Международный журнал информационных технологий и энергоэффективности

Том 11 Номер 1 (63)

2026

Международный журнал информационных технологий и энергоэффективности
Т.11 №1(63) 2026 г.

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

СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

1.	**Дербеденев Д.И., Смирнов Д.А., Ворокова Н.Х.** Аналитический калькулятор вариационных рядов **Derbedenev D.I.**, **Smirnov D.A.**, **Vorokova N.Kh**. Analytical calculator of variation series	**6**
2.	**Апкарова Т.Т.** Современные направления модернизации автоматизированных систем управления технологическими процессами (АСУТП) производства шоколадных конфет в условиях ИНДУСТРИИ 4.0 **Apkarova T.T**. Contemporary trends in the modernization of automated process control systems (APCS) for chocolate candies production in INDUSTRY 4.0	**12**
3.	**Черномор Н.А., Плотников В.В.** Философия техники и образы будущего человека и среды в контексте развития информационных технологий **Chernomor N.A., Plotnikov V.V.** Philosophy of technology and images of the future person and environment in the context of information technology development	**17**
4.	**Скроцкий И.О.** Фреймворк для динамического развертывания сетевых сегментов (NETWORK SEGMENTATION) в промышленных сетях IIoT **Skrotskiy I.O.** Framework for dynamic deployment of NETWORK SEGMENTATION in industrial IIoT networks	**25**
5.	**Гарматюк В.В.** Интеграция блокчейн-технологий и методов обеспечения информационной безопасности для защиты конфиденциальных данных **Garmatyuk V.V.** Integration of blockchain technologies and information security methods for the protection of confidential data	**32**
6.	**Ткач Г.А.** Концепция нулевого доверия как основа современной корпоративной безопасности **Tkach G.A.** The concept of zero trust as the basis of modern corporate security	**40**
7.	**Кузнецов А.К.** Повышение эффективности мониторинга серверных систем на основе технологий искусственного интеллекта **Kuznetsov A.K.** Improving the efficiency of server system monitoring based on artificial intelligence technologies	**46**
8.	**Садыков Р.Р.** Социальная инженерия: атаки с использованием синтетических личностей и дипфейков **Sadykov R.R.** Social engineering: synthetic identity and deepfake attacks	**52**
9.	**Семеняка И.А.** Метрики, логи и трейсы как основа мониторинга виртуализированной инфраструктуры	**62**

	Semenyaka I.A. The concept of zero trust as the basis of modern corporate security	
10.	**Воронов Д.С., Ачкасова В.А. (научный руководитель)**. Роль технологий искусственного интеллекта в электоральных проектах **Voronov D.S**., **Achkasova V.A**. (supervisor) The role of generative neural networks in electoral projects	**70**
11.	**Зюзин А.О.** Вероятностная методика оценки риска нарушения стабильности банковских информационных систем при выпуске релиза на основе имитационного моделирования (MONTE CARLO) **Zyuzin A.O.** Probabilistic method for assessing the risk of banking information system stability violation during a software release using MONTE CARLO simulation	**82**
12.	**Немчинов А.В.** Методы обнаружения аномалий в информационной инфраструктуре на основе статистического анализа и корреляции трафика **Nemchinov A.V**. Methods for detecting anomalies in the information infrastructure based on statistical analysis and traffic correlation	**88**
13.	**Захарова М.М.** Сравнительный анализ эффективности стратегий ZTNA и традиционных VPN для защиты гибридной ИТ-инфраструктуры предприятия **Zakharova M.M**. A comparative analysis of the effectiveness of ZTNA and traditional VPN strategies for securing hybrid enterprise IT infrastructure	**95**
14.	**Гордеева А. М.** Влияние отключения протокола SMB в Windows на безопасность корпоративных сетей **Gordeeva A. M.** Impact of disabling the SMB protocol in WINDOWS ON corporate network security	**99**
15.	**Кайралапов А.М.** Эволюция оптических измерений на конечном участке траектории: от регистрации координат к интеллектуальному анализу физических процессов **Kayralapov A.M.** Evolution of optical measurements on the final trajectory segment: from registration to intelligent analysis	**105**
16.	**Белов М.Э.** Алгоритмическое управление в государственных цифровых платформах: архитектура, данные и интеллектуальные модели **Belov M.E.** Algorithmic management in government digital platforms: architecture, data, and intelligent models	**113**
17.	**Белов М.Э.** Персональные данные: локализация «первичной записи» и архитектура комплаенса **Belov M.E.** Personal data: localization of the "primary record" and compliance architecture	**118**
18.	**Ким А.С., Крепак И.П.** Эволюция APT-атак: применение обфускации и ИИ для обхода от средств защиты информации **Kim A.S., Krepak I.P.** Evolution of APT attacks: the use of obfuscation and AI to evade security measures	**133**
19.	**Маркевич Д.В.** Методика оценки систем безопасности микросервисов с учётом ложных срабатываний и концептуального дрейфа	**139**

Markevich D.V. Methodology for evaluating microservice security systems based on false alarms and conceptual drift

20. **Дудин В.Д.** Общеканальная система сигнализации объекта информатизации как элемент защиты информационно-телекоммуникационной сети **152**

Dudin V.D. Channel-wide alarm system for an information facility as an element of information and telecommunication network protection

21. **Погорова М.А., Фаргиева З.С. (научный руководитель)** Методические и практические рекомендации к использованию ИИ в образовании **157**

Pogorova M.A., **Fargieva Z.S. (supervisor)** Methodoligical AND PRACTICAL recommedations for the use of AI in education

22. **Нестерова В.А., Дробкова О.С.** Обзор использования технологий искусственного интеллекта в бизнес-аналитике: навигатор BI как кейс ИИ-трансформации **163**

Nesterova V.A., Drobkova O.S. A review of artificial intelligence technologies in business analytics: BI navigator as a case study of AI transformation

23. **Нестерова В.А.** Влияние внешних факторов на предприятия авиастроительного комплекса России: систематический обзор литературы **171**

Nesterova V.A. Influence of external factors on enterprises of the russian aircraft manufacturing complex: a systematic review of the literature

24. **Сеидов М.С-А., Ясевич Б.О.** Мониторинг аномальной активности в операционной системе ЗОСРВ «Нейтрино» **177**

Seidov M.S.-A., **Yasevich B.O.** Monitoring anomalous activity in the NEUTRINO research system

25. **Капитанчук В.В. Забелин А.Н., Гамза С.А.** Разработка модели процесса посадки самолета ТУ-134 **186**

Kapitanchuk V. V., Zabelin A. N., Gamza S. A. Development of a landing process model for the TU 134 aircraft

26. **Павлов К.К.** Сравнительный анализ эффективности ZTNA и SASE для защиты распределённых удалённых рабочих мест **196**

Pavlov K.K. Comparative analysis of the effectiveness of ZTNA and sase for the protection of distributed remote workplaces

27. **Исламова А.Р.** Методы генерации API-автотестов на основе нейросетей: современное состояние, проблемы и перспективы **202**

Islamova A.R. API autotest generation methods based on neural networks: current status, problems and prospects

28. **Коровин Н.А., Коровин М.А., Коровин Н.А**. Апскейл фотоматериалов с применением нейронных сетей **206**

Korovin N.A., Korovin M.A., Korovin N.A. Upscale of photographic materials using neural networks

ЭНЕРГЕТИКА И ЭНЕРГОЭФФЕКТИВНОСТЬ

29.	**Петров А.О.** Модель кластеризации малоэффективных источников теплоснабжения как инструмент модернизации коммунальной инфраструктуры «полупериферийных» территорий **Petrov A.O.** A clustering model for inefficient heat supply sources as a tool for modernizing the communal infrastructure of «semi-peripheral» territories	**215**
30.	**Жильцов Д.А.** Проектирование корпуса ракеты носителя среднего класса из модифицированного композита **Zhiltsov D.A.** Design of a middle-class carrier missile body made of a modified composite	**219**
31.	**Павлов И.С. Елохов А.В., Жуйков И.О**. Особенности конструкции и расчёта анкерных участков контактной сети переменного тока на железнодорожных линиях **Pavlov I.S., Elokhov A.V., Zhuykov I.O.** Design and calculation features of anchor sections of ac contact networks on railway lines	**224**
32.	**Черных П.А.** Совершенствование режимов работы тепловых сетей для северных территорий **Chernykh P.A**. Improving the operating modes of heating networks for northern territories	**230**
	ПРОИЗВОДСТВЕННАЯ БЕЗОПАСНОСТЬ	
33.	**Назаров Н.В.** Исследование характера работы защитных сооружений стенок котлована в стеснённых городских условиях **Nazarov N.V**. Investigation of the nature of the protective structures of the excavation walls in cramped urban conditions	**235**

Дербеденев Д.И., Смирнов Д.А., Ворокова Н.Х. Аналитический калькулятор вариационных рядов// Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 6–11

Международный журнал информационных технологий и энергоэффективности

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

УДК 519.24:004.42

АНАЛИТИЧЕСКИЙ КАЛЬКУЛЯТОР ВАРИАЦИОННЫХ РЯДОВ

[1]Дербеденев Д.И., Смирнов Д.А., Ворокова Н.Х.
ФГБОУ ВО «КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМ. И.Т. ТРУБИЛИНА», Краснодар, Россия (350044, Краснодарский край, город Краснодар, ул. им. Калинина, д.13), e-mail: [1]dderbedenev21@mail.ru

В данной статье описывается процесс разработки аналитического калькулятора для работы с вариационными рядами в математической статистике. Инструмент автоматизирует расчёт ключевых характеристик: средних значений, дисперсии, коэффициента вариации, эксцесса, среднего квадратического отклонения и показателей асимметрии. Предназначен для студентов, исследователей и аналитиков, работающих с большими выборками и данными.

Ключевые слова**:** Вариационный ряд, математическая статистика, аналитический калькулятор, статистические характеристики, обработка данных, автоматизация расчётов.

