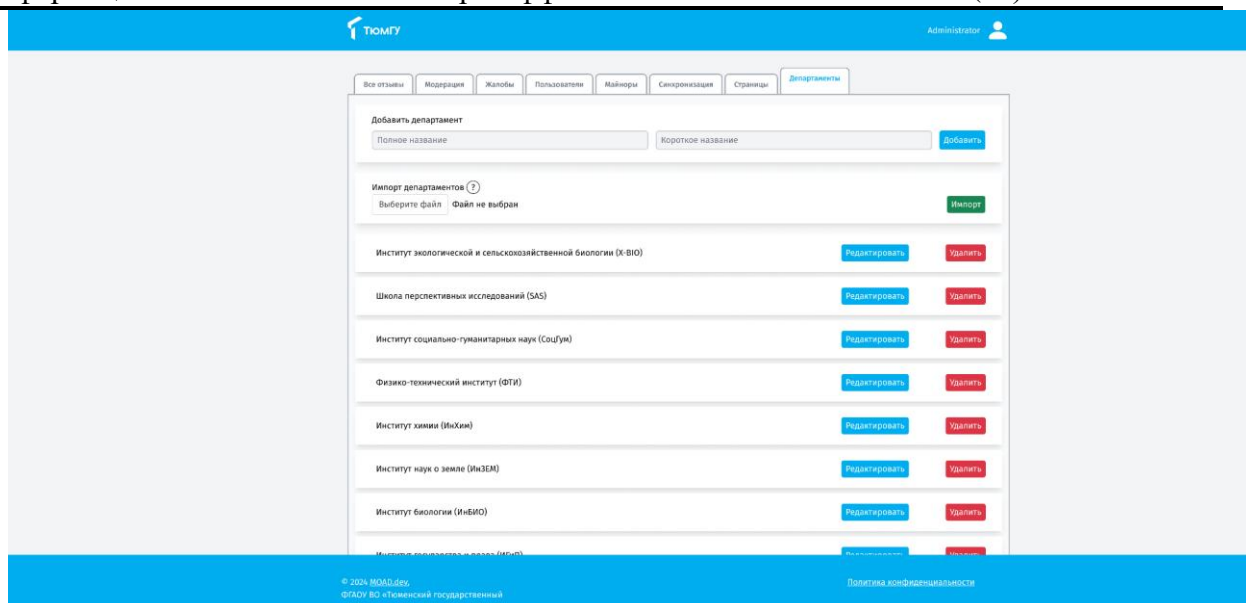


Рисунок 1 - Интерфейс

Был реализован `DepartmentController.php`. Этот компонент переносит действия пользователя “Отзывус” на БД. Он реализует методы описанные в таблице 4
Таблица 4 – Методы реализации `DepartmentController.php`.

Название метода	Описание метода
index	Метод для отображения списка подразделений. Загружает данные из базы данных и передает их в представление.
update	Обрабатывает запрос на обновление данных конкретного подразделения в базе данных.
edit	Отображает форму редактирования информации о подразделении.
delete	Удаляет выбранное подразделение из базы данных.
store	Обрабатывает запрос на создание нового подразделения и сохраняет его данные в базе.

Следующем этапом была реализация Livewire компонентов - `ShowDepartment.php` и `EditDepartment.php`. Эти компоненты реализует метод `render`, который отвечает за отображение соответствующего представления (view) Livewire, передавая данные для отображения в этих представлениях.

Далее следовало создание Blade-представлений. `departments-edit.blade.php` - представление для отображения формы редактирования информации о подразделении. `departments.blade.php` - Представление для отображения списка всех подразделений. Эти представления содержат разметку HTML, которая будет использоваться для отображения данных, а также формы для редактирования или удаления подразделений.

Последний шаг создание Livewire представлений - `show-departments.blade.php` и `edit-department.blade.php`: они используются для отображения данных и обработки действий пользователей, которые могут быть вызваны во время использования компонентов Livewire.

Каждый из этих шагов представляет часть функционала для управления подразделениями. Контроллер отвечает за маршрутизацию запросов и обработку действий пользователя. Livewire компоненты позволяют создавать динамические интерфейсы без использования JavaScript, а Blade-представления отображают данные и обеспечивают пользовательский интерфейс для управления подразделениями.

Заключение

В рамках проекта по модернизации информационной системы «Отзывус», нацеленного на сбор отзывов на различные типы учебных курсов, было выполнено следующее:

1. Создана и настроена конфигурация автоматизированной среды разработки и тестирования Docker, предназначенная для стандартизации процессов разработки и тестирования.
2. Разработан интерфейс для конфигурации подразделений университета, позволяющий управлять подразделениями университета.

Перспективы развития включают усовершенствование пользовательского интерфейса и расширение функциональности сервиса для улучшения взаимодействия пользователей с системой. Эти шаги направлены на обеспечение более эффективного управления учебным процессом и оптимизацию работы сервиса.

Список литературы

1. Буренков, И. А. Применение виртуальных контейнеров Docker для запуска сервисов: [Электронный ресурс]. CyberLeninka. URL: <https://cyberleninka.ru/article/n/primenenie-virtualnyh-konteynerov-docker-dlya-zapuska-servisov> (дата обращения: 22.11.2023).
2. PHP Manual: [Электронный ресурс]. URL: <https://www.php.net/manual/en/index.php> (дата обращения: 02.11.2023).
3. Laravel - The PHP Framework For Web Artisans: [Электронный ресурс] // Laravel : [сайт]. URL: <https://laravel.com/docs/10.x> (дата обращения: 02.11.2023).
4. Стаффер, М. Laravel. Полное руководство. Санкт-Петербург: Питер, 2020. 512 с.: ил. ISBN 978-5-4461-1396-5.
5. PhpMyAdmin: [Электронный ресурс] // PhpMyAdmin: [сайт]. URL: <https://www.phpmyadmin.net> (дата обращения: 02.11.2023).
6. Миграции в Laravel: [Электронный ресурс] // Laravel: [сайт]. URL: <https://laravel.com/docs/10.x/migrations> (дата обращения: 02.11.2023).
7. Эдриен Моуэт. Использование Docker (2017): [Электронный ресурс]. URL: <https://vtome.ru/knigi/programming/534325-ispolzovanie-docker.html> (дата обращения: 02.11.2023).

References

1. Burenkov, I.A. Application of Docker virtual containers for launching services: [Electronic resource]. CyberLeninka. URL: <https://cyberleninka.ru/article/n/primenenie-virtualnyh-konteynerov-docker-dlya-zapuska-servisov> (accessed: 22.11.2023).

2. PHP Manual: [Electronic resource]. URL: <https://www.php.net/manual/en/index.php> (accessed: 02.11.2023).
 3. Laravel - The PHP Framework For Web Artisans: [Electronic resource] // Laravel: [website]. URL: <https://laravel.com/docs/10.x> (accessed: 02.11.2023).
 4. Stauffer, M. Laravel: The Definitive Guide. St. Petersburg: Piter, 2020. 512 p.: ill. ISBN 978-5-4461-1396-5.
 5. PhpMyAdmin: [Electronic resource] // PhpMyAdmin: [website]. URL: <https://www.phpmyadmin.net> (accessed: 02.11.2023).
 6. Migrations in Laravel: [Electronic resource] // Laravel: [website]. URL: <https://laravel.com/docs/10.x/migrations> (accessed: 02.11.2023).
 7. Mouat A. Using Docker (2017): [Electronic resource]. URL: <https://vtome.ru/knigi/programming/534325-ispolzovanie-docker.html> (accessed: 02.11.2023).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.8

СОЗДАНИЕ ПРИЛОЖЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ И ПЕРЕВОДА ТЕКСТА С ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОГО ЗРЕНИЯ И ОБРАБОТКИ ЕСТЕСТВЕННОГО ЯЗЫКА

¹Титов П.С., ²Чупеев А.Д., Шеремет А.А.

ФГБОУ ВО "ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ", Тюмень, Россия (625000, Тюменская область, город Тюмень, ул. Володарского, д. 38), e-mail: ¹tpptgs@bk.ru, ²cen21217@gmail.com

В данной работе рассматривается процесс разработки приложения для распознавания и перевода текста с изображений с одного языка на другой. Основной целью работы является создание программного средства, использующее алгоритмы компьютерного зрения для точного извлечения текстовой информации из визуальных данных и применяющее технологии машинного перевода для автоматического преобразования текста на целевой язык.

Структура приложения включает несколько ключевых модулей: модуль оптического распознавания символов (OCR), система машинного перевода, а также пользовательский интерфейс для удобного доступа к функционалу приложения.

Для реализации проекта используются следующие библиотеки и фреймворки: OpenCV для задач компьютерного зрения и TensorFlow для разработки и обучения нейронных сетей, что обеспечивает высокую точность и производительность системы.

Ключевые слова: Оптическое распознавание символов, компьютерное зрение, машинное обучение, перевод текста, обработка изображений.

CREATING AN APPLICATION FOR RECOGNIZING AND TRANSLATING TEXT FROM IMAGES USING COMPUTER VISION AND NATURAL LANGUAGE PROCESSING

¹Titov P.S., ²Chupeev A.D., Sheremet A.A.

TYUMEN INDUSTRIAL UNIVERSITY, Tyumen, Russia (625000, Tyumen Region, Tyumen, Volodarskogo St., 38), e-mail: ¹tpptgs@bk.ru, ²cen21217@gmail.com

This paper examines the process of developing an application for recognizing and translating text from images from one language to another. The main goal of the work is to create a software tool that uses computer vision algorithms to accurately extract text information from visual data and uses machine translation technologies to automatically convert text into the target language.

The application structure includes several key modules: an optical character recognition (OCR) module, a machine translation system, and a user interface for easy access to the application's functionality.

The following libraries and frameworks are used to implement the project: OpenCV for computer vision tasks and TensorFlow for the development and training of neural networks, which ensures high accuracy and system performance.

Keywords: Optical character recognition, computer vision, machine learning, text translation, image processing.

Введение

Современные технологии компьютерного зрения и обработки естественного языка (NLP) значительно расширили возможности автоматического распознавания и перевода текста. Однако, несмотря на значительные достижения в этих областях, интеграция оптического распознавания символов (OCR) и машинного перевода для создания универсальных приложений, способных работать с изображениями и видео в реальном времени, остается сложной задачей. Основная цель данного проекта заключается в разработке приложения, способного распознавать текст с изображений и переводить его с одного языка на другой. Выделенные задачи проекта:

1. Изучить и проанализировать текущие достижения в области компьютерного зрения и NLP, связанные с распознаванием и переводом текста.
2. Разработать модуль оптического распознавания символов (OCR), способный извлекать текст из изображений и видео с высокой точностью.
3. Интегрировать систему машинного перевода, обеспечивающую точный и контекстно-зависимый перевод текста на целевой язык.
4. Провести тестирование и оценку эффективности приложения в различных сценариях использования.

В процессе работы мы использовали такие технологии: Tesseract (для OCR) [1, 6], EasyOCR [2], Google Translate [3], так как они показали высокую эффективность в своих областях. А также модели BERT [4] и GPT [5].

Теоретическая часть

Для распознавания символов на изображении используется алгоритм сегментации текста на уровне слов. Изображение разбивается на части, соответствующие отдельным словам, после чего внутри каждого слова осуществляется дальнейшая сегментация на буквы. Каждая выделенная буква передается на классификацию в качестве отдельного изображения, результаты которой сохраняются в массив символов. По завершении, массив символов преобразуется в строку, которая затем передается на этап перевода.

Для сегментации слов на изображении был применен метод *morphologyEx* из библиотеки OpenCV с использованием ядра свертки размером 8x8 пикселей, что обеспечило эффективное выделение текста на уровне слов. Функция *findContours* из библиотеки OpenCV была использована для обнаружения границ каждого слова, что позволило сформировать массив изображений, содержащих отдельные слова. При помощи встроенной функции *sorted* из Python контуры были отсортированы сначала по вертикали (сверху вниз), что позволило разбить текст на строки, затем по горизонтали (слева направо), что сохранило порядок слов в строке.

Для изображений отдельных слов вновь применялись морфологические преобразования, которые описаны в предыдущем абзаце, но с меньшим ядром свертки размером 8x1 пикселей. Это позволило объединить точки над буквами *i* и *j* с основными частями букв, сохраняя при этом разделение между символами.

Пример алгоритма приведен на Рисунке 1

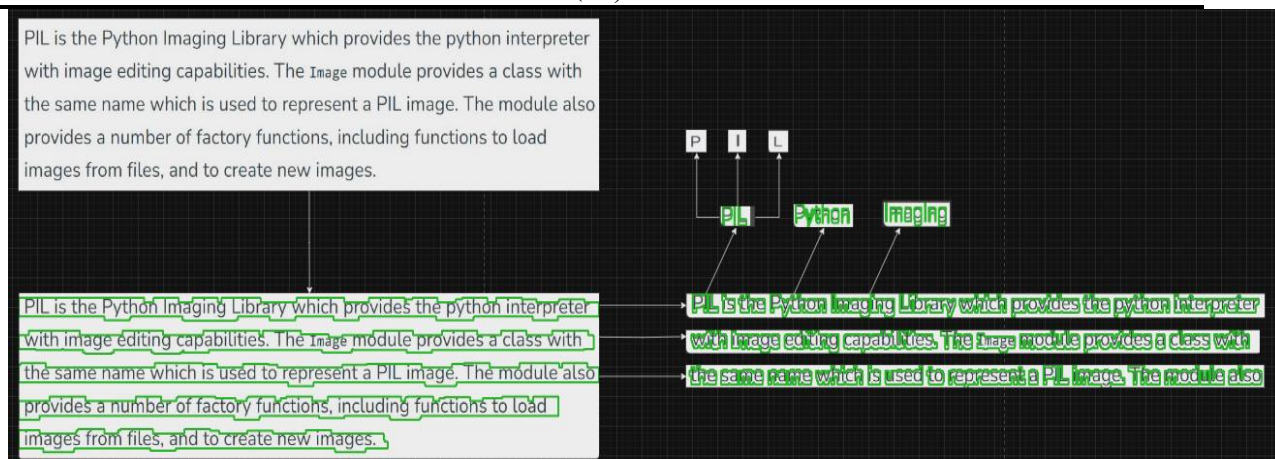


Рисунок 1 - Пошаговое преобразование

Практическая часть

Для решения задачи «распознавания букв на изображении», нужно было подготовить данные. Был собран набор данных, включающий изображения текста в различных стилях и шрифтах. Далее буквы различных шрифтов и стилей были выделены в изображения 28x28 пикселей. Далее для расширения выборки и улучшения качества обучения модели была проведена аугментация данных, а именно повороты, сдвиги, изменения яркости изображений. Также для повышения точности обучения модели на каждом изображении были размечены точные границ букв. Следующим этапы было предобработка изображений алгоритмом, описанным в теоретической частей, выделение, сегментация слов и букв на изображении для дальнейшей обработки. Методы предобработки изображений были реализованы с использованием библиотеки OpenCV.

Для решения задачи распознавания букв на изображении, была разработана и обучена модель сверточной нейронной сети (CNN) на основе архитектуры Xception, которая состояла из 4 сверточных слоев и 2 полносвязных слоев. В качестве функции активации использовалась ReLu, а также функция регуляризации для предотвращения переобучения. Обучение с оптимизационным алгоритмом Adam проходило на ранее размеченном наборе данных. Для оценки точности использовался валидационный набор данных, который не участвовал в процессе обучения. Точность на валидационной выборке 70% и 95% на обучающей. Для обучения и создания модели применялся фреймворк TensorFlow.

После успешного завершения обучения модель была использована для распознавания текста на изображении. Модель предсказывала буквы, которые сохранялись в массив символов. Массив преобразовывался в строку и передавался на этап перевода. Постобработка результатов с использованием Google Translate и ChatGPT позволила автоматически исправлять и корректировать распознанные символы, что значительно повысило качество итогового текста.

Результаты

Результаты работы программы представляются в виде 3 изображений: исходное изображение с текстом (Рисунок 2), распознанный текст и перевод уже распознанного текста.

Physics is the fundamental science that explores the laws governing the behavior of matter and energy in the universe. It seeks to understand the fundamental forces and particles that constitute the fabric of reality, from the subatomic to the cosmological scale. The discipline is traditionally divided into several branches, each focusing on specific aspects of nature.

Рисунок 2 - Исходный текст

Распознанный нашей моделью текст: Physics is the fundamental science that explores the laws governing the behavior of matter and energy in the universe. It seeks to understand the fundamental forces and particles that constitute the fabric of reality, from the subatomic to the cosmological scale. The discipline is traditionally divided into several branches, each focusing on specific aspects of nature.

Распознанный Tesseract текст: Physics is the fundamental science that explores the laws governing the behavior of matter and energy in the universe. It seeks to understand the fundamental forces and particles that constitute the fabric of reality, from the subatomic to the cosmological scale. The discipline is traditionally divided into several branches, each focusing on specific aspects of nature.

Текст, распознанный нашей моделью и переведенный ChatGPT: Физика — это основная наука, исследующая законы, управляющие материей и энергией во Вселенной. Её цель понять фундаментальные силы и частицы, из которых состоит ткань реальности, охватывая масштабы от субатомного уровня до космологических явлений. Эта дисциплина традиционно делится на несколько областей, каждая из которых сосредоточена на изучении определённых аспектов природы.

Текст, распознанный Tesseract и переведенный GoogleTranslate: Физика - является фундаментальной наукой, изучающей законы, которые определяют поведение материи и энергии во Вселенной. Её задача состоит в исследовании фундаментальных сил и частиц, формирующих структуру реальности, начиная от субатомного уровня и заканчивая космологическими масштабами. Традиционно физика делится на несколько направлений, каждое из которых посвящено изучению конкретных аспектов природы.

Заключение

В результате работы разработано приложение, распознающее текст с изображений и переводящее его в реальном времени. Приложение показало удовлетворительные результаты, но выявило области для улучшений.

1. Расширение датасета: увеличение тренировочного набора данных повысит устойчивость модели к различным шрифтам, улучшая точность распознавания.