ANALYTICAL CALCULATOR OF VARIATION SERIES

[1]Derbedenev D.I., Smirnov D.A., Vorokova N.Kh.
"KUBAN STATE AGRARIAN UNIVERSITY". I.T. TRUBILINA", Krasnodar, Russia (350044, Krasnodar City, Kalinina Street, 13), e-mail: [1]dderbedenev21@mail.ru

This article describes the process of developing an analytical calculator for working with variation series in mathematical statistics. The tool automates the calculation of key characteristics: mean values, variance, coefficient of variation, kurtosis, standard deviation, and asymmetry indicators. It is intended for students, researchers, and analysts working with large samples and data.

Keywords: Variation series, mathematical statistics, analytical calculator, statistical characteristics, data processing, calculation automation.

Введение

Работа с данными в современном мире имеет ключевое значение, так как возрастающие объемы информации и сложность исследовательских задач требуют применения эффективных инструментов. Анализ числовых совокупностей, включающий расчет основных характеристик распределения, помогает систематизировать информацию, выявлять закономерности и принимать обоснованные решения. Автоматизация этих процессов становится не только технической необходимостью, но и конкурентным преимуществом. Осознанное применение аналитических инструментов, таких как калькулятор вариационных рядов, лежит в основе методологически грамотного исследования.

Цель исследования – продемонстрировать практическую значимость и последовательность анализа вариационных рядов с использованием специализированного аналитического калькулятора для извлечения содержательных выводов из первичных данных.

Материал и методы исследования

В качестве материала исследования использован смоделированный массив данных, представляющий результаты условного измерения. Основным методом исследования выступил метод описательной статистики, реализуемый с помощью аналитического калькулятора вариационных рядов для расчёта средних величин и показателей вариации.

Вариационный ряд — это фундаментальное понятие математической статистики, представляющее собой упорядоченное распределение единиц исследуемой совокупности (выборки) по возрастанию или убыванию значений конкретного признака. Его построение и анализ являются первым и обязательным этапом обработки любых эмпирических данных. Вариационные ряды используются повсеместно: от социологии для анализа результатов опросов до экономики для изучения распределения доходов. Они позволяют перейти от хаотичного набора чисел к структурированной картине, наглядно демонстрирующей концентрацию данных, разброс и форму распределения [1].

Ключевое значение имеет тип вариационного ряда. *Дискретный ряд* строится для прерывных (дискретных) признаков, принимающих отдельные, изолированные значения (например, число бракованных деталей в партии). *Интервальный (непрерывный) ряд* формируется для признаков, которые могут принимать любые значения в определенном интервале (рост, вес, время выполнения задачи), что требует предварительного группирования данных. Правильный выбор типа ряда определяет корректность всех последующих вычислений [2].

Аналитический *калькулятор вариационных рядов* служит эффективным инструментом для автоматизации этой критически важной стадии исследования. Он призван минимизировать временные затраты и исключить арифметические ошибки при расчётах.

После ввода исходных данных калькулятор мгновенно выполняет комплексную обработку, предоставляя исследователю всю необходимую сводку. Ключевым результатом является расчёт *показателя центра распределения:* средней арифметической, характеризующей общий уровень признака. Не менее важны *показатели вариации*: дисперсия, среднее квадратичное отклонение, коэффициент вариации, коэффициент асимметрии и эксцесс, которые количественно оценивают степень разнообразия и распределения данных в выборке.

Разработка аналитического калькулятора вариационных рядов на С++:

Для написания калькулятора необходимы формулы расчета дисперсии, среднего квадратичного отклонения, коэффициента вариации, коэффициента асимметрии и эксцесса [3]:

Дисперсия: $\sigma^2 = \frac{\sum_{i=1}^{n}(x_1 - \bar{x})^2}{n} = \frac{\sum x_i^2}{n} - (\bar{x})^2$ – простая; (8.6)

$\sigma^2 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2 n_i}{\sum_{i=1}^{n} n_i} = \frac{\sum x_i^2 n_i}{n} - (\bar{x})^2$ – взвешенная. (8.7)

Среднее квадратичное отклонение: $\sigma = \sqrt{\sigma^2}$. (8.8)

Коэффициент вариации: $V = \frac{\sigma}{\bar{x}} \cdot 100\%$. (8.9)

Если V > 33%, то считается, что совокупность может быть статистически неоднородной в отношении данного признака.

Рисунок 1 - Формулы вариационных рядов

Напишем код на C++, который рассчитывает требуемые значения и подбирает им соответствующие характеристики ряда из этих условий:

$$K_A = \frac{m_3}{\sigma^3}, \quad (8.15)$$

где m_3 - центральный момент третьего порядка.

Если $K_A = 0$, то вариационный ряд является симметричным;
если $K_A < 0$, то вариационный ряд с левосторонней асимметрией;
если $K_A > 0$, то вариационный ряд с правосторонней симметрией.

Мерой крутости (островершинной) ряда распределения является **эксцесс**:

$$Э = \frac{m_4}{\sigma^4} - 3, \quad (8.16)$$

где m_4 – центральный момент четвертого порядка.
Если $Э \approx 0$, то распределение средне вершинное;
если $Э < 0$, то распределение островершинное;
если $Э > 0$, то распределение плосковершинное.

Рисунок 2 - Характеристики вариационных рядов

```
private:
    System::Void button1_Click(System::Object^ sender, System::EventArgs^ e) {
        try {
            double sum_Xi = Convert::ToDouble(textBox1->Text);
            double sum_Ni = Convert::ToDouble(textBox2->Text);
            double sum_XiNi = Convert::ToDouble(textBox3->Text);
            double sum_Xi_minus_Xavg_squared_Ni = Convert::ToDouble(textBox4->Text);
            double sum_Xi_minus_Xavg_cubed_Ni = Convert::ToDouble(textBox5->Text);
            double sum_Xi_minus_Xavg_4th_Ni = Convert::ToDouble(textBox6->Text);

            double X_avg = sum_XiNi / sum_Ni;
            textBox7->Text = X_avg.ToString("F4");

            double variance = sum_Xi_minus_Xavg_squared_Ni / sum_Ni;
            textBox8->Text = variance.ToString("F4");

            double sigma = System::Math::Sqrt(variance);
            textBox9->Text = sigma.ToString("F4");

            double V_coefficient = (sigma / X_avg) * 100;
            textBox10->Text = V_coefficient.ToString("F2") + "%";

            if (V_coefficient > 33) {
                textBox13->Text = "Совокупность может быть статистически неоднородной в отношении данного признака";
            }
            else {
                textBox13->Text = "Совокупность статистически однородна в отношении данного признака";
            }

            double m3 = sum_Xi_minus_Xavg_cubed_Ni / sum_Ni;
            double KA = m3 / System::Math::Pow(sigma, 3);
```

Рисунок 3 - C++-код калькулятора вариационных рядов

```
if (System::Math::Abs(KA) < 0.001) {
    textBox14->Text = "Вариационный ряд является симметричным";
}
else if (KA < 0) {
    textBox14->Text = "Вариационный ряд с левосторонней асимметрией";
}
else {
    textBox14->Text = "Вариационный ряд с правосторонней асимметрией";
}

double m4 = sum_Xi_minus_Xavg_4th_Ni / sum_Ni;
double excess = (m4 / System::Math::Pow(sigma, 4)) - 3;
textBox12->Text = excess.ToString("F4");

if (System::Math::Abs(excess) < 0.1) {
    textBox15->Text = "Распределение средневершинное (нормальное)";
}
else if (excess < 0) {
    textBox15->Text = "Распределение островершинное (лептокуртическое)";
}
else {
    textBox15->Text = "Распределение плосковершинное (платикуртическое)";
}

if (!String::IsNullOrEmpty(textBox16->Text)) {
    try {
        double sum_abs_Xi_minus_Xavg_Ni = Convert::ToDouble(textBox16->Text);
        double mean_linear_deviation = sum_abs_Xi_minus_Xavg_Ni / sum_Ni;

    }
    catch (FormatException^) {
    }
}
```

Рисунок 4 - Реализация условий для определения характеристик вариационных рядов

Этот код решает задачу вычисления значений по заданным формулам и проводит анализ характеристик вариационного ряда.

Далее разрабатываем форму ввода данных. Получаем результат:

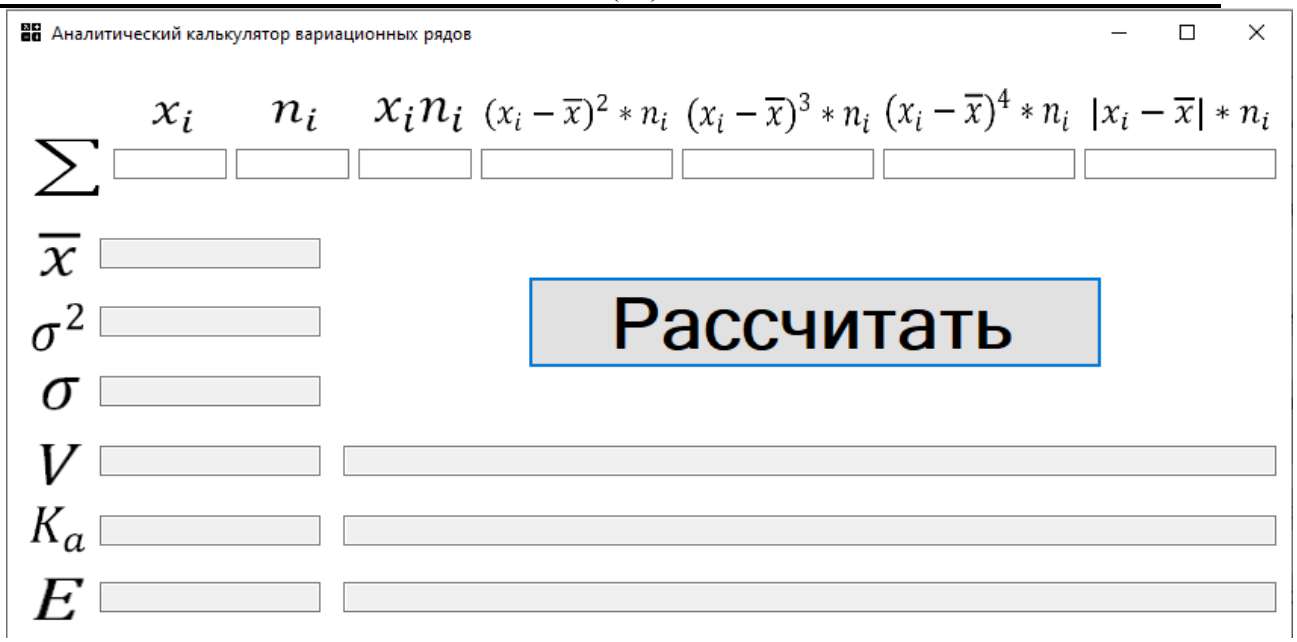

Рисунок 5 - Интерфейс калькулятора

Теперь необходимо подставить значения и произвести расчёт. Получим следующее:

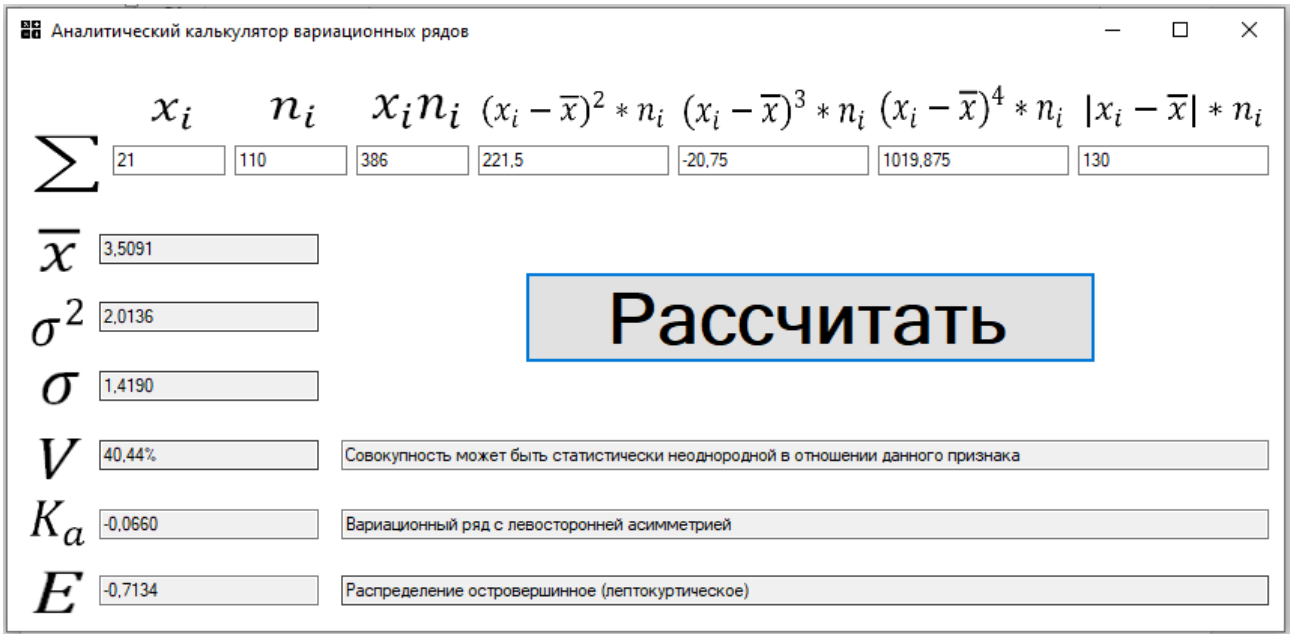

Рисунок 6 - Результат расчета калькулятора

На Рисунке 6 видно, как приложение исходя из формул на Рисунке 1 и характеристик ряда на Рисунке 2 вычисляет значения, сопоставляет их с критериями и выводит результат.

Выводы

Аналитический калькулятор вариационных рядов — это не просто математический алгоритм, а фундаментальный инструмент, способный стать основой для осознанного анализа данных. Его ценность объясняется методологической универсальностью: от студентов, осваивающих основы статистики, до профессиональных аналитиков, применяющих эти вычисления для исследований. Благодаря возможности быстро получить ключевые

характеристики распределения, калькулятор помогает понять структуру данных, оценить их разброс и центральную тенденцию.

Однако важно помнить, что рассчитанные показатели — это только отправная точка. Они не учитывают природу исследуемой выборки, содержательные гипотезы или возможные аномалии в данных. Поэтому результаты калькулятора должны интерпретироваться в сочетании с другими методами анализа, включая визуализацию и проверку статистических предположений.

Несмотря на свои ограничения, аналитический калькулятор вариационных рядов играет важную роль в первичном исследовании данных. Он позволяет оперативно выявить основные закономерности и сформулировать гипотезы для дальнейшей, более глубокой проверки. Кроме того, этот инструмент помогает структурировать работу с информацией, что, в конечном итоге, способствует повышению качества выводов и обоснованности принимаемых решений.

Используя такой калькулятор, можно не только автоматизировать вычисления, но и развивать навык системного подхода к данным. Это простой, но мощный шаг к грамотному анализу, который доступен каждому исследователю. Главное — помнить, что работа с данными — это не механический расчёт, а интерпретационный процесс, который требует критического мышления и понимания контекста.

Список литературы

1. Бондаренко П. С. Теория вероятностей и математическая статистика: учебное пособие / П. С. Бондаренко, Г. В. Горелова, И. А. Кацко; под ред. И. А. Кацко, А. И. Трубилина. – М.: КНОРУС, 2019. – 390 с.
2. Гмурман В. Е. Теория вероятностей и математическая статистика: учебник. - М.: Юрайт, 2016. – 479 с.
3. Сборник задач по теории вероятностей и математической статистике / Кацко И.А., Бондаренко П.С., Горелова Г.В., Куижева С.К., Ворокова Н.Х., Жминько Н.С. учебное пособие для вузов / (2-е издание, исправленное) Санкт-Петербург, 2024.

References

1. Bondarenko P. S. Probability Theory and Mathematical Statistics: a textbook / P. S. Bondarenko, G. V. Gorelova, I. A. Katsko; ed. by I. A. Katsko, A. I. Trubilin. – Moscow: KNORUS, 2019. – 390 p.
2. Gmurman V. E. Probability Theory and Mathematical Statistics: a textbook. – Moscow: Yurait, 2016. – 479 p.
3. Collection of Problems in Probability Theory and Mathematical Statistics / I. A. Katsko, P. S. Bondarenko, G. V. Gorelova, S. K. Kujezheva, N. Kh. Vorokova, N. S. Zhminko: a textbook for universities / (2nd edition, revised) Saint Petersburg, 2024.

Апкарова Т.Т. Современные направления модернизации автоматизированных систем управления технологическими процессами (АСУТП) производства шоколадных конфет в условиях ИНДУСТРИИ 4.0// Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 12–16

Международный журнал информационных технологий и энергоэффективности

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

УДК 664.145:658.5:681.51:004.89

СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ МОДЕРНИЗАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ (АСУТП) ПРОИЗВОДСТВА ШОКОЛАДНЫХ КОНФЕТ В УСЛОВИЯХ ИНДУСТРИИ 4.0

Апкарова Т.Т.
ФГБОУ ВО "ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М. Д. МИЛЛИОНЩИКОВА", Грозный, Россия (364051, Чеченская Республика, город Грозный, пр-кт Имени Хусейна Абубакаровича Исаева, д. 100), e-mail: [1]tanzila.apkarova@mail.ru

В статье проведен комплексный анализ эволюции и перспективных векторов модернизации автоматизированных систем управления технологическими процессами (АСУТП) на предприятиях кондитерской промышленности, специализирующихся на выпуске шоколадных конфет. Рассмотрены технологические, экономические и организационные аспекты внедрения решений, соответствующих концепции «Индустрия 4.0». Акцент сделан на интеграции сенсорных систем нового поколения, распределенных систем управления, предиктивной аналитики и цифровых двойников в единый киберфизический контур. Особое внимание уделено проблеме обеспечения стабильности рецептурных и органолептических характеристик продукции в условиях изменчивости сырьевых параметров. Приведены результаты имитационного моделирования работы модернизированной АСУТП участка темперирования и формования шоколадной массы, демонстрирующие повышение точности управления на 18-22% и снижение коэффициента брака по массе готового изделия на 15%. Доказана экономическая целесообразность поэтапной модернизации с фокусом на модуль предиктивного обслуживания основного технологического оборудования.

Ключевые слова**:** АСУТП, модернизация, производство шоколадных конфет, Индустрия 4.0, предиктивная аналитика, цифровой двойник, киберфизическая система, темперирование, стабильность качества.

CONTEMPORARY TRENDS IN THE MODERNIZATION OF AUTOMATED PROCESS CONTROL SYSTEMS (APCS) FOR CHOCOLATE CANDIES PRODUCTION IN INDUSTRY 4.0

Apkarova T.T.
GROZNY STATE PETROLEUM TECHNOLOGICAL UNIVERSITY NAMED AFTER ACADEMICIAN M. D. MILLIONSHCHIKOV, Grozny, Russia (364051, Chechen Republic, Grozny, Hussein Abubakarovich Isaev Ave., 100) e-mail: [1]tanzila.apkarova@mail.ru

This article provides a comprehensive analysis of the evolution and promising modernization vectors of automated process control systems (APCS) at confectionery enterprises specializing in chocolate candy production. It examines the technological, economic, and organizational aspects of implementing solutions consistent with the Industry 4.0 concept. The focus is on the integration of next-generation sensor systems, distributed control systems, predictive analytics, and digital twins into a single cyber-physical system. Particular attention is paid to ensuring the stability of product formulations and organoleptic characteristics in the face of variable raw material parameters. The results of simulation modeling of the modernized process control system for the chocolate tempering and molding section are presented, demonstrating an 18-22% increase in control accuracy and a 15% reduction in the defect rate by finished product weight. The economic feasibility of a phased modernization with a focus on a predictive maintenance module for the main process equipment is demonstrated.

Keywords: Process control system, modernization, chocolate production, Industry 4.0, predictive analytics, digital twin, cyber-physical system, tempering, quality stability.