2. Фильтрация некорректных символов: для устранения ошибок распознавания символов, отсутствующих в обучающем датасете, возможно создание алгоритмов фильтрации и применение методов обработки естественного языка. Это улучшит качество перевода и итоговые результаты.

Дополнительно можно внедрить интерактивную систему для ручной коррекции ошибок пользователем, что повысит точность работы и улучшит процесс.

Список литературы

1. Смит Р. Обзор движка Tesseract OCR // Труды Девятой международной конференции по анализу и распознаванию документов. – IEEE, 2007. – С. 629–633.
2. Джайдед Дж. EasyOCR: Простое оптическое распознавание текста с использованием OpenCV и глубокого обучения [Электронный ресурс]. – Репозиторий GitHub, 2020. – URL: <https://github.com/JaidedAI/EasyOCR> (дата обращения: 30.03.2024).
3. Ву Й., Шустер М., Чен З., Ле К.В., Норуози М., Махере В. Нейронная система машинного перевода от Google: преодоление разрыва между человеком и машинным переводом // arXiv preprint arXiv:1609.08144, 2016. – 23 с.
4. Девлин Дж., Чанг М.-В., Ли К., Тоутаван К. BERT: Предобучение глубоких двунаправленных трансформеров для понимания языка // Труды Конференции 2019 года Североамериканского отделения Ассоциации по вычислительной лингвистике: Технологии обработки естественного языка. – 2019. – С. 4171–4186.
5. Браун Т., Манн Б., Райдер Н., Суббия М., Каплан Дж., Дхаривал П. Языковые модели как обучающиеся с ограниченным количеством примеров // arXiv preprint arXiv:2005.14165, 2020. – 61 с.
6. Tesseract OCR. Tesseract documentation [Электронный ресурс]. – Режим доступа: <https://tesseract-ocr.github.io/tessdoc/> (дата обращения: 05.04.2024).

References

1. Smith R. An overview of the Tesseract OCR engine // Proceedings of the Ninth International Conference on Document Analysis and Recognition. – IEEE, 2007. – pp. 629–633. Smith R.
 2. Jaided J. EasyOCR: Easy-to-use Optical Character Recognition with OpenCV and deep learning [Electronic resource]. – GitHub Repository, 2020. – URL: <https://github.com/JaidedAI/EasyOCR> (accessed: 30.03.2024).
 3. Wu Y., Schuster M., Chen Z., Le Q.V., Norouzi M., Macherey W. Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation // arXiv preprint arXiv:1609.08144, 2016. – p.23/
 4. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. – 2019. – pp. 4171–4186.
 5. Brown T., Mann B., Ryder N., Subbiah M., Kaplan J., Dhariwal P. Language Models are Few-Shot Learners // arXiv preprint arXiv:2005.14165, 2020. – p.61.
 6. Tesseract OCR. Tesseract documentation [Electronic resource]. – URL: <https://tesseract-ocr.github.io/tessdoc/> (accessed: 05.04.2024).
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

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



УДК 004.056.5

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ В АЛГОРИТМАХ ЭНЕРГОСБЕРЕЖЕНИЯ ПРОЦЕССОРОВ ДЛЯ АТАК

Бютнер С.И.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (19232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: serafimkavasaki@gmail.com

С развитием процессоров и переходом к многоядерным системам, алгоритмы энергосбережения становятся важной частью их архитектуры. Эти алгоритмы направлены на оптимизацию потребления энергии в зависимости от нагрузки, однако в последние годы было выявлено несколько уязвимостей, которые могут быть использованы для атак. Статья рассматривает, как злоумышленники могут эксплуатировать недостатки в алгоритмах энергосбережения процессоров, приводящие к утечке информации, производительным атакам и сбоям системы. Также рассматриваются методы защиты, включая усовершенствования алгоритмов и аппаратные решения.

Ключевые слова: Уязвимости, алгоритмы энергосбережения, процессоры, атаки, многоядерные системы, утечка информации, защита.

EXPLOITING VULNERABILITIES IN PROCESSOR POWER-SAVING ALGORITHMS FOR ATTACKS

Buetner S.I.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (19232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com

As processors evolve and move to multi-core systems, power management algorithms become an essential part of their architecture. These algorithms aim to optimize energy consumption based on load, but in recent years, several vulnerabilities have been discovered that can be exploited for attacks. This article discusses how attackers can exploit weaknesses in processor power management algorithms leading to information leakage, performance attacks, and system crashes. It also explores protection methods, including algorithm improvements and hardware-based solutions.

Keywords: Vulnerabilities, power management algorithms, processors, attacks, multi-core systems, information leakage, protection.

Введение

В последние десятилетия процессоры стали гораздо более мощными и энергоэффективными благодаря многочисленным достижениям в области микроархитектуры. Одним из ключевых факторов повышения энергоэффективности является использование алгоритмов энергосбережения, которые регулируют работу процессора в зависимости от его нагрузки. Эти алгоритмы позволяют процессорам автоматически снижать потребление энергии при низкой нагрузке и увеличивать производительность при повышении требуемых вычислительных мощностей. Тем не менее, несмотря на очевидные преимущества таких

решений, исследования показали, что алгоритмы энергосбережения могут стать уязвимыми к различным типам атак. Эксплуатация этих уязвимостей может привести к утечке конфиденциальной информации, сбоям в системе или даже к целенаправленным атакам, направленным на разрушение работы процессора и его компонентов.

В отличие от других уязвимостей, таких как те, что связаны с ошибками в операционных системах или программном обеспечении, уязвимости в алгоритмах энергосбережения более трудно обнаружимы, так как они часто скрыты внутри низкоуровневых функций управления энергопотреблением. Такие уязвимости могут быть использованы злоумышленниками для проведения атак, которые могут быть неочевидными и продолжаться в течение длительного времени без заметных последствий для пользователя. Важно понимать, что алгоритмы энергосбережения не только оптимизируют расход энергии, но и в некоторых случаях управляют состоянием кэш-памяти, производительностью процессора и временем отклика, что дает атакующим возможность манипулировать этими параметрами для получения несанкционированного доступа к данным или для снижения производительности системы.

Эксплуатация уязвимостей в алгоритмах энергосбережения процессоров для атак

Среди основных типов атак, направленных на алгоритмы энергосбережения процессоров, можно выделить несколько ключевых. Одной из них является атака на канал побочных воздействий, при которой злоумышленники используют изменения в энергопотреблении процессора для получения информации о выполняемых вычислениях. Например, при использовании алгоритмов энергосбережения процессор может снижать свою тактовую частоту или отключать некоторые ядра, что изменяет потребляемую мощность. Эти изменения могут быть зафиксированы с помощью специальных датчиков или анализом времени отклика системы, что позволяет злоумышленникам собирать информацию о процессе вычислений. Таким образом, даже при отсутствии прямого доступа к данным процессора, хакеры могут извлечь конфиденциальную информацию[1].

Другим типом атаки являются так называемые атаки на производительность, когда алгоритмы энергосбережения используются для уменьшения мощности процессора или временного отключения некоторых его ядер в моменты, когда система должна работать на полную мощность. Злоумышленники могут инициировать такие атаки с целью замедлить работу целевой системы или нарушить её нормальную работу. Например, если вредоносное ПО может принудить процессор работать на низких частотах, это приведет к заметному снижению производительности, что особенно опасно в критических вычислительных задачах[2].

Также стоит отметить проблему утечек информации через "состояния энергосбережения". При переключении процессора в режим энергосбережения могут возникать несанкционированные изменения в его конфигурации, такие как состояния кеша или регистров, которые могут использоваться для восстановления частичной информации о данных, с которыми работал процессор до перехода в этот режим. В некоторых случаях это может привести к утечке криптографических ключей или паролей[3].

Кроме того, более сложные уязвимости могут проявляться при эксплуатации слабых мест в аппаратных решениях, таких как методы мониторинга или системы для детектирования и защиты от атак. Недавние исследования показали, что процессоры, поддерживающие определённые алгоритмы энергосбережения, могут иметь уязвимости, которые позволяют

нарушить их работу, в том числе при работе с многозадачностью, когда несколько программ одновременно используют различные режимы энергосбережения[4].

Защита от таких атак требует применения нескольких подходов. Во-первых, необходимо улучшение алгоритмов энергосбережения, чтобы минимизировать вероятность утечек данных через побочные каналы. Это включает в себя использование более сложных методов шифрования и проверок целостности данных в процессорах, чтобы сделать процессоры менее уязвимыми к такого рода атакам. Во-вторых, важно обновлять прошивки процессоров и использовать аппаратные решения для защиты, такие как специальные датчики и системы мониторинга, которые могут обнаружить попытки манипулировать режимами энергосбережения и предсказать возможные атаки. Также можно ограничить использование некоторых режимов энергосбережения в критических приложениях, где производительность важнее, чем экономия энергии, что поможет снизить риски[5].

Кроме того, операционные системы и приложения должны быть настроены так, чтобы они учитывали потенциал атак, использующих алгоритмы энергосбережения, и принимали дополнительные меры для защиты от них. Например, системы могут быть настроены для работы только в определённом диапазоне энергопотребления, чтобы избежать неожиданных изменений в режиме работы процессора. Также можно использовать сегментацию приложений и вычислительных ресурсов для того, чтобы гарантировать, что приложения с повышенными требованиями к безопасности не используют общие ядра или режимы энергосбережения, которые могут быть уязвимы к атакам.

Заключение

Уязвимости в алгоритмах энергосбережения процессоров становятся всё более важной темой в контексте безопасности современных вычислительных систем. Хотя алгоритмы энергосбережения играют ключевую роль в снижении потребления энергии и повышении эффективности работы процессоров, их уязвимости могут быть использованы для проведения атак, которые серьёзно угрожают безопасности данных и стабильности системы. Эксплуатация таких уязвимостей возможна через каналы побочных воздействий, манипулирование производительностью процессора и утечки информации. Для защиты от таких атак необходим комплексный подход, включающий как улучшение самих алгоритмов энергосбережения, так и использование аппаратных и программных средств защиты, которые могут минимизировать риски.

Список литературы

1. Гельфанд А. М. Способы выбора стежоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262
2. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.

4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348
5. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

References

1. Gelfand A.M. Ways of choosing stegocontainers for data transmission //Regional informatics and information security. - 2020. – pp. 260-262
 2. Kushnir D. V. Research and development of methods for distributing confidential data over quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
 3. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
 4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelec communications in science and education (APINO 2023). – 2023. – pp. 345-348
 5. Petrova T. V. and others. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 621.45.015.4

ОПРЕДЕЛЕНИЕ ЗНАЧЕНИЯ ТЯГИ И УДЕЛЬНОГО ИМПУЛЬСА КАМЕРЫ РАКЕТНОГО ДВИГАТЕЛЯ СРЕДСТВАМИ ПРОГРАММНОГО ПАКЕТА ANSYS

¹Савиных А.А., Марк М.А., Погорелов М.А., Юрьев В.А.

ФГБОУ ВО "БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
"ВОЕНМЕХ" ИМ. Д.Ф. УСТИНОВА", Санкт-Петербург, Россия (190005, город Санкт-
Петербург, 1-я Красноармейская ул., д.1), e-mail: ¹alex.savinyh02@mail.ru

Статья посвящается исследованию результирующих параметров течения камеры ракетного двигателя. Цель работы – выполнение комплекса работ по расчету и моделированию камеры ракетного двигателя. В процессе работы проводилось моделирование камеры ракетного двигателя, расчет течения продуктов сгорания с помощью программного пакета Ansys, сопоставление полученных результатов с параметрами аналитического расчета согласно проектировочным пособиям. В результате проделанной работы произведен расчет течения продуктов сгорания в камере ракетного двигателя, а также произведено аналитическое сравнение параметров расчета Ansys и аналитического расчета.

Ключевые слова: Камера ракетного двигателя, течение продуктов сгорания, тяга, удельный импульс, Ansys, температура, давление, массовый расход, азотный тетраоксид, несимметричный демитилгидразин, Workbench, Fluent.

DETERMINING THE VALUE OF THRUST AND SPECIFIC IMPULSE OF A ROCKET ENGINE CHAMBER USING THE ANSYS SOFTWARE PACKAGE

¹ Savinykh A.A., Mark M.A., Pogorelov M.A., Yuryev V.A.

"BALTIC STATE TECHNICAL UNIVERSITY "VOENMEH" D.F. USTINOVA", St. Petersburg,
Russia (190005, Saint-Petersburg, 1st Krasnoarmeyskaya str., 1), e-mail: ¹alex.savinyh02@mail.ru

The article is devoted to the study of the resulting parameters of the rocket engine chamber flow. The purpose of the work is to perform a set of works on the calculation and modeling of the rocket engine chamber. In the process of work, the rocket engine chamber was modeled, the combustion products flow was calculated using the Ansys software package, and the obtained results were compared with the parameters of the analytical calculation according to design manuals. As a result of the work done, the combustion products flow in the rocket engine chamber was calculated, and an analytical comparison of the Ansys calculation parameters and the analytical calculation was made.

Keywords: Rocket engine chamber, combustion flow, thrust, specific impulse, Ansys, temperature, pressure, mass flow, nitrogen tetroxide, unsymmetrical dimethylhydrazine, Workbench, Fluent.

Определение исходных параметров расчета

Исходными данными для проектирования являются следующие параметры:

- топливо – АТ+НДМГ (азотный тетраоксид + несимметричный диметилгидразин) с характеристиками согласно работе [3];
- тяга в пустоте 140 кН;
- давление на срезе сопла 0,007 МПа.

Таким образом, сведем все известные параметр в Таблицу 1.

Таблица 1 - Исходные параметры проектирования

Тяга в пустоте, кН	140
Давление на срезе сопла, МПа	0,007
Плотность АТ, кг/м ³	1441
Плотность НДМГ, кг/м ³	787

Дальнейший расчет проведен согласно методическим пособиям [4, 5] и программе Termogas. Результаты представлены в таблице 2 и на рисунке 1.

Таблица 2 - Результирующие параметры проектирования

Давление в камере сгорания (КС), МПа	8
Рабочее соотношение компонентов	2,078
Массовый расход в КС, кг/с	43
Температура в КС, К	3270
Газовая постоянная продуктов сгорания (ПС), Дж/(кг×К)	382
Показатель процесса	1,182
Удельный импульс КС, м/с	3188

```

: 1:Alfa: .67850: .67850: .67850: .67850: .67850: .67850:
: 2:K1 : 2.07756: 2.07756: 2.07756: 2.07756: 2.07756: 2.07756:
: 3:Pps : 7.00000: 3.97558: .00700: 8.00000: 4.53742: .00700:
: 4:Tps : 3267.16545: 3027.12404: 897.36191: 3275.89274: 3032.08054: 869.83883:
: 5:Ips : 91.10866: -587.32947: -4948.36990: 91.05287: -589.87992: -4993.48009:
: 6:Sps : 11.52128: 11.52125: 11.52127: 11.47021: 11.47024: 11.47021:
: 7:Mu : 21.74163: 21.89837: 22.13321: 21.75835: 21.91026: 22.13322:
: 8:Cp.r: 3.22911: 2.98910: 1.64418: 3.37566: 2.91415: 1.63378:
: 9:Cp.g: 3.22911: 2.98910: 1.92034: 3.37566: 2.91415: 1.92341:
:10:Cp.f: 2.08328: 2.06381: 1.64418: 2.08399: 2.06424: 1.63378:
:11:????: 382.41887: 379.68172: 375.65311: 382.12500: 379.47557: 375.65290:
:12:n : 1.18324: 1.18666: 1.29613: 1.18218: 1.18943: 1.29858:
:13:z : .00000: .00000: .00000: .00000: .00000: .00000:
:14:a : 1210.04877: 1164.56544: 661.00085: 1210.97099: 1166.75779: 651.39934:
:15:Nu : .00010: .00009: .00004: .00010: .00009: .00004:
:16:Al.g: .34075: .32002: .10599: .34137: .32037: .10273:
:17:Al.r: .52817: .46350: .12379: .55295: .45227: .12095:
:18:Pr : .59619: .59861: .57766: .59655: .59887: .57687:
:19:k.z: .00000: 1.17313: 1.23404: .00000: 1.17461: 1.23571:
:20:M : .00000: 1.00021: 4.80278: .00000: 1.00017: 4.89531:
:21:Is : .00000: 1164.81494: 3174.64090: .00000: 1166.95452: 3188.80043:
:22:Ip : .00000: 2151.53275: 3280.82513: .00000: 2152.94023: 3291.27078:
:23:Beta: .00000: 1737.36383: .00000: .00000: 1738.40927: .00000:
:24:F.ud: .00000: 2.48195: 151.69176: .00000: 2.17301: 146.38621:
:25:F.*: .00000: 1.00000: 61.11801: .00000: 1.00000: 67.36559:

```

Рисунок 1 – Параметры продуктов сгорания в программе Termogas

Расчет газодинамического профиля камеры ракетного двигателя (КРД) производится согласно пособию [7] и имеет следующий вид (Рисунок 2).

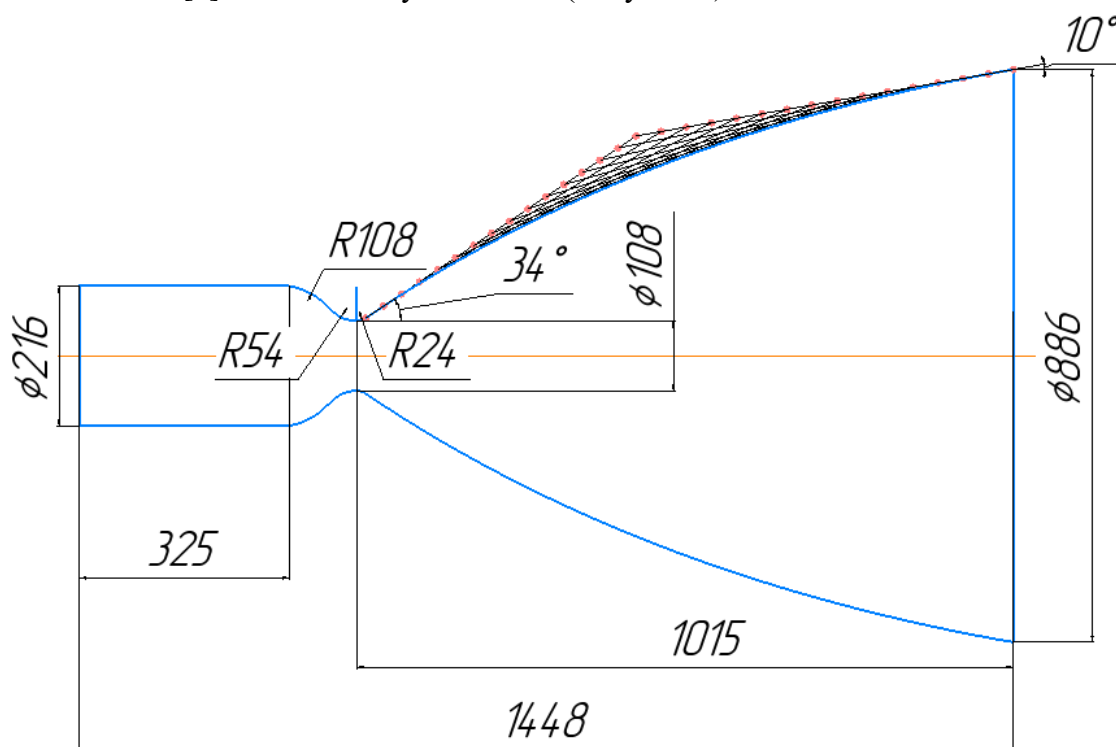


Рисунок 2 – Газодинамический профиль КРД

Эти параметры КРД являются исходными для моделирования процессов в программном пакете Ansys.

Моделирование расчетной области и расчет течения в программе Ansys

Для начала построим модель камеры и расчетной области в 2D, используя программу Компас, согласно исходным данным. Расчет будет выполняться посредством осесимметричного 2D тела, а не воспроизведением полноразмерной 3D модели, так как это экономит вычислительные затраты. Полученный результат представлен на рисунках 3-4. Файл сохраняем в формате x.t.

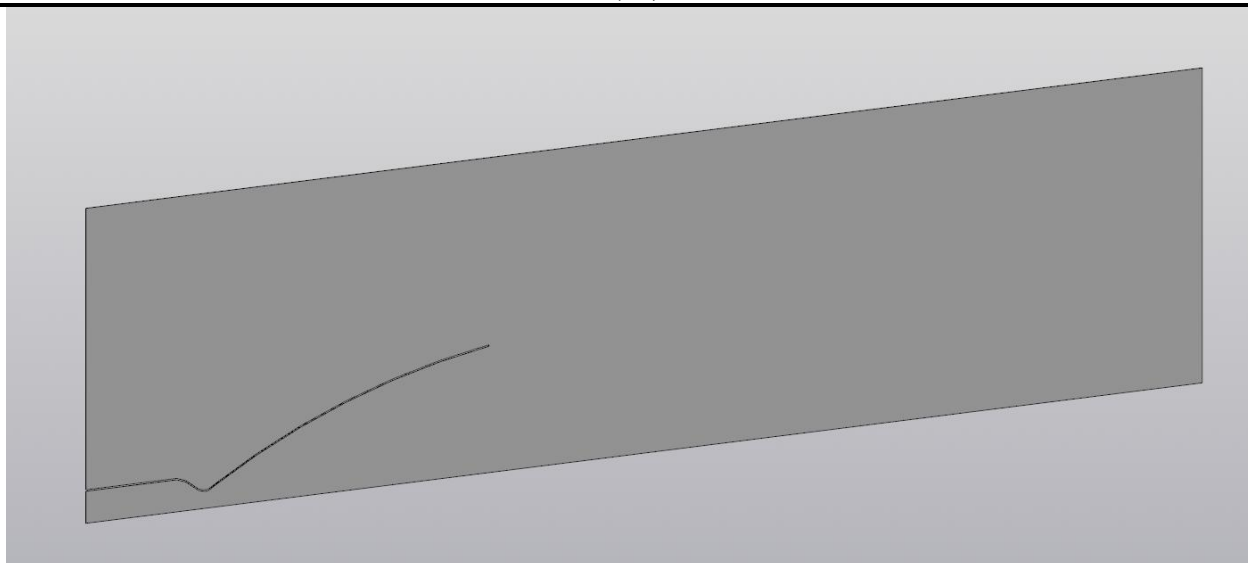


Рисунок 3 – Модель расчетной области в Компас

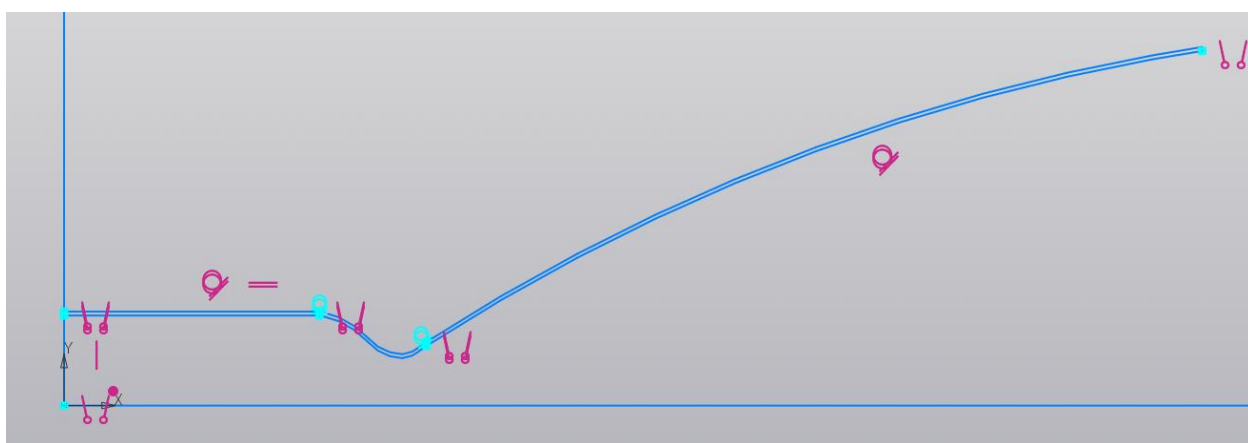


Рисунок 4 – Эскиз газодинамического профиля КРД

Затем переходим в программу Ansys, где итоговое окно Workbench выглядит следующим образом (рисунок 5). Расчет проведен согласно методическим пособиям [1, 2, 6, 8].

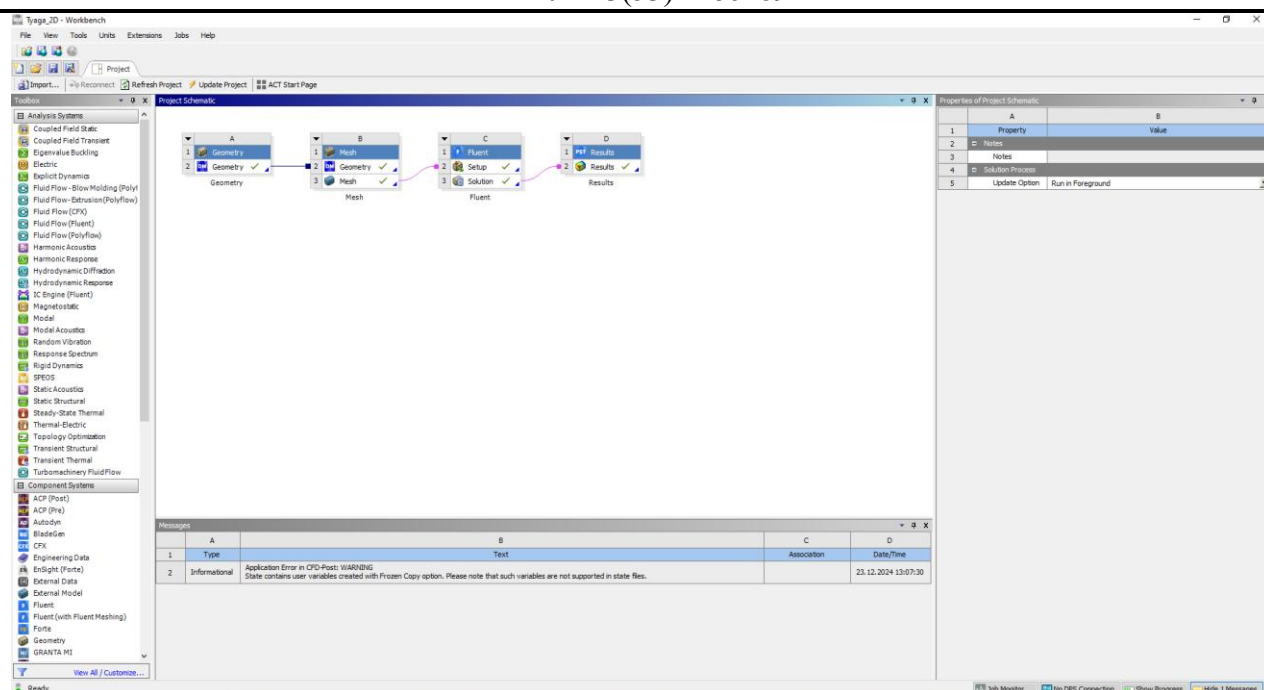


Рисунок 5 – Рабочее окно Workbench (итоговый)

В программном пакете Ansys нам необходимо:

1. задать геометрию;
2. построить сетку;
3. провести расчет течения;
4. сравнить полученные результаты с аналитическими.

Открываем модуль Geometry с помощью DesignModeler и выполняем следующий порядок операций:

1. импортировать построенную геометрию;
2. переопределить толщину пластины до 0 м с помощью функции Thin;
3. определить с помощью функции Named Selection входную границу (inlet), выходную (outlet), стенку (wall) и ось вращения (axis);
4. задать дополнительные построения в Sketching и разделить поверхность на подповерхности с помощью Face split для дальнейшего формирования сетки с областями разноразмерных ячеек;
5. переопределить расчетную область с твердого тела (solid) на жидкое (fluid).

Результаты операций представлены на Рисунках 6-9.

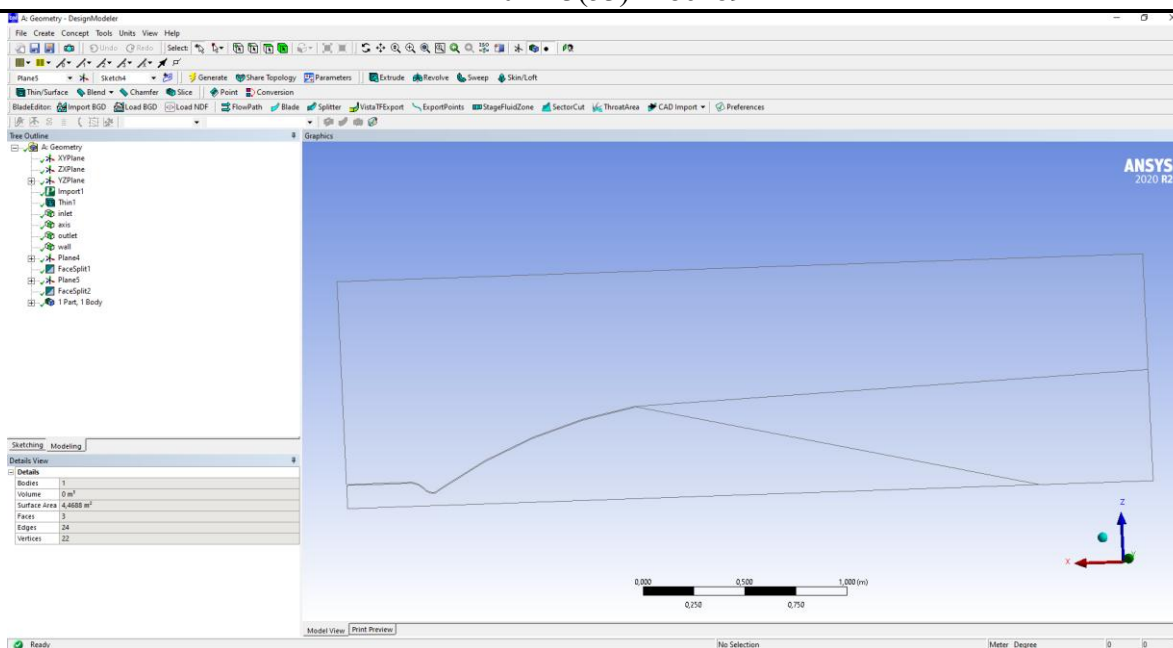


Рисунок 6 – Модель расчетной области в Geometry

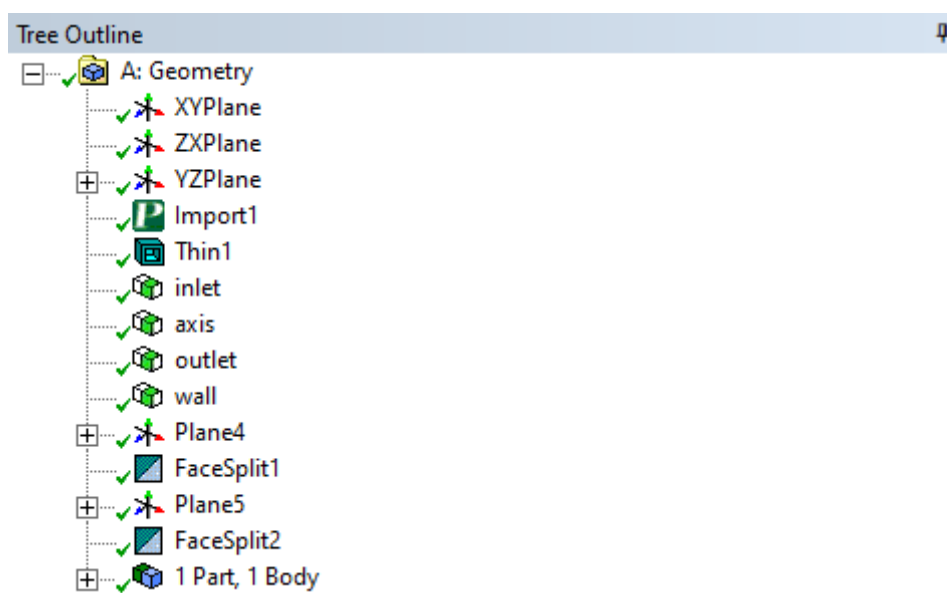


Рисунок 7 – Дерево модели в Geometry

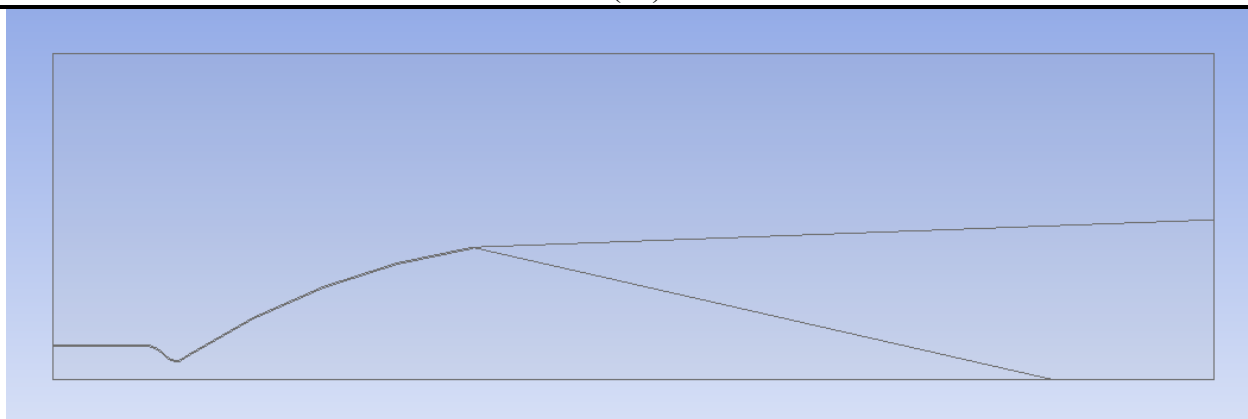


Рисунок 8 – Расчетная область после дополнительных построений

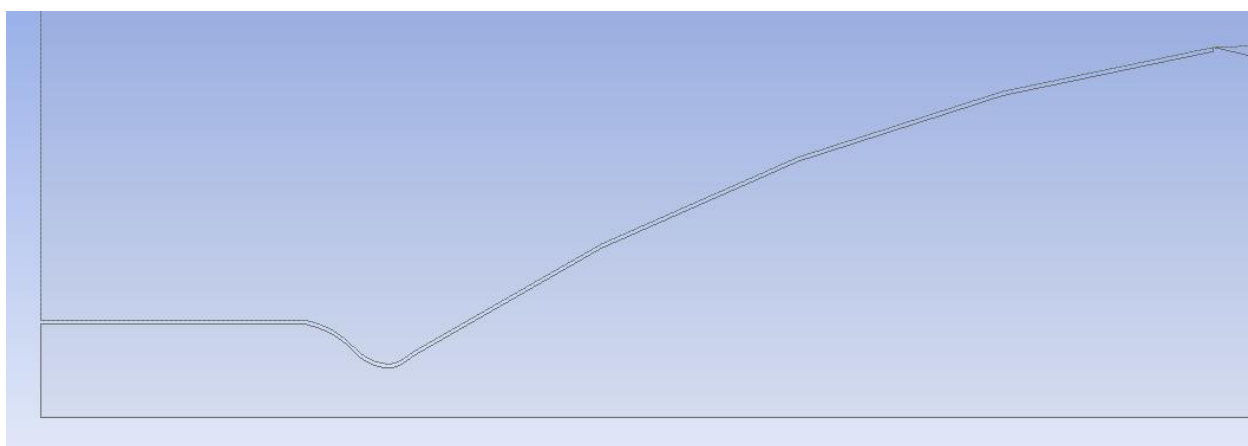


Рисунок 9 – Увеличенный вид стенки (wall) расчетной области

Завершив операции в модуле Geometry, переходим в окне Workbench в сеточный построитель Mesh. Здесь нам необходимо:

1. через операцию Face Sizing выставить элементарный размер ячеек для трех полученных с помощью дополнительных построений в модуле Geometry областей;
2. задать сгущение сетки в зоне пограничного слоя КС операцией Inflation;
3. проверить Named Selection на соответствие заданным ранее входной границы (inlet), выходной (outlet), оси (axis) и стенки (wall).