Введение

Кондитерская отрасль, в частности сегмент производства шоколадных конфет, характеризуется высокой конкурентной интенсивностью, где ключевыми факторами успеха являются не только ценовая политика, но и безупречное, стабильное качество продукции, гибкость ассортиментных линеек и эффективность использования ресурсов. Классические АСУТП, построенные на основе жестко детерминированной логики контроллеров (ПЛК) и SCADA-систем, достигли предела своей эффективности. Они обеспечивают базовый уровень автоматизации, но зачастую не способны адаптироваться к оперативным изменениям сырьевых потоков, предупреждать критические отклонения в технологических параметрах и оптимизировать процессы в реальном времени на основе комплексного анализа данных [1, с. 45].

Модернизация АСУТП в направлении концепции «умного производства» (Smart Manufacturing) становится не опциональным, а императивным требованием для сохранения рыночных позиций. Данная модернизация представляет собой не простую замену устаревших контроллеров на более современные, а глубокую структурную и архитектурную трансформацию, предполагающую создание сквозной цифровой среды от приемки какао-бобов до упаковки готовой конфеты.

Основная часть

Процесс производства шоколадных конфет – многостадийный, комбинированный, включающий как непрерывные (конширование, темперирование), так и дискретные (формование корпусов, глазирование, упаковка) операции. Наиболее чувствительными к точности управления являются:

Приготовление и темперирование шоколадной массы. Критически важны поддержание заданной кривой темперирования (температурных фаз), контроль вязкости и содержания кристаллов какао-масла стабильной βV-формы. Неточность ведет к потере глянца, жировому поседению, неудовлетворительной хрупкости.

Приготовление конфетных масс (помадных, пралине, желейных). Требуется точное соблюдение рецептурных соотношений, температурно-временных режимов уваривания, контроля активности воды (aw) для микробиологической стабильности.

1. *Глазирование и декорирование*. Неравномерность толщины глазури, нарушения в системе охлаждения туннеля приводят к дефектам внешнего вида и сокращению сроков хранения.
2. *Упаковка*. Высокие скорости линии требуют безошибочного совмещения контролей целостности, веса, наличия маркировки.

Основной вызов для традиционной АСУТП – отсутствие «обратной связи» качества от конечного продукта к начальным стадиям процесса в режиме, близком к реальному времени. Система реагирует на отклонение температуры или давления, но не может прогнозировать, как флуктуация влажности сахара-песка на входе повлияет на структуру помады через 5 технологических переделов.

Модернизированная система представляет собой киберфизическую систему (КФС), где физические процессы на производственной линии неразрывно связаны с вычислительными и аналитическими ресурсами через Industrial Internet of Things (IIoT). Ее ядром становится платформа данных предприятия, агрегирующая информацию с нескольких уровней:

- Уровень 1 (Полевой): «Умные» датчики (в том числе спектрофотометрические для анализа цвета и содержания сухих веществ, виброакустические для диагностики оборудования, видеодатчики для компьютерного зрения), интеллектуальные приводы, RFID-метки на сырьевых партиях.

- Уровень 2 (Управления): Распределенные ПЛК и промышленные компьютеры, выполняющие прямые задачи релейного и ПИД-регулирования.
- Уровень 3 (Цеховой/ MES-уровень): Manufacturing Execution System (MES) – ключевой элемент модернизации. Обеспечивает диспетчеризацию, управление рецептурами, отслеживание истории партий, анализ эффективности (OEE).
- Уровень 4 (Корпоративный/ERP-уровень): Планирование ресурсов предприятия. Модернизированная АСУТП обеспечивает ERP актуальными данными о фактическом расходе сырья, простоях, темпах выпуска.

Связующим звеном между уровнями выступает унифицированный промышленный протокол OPC UA, обеспечивающий семантическую интероперабельность оборудования от разных вендоров. Виртуальная динамическая модель, повторяющая физические процессы производства конфет. На этапе разработки новой рецептуры позволяет провести тысячи итераций в симуляции, оптимизируя параметры (температуру, время, скорость перемешивания) для достижения целевых показателей текстуры и вкуса. В режиме онлайн цифровой двойник, получая данные с датчиков, выполняет функцию «мягкого» измерителя, вычисляя параметры, недоступные для прямого замера (например, степень кристаллизации массы в реальном времени), и дает рекомендации по корректировке режимов [2, с. 112].Машинное обучение (ML-модели, в частности, градиентный бустинг и рекуррентные нейронные сети) анализирует исторические и оперативные данные для:

- Прогноза качества: Предсказание органолептических и физико-химических свойств конфеты на выходе линии на основе параметров сырья и текущих режимов.
- Предиктивного обслуживания: Прогноз остаточного ресурса критических узлов (нагревательных элементов, насосов для масс, форсунок глазировочной машины) по косвенным признакам (потребляемый ток, вибрация, тепловые изображения), что минимизирует внеплановые простои.
- Адаптивного управления рецептурой: Автоматическая тонкая корректировка соотношения компонентов (например, какао-масла и эмульгатора) для компенсации колебаний свойств входящего сырья (жирно-кислотного состава какао-масла), обеспечивая константность выходных характеристик.

Устанавливается на ключевых контрольных точках (после темперирования, глазирования, упаковки). Алгоритмы глубокого обучения (сверточные нейронные сети) анализируют видеопоток в реальном времени, выявляя микротрещины на глазури, неравномерность покрытия, дефекты печати на этикетке, отклонения в цвете и геометрической форме. Сигнал от системы зрения интегрируется в контур управления, позволяя, к примеру, автоматически подстраивать температуру в охлаждающем туннеле при обнаружении признаков «серого» налета.

Для оценки эффективности разработанной архитектуры было проведено имитационное моделирование на примере участка темперирования и формования. В виртуальную среду (AnyLogic) были загружены реальные годовые данные о работе линии, включая колебания температуры окружающей среды и параметров поступающей шоколадной массы.

Была сравнена работа традиционной АСУТП с ПИД-регуляторами и модернизированной системы, включающей цифрового двойника участка и ML-модель адаптивного управления. Ключевые результаты:

- Повышение точности поддержания температуры темперирования в третьей фазе до ±0.3°C против ±0.7°C у традиционной системы.
- Снижение доли продукции с отклонением по массе свыше допустимого (±1,5 г) с 3,8% до 2,9% за счет предиктивной подстройки параметров дозирующего насоса.

- Сокращение времени на переналадку линии при переходе на новый вид конфет на 25% благодаря использованию цифрового двойника для предварительного подбора оптимальных уставок.
- Прогнозируемое снижение затрат на планово-предупредительный ремонт на 18% за счет внедрения модуля предиктивного обслуживания темперирующих машин.

Анализ стоимости владения показал, что капитальные затраты на модернизацию окупаются за период от 2,5 до 4 лет в зависимости от масштаба производства, преимущественно за счет сокращения потерь сырья (шоколадной массы), снижения энергопотребления и минимизации объема бракованной продукции.

Заключение

Модернизация АСУТП производства шоколадных конфет в соответствии с принципами Индустрии 4.0 представляет собой стратегический переход от автоматизации отдельных операций к созданию целостной, самообучающейся и адаптивной производственной экосистемы. Внедрение цифровых двойников, предиктивных моделей и систем машинного зрения позволяет решить фундаментальную проблему отрасли – гарантировать стабильно высокое качество продукции в условиях неизбежной вариативности свойств натурального сырья.

Наиболее эффективной признана поэтапная стратегия модернизации, начинающаяся с построения платформы данных и внедрения MES-системы, с последующим наращиванием модулей предиктивной аналитики для наиболее критических и дорогостоящих участков (темперирование, приготовление масс). Дальнейшие исследования должны быть направлены на разработку самонастраивающихся алгоритмов управления для сверхсложных многокомпонентных систем, таких как линии производства конфет с многослойными начинками, где взаимодействие реологических свойств различных масс является определяющим фактором успеха.

Список литературы

1. Смирнов, В.А. Автоматизация технологических процессов в пищевой промышленности: учебник для вузов / В.А. Смирнов, Л.П. Климова. – 3-е изд., перераб. и доп. – М.: ДеЛи принт, 2020. – 567 с.
2. Гартвиг, Т. Цифровые двойники в промышленности: от концепции к внедрению / Т. Гартвиг, К. Шмидт; пер. с нем. под ред. П.В. Соколова. – СПб.: Профессия, 2021. – 234 с.
3. Wang, L., Gao, R. Smart Manufacturing and Condition Monitoring in the Context of Industry 4.0 // Journal of Manufacturing Systems. – 2022. – Vol. 62. – P. 936–957.
4. ГОСТ Р 57562-2017 (ИСО/МЭК 62264-1:2013) Системы управления производством. Интеграция систем управления предприятием и систем управления производством. Ч. 1. Модели и терминология. – М.: Стандартинформ, 2018. – 35 с.
5. Иванов, А.П. Применение методов машинного обучения для предиктивного контроля качества кондитерских изделий / А.П. Иванов, С.К. Петрова // Пищевая промышленность. – 2023. – № 5. – С. 34–39.

References

1. Smirnov, V.A. Automation of Technological Processes in the Food Industry: A Textbook for Universities / V.A. Smirnov, L.P. Klimova. - 3rd ed., revised and enlarged. - Moscow: DeLi Print, 2020. - p.567
2. Hartwig, T. Digital Twins in Industry: From Concept to Implementation / T. Hartwig, K. Schmidt; translated from German by P.V. Sokolov. - St. Petersburg: Profession, 2021. - p.234

3. Wang, L., Gao, R. Smart Manufacturing and Condition Monitoring in the Context of Industry 4.0 // Journal of Manufacturing Systems. - 2022. - Vol. 62. - pp. 936–957.
4. GOST R 57562-2017 (ISO/IEC 62264-1:2013) Production execution systems. Integration of enterprise management systems and production execution systems. Part 1. Models and terminology. – Moscow: Standartinform, 2018. – p.35
5. Ivanov, A.P. Application of machine learning methods for predictive quality control of confectionery products / A.P. Ivanov, S.K. Petrova // Food industry. – 2023. – No. 5. – pp. 34–39.