Результаты перечисленных выше операций представлены на рисунках 10-18.

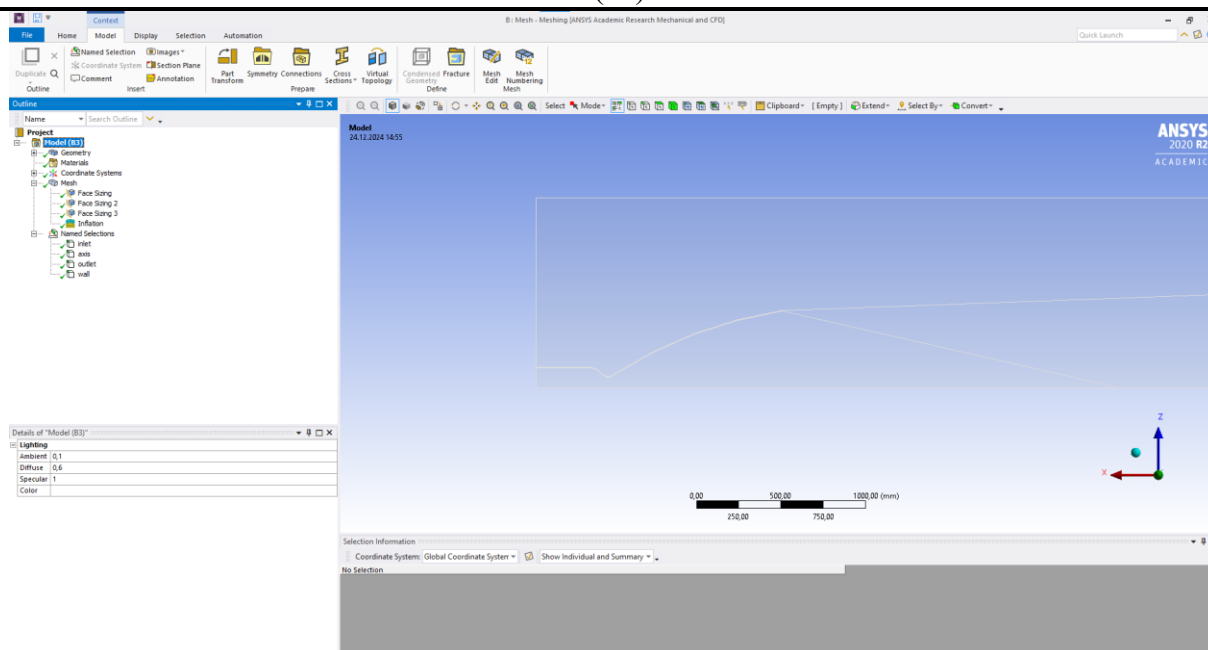


Рисунок 10 – Рабочее окно Mesh

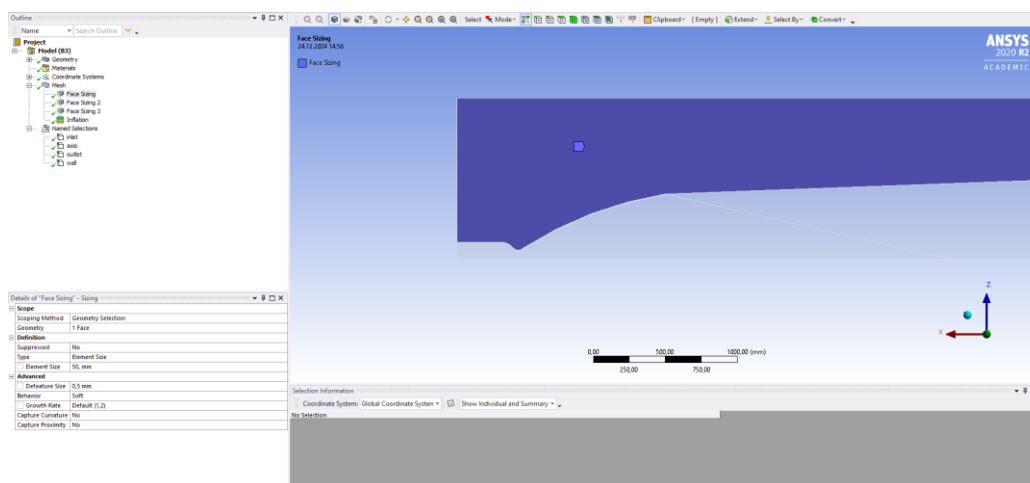


Рисунок 11 – Настройка первой области в Face Sizing

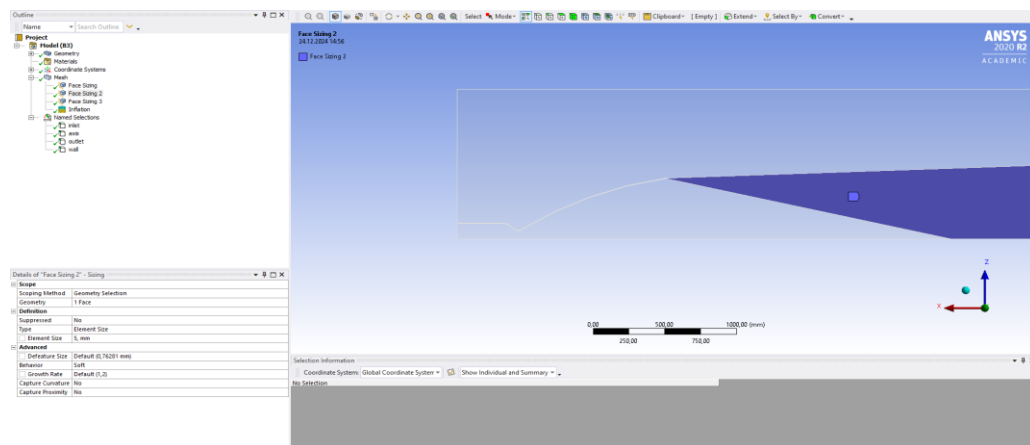


Рисунок 12 – Настройка второй области в Face Sizing

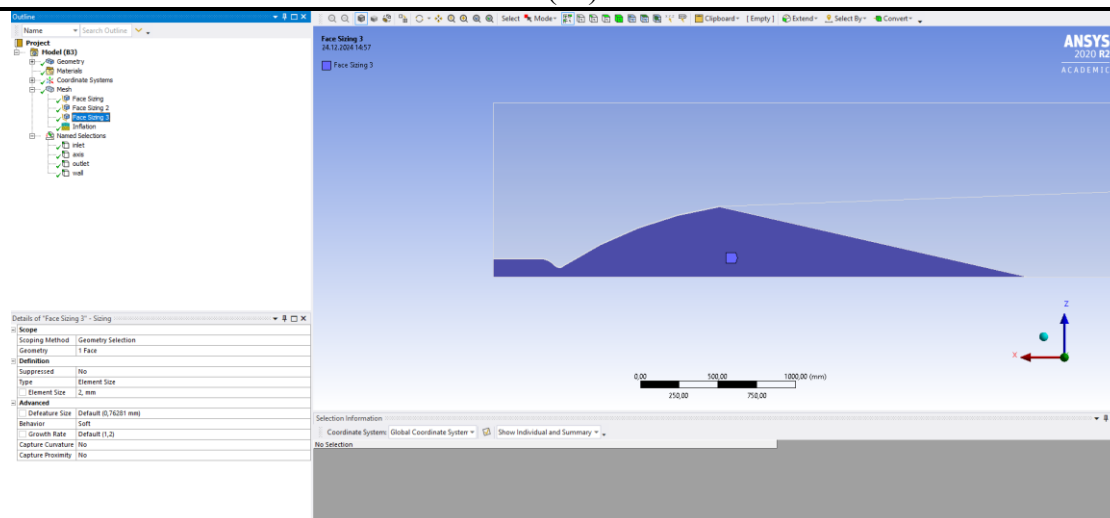


Рисунок 13 – Настройка третьей области в Face Sizing

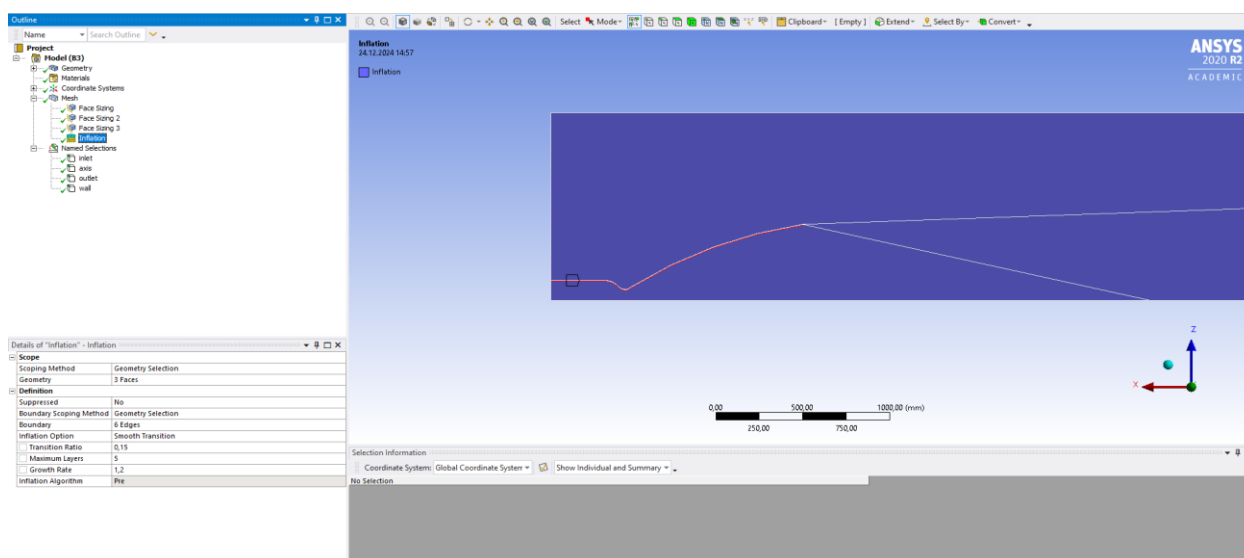


Рисунок 14 – Задание сгущения возле стенки (wall) через Inflation

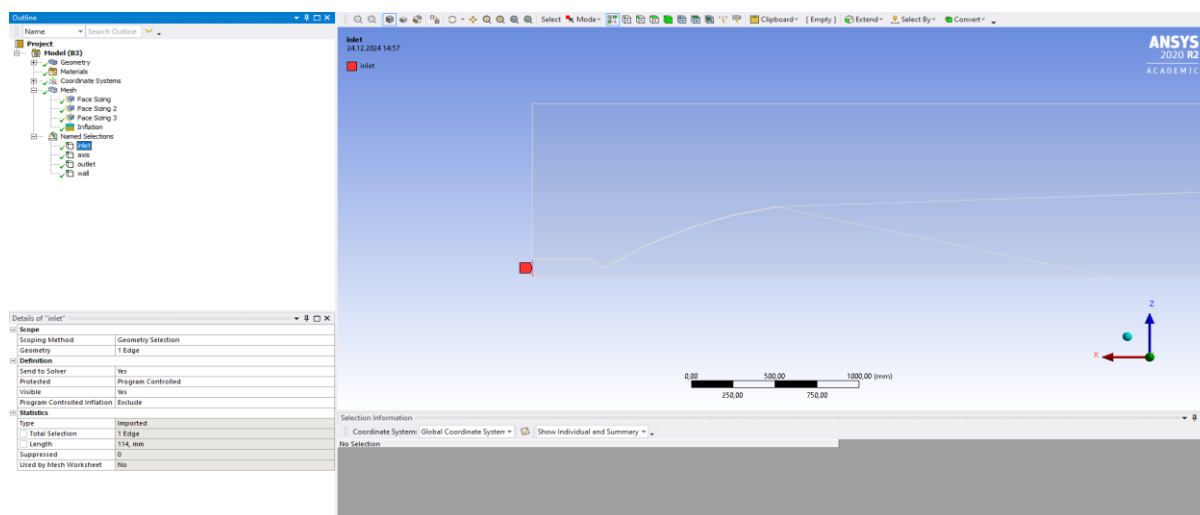


Рисунок 15 – Проверка правильности задания Inlet

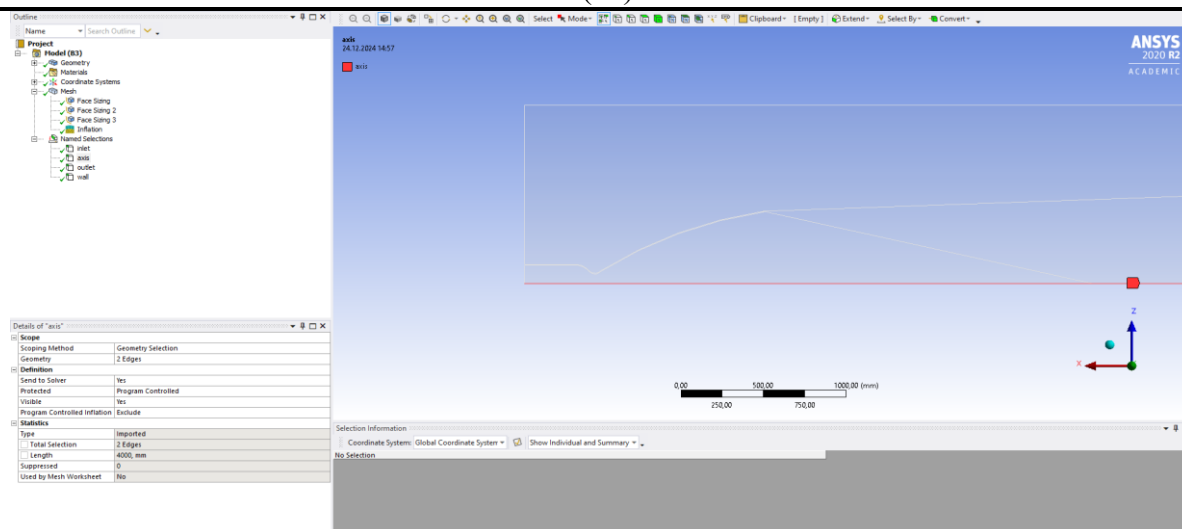


Рисунок 16 – Проверка правильности задания Axis

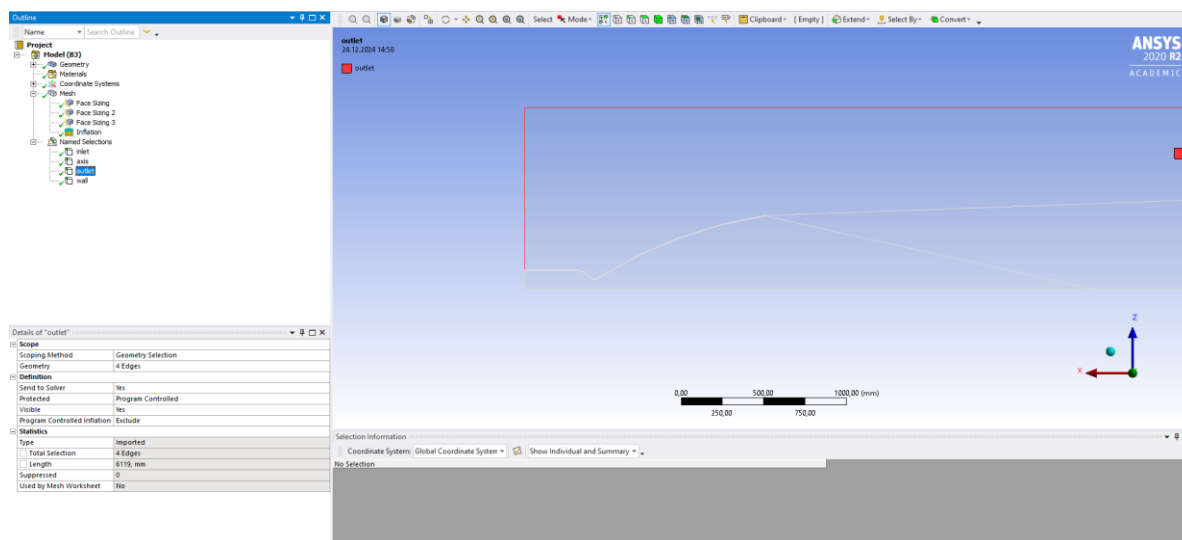


Рисунок 17 – Проверка правильности задания Outlet

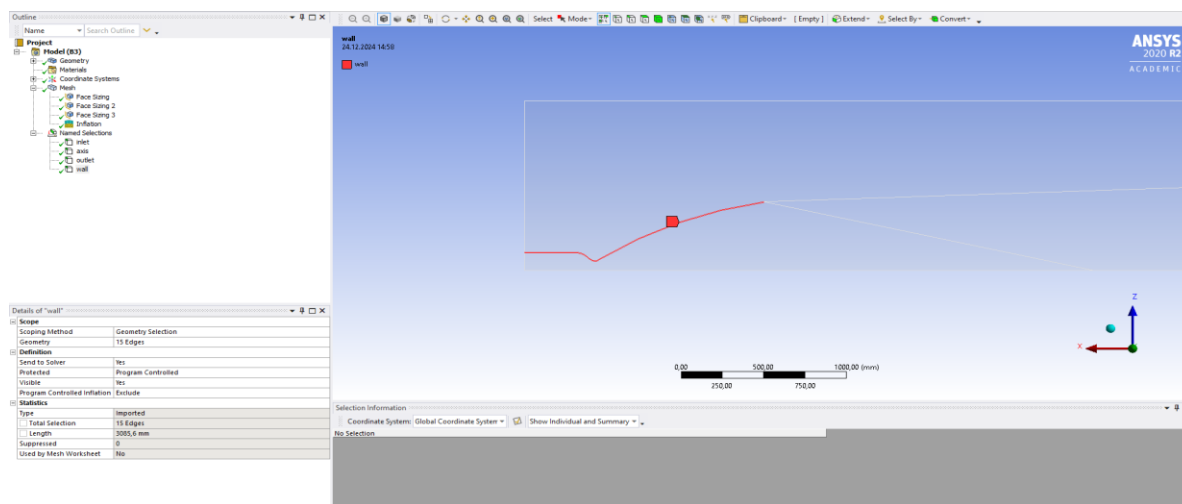


Рисунок 18 – Проверка правильности задания Wall

В результате запуска сеточного построителя программа выдала следующий результат – рисунки 19-21.

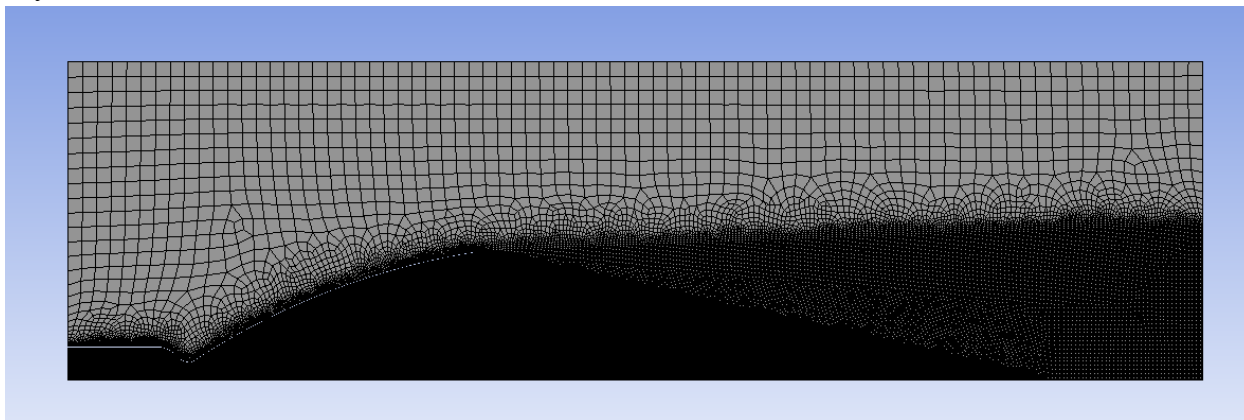


Рисунок 19 – Сетка расчетной области

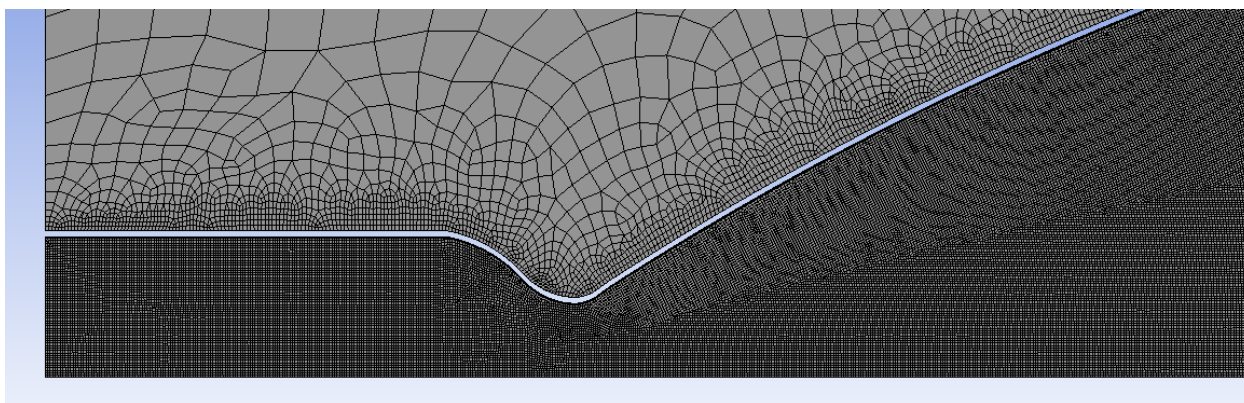


Рисунок 20 – Увеличенный вид сетки в зоне КС

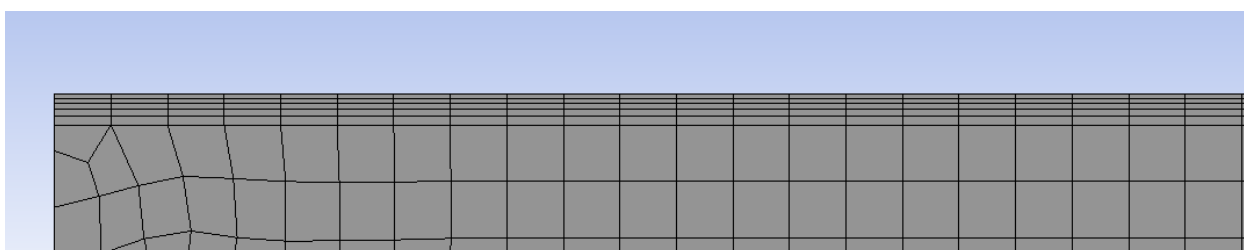


Рисунок 21 – Результат сгущения сетки возле стенки КС

После завершения построения сетки переносим результаты и переходим в модуль Fluent. В модуле Fluent выполняем следующие шаги:

1. выставляем осесимметричное тело (axisymmetric);
2. включаем модель Energy и модель турбулентности SST k-omega;
3. задаем параметры газа, на основе ПС (рисунок 1);
4. в Cell Zone Conditions выставляем параметр окружающего давления 0 Па, так как двигатель второй ступени (значение давления на срезе сопла согласно исходным данным 0,007 МПа);

5. в Boundary Conditions выставляем параметры Pressure-Inlet и Pressure-Outlet;
6. задаем методику расчета;
7. проводим инициализацию;
8. запускаем решатель с определенным количеством итераций.

Перечисленные шаги представлены на рисунках 22-32. Исходные данные для газа и для граничных условий принимались из результирующих параметров программы Termogas для ПС (Рисунок 1) и расчета согласно пособию (Таблица 2).

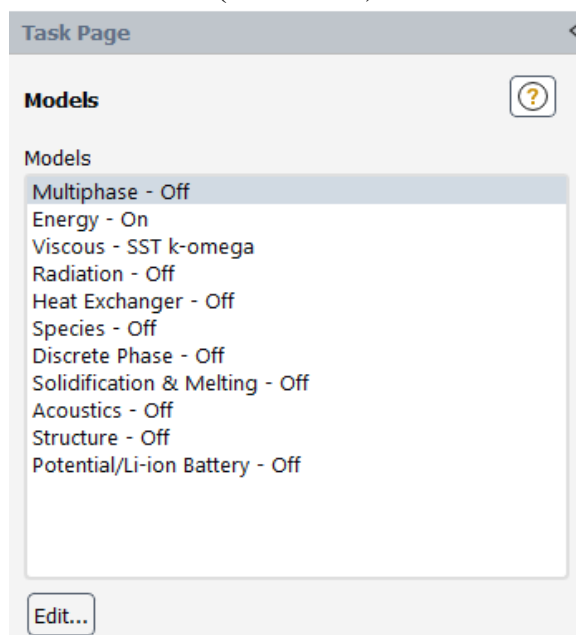


Рисунок 22 – Настройки расчетной модели

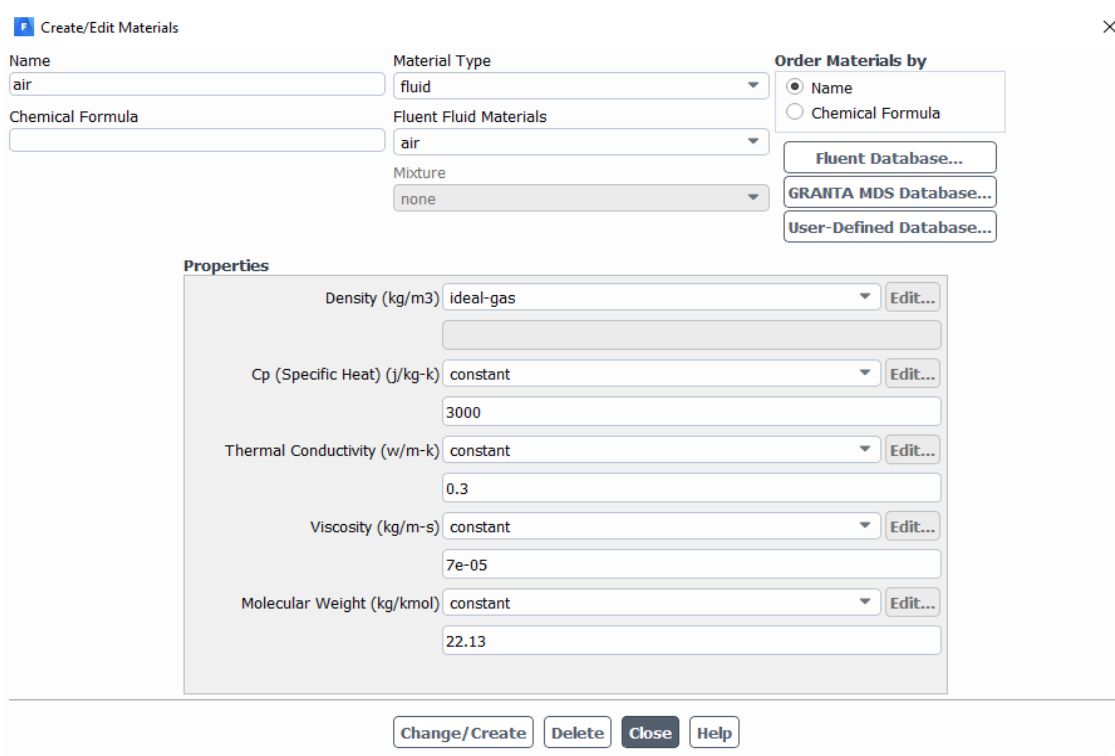


Рисунок 23 – Задание параметров газа на основе ПС

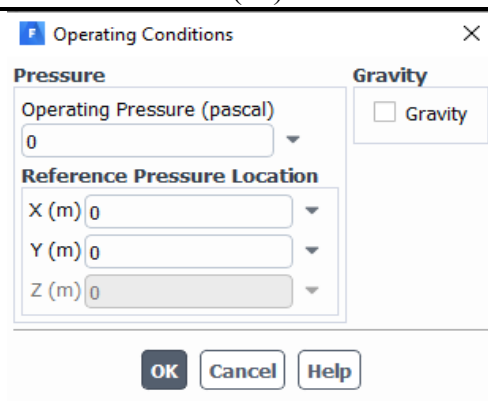


Рисунок 24 – Настройка условий эксплуатации

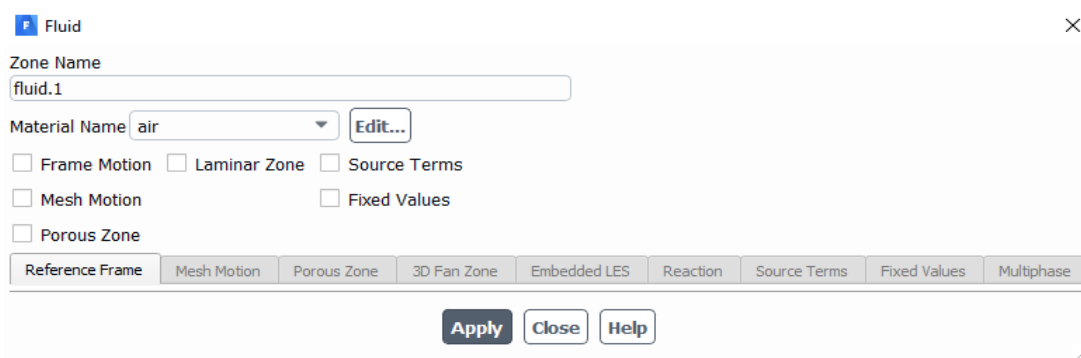


Рисунок 25 – Применение заданного материала для расчетной области

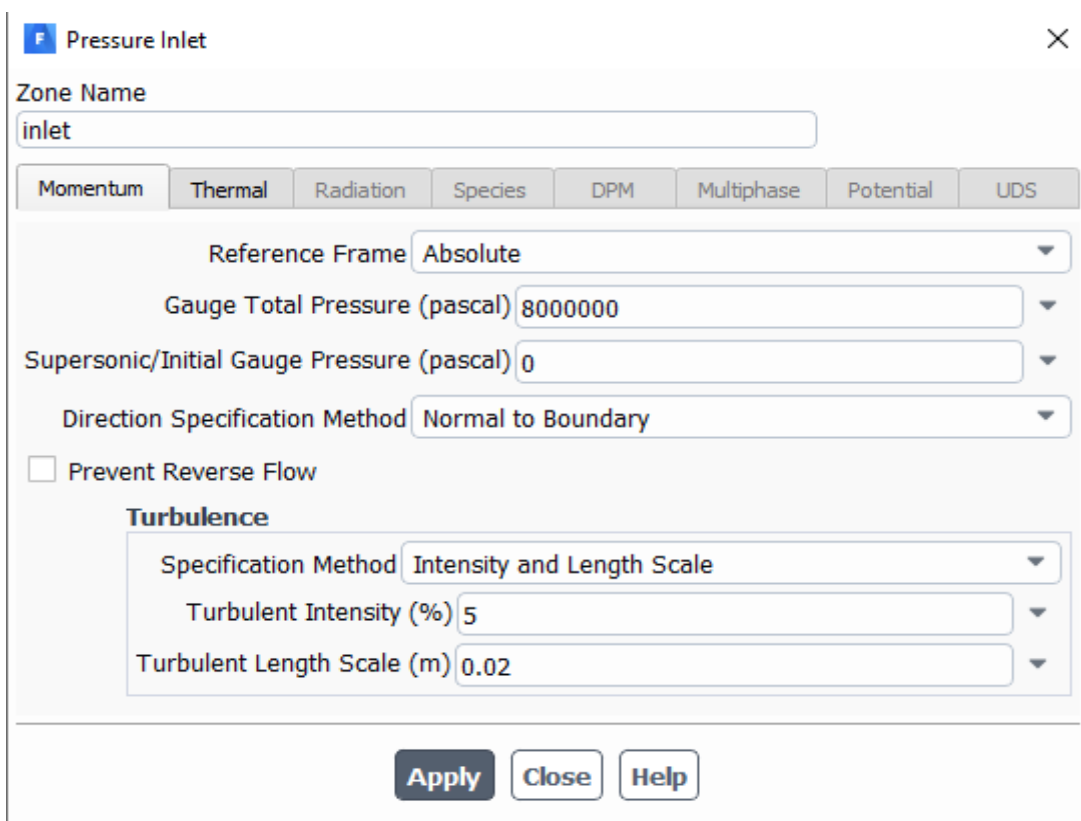


Рисунок 26 – Задание входных условий (давления)

Pressure Inlet

Zone Name
inlet

Momentum Thermal Radiation Species DPM Multiphase Potential UDS

Total Temperature (k) 3270

Apply Close Help

Рисунок 27 – Задание входных условий (температуры)

Pressure Outlet

Zone Name
outlet

Momentum Thermal Radiation Species DPM Multiphase Potential UDS

Backflow Reference Frame Absolute

Gauge Pressure (pascal) 7000

Pressure Profile Multiplier 1

Backflow Direction Specification Method Normal to Boundary

Backflow Pressure Specification Total Pressure

☐ Prevent Reverse Flow

☐ Average Pressure Specification

☐ Target Mass Flow Rate

Turbulence

Specification Method Intensity and Length Scale

Backflow Turbulent Intensity (%) 5

Backflow Turbulent Length Scale (m) 1

Apply Close Help

Рисунок 28 – Задание выходных условий (давления)

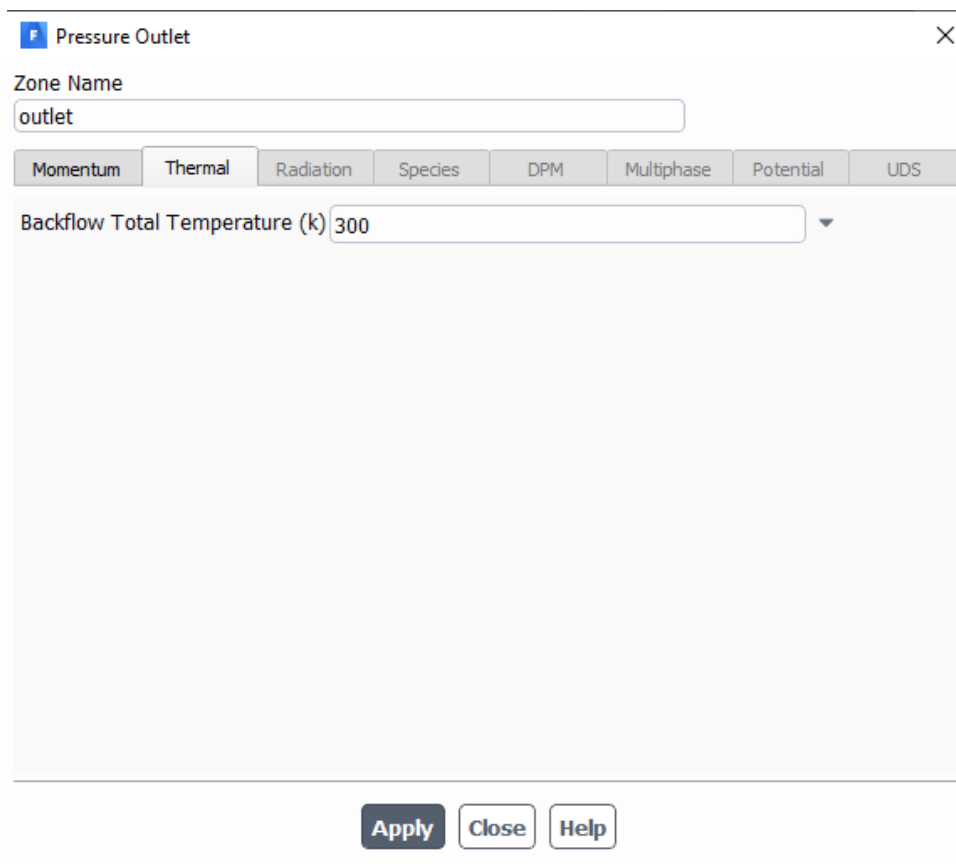


Рисунок 29 – Задание выходных условий (температуры)