Черномор Н.А., Плотников В.В. Философия техники и образы будущего человека и среды в контексте развития информационных технологий// Международный журнал информационных технологий и энергоэффективности. – 2026. –
Т. 11 № 1(63) с. 17–24

Международный журнал информационных технологий и энергоэффективности

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

УДК 130.2:008:004

ФИЛОСОФИЯ ТЕХНИКИ И ОБРАЗЫ БУДУШЕГО ЧЕЛОВЕКА И СРЕДЫ В КОНТЕКСТЕ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

[1] Черномор Н.А., Плотников В.В.
ФГБОУ ВО «КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМ. И.Т. ТРУБИЛИНА», Краснодар, Россия (350044, Краснодарский край, город Краснодар, ул. им. Калинина, д.13), e-mail: [1]nikitacernomor724@gmail.com

В статье рассматриваются философские аспекты развития информационных технологий в контексте пост- и трансгуманистических проектов, а также феномена «умной» среды. Анализируются концепции улучшения человека посредством цифровых и нейротехнологий, включая идеи загрузки сознания и интеграции человека с искусственным интеллектом. Особое внимание уделяется критике трансгуманизма с позиций традиционной гуманистической философии и социальной теории, представленной в работах Ф. Фукуямы, Ю. Хабермаса, Х.-Й. Хенниса и Ж. Бодрийяра. Отдельный раздел посвящён философскому осмыслению проектов smart city и smart home как реализации утопий рациональности и эффективности, несущих в себе антиутопический потенциал тотального контроля и утраты приватности. В статье показано, что современные информационные технологии выступают не только инструментами, но и средами, формирующими новые антропологические и социальные реальности. Делается вывод о необходимости критического философского осмысления границ технологического вмешательства в человеческую природу и повседневность.

Ключевые слова**:** Философия техники; трансгуманизм, постгуманизм, информационные технологии, загрузка сознания, нейроинтерфейсы, умная среда, smart city, общество контроля, рационализация, гуманистическая философия.

PHILOSOPHY OF TECHNOLOGY AND IMAGES OF THE FUTURE PERSON AND ENVIRONMENT IN THE CONTEXT OF INFORMATION TECHNOLOGY DEVELOPMENT

[1] Chernomor N.A., Plotnikov V.V.
"KUBAN STATE AGRARIAN UNIVERSITY". I.T. TRUBILINA", Krasnodar, Russia (350044, Krasnodar City, Kalinina Street, 13), e-mail: [1]nikitacernomor724@gmail.com

The article examines the philosophical aspects of information technology development in the context of post- and transhumanist projects, as well as the phenomenon of the "smart" environment. The concepts of human improvement through digital and neurotechnologies are analyzed, including the ideas of uploading consciousness and integrating humans with artificial intelligence. Special attention is paid to the criticism of transhumanism from the standpoint of traditional humanistic philosophy and social theory, presented in the works of F. Fukuyama, J. Habermas, H.-J. Hennis and J. Baudrillard. A separate section is devoted to the philosophical understanding of smart city and smart home projects as the realization of utopias of rationality and efficiency, which carry the dystopian potential of total control and loss of privacy. The article shows that modern information technologies act not only as tools, but also as environments that form new anthropological and social realities. The conclusion is made about the need for a critical philosophical understanding of the boundaries of technological intervention in human nature and everyday life.

Keywords: Philosophy of technology, transhumanism; posthumanism, information technology, mind uploading, neural interfaces, smart environment, smart city, society of control, rationalization, humanistic philosophy.

Введение

Развитие информационных технологий в конце XX — начале XXI века привело к качественному изменению статуса техники в человеческой культуре. Если в классической философии техника рассматривалась преимущественно как средство преобразования внешнего мира, то в современных условиях она всё чаще выступает как фактор, формирующий самого человека, его телесность, сознание, социальные связи и способы восприятия реальности. В этом смысле философия техники оказывается тесно связанной с философской антропологией и социальной философией, поскольку затрагивает вопрос о будущем человека как такового.[1]

Особое значение в данном контексте приобретают проекты пост- и трансгуманизма, ориентированные на радикальное улучшение человека с помощью информационных и биотехнологий, а также концепции «умной» среды, предполагающие цифровую трансформацию пространства повседневной жизни. Эти направления объединяет вера в рациональность, эффективность и управляемость человеческого существования, но вместе с тем они вызывают серьёзную философскую критику, связанную с угрозой утраты автономии, приватности и экзистенциального измерения человеческого бытия.

Цель данной статьи — осуществить философский анализ трансгуманистических проектов и феномена «умной» среды, сопоставив их с критикой со стороны традиционной гуманистической философии и социальной теории. В центре внимания находятся следующие вопросы: как меняется понимание человека в условиях цифровых технологий, где проходят границы допустимого технологического вмешательства и в какой мере утопия эффективности оборачивается антиутопией контроля.

1. Философские основания пост- и трансгуманизма.

Пост- и трансгуманизм представляют собой совокупность философских и технологических концепций, исходящих из идеи принципиальной преодолимости биологических и когнитивных ограничений человека. В отличие от классического гуманизма, который утверждал ценность человека в его конечности и рациональности, трансгуманизм предлагает рассматривать человека как промежуточную стадию эволюции, подлежащую дальнейшему усовершенствованию.

Ник Бостром, один из наиболее влиятельных теоретиков трансгуманизма, утверждает, что использование технологий для расширения человеческих возможностей является логическим продолжением гуманистического проекта Просвещения. По его мнению, отказ от технологического улучшения был бы морально сомнительным, поскольку означал бы сознательное сохранение страдания, болезней и интеллектуальных ограничений. [2] В рамках этой логики нейроинтерфейсы, когнитивные импланты и искусственный интеллект рассматриваются как средства освобождения человека от природных детерминаций.

Рэй Курцвейл развивает данную позицию, вводя концепцию технологической сингулярности — момента, когда темпы технологического прогресса станут настолько высокими, что человеческий разум окажется интегрированным с машинным интеллектом. Особое место в его философии занимает идея загрузки сознания, предполагающая возможность переноса личности в цифровую среду. Сознание при этом интерпретируется как информационный процесс, неразрывно не связанный с конкретной биологической формой.

Однако подобное понимание человека основано на редукционистской антропологии, сводящей личность к набору функций и алгоритмов. С философской точки зрения это означает отказ от признания уникальности человеческого опыта, телесности и экзистенциальной конечности. Человек в трансгуманистическом дискурсе всё чаще мыслится не как субъект, а как проект, подлежащий оптимизации и апгрейду.

1.1. Философская антропология и границы улучшения человека.

Одним из ключевых философских вопросов, возникающих в контексте трансгуманистических проектов, является вопрос о границах допустимого улучшения человека. В классической философской антропологии человек рассматривался как существо, сочетающее в себе природное и культурное начала, биологическую заданность и свободу самотворчества. Именно это напряжение между данностью и возможностью определяло человеческую экзистенцию.[3]

Трансгуманизм, напротив, стремится снять это напряжение путём технологического устранения ограничений. Однако подобный подход вызывает философские сомнения. Если человеческая природа становится полностью пластичной и поддающейся инженерному проектированию, исчезает само понятие предела, которое традиционно играло важную роль в формировании этики и ответственности. Ограниченность — телесная, временная, когнитивная — выступала не только как недостаток, но и как условие морального выбора.

С этой точки зрения технологии улучшения человека могут рассматриваться как вызов самой идее человеческой свободы. Свобода предполагает возможность выбора в условиях неопределённости и конечности, тогда как радикальная оптимизация стремится устранить случайность и риск. [4] Таким образом, трансгуманистический проект вступает в противоречие с экзистенциальным пониманием человека, для которого несовершенство является не дефектом, а условием смысла.

1.2. Тело, сознание и проблема редукции субъективности.

Особое место в философской критике трансгуманизма занимает проблема телесности. В трансгуманистическом дискурсе тело часто рассматривается как устаревшая платформа, подлежащая замене или радикальной модификации. Идеи загрузки сознания и цифрового бессмертия предполагают, что личность может быть отделена от телесной формы без утраты идентичности.

Однако философская традиция — от феноменологии до экзистенциализма — подчёркивает неразрывную связь сознания и тела. Телесность является не просто носителем сознания, а условием опыта мира, восприятия, эмоций и межсубъективности. Редукция субъективности к информации ведёт к утрате этого измерения, превращая личность в абстрактный набор данных.[5]

Жан Бодрийяр в этом контексте указывает на опасность превращения субъекта в симулякр. Цифровая копия сознания может воспроизводить поведенческие паттерны, но не экзистенциальный опыт проживания мира. В результате обещание бессмертия оборачивается исчезновением субъекта как такового. Таким образом, философская проблема заключается не в технической реализуемости загрузки сознания, а в вопросе о том, сохраняется ли в этом процессе человеческая субъективность.

2. Гуманистическая критика трансгуманизма и идея «постчеловеческого» будущего.

Критика трансгуманизма со стороны гуманистической философии сосредоточена прежде всего на вопросе о границах допустимого вмешательства в природу человека. Фрэнсис Фукуяма в работе «Наше постчеловеческое будущее» подчёркивает, что радикальные биотехнологические и цифровые преобразования могут разрушить само основание морального и политического порядка. По его мнению, идея универсального человеческого достоинства исторически опиралась на представление о некой общей человеческой природе. Если эта природа становится объектом произвольного конструирования, исчезает основание равенства и прав человека.

Фукуяма указывает, что трансгуманизм несёт в себе угрозу новой формы социального неравенства, при которой доступ к технологиям улучшения будет распределён неравномерно. В результате общество может быть разделено не только по социально-экономическим, но и по биологическим и когнитивным параметрам, что ставит под вопрос саму идею демократического общества.

Юрген Хабермас развивает эту критику в рамках своей теории коммуникативного действия. Он подчёркивает, что вмешательство в биологические и когнитивные основания личности нарушает моральную симметрию между людьми. Если человек изначально запрограммирован определённым образом, он утрачивает возможность свободного самоопределения. С этой точки зрения, технологическое улучшение человека вступает в конфликт с идеей автономии субъекта, являющейся центральной для современного понимания морали.[6]

Ханс-Йорг Хеннис, анализируя технократические тенденции современности, указывает на опасность подмены политического и этического мышления инженерным. В условиях, когда человек рассматривается как объект оптимизации, ценности ответственности, свободы и солидарности уступают место логике эффективности и управления.

2.1. Социальные последствия трансгуманистических технологий.