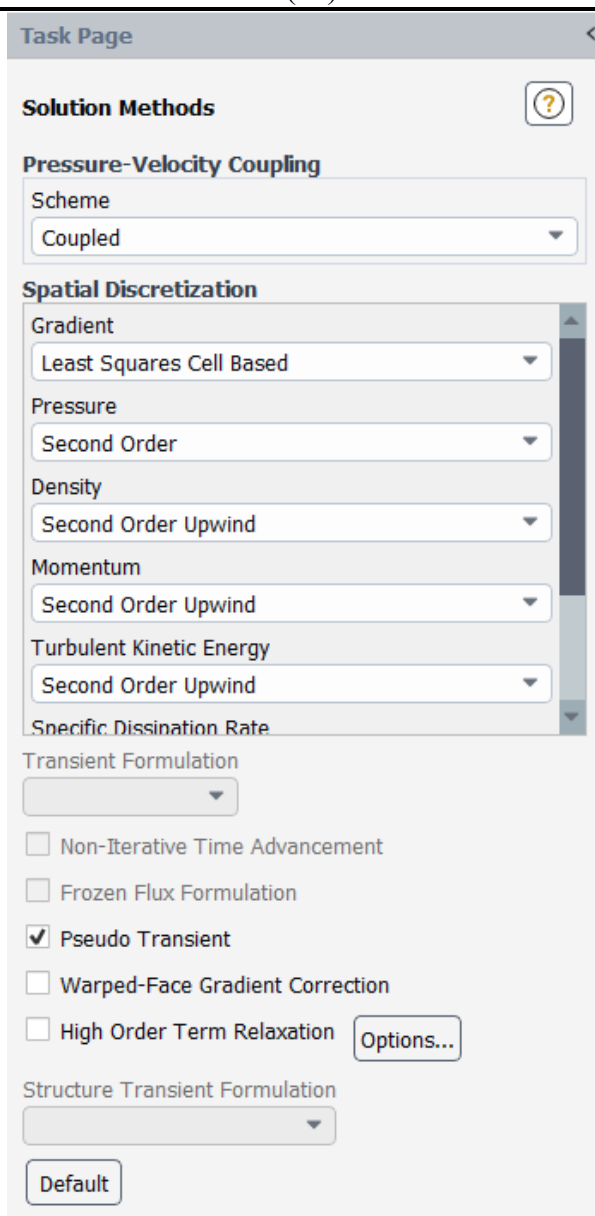


Рисунок 30 – Настройка метода решения задачи

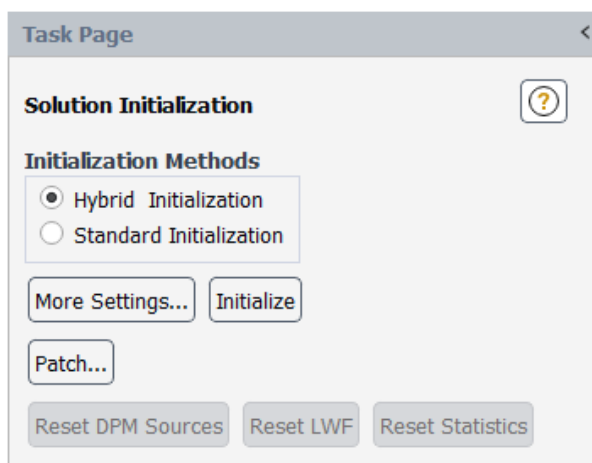


Рисунок 31 – Проведение гибридной инициализации

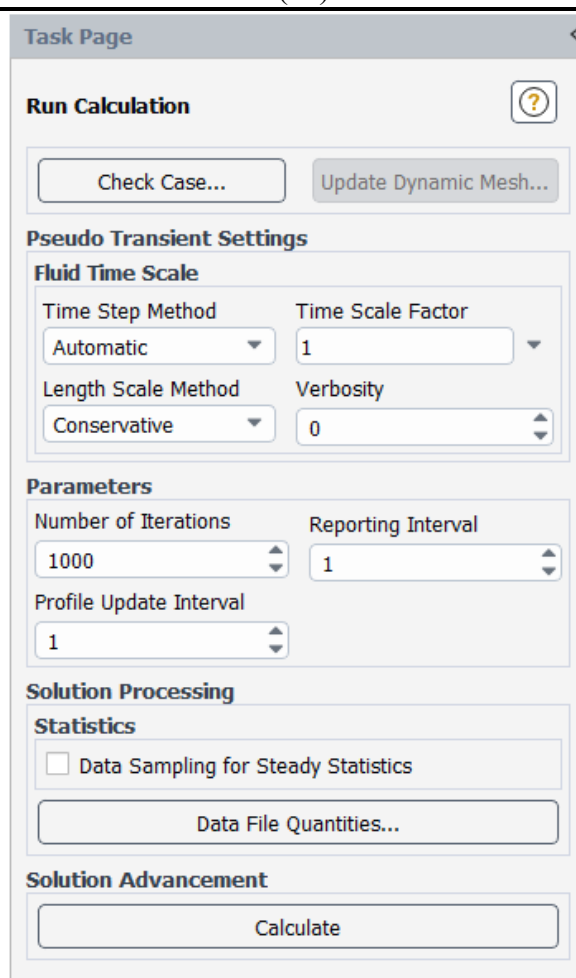


Рисунок 32 – Запуск решателя с 1000 итераций

Таким образом, после завершения расчета, мы получили картины течения для различных параметров и их численные значения. Картины течения представлены на рисунках 33-36.

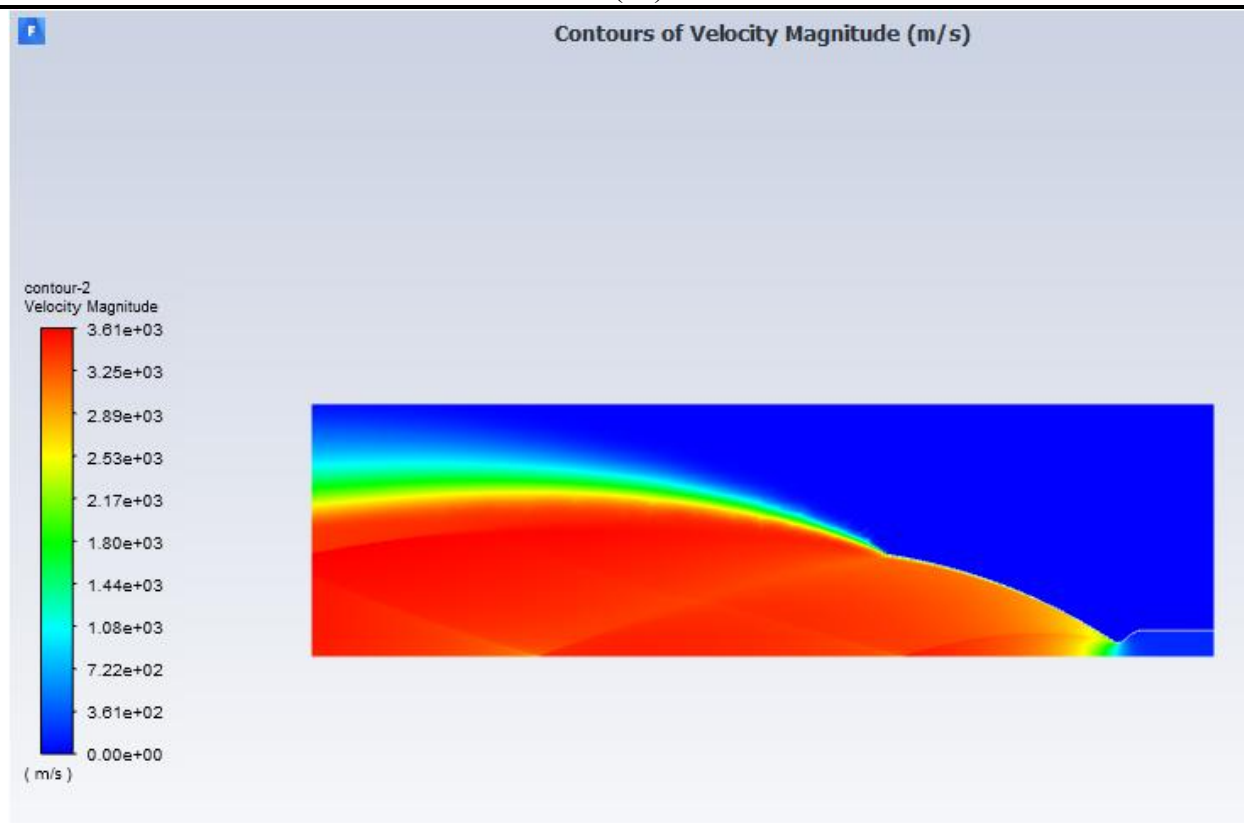


Рисунок 33 – Эпюра параметра скорости

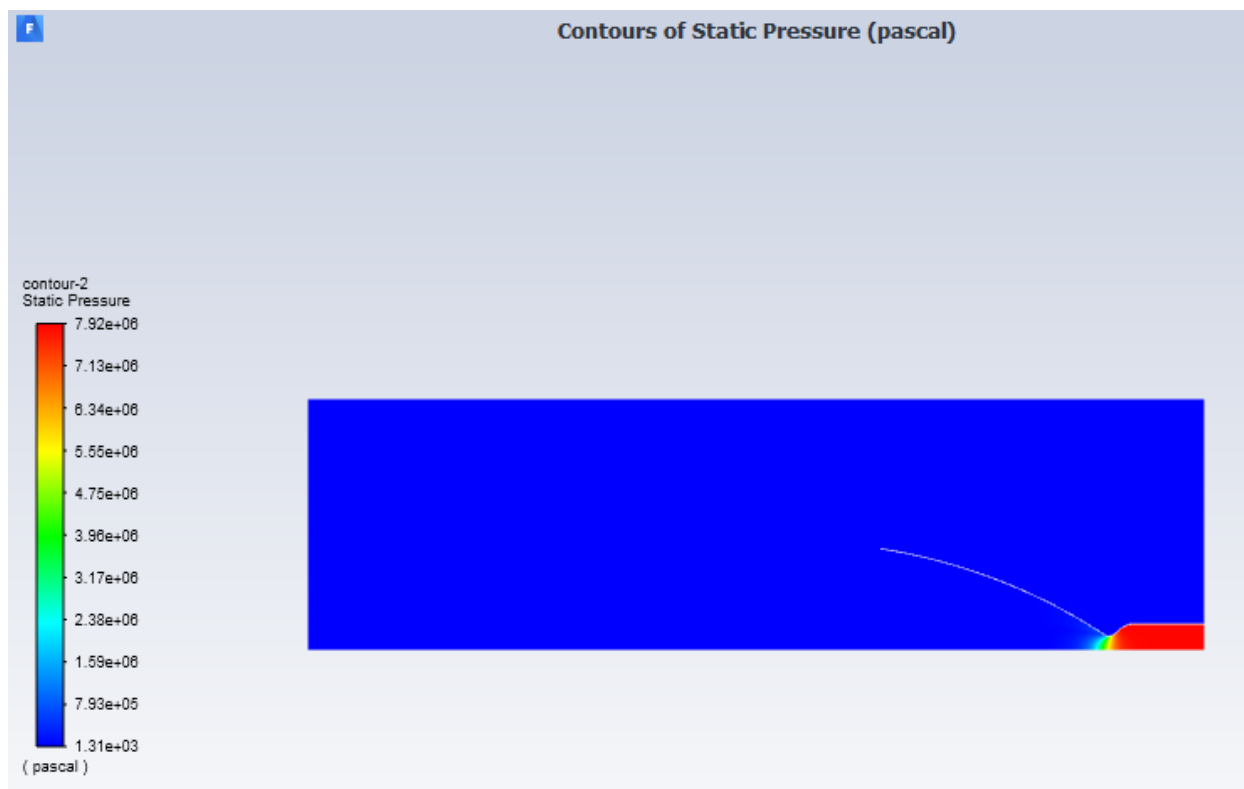


Рисунок 34 – Эпюра параметра давления

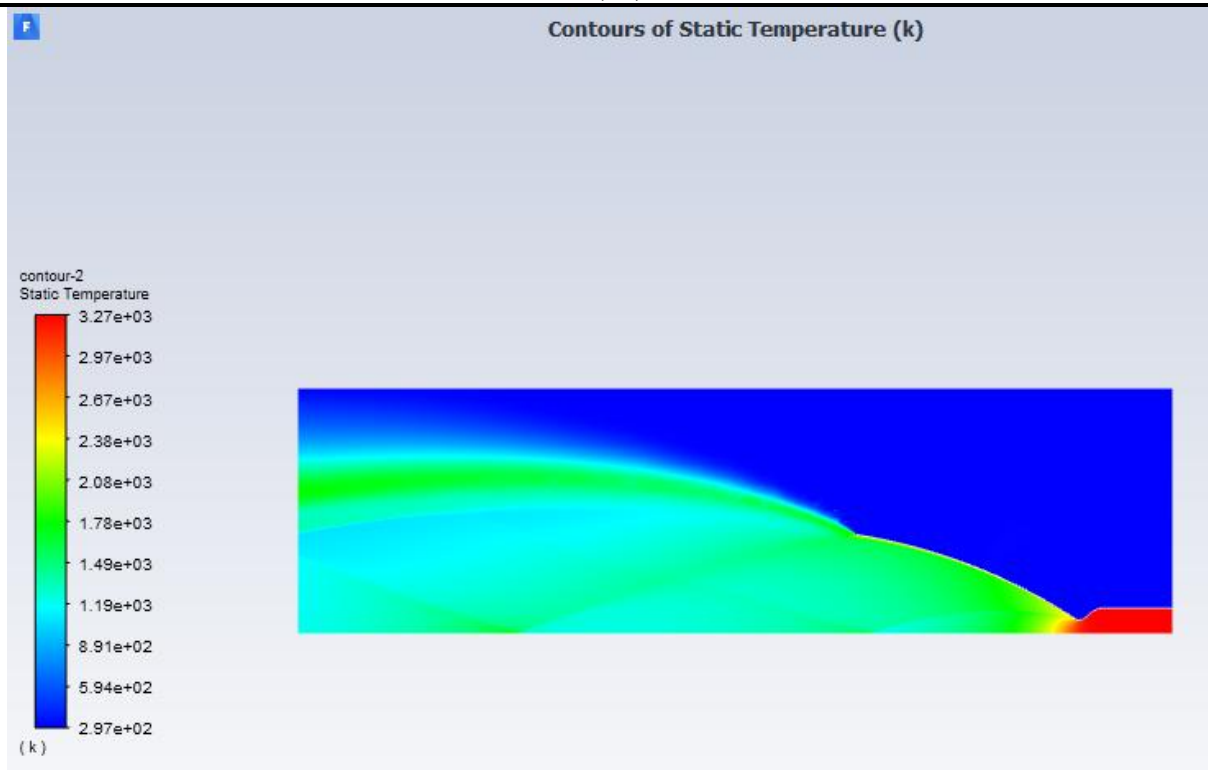


Рисунок 35 – Эпюра параметра температуры

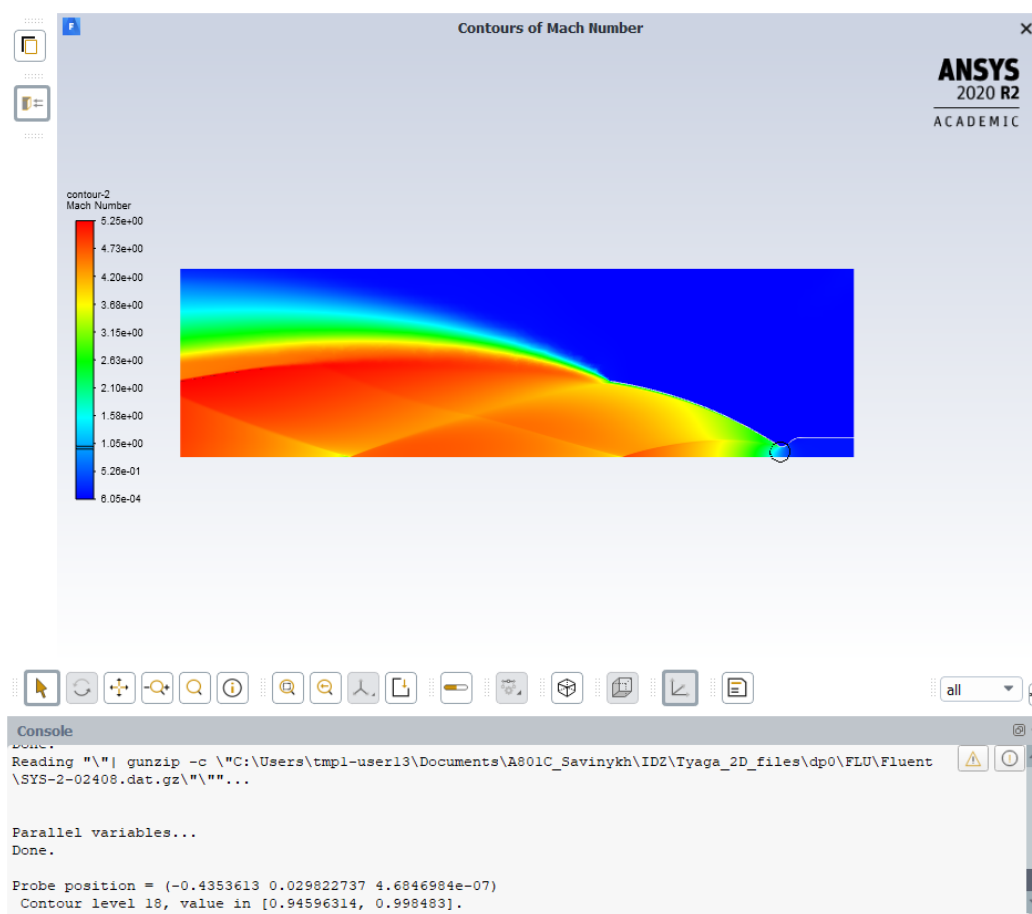


Рисунок 36 – Параметр Маха в критическом сечении

В заключение расчета переходим в модуль Results (Рисунок 37), где вычисляем тягу КРД (рисунок 39-40) путем задания новой переменной Variable 1 (Рисунок 38).