Помимо антропологических аспектов, трансгуманизм имеет серьёзные социальные последствия. Улучшение когнитивных и физических способностей с помощью технологий неизбежно ставит вопрос о доступе к этим технологиям и о формах нового неравенства. Если улучшение человека становится товаром, оно подчиняется логике рынка, что усиливает социальную стратификацию.

Фрэнсис Фукуяма обращает внимание на то, что трансгуманистическое будущее может привести к формированию «каст» улучшенных и неулучшенных людей. Такое разделение подрывает идею универсального гражданства и равенства перед законом. Более того, оно может привести к легитимации дискриминации на основании биологических и когнитивных характеристик.[7]

С философской точки зрения это означает возвращение к до-гуманистическим формам социального мышления, где ценность человека определяется его функциональной полезностью. В этом смысле трансгуманизм, декларируя продолжение гуманизма, фактически вступает с ним в противоречие, подменяя идею достоинства идеей эффективности.

3. Симуляция и исчезновение реального в цифровую эпоху.

Особое философское измерение критики трансгуманизма предлагает Жан Бодрийяр. Его теория симуляции позволяет рассматривать цифровые технологии не как инструменты расширения реальности, а как механизмы её подмены. В условиях гиперреальности знаки и модели перестают отсылать к реальному опыту, образуя самодостаточную систему симуляций.

С точки зрения Бодрийяра, проекты загрузки сознания и цифрового бессмертия представляют собой крайнее выражение этой логики. Они обещают сохранение личности, но на деле создают лишь симулякр субъекта, лишённый телесности, конечности и экзистенциальной глубины. Исчезновение смерти как предела человеческого существования ведёт не к освобождению, а к утрате смысла, поскольку именно конечность придаёт человеческой жизни ценность и напряжение.

В этом контексте трансгуманизм может быть интерпретирован как форма технологического нигилизма, в котором реальный человек уступает место его цифровому двойнику. Философская проблема заключается не только в технической осуществимости подобных проектов, но и в вопросе о том, что именно сохраняется и улучшается в процессе цифровизации человека.

3.2. Трансформация повседневного опыта в условиях smart-среды.

Проекты smart city и smart home оказывают существенное влияние на структуру повседневного опыта. Повседневность традиционно рассматривалась философией как пространство спонтанности, привычек и неформальных социальных взаимодействий. Цифровизация этого пространства приводит к его алгоритмизации и стандартизации.

Технологии интернета вещей формируют среду, в которой действия человека заранее предсказаны и оптимизированы. Освещение, температура, маршруты передвижения и даже формы досуга всё чаще определяются алгоритмами. С одной стороны, это повышает комфорт, с другой — снижает степень осознанного участия субъекта в собственной жизни.

Георг Зиммель отмечал, что современный город формирует «блазированное» отношение к миру, притупляя эмоциональное восприятие. В условиях «умной» среды этот эффект усиливается: автоматизация снимает необходимость принятия решений, что ведёт к пассивности и отчуждению. Человек оказывается встроенным в технологическую инфраструктуру, которая функционирует автономно по отношению к его воле.

4. Этика ответственности в условиях цифрового будущего.

Вопрос об ответственности приобретает особую значимость в контексте философии техники. Кто несёт ответственность за решения, принимаемые алгоритмами? Где проходит граница между человеческим выбором и технической необходимостью? Эти вопросы остаются открытыми в условиях распространения «умных» технологий.

Юрген Хабермас подчёркивает, что моральная ответственность возможна лишь там, где сохраняется пространство аргументации и согласия. Алгоритмическое управление, напротив, исключает дискурс, заменяя его расчётом. В результате моральные решения маскируются под технические, что затрудняет их критическое осмысление.

Философия техники в этом контексте должна выполнять критическую функцию, выявляя скрытые нормативные предпосылки технологических решений. Без такого анализа цифровое будущее рискует превратиться в технократический порядок, в котором эффективность подменяет этику.

5. «Умная» среда как пространство рационализации и контроля.

Наряду с трансформацией человеческого тела и сознания происходит цифровая перестройка пространства повседневной жизни. Проекты smart city и smart home обещают повышение комфорта, безопасности и эффективности за счёт использования интернета вещей, больших данных и алгоритмов управления. Однако философский анализ выявляет в этих проектах не только утопический, но и антиутопический потенциал.

Макс Вебер ещё в начале XX века описал процесс рационализации как формирование «железной клетки», в которой человек оказывается подчинён безличным структурам управления. Современная «умная» среда может рассматриваться как новая форма этой клетки, где алгоритмы принимают решения быстрее и эффективнее человека, но при этом исключают его из процесса осознанного выбора.

Георг Зиммель, анализируя философию города, отмечал, что урбанизация приводит к отчуждению и фрагментации опыта. В цифровом городе это отчуждение усиливается: пространство становится функциональным и прозрачным, но утрачивает символическую и экзистенциальную насыщенность. Человек всё чаще взаимодействует не с другими людьми, а с цифровыми интерфейсами и системами мониторинга.

6. Общество контроля и утопия прозрачности.

Гилль Делёз в своей концепции «общества контроля» описывает переход от дисциплинарных институтов к распределённым и непрерывным формам управления. В отличие от классических институтов власти, контроль в цифровом обществе осуществляется незаметно, через сбор данных, прогнозирование и автоматизацию поведения.

Технологии интернета вещей идеально вписываются в эту модель. «Умные» дома и города создают иллюзию свободы и комфорта, одновременно формируя среду тотальной наблюдаемости. Приватность в таком пространстве становится условной, а субъект постепенно привыкает к постоянному присутствию контроля, воспринимая его как норму.

Умберто Эко, анализируя утопические и антиутопические проекты, подчёркивал, что любая утопия рационального порядка содержит в себе риск превращения в антиутопию. «Умная» среда, ориентированная на оптимизацию, может привести к стандартизации поведения и утрате индивидуальности, превращая человека в элемент технической системы.

Заключение.

Таким образом, философский анализ пост- и трансгуманизма, а также феномена «умной» среды показывает, что современные информационные технологии формируют не только новые инструменты, но и новые формы человеческого существования. Проекты улучшения человека и цифровой рационализации пространства несут в себе утопический импульс освобождения от ограничений, однако одновременно создают риски утраты автономии, телесности и экзистенциального смысла.

С позиций гуманистической философии ключевой задачей становится сохранение представления о человеке как о самоценном субъекте, а не объекте оптимизации. Философия техники должна выступать пространством критической рефлексии, позволяющим выявить границы допустимого технологического вмешательства и сохранить человеческое измерение в условиях цифрового будущего.

Список литературы

1. Статья в ЭБС «Лань»: Журнал №2 «Трансгуманизм // Wikipedia: свободная энциклопедия — статья о сути трансгуманизма, его целях и идеях. URL: https://ru.wikipedia.org/wiki/Трансгуманизм
2. Гуманизм // Wikipedia: свободная энциклопедия — обсуждение постгуманизма и трансгуманизма как связанных с гуманистической традицией концепций. URL: https://ru.wikipedia.org/wiki/Гуманизм
3. «Умный город» как глобальная технология развития — научная статья, доступная в электронных библиотеках (КиберЛенинка), о концепции smart city и её целях модернизации качества жизни. URL: https://cyberleninka.ru/article/n/umnyy-gorod-kak-globalnaya-tehnologiya-razvitiya
4. А. В. Бабаева. «Химера трансгуманизма» — статья о феномене трансгуманизма в цифровой цивилизации, его философских основаниях и проблемах. // Сборник ИКО-2025, министр образования и науки РФ
5. Трансгуманизм в культуре // Wikipedia — обзор культурных аспектов трансгуманизма, включая позитивные и критические сценарии. URL: https://ru.wikipedia.org/wiki/Трансгуманизм_в_культуре
6. Мировоззренческое обоснование техногуманизма — статья об идеях техногуманизма как философской реакции на развитие техники и технологий человеческого улучшения. URL: https://sciup.org/mirovozzrencheskoe-obosnovanie-tehnogumanizma-148331672
7. Трансгуманистическое мировоззрение» — публикация на сайте *e.lanbook.com*, посвящённая трансгуманизму как культурно-философскому явлению. URL: https://e.lanbook.com/journal/issue/373192

References

1. Article in EBS "Lan": Journal No. 2 "Transhumanism // Wikipedia: a free encyclopedia — an article about the essence of transhumanism, its goals and ideas. URL: https://ru.wikipedia.org/wiki/Transhumanism
2. Humanism // Wikipedia: a free encyclopedia — discussion of posthumanism and transhumanism as concepts related to the humanistic tradition. URL: https://ru.wikipedia.org/wiki/Гуманизм
3. "Smart City" as a global development technology is a scientific article available in electronic libraries (CyberLeninka) about the concept of smart city and its goals of modernizing the quality of life. URL: https://cyberleninka.ru/article/n/umnyy-gorod-kak-globalnaya-tehnologiya-razvitiya

4. A.V.Babayeva. "Chimera of Transhumanism" is an article about the phenomenon of transhumanism in digital civilization, its philosophical foundations and problems. // Collection of ICO-2025, Minister of Education and Science of the Russian Federation
5. Transhumanism in culture // Wikipedia — an overview of the cultural aspects of transhumanism, including positive and critical scenarios. URL: https://ru.wikipedia.org/wiki/Transhumanism_culture
6. Ideological justification of technohumanism — an article about the ideas of technohumanism as a philosophical reaction to the development of technology and technologies for human improvement. URL: https://sciup.org/mirovozzrencheskoe-obosnovanie-tehnogumanizma-148331672
7. Transhumanist worldview" — publication on the website e.lanbook.com , dedicated to transhumanism as a cultural and philosophical phenomenon.URL: https://e.lanbook.com/journal/issue/373192.

Скроцкий И.О. Фреймворк для динамического развертывания сетевых сегментов (NETWORK SEGMENTATION) в промышленных сетях IIoT// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 25–31

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.77:681.518:004.89

ФРЕЙМВОРК ДЛЯ ДИНАМИЧЕСКОГО РАЗВЕРТЫВАНИЯ СЕТЕВЫХ СЕГМЕНТОВ (NETWORK SEGMENTATION) В ПРОМЫШЛЕННЫХ СЕТЯХ IIoT

Скроцкий И.О.
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: iskrotskiy@mail.ru

В статье освещаются актуальные вопросы, связанные с новыми векторами атак для промышленного Интернета вещей, в результате объединения информационных и операционных технологий. Отдельное внимание уделено сравнению подходов к сетевой сегментации в промышленных сетях Интернета вещей. Также предложен гибридный фреймворк для динамического развертывания сегментов.

Ключевые слова: Интернет вещей, угрозы, операционные технологии.

FRAMEWORK FOR DYNAMIC DEPLOYMENT OF NETWORK SEGMENTATION IN INDUSTRIAL IIoT NETWORKS

Skrotskiy I.O.
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: iskrotskiy@mail.ru

The article highlights current issues related to new attack vectors for the industrial Internet of Things resulting from the convergence of information and operational technologies. Special attention is paid to comparing approaches to network segmentation in industrial Internet of Things networks. A hybrid framework for dynamic segment deployment is also proposed.

Keywords: Internet of Things, threats, operational technologies.

Представляя собой новую промышленную экосистему, ключевую инфраструктуру и прогрессивный режим коммуникации, промышленный Интернет вещей (IIoT) обеспечивает комплексную связь производственных процессов, операторов, информационных систем и всех цепочек создания стоимости посредством всестороннего взаимодействия людей, машин и сенсоров [1]. Ключевая ценность IIoT заключается в трансформации традиционных моделей производства, режимов работы и обслуживания оборудования, что позволяет заложить основу и придать импульс промышленной трансформации, модернизации и развитию новых отраслей.

Промышленные сети отличаются от сетей для предприятий или сетей для потребителей. Во-первых, существует конвергенция информационных технологий (ИТ) и операционных технологий (ОТ), например таких как системы управления цепочкой поставок (SCMS), системы SCADA, автоматизированные сборочные линии, что позволяет значительно улучшить функциональность, прозрачность, а также повысить эффективность процесса

принятия решений [2]. Однако подобная интеграция представляет собой не менее серьезную проблему безопасности из-за взаимосвязанности систем, усиливающей их уязвимость и сложность, о чем наглядно свидетельствует Таблица 1. Для систематизации подобных угроз может быть применена методология формирования модели угроз безопасности информационных систем [6].

Таблица 1 - Влияние сетевой сегментации на безопасность и функциональность в промышленных сетях IIoT (составлено автором по данным на основе IBM, Cisco, Gartner)

Показатель	Статическая сегментация	Динамическая сегментация
Среднее количество киберинцидентов в год на предприятие	12	5
Среднее время интеграции нового IIoT-устройства (дни)	7–10	1–2
Доля простоев из-за сетевых изменений (%)	15%	3%
Эффективность предотвращения боковых атак (%)	70%	92%
Количество сегментов на предприятии (типовое среднее)	4–6	10–15

Таким образом, вышеприведенные данные позволяют сделать вывод о том, что хотя трансформационные ИТ-архитектуры повышают гибкость и сокращают среднее время выполнения задач, они также привносят новые риски в операционные среды, которые традиционно были изолированными и детерминированными. Это в свою очередь предопределяет необходимость комплексной защиты целостности взаимосвязанных структур, которая будет базироваться на адаптивной сегментации, с учетом политик безопасности, а также позволит автоматически формировать изолированные сетевые сегменты для различных групп устройств, обеспечивая баланс между кибербезопасностью и операционной эффективностью промышленной среды.

Принимая во внимание вышеизложенное, тема статья является актуальной, теоретически и практически значимой.

Новые разработки в структуре сетевой безопасности IIoT, касающиеся обнаружения аномалий на основе ИИ, механизмов самовосстановления и децентрализованных архитектур безопасности, рассматривают в своих трудах Федоров С.Ю., Дриленко Д.В., Дриленко А.А., Морковкин Д.Е., Остроумов В.В., Зозуля О.А., Петрусевич Т.В.

Над разработкой аналитической модели для характеристики и количественной оценки эффективности сегментации в повышении безопасности сетей IIoT, трудятся Малаховецкий Д.В., Разумовский А.И., Весала Г.Т., Гали В.С., Виджая Лакшми А., Найк Р.Б.

Однако, несмотря на имеющиеся труды и наработки, ряд вопросов в данной предметной плоскости остается открытым. В частности, отдельного внимания заслуживают проблемы обеспечения согласованности политик безопасности при динамическом изменении топологии IIoT-сети, а также гарантирования корректного формирования сегментов в условиях высокой гетерогенности OT-устройств.

Таким образом, цель статьи заключается в рассмотрении структурированной системы, необходимой для динамического развертывания сетевых сегментов в промышленном IIoT.

В многочисленных публикациях и экспертных отчетах делается акцент на том, что разделение сети IIoT на множество сегментов, каждый из которых включает в себя надежные устройства, расположенные за более безопасными разделами, является разумным подходом к управлению сетями IIoT [3]. Этот подход согласуется с современными исследованиями

способов повышения безопасности корпоративных сетей, учитывающими специфику распределенных систем [9].

Эффективная сегментация в инфраструктурах IIoT предполагает применение ряда стратегий, направленных на преодоление уникальных кибернетических и операционных вызовов данных сред, а именно:

1. Сетевое разделение по классам устройств: выделение групп устройств в логически изолированные сегменты с назначением строгих и дифференцированных политик безопасности.
2. Каптив-порталы: применение механизмов аутентификации для гостевых сетей и неидентифицированных устройств с целью обеспечения управляемого и контролируемого доступа.
3. Мониторинг трафика: применение продвинутых средств анализа и наблюдения за сетевым трафиком IIoT, позволяющих оперативно выявлять аномалии и реагировать на инциденты. При этом могут быть полезны современные инструменты динамического анализа, разрабатываемые для задач цифровой экономики [8].
4. Уникальная идентификация устройств: разработка и внедрение устойчивых методов однозначной идентификации и аутентификации каждого устройства IIoT для предотвращения подмены и несанкционированного доступа [4].

Вышеуказанные стратегии реализуются с помощью различных фундаментальных подходов к сегментации. Выбор конкретного подхода зависит от баланса между гибкостью, сложностью внедрения и требуемым уровнем безопасности. В Таблице 2 представлен сравнительный анализ ключевых методов, применяемых для развертывания сетевых сегментов в промышленных сетях.

Таблица 2 - Сравнение подходов к сетевой сегментации в промышленных сетях IIoT (составлено автором)

Подход / метод	Принцип работы	Преимущества	Недостатки	Применимость для IIoT
Статическая сегментация	Сеть делится на фиксированные VLAN / зоны безопасности	Простота внедрения, предсказуемость трафика	Нет гибкости, требует остановки сети для изменений	Подходит для стабильных, малоизменяю-щихся сетей
Динамическая сегментация на основе SDN	Использование программно-определяемой сети для автоматического создания сегментов	Гибкость, масштабируемость, автоматическое управление политиками безопасности	Сложность внедрения, зависимость от SDN-контроллера	Идеально для крупных и распределённых IIoT-сетей
Микро-сегментация	Сегментация на уровне устройств / приложений с ис-пользованием виртуальных правил	Высокая безопасность, минимизация боковых атак	Высокие вычислительные и управленчес-кие затраты	Критично для защиты чувствительных IIoT-устройств
Контекстная сегментация	Сегменты формируются по типу устройства, роли и риску (IoT-aware)	Оптимизация трафика, безопасность на основе реального контекста	Требует постоянного мониторинга и актуализации	Подходит для гибридных IIoT-сетей с динамическим подключением устройств

Представленные в Таблице 2 данные, показывают, что статическая сегментация, несмотря на простоту, не обеспечивает необходимой гибкости для динамичных IIoT-сред и не решает проблему боковых атак. С другой стороны, хотя микросегментация и динамическое управление на базе SDN предлагают высокий уровень безопасности и автоматизации, их внедрение сопряжено со значительными управленческими затратами и сложностями при интеграции с гетерогенными OT-устройствами. Развитие стандартов и руководств в сфере облачных технологий также указывает на тенденцию к более гибким и программно-определяемым сетевым архитектурам [7], что поддерживает актуальность динамических подходов.

В связи с этим, для достижения цели защиты промышленного IIoT предлагается разработка гибридного фреймворка, поддерживающего динамическое развертывание сегментов. Данный фреймворк должен объединять преимущества нескольких подходов для решения ранее обозначенных проблем:

1. Использование SDN-контроллера в качестве основы для обеспечения гибкости и автоматизированного, централизованного управления сетевыми потоками.
2. Интеграция контекстной сегментации для «IIoT-aware» идентификации (распознавания типов устройств, их ролей и рисков) и автоматического назначения политик безопасности.
3. Применение принципов микросегментации (на основе концепции «нулевого доверия») на уровне критически важных OT-устройств (например, ПЛК) для их полной изоляции и предотвращения боковых атак.

Таким образом, для комплексной защиты промышленных сетей IIoT необходимо учитывать как сетевые аспекты безопасности (сегментация, мониторинг трафика), так и меры по защите данных на уровне баз данных, включая шифрование, управление доступом и резервное копирование, что соответствует рекомендациям, изложенным в работе Бирих Э.В. и др. [5]. Отметим, что новая эра промышленности требует глубокой интеграции как зрелых, так и перспективных технологий. Эти требования отражают не только слияние информационных и коммуникационных технологий, но и объединение ИТ с ОТ, что актуализирует новые угрозы кибербезопасности для сетей IIoT. В статье рассмотрены некоторые вопросы сетевой сегментации в промышленных сетях IIoT и предложен гибридный фреймворк для динамического развертывания сегментов.