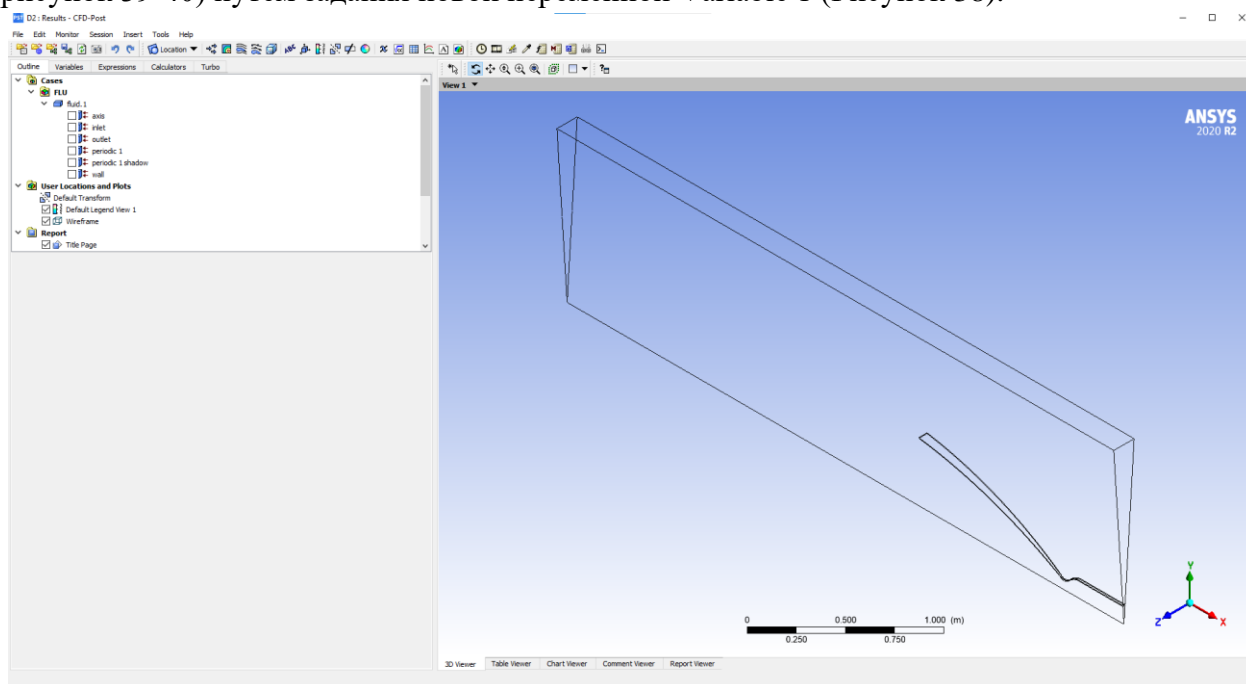


Рисунок 37 – Рабочее окно Results

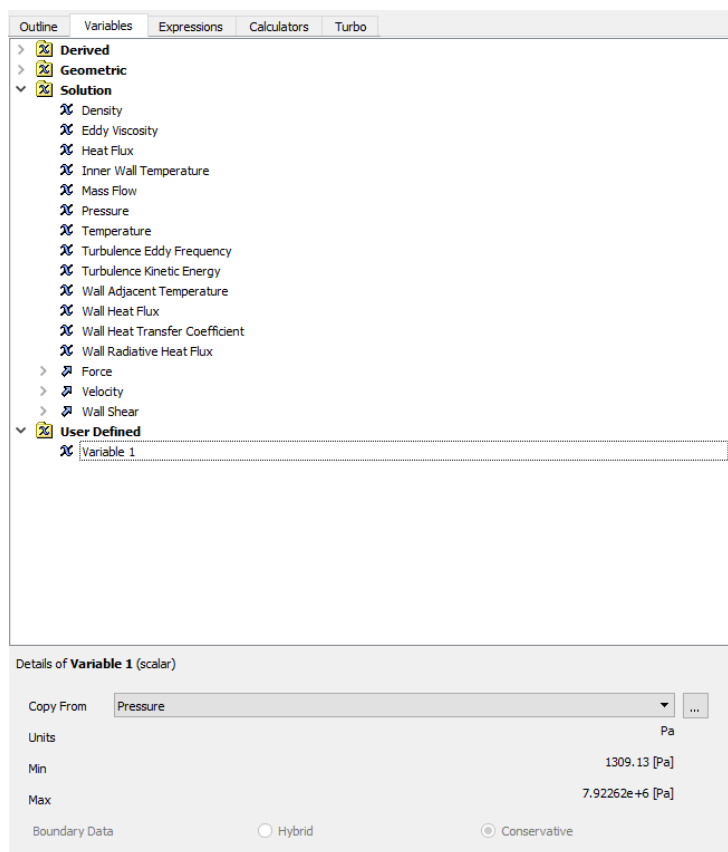


Рисунок 38 – Задание переменной Variable 1

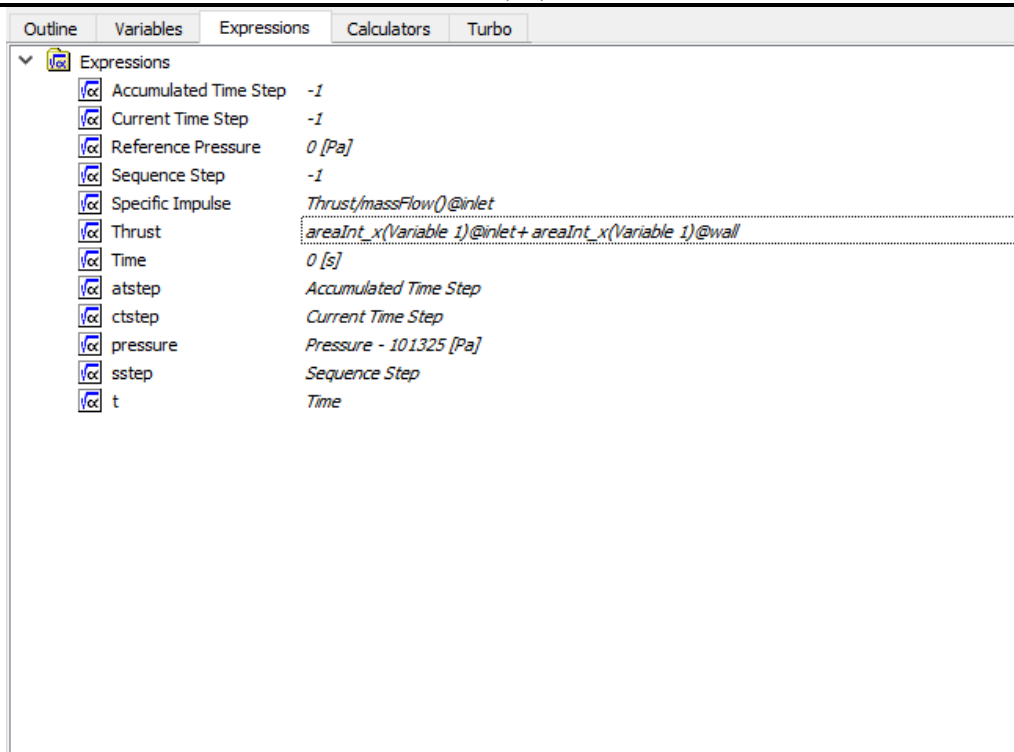


Рисунок 39 – Добавление нового уравнения Thrust (тяги)

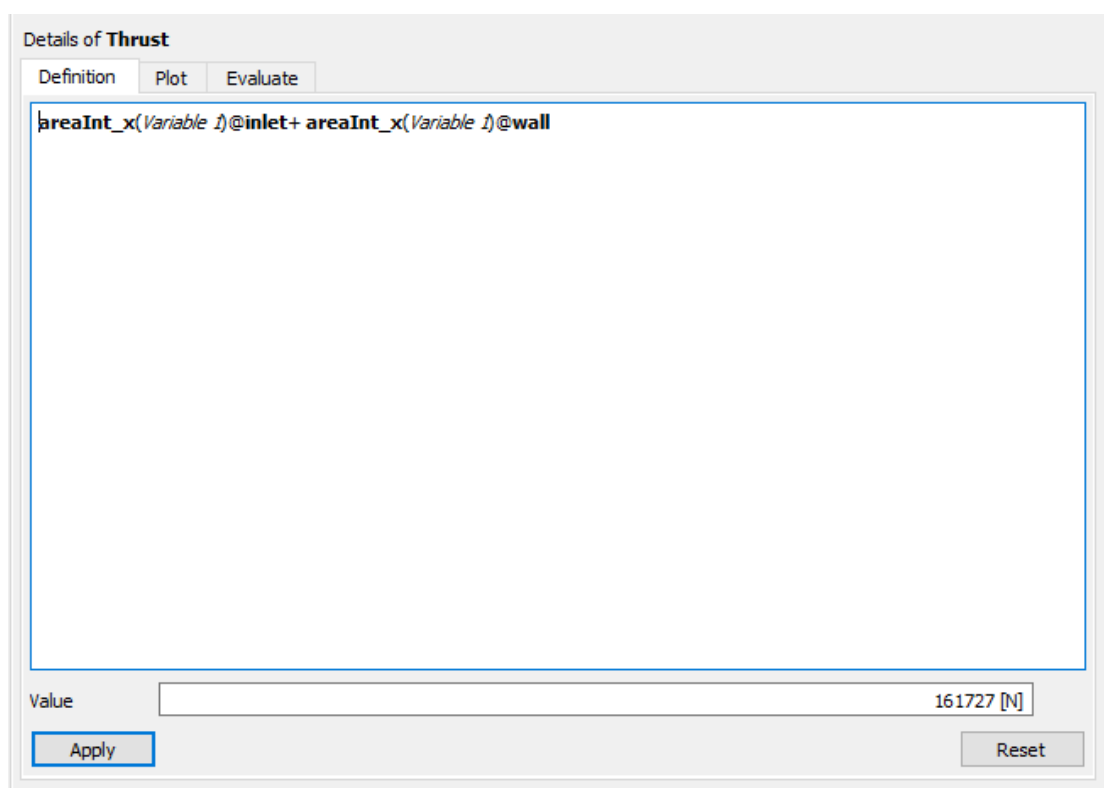


Рисунок 40 – Вычисление тяги

Согласно Рисунку 40, мы видим, что значение тяги примерно 160 кН, что превышает принятое в ходе аналитического расчета значение – 140 кН. Такая погрешность может быть

вызвана несоответствием рассчитанного программой Ansys массового расхода и полученного аналитически. В таком случае сравним удельные импульсы. Для этого разделим тягу на массовый расход (Рисунок 42), посчитанный программой самостоятельно для данной задачи (Рисунок 41).

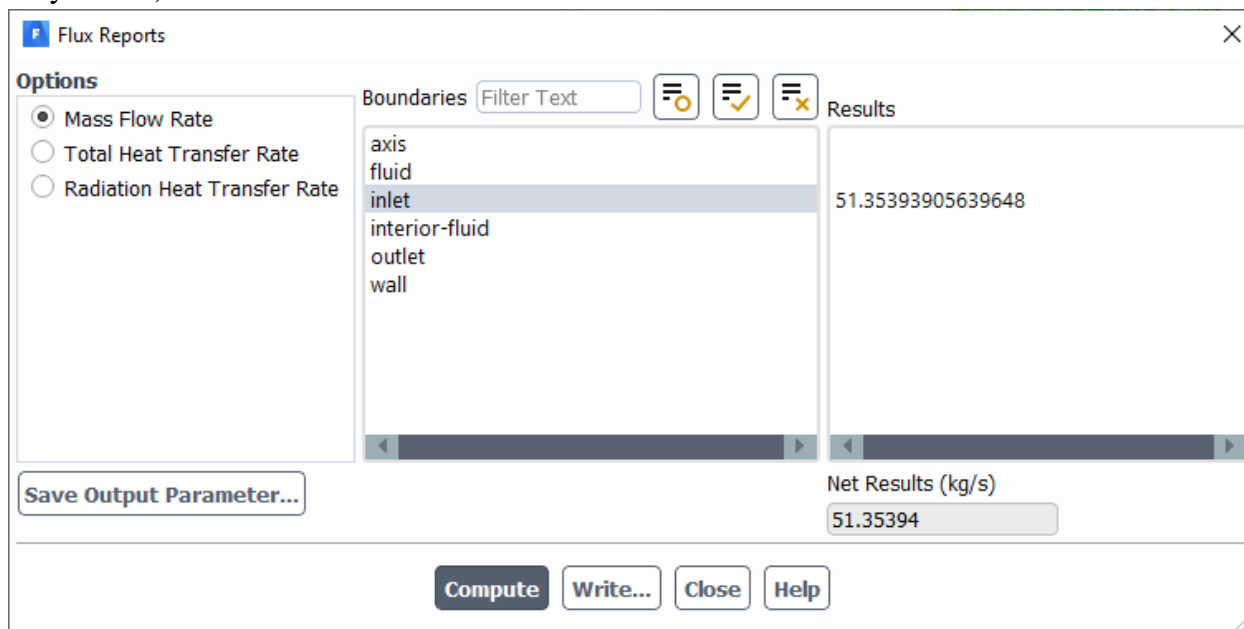


Рисунок 41 – Параметр массового расхода на входной границе согласно программе Ansys

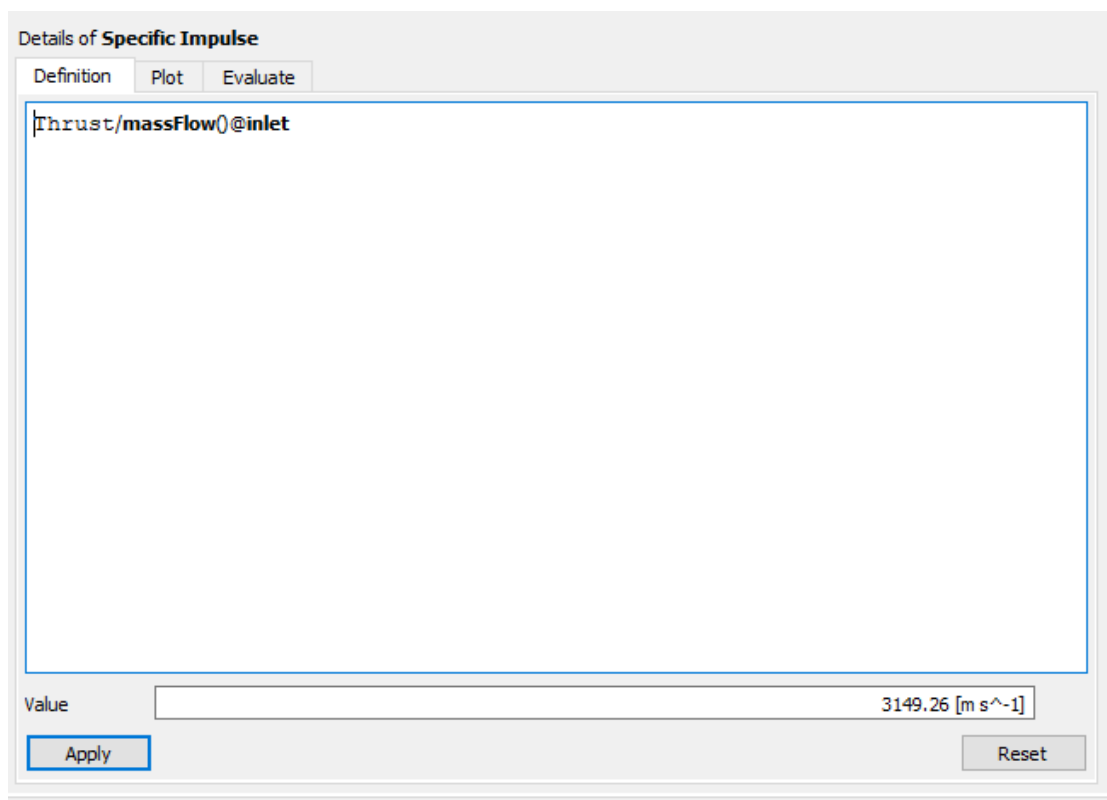


Рисунок 42 – Расчет удельного импульса

В результате получено значение удельного импульса 3150 м/с, что соответствует в пределах погрешности (1.2%) аналитическому значению 3188 м/с, согласно Рисунку 1 и Таблице 2.

Таким образом, можно считать расчет с помощью программного пакета Ansys верным, а это дает возможность опираться на графические отображения параметров в любой точки расчетной области. Исходя из этого, можно делать выводы о целесообразности создания испытываемого изделия, а также своевременно обнаружить недочеты в конструкции.