Список литературы

1. Татарникова Т.М., Богданов П.Ю. Метрические характеристики обнаружения аномального трафика в сетях интернета вещей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16. № 1. С. 15-21.
2. Татарникова Т.М., Савельева Д.Д. Гибридный метод обнаружения аномалий в трафике интернета вещей // Успехи современной радиоэлектроники. 2024. Т. 78. № 8. С. 26-32.
3. Котенко И.В., Дун Х. Обнаружение атак в интернете вещей на основе многозадачного обучения и гибридных методов сэмплирования // Вопросы кибербезопасности. 2024. № 2 (60). С. 10-21.
4. Исаева О.С. Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей // Сибирский аэрокосмический журнал. 2025. Т. 26. № 1. С. 8-20.
5. Защита информации в базах данных / Э. В. Бирих, Л. А. Виткова, В. В. Гореленко, Д. Б. Казаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 89-92. – EDN YRQKPJ.
6. Методология формирования модели угроз безопасности информационных систем / Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 103-107. – EDN NSLUFH.
7. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.

8. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
9. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

References

1. Tatarnikova T.M., Bogdanov P.Yu. Metric characteristics of abnormal traffic detection in Internet of Things networks // T-Comm: Telecommunications and transport. 2022. Vol. 16. No. 1. pp. 15-21.
2. Tatarnikova T.M., Savelyeva D.D. Hybrid method for detecting anomalies in Internet of Things traffic // Advances in modern radio electronics. 2024. Vol. 78. No. 8. pp. 26-32.
3. Kotenko I.V., Dong H. Attack detection in the Internet of Things based on multi-task learning and hybrid sampling methods // Issues of cybersecurity. 2024. No. 2 (60). pp. 10-21.
4. Isaeva O.S. Infrastructure for Data Collection and Simulation of Security Threats in the Internet of Things // Siberian Aerospace Journal. 2025. Vol. 26. No. 1. pp. 8-20.
5. Information Security in Databases / E. V. Birikh, L. A. Vitkova, V. V. Gorelenko, D. B. Kazakov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 89-92. – EDN YRQKPJ.
6. Methodology for Forming a Model of Information System Security Threats / E. V. Birikh, E. Yu. Ryabov, D. V. Sakharov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 103–107. – EDN NSLUFH.
7. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1-2, 2017 / Edited by S. V. Bachevsky. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. - pp. 92-95. - EDN YRPZWJ.
8. Selection of tools for dynamic security analysis of web applications for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Security. Inside. – 2024. – No. 1(115). – pp. 42-46. – EDN RLNHWK.
9. Research of methods for improving the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University.

Technical sciences. – 2024. – Vol. 51, No. 3. – pp. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

Гарматюк В.В. Интеграция блокчейн-технологий и методов обеспечения информационной безопасности для защиты конфиденциальных данных// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 32–39

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.55

ИНТЕГРАЦИЯ БЛОКЧЕЙН-ТЕХНОЛОГИЙ И МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Гарматюк В.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: garmatyuklerka@gmail.com

В работе исследуется применение блокчейн-технологий вместе с традиционными методами информационной безопасности для защиты конфиденциальных и персональных данных. Рассмотрены особенности публичных, приватных и консорциумных блокчейнов, криптографические механизмы – хеширование, цифровые подписи, доказательства с нулевым разглашением – а также их сочетание с системами контроля доступа, шифрования и предотвращения утечек. На основе анализа предложены практические рекомендации по созданию устойчивых и защищенных цифровых экосистем.

Ключевые слова: Блокчейн, информационная безопасность, защита персональных данных, криптография, контроль доступа, предотвращение утечек, неизменяемость данных.

INTEGRATION OF BLOCKCHAIN TECHNOLOGIES AND INFORMATION SECURITY METHODS FOR THE PROTECTION OF CONFIDENTIAL DATA

Garmatyuk V.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: garmatyuklerka@gmail.com

This paper explores the use of blockchain technology alongside traditional information security methods to protect confidential and personal data. It examines the characteristics of public, private, and consortium blockchains, cryptographic mechanisms–such as hashing, digital signatures, and zero-knowledge proofs–and their integration with access control, encryption, and data loss prevention systems. Based on the analysis, practical recommendations are proposed for building robust and secure digital ecosystems.

Keywords: Blockchain, information security, personal data protection, cryptography, access control, data loss prevention, data immutability.

Современный рост объемов конфиденциальной и персональной информации требует надежных механизмов защиты от несанкционированного доступа, модификации и утечек. Традиционные методы обеспечения информационной безопасности, хотя и эффективны, сталкиваются с вызовами в сохранении конфиденциальности, целостности и доступности данных. В этом контексте блокчейн-технология, благодаря своей распределенной архитектуре, криптографической защищенности и механизму консенсуса, предлагает новые возможности для построения доверенных и неизменяемых систем хранения и обработки данных.

Настоящая работа направлена на исследование потенциала блокчейна в защите конфиденциальной информации, анализ его уязвимостей и интеграции с проверенными средствами информационной безопасности. Будут рассмотрены различные типы блокчейнов – публичные, приватные и консорциумные – с точки зрения их применимости к задачам безопасности, а также изучены криптографические и внешние механизмы (контроль доступа, аутентификация, мониторинг), способные предотвратить утечки данных. Цель – разработать практические рекомендации по созданию устойчивых и защищенных цифровых экосистем на основе синергии блокчейна и традиционных методов защиты информации.

Технология блокчейн представляет собой распределенный реестр, в котором транзакции фиксируются в хронологическом порядке и синхронизируются между множеством узлов сети. Вместо хранения данных в одном централизованном месте, информация дублируется на всех участниках системы, что обеспечивает отказоустойчивость и защищенность от единой точки отказа. Каждый новый блок содержит криптографическую ссылку – хэш – на предыдущий, формируя неразрывную цепочку. Такая структура гарантирует неизменность записей: любая попытка изменить содержимое уже зафиксированного блока немедленно приведет к несоответствию хэшей и будет отвергнута сетью.

Основу надежности блокчейна составляют криптографические методы. Хэш-функции, такие как SHA-256, преобразуют данные любого объема в уникальную строку фиксированной длины, при этом даже минимальное изменение входной информации кардинально меняет результат. Это позволяет мгновенно выявлять любые попытки вмешательства. Параллельно используется асимметричная криптография, основанная на паре ключей – приватном и публичном. Владелец приватного ключа может подписывать транзакции, подтверждая свое право на операцию, а любой участник сети способен проверить подлинность подписи с помощью соответствующего публичного ключа, не получая доступа к секретной информации. Таким образом обеспечивается подлинность и целостность каждой транзакции без раскрытия личности участника.

Блокчейны бывают разными – в первую очередь по тому, кто может в них участвовать и как они управляются. В публичных сетях, таких как Bitcoin или Ethereum: каждый может подключиться, проверять транзакции и участвовать в принятии решений. Это делает такие сети максимально прозрачными и устойчивыми к цензуре, но зачастую жертвует производительностью и конфиденциальностью.

В приватных блокчейнах все наоборот: доступ строго ограничен. Только утвержденные участники могут просматривать данные, инициировать или подтверждать транзакции. Такие системы популярны внутри компаний или между доверенными партнерами – например, при управлении цепочками поставок, где критически важны скорость, контроль и защита коммерческой информации.

А есть и промежуточный вариант – консорциумные блокчейны. Ими управляют сразу несколько организаций, заранее договорившихся о правилах игры. Такой подход позволяет сохранить преимущества децентрализации, не теряя при этом согласованности и взаимного доверия между участниками.

Хотя все транзакции в блокчейне видны участникам сети, они остаются псевдонимными: вместо имен используются публичные адреса. Это осложняет привязку операций к конкретным людям – если, конечно, пользователи сами не раскрывают свою личность.

В целом, блокчейн – это сложная, но саморегулируемая экосистема, построенная на криптографии, распределенном консенсусе и децентрализации. Он позволяет сторонам доверять друг другу без посредников, гарантируя при этом прозрачность, безопасность и неизменность данных. Сегодня технология уже применяется в самых разных сферах: от финансовых переводов и управления активами до логистики, здравоохранения и цифровых удостоверений личности – и продолжает открывать новые возможности для честных и надежных цифровых взаимодействий.

Несмотря на высокую безопасность, которую обещают такие технологии, как блокчейн, угрозы остаются разнообразными и постоянно развиваются. Они проникают через уязвимости, связанные как с человеческим фактором, так и с недостатками программного обеспечения.

Одной из самых частых угроз является социальная инженерия: злоумышленники обманом заставляют пользователей раскрыть пароли или конфиденциальные данные через поддельные письма, звонки или сообщения. Технические уязвимости – такие как ошибки в коде, неправильная настройка систем или отсутствие обновлений – также создают риски. Даже в блокчейне возможны проблемы, особенно на уровне смарт-контрактов или алгоритмов консенсуса, что подтверждают случаи взломов децентрализованных приложений.

Физические угрозы, включая кражу устройств с данными или несанкционированный доступ к серверным помещениям, также представляют реальную опасность. Внутренние угрозы со стороны сотрудников – как умышленные, так и случайные – усиливаются при избыточных правах доступа или отсутствии контроля. Именно халатное поведение сотрудников является причиной 50 % утечек конфиденциальной информации [5], что подчеркивает критическую важность не только технических, но и организационных мер. Управление данными само по себе может стать источником риска: слабая политика резервного копирования, отсутствие шифрования или несвоевременное удаление устаревшей информации открывают путь для утечек.

Для противодействия этим угрозам применяется комплекс мер. Шифрование данных как при хранении, так и при передаче (например, с использованием TLS или AES-256) делает информацию бесполезной для злоумышленников даже в случае перехвата. Маскировка и анонимизация позволяют использовать данные без раскрытия личной информации. Системы предотвращения утечек (DLP) отслеживают перемещение чувствительных данных и применяют правила – от блокировки до уведомления администратора.

Контроль доступа, основанный на принципе наименьших привилегий и усиленный многофакторной аутентификацией, ограничивает возможности злоумышленников даже при компрометации учетных данных. Обучение сотрудников помогает снизить риски, связанные с фишингом и неосторожным обращением с информацией. Регулярный аудит и мониторинг с использованием систем SIEM обеспечивают своевременное обнаружение подозрительной активности.

Блокчейн усиливает безопасность за счет децентрализации: изменение данных требует контроля над большинством узлов сети, что практически невозможно в крупных системах. Криптография – хэширование и асимметричное шифрование – обеспечивает целостность и подлинность транзакций. Смарт-контракты автоматизируют процессы, но требуют тщательного аудита кода. Доступ к данным в блокчейне