Список литературы

1. Каплун А.Б. ANSYS в руках инженера [Текст] : практическое руководство / А. Б. Каплун, Е. М. Морозов, М. А. Олферьева. - М. : УРСС, 2003. - 270 с.
2. Каратушин С.И. ANSYS Workbench в деталях машин [Текст] : учебное пособие [для вузов] / С. И. Каратушин [и др.]. - Санкт-Петербург : [б. и.], 2019. - 55 с.
3. Левихин А.А. Рабочие тела и топлива ракетных двигателей: учебное пособие / А.А. Левихин, Л.П. Юнаков; Балт. гос. техн. ун-т. – СПб., 2015. – 78 с.
4. Пинчук В.А., Сиротко В.А. Основы проектирования двигателей летательных аппаратов: Учеб. пособие. Ч.1. Обоснование и выбор рабочих параметров двигательной установки / В.А. Пинчук, В.А. Сиротко. Л., 1990. 60 с.
5. Пинчук В.А. Энергетический расчет ЖРД с нагнетательными системами питания / В.А. Пинчук; Балт. гос. техн. ун-т. – СПб., 2018. – 90 с.
6. Побелянский А.В. Проектирование авиационных и ракетных двигателей с применением CAD/CAM/CAE – систем: учебное пособие / А.В. Побелянский, А.А. Левихин; Балт. гос. техн. ун-т. – СПб., 2019. – 62 с.
7. Потехин Е.С., Филимонов Ю.Н. Основы проектирования двигателей летательных аппаратов: Учеб. пособие. Ч.3. Проектирование камер / Е.С. Потехин, Ю.Н. Филимонов. 1990. 99 с.
8. Шаблий Л.С. Компьютерное моделирование типовых гидравлических и газодинамических процессов двигателей и энергетических установок в ANSYS Fluent: учеб. пособие / Л.С. Шаблий, А.В. Кривцов, Д.А. Колмакова. – Самара: Изд-во Самар. ун-та, 2017. – 108 с.

References

1. Kaplun A.B. ANSYS in the hands of an engineer [Text]: a practical guide / A. B. Kaplun, E. M. Morozov, M. A. Olferyeva. - M.: URSS, 2003. - 270 p.
2. Karatushin S.I. ANSYS Workbench in machine parts [Text]: a tutorial [for universities] / S. I. Karatushin [et al.]. - St. Petersburg: [b. and.], 2019. - 55 p.
3. Levikhin A.A. Working fluids and fuels of rocket engines: a tutorial / A.A. Levikhin, L.P. Yunakov; Baltic state tech. univ. - St. Petersburg, 2015. - 78 p.
4. Pinchuk V.A., Sirotko V.A. Fundamentals of Aircraft Engine Design: Textbook. Part 1. Justification and Selection of Operating Parameters of the Propulsion System / V.A. Pinchuk, V.A. Sirotko. L., 1990. 60 p.
5. Pinchuk V.A. Energy Calculation of Liquid Rocket Engines with Pressurized Fuel Systems / V.A. Pinchuk; Baltic State Tech. Univ. – St. Petersburg, 2018. – 90 p.

6. Pobelyansky A.V. Design of Aircraft and Rocket Engines Using CAD/CAM/CAE Systems: Textbook / A.V. Pobelyansky, A.A. Levikhin; Baltic State Tech. Univ. – St. Petersburg, 2019. – 62 p.
 7. Potekhin E.S., Filimonov Yu.N. Fundamentals of Aircraft Engine Design: Textbook. Part 3. Design of Chambers / E.S. Potekhin, Yu.N. Filimonov. 1990. 99 p.
 8. Shabliy L.S. Computer Simulation of Typical Hydraulic and Gas-Dynamic Processes of Engines and Power Plants in ANSYS Fluent: textbook / L.S. Shabliy, A.V. Krivtsov, D.A. Kolmakova. - Samara: Publishing House of Samara University, 2017. - 108 p.
-



ОТКРЫТАЯ НАУКА
издательство

Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

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



УДК 614.846.6

СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИЙ НАРУЖНОГО ПРОТИВОПОЖАРНОГО ВОДОСНАБЖЕНИЯ ПРОМЫШЛЕННОГО ОБЪЕКТА

Голякова Е.И.

ФГБОУ ВО "СИБИРСКАЯ ПОЖАРНО-СПАСАТЕЛЬНАЯ АКАДЕМИЯ" ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ", Железногорск, Россия (662972, Красноярский край, город Железногорск, Северная ул., д. 1), e-mail: elenagolyakova@inbox.ru

В статье рассматривается технология совершенствования наружного противопожарного водоснабжения конкретного промышленного объекта – здания предприятия АО «ФНПЦ Алтай», расположенного в городе Бийск. На основании фактического обследования результаты испытания на водоотдачу функционирующих на территории предприятия пожарных гидрантов показали отклонения от нормативных показателей по расходу пожарных струй, а также по создаваемому напору. Расчет потребности расхода для наружного пожаротушения согласно действующих нормативных документов позволил дать рекомендации по совершенствованию противопожарного водоснабжения за счет установки двух пожарных резервуаров с хранением требуемого запаса воды. Данное техническое решение тем более оправдано на исследуемом объекте ввиду значительного устаревания объединенного противопожарного водопровода, что исключает установку более мощного насосного агрегата для обеспечения требуемым напором здания, ввиду высокого риска аварийной ситуации в системе.

Ключевые слова: Противопожарное водоснабжение, водоотдача, пожарные гидранты, специализированные емкости.

IMPROVEMENT OF TECHNOLOGIES FOR OUTDOOR FIRE-FIGHTING WATER SUPPLY OF AN INDUSTRIAL FACILITY

Golyakova E.I.

"SIBERIAN FIRE AND RESCUE ACADEMY" OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS", Zhelenogorsk, Russia (662972, Krasnoyarsk region, Zheleznogorsk, Severnaya ul., d. 1), e-mail: elenagolyakova@inbox.ru

The article discusses the technology for improving the external fire-fighting water supply of a specific industrial facility - the building of the enterprise JSC "FSPC Altai", located in the city of Biysk. Based on the actual survey, the results of the water discharge test for fire hydrants operating on the territory of the enterprise showed deviations from the standard indicators for the consumption of fire jets, as well as for the pressure created. The calculation of the flow rate for outdoor fire extinguishing in accordance with the current regulatory documents allowed us to make recommendations for improving fire-fighting water supply by installing two fire tanks with storage of the required water supply. This technical solution is all the more justified at the facility under study due to the significant obsolescence of the integrated fire-fighting water supply system, which precludes the installation of a more powerful pumping unit to provide the required building pressure, due to the high risk of an emergency in the system.

Keywords: Fire-fighting water supply, water drainage, fire hydrants, specialized containers.

В составе территорий промышленных предприятий зачастую имеются зоны, в которых не удовлетворяется потребность в воде для пожаротушения в соответствии с требованиями действующего законодательства. Эти так называемые безводные участки классифицируются как зоны с ограниченным доступом к водным ресурсам для ликвидации пожара, что означает, что ближайший источник воды находится на расстоянии свыше 500 метров от потенциального очага возгорания, или же пропускная способность системы водоснабжения не соответствует нормативным показателям.

Общепринятые нормы и стандарты по обеспечению пожарной безопасности закреплены в пунктах 48, 49, 50, 53 Правил противопожарного режима в Российской Федерации [1].

Обследование систем противопожарного водоснабжения промышленных объектов путем испытания на водоотдачу осуществляется для оценки их функциональной эффективности, измерения фактического объёма воды, задействованной при ликвидации пожаров, и сопоставления полученных параметров с нормативными [2].

Рассмотрим на конкретном промышленном объекте пример совершенствования технологий наружного противопожарного водоснабжения.

Организация наружного противопожарного водоснабжения производственного здания АО ФНПЦ «Алтай», расположенного в г. Бийск Алтайского края, осуществляется через подключение к двум ближайшим пожарным гидрантам (№ 4 и № 5) на кольцевом хозяйственно-противопожарном водопроводе диаметром трубы 300 мм, рассчитанном на пропуск расхода 170 л/с.

Пожарный гидрант № 4 установлен на расстоянии 160 метров от исследуемого объекта, находясь с северной стороны; пожарный гидрант № 5 - на расстоянии 80 метров на северо-восток (Рисунок 1).

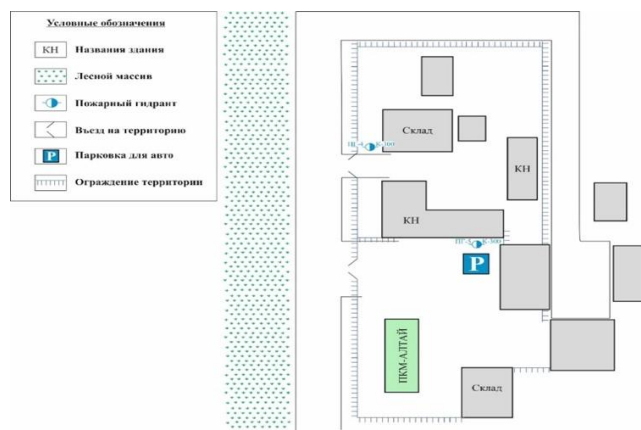


Рисунок 1 - Расположение пожарных гидрантов на территории объекта

Обследование функционирования пожарных гидрантов на объекте включало визуальный осмотр внешнего и внутреннего состояния колодцев, ревизию самих гидрантов, а также их тестирование на способность к надлежащей водоотдаче. В рамках комплексной проверки была оценена четкость и видимость сигнальных указателей пожарных гидрантов, а также доступность подъездных путей к точкам водоотбора для оперативного реагирования на пожарные ситуации.

Было установлено, что обеспечение доступа к пожарному гидранту № 4 не в полной мере удовлетворяет нормативным требованиям, вместе с тем его состояние оценивается как удовлетворительное. Внешний осмотр корпуса гидранта не выявил каких-либо механических

повреждений. Доступ к гидранту № 5 также нормально обеспечен, его состояние приемлемое. Отчет о проведенных испытаниях гидранта ПГ-5 объемным способом содержится в Таблице 1.

Таблица 1 - Результаты испытания на водоотдачу ПГ-5.

$Q_{\Phi}=W/t$	Диаметр выходного отверстия		
	13 мм	16 мм	19 мм
t, с	7,5	5,2	4,1
W, л	25	25	25
Q_{Φ} , л/с	3,3	4,8	6,09

Учитывая, что для наружного тушения пожара в одноэтажном производственном здании класса функциональной пожарной опасности Ф 5.1, в соответствии с пунктом 5.5 СП 8.13130.2020 [3], минимальный требуемый расход воды равен 15 литрам в секунду, вывод о недостаточной эффективности водоотдачи пожарного гидранта № 5 правомерен.

Согласно СП 8.13130.2020, в ситуациях, когда наружные противопожарные системы не обеспечивают необходимый расход для эффективной подачи воды при тушении пожаров, актуализируется решение о возможности установки специализированных емкостей с нормативным неприкосновенным противопожарным запасом воды.

Данное техническое решение тем более оправдано на объекте АО ФНПЦ «Алтай» ввиду значительного устаревания объединенного противопожарного водопровода, что исключает установку более мощного насосного агрегата для обеспечения требуемым напором здания, ввиду высокого риска аварийной ситуации в системе.

В этой связи предлагается разместить два противопожарных резервуара на максимальном удалении 200 метров от объекта, в соответствии с п. 10.4 СП 8.13130.2020, что гарантирует эффективность тушения пожара на протяжении трех часов с минимальным потреблением воды в 15 л/сек.

Противопожарный объем с учетом минимального расхода воды $Q = 15$ л/с, в течении времени $t = 3 \text{ ч} = 10800$ с, рассчитывается по формуле [4]:

$$W_p = Q \times t = 15 \times 10800 = 162000 \text{ л} = 162 \text{ м}^3, \quad (1)$$

Так как нормативный объем каждого резервуара должен составлять 50 % , необходимо установить два пожарных резервуара объемом по 100 м³. По типу исполнения это могут быть стальные вертикальные РВС-100 (Рисунок 2) или горизонтальные резервуары РГС-100 (Рисунок 3) [5].

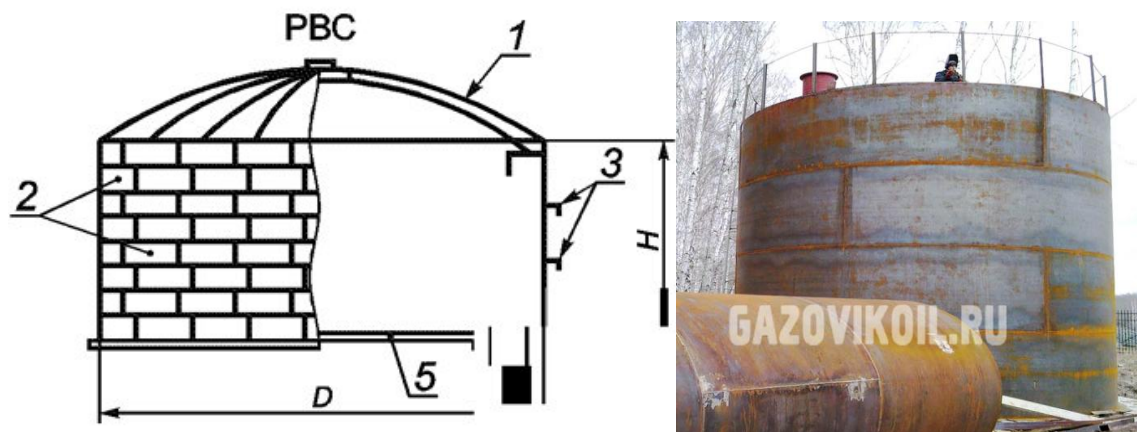


Рисунок 2 - Пожарный резервуар PBC-100

1 - стропильная система кровли, 2 - обвязочные ригели стен, 3 - вставные элементы жесткости, 5 - сердцевина основания.



Рисунок 3 - Внешний вид пожарного резервуара PGC-100

В условиях, когда существует риск замерзания воды в пожарном резервуаре, рекомендуется принять меры по его тепловой изоляции и установке систем обогрева.

Для предотвращения коррозионных повреждений внешняя поверхность пожарного резервуара обрабатывается антикоррозийным покрытием и эмалевым слоем. Обычный срок эксплуатации данных емкостей для хранения огнетушащих веществ составляет 20 лет [5].

Период времени, предусмотренный для восстановления объема воды, необходимого для тушения пожара, должен производиться круглосуточно на промышленных объектах, отнесенных к категориям А, Б, и В согласно классификации по уровню пожарной и взрывопожарной угрозы.

Экономическое обоснование технического решения по установке двух пожарных резервуаров проводилось по методике МДС 21-3.2001 «Методика и примеры технико-экономического обоснования противопожарных мероприятий» [6].

Предлагаемое решение ориентировано на соответствие критериям устойчивости к огню конструкций, препятствия распространению пламени и минимизации прямого и косвенного

материального ущерба от пожара.

Для оценки эффективности мер, направленных на предотвращение пожаров, использовался финансовый анализ, который включает в себя сравнение денежных потоков: доходов и расходов, возникающих в результате внедрения противопожарных мер.

Получение доходов в данном случае является результатом избежания убытков благодаря внедрению превентивных противопожарных стратегий. Эти стратегии включают расчет и сравнение предотвращённых материальных потерь в случае возгорания благодаря применению определённой меры безопасности (проектируемый сценарий) по сравнению с потенциальными убытками, которые произошли бы при отсутствии такой меры (базовый сценарий).

Следует отметить, что расчет касался исключительно финансовых потерь, игнорируя человеческие жертвы, которые, как общеизвестно, представляют собой наиболее серьёзные убытки.

Проведенный расчет технико-экономического эффекта, выходящий за рамки настоящей статьи, доказывает экономическую целесообразность внедрения данной технологии увеличения эффективности и надежности пожаротушения на конкретном промышленном объекте.

Предлагаемое техническое решение по совершенствованию наружного противопожарного водоснабжения по результатам испытания на фактическую водоотдачу, может быть использована для противопожарной защиты иных промышленных предприятий..

Список литературы

1. Постановление Правительства РФ от 16 сентября 2020 г. N 1479 «Об утверждении Правил противопожарного режима в РФ».
2. Шипигузов В. А., Бондарев В. Ф., Саватеев А. И., Копейкин Н. Н. Методика проверки сетей противопожарного водоснабжения на водоотдачу. СПб.: Санкт-Петербургский филиал ФГУ ВНИИПО МЧС России, 2003. 36 с.
3. СП 10.13130.2020 «Системы противопожарной защиты. Внутренний противопожарный водопровод. Нормы и правила проектирования».
4. Гидравлика и противопожарное водоснабжение. Учебник. / Ю. Г. Абросимов, А. И. Иванов, А. А. Качалов [и др]. М.: Академия ГПС МЧС России, 2003. 392 с.
5. Резервуар стальной URL: <https://krasnoyarsk.snmarsh.ru/>
6. Методика и примеры технико-экономического обоснования противопожарных мероприятий к СНиП 21-01-97*. МДС 21-3.2001 / ОАО «ЦНИИ-промзданий». М.: ГУП ЦПП, 2001. 86 с.

References

1. Decree of the Government of the Russian Federation No. 1479 dated September 16, 2020 "On Approval of Fire Safety Regulations in the Russian Federation".
2. Shipiguzov V. A., Bondarev V. F., Savvateev A. I., Kopeikin N. N. Methods of checking fire-fighting water supply networks for water discharge. St. Petersburg: St. Petersburg branch of the Federal State Institution VNIPO of the Ministry of Emergency Situations of Russia, 2003. p.36
3. SP 10.13130.2020 "Fire protection systems. Internal fire-fighting water supply. Norms and rules of design".

4. Hydraulics and fire-fighting water supply. Textbook. / Yu. G. Abrosimov, A. I. Ivanov, A. A. Kachalov [and others]. Moscow: Academy of GPS of the Ministry of Emergency Situations of Russia, 2003. p.392
 5. Steel tank URL: <https://krasnoyarsk.snmash.ru/>
 6. Methodology and examples of the feasibility study of fire prevention measures for SNiP 21-01-97*. MDS 21-3.2001 / JSC "TsNII-promzdaniy". Moscow: GUP TSPP, 2001. p.86
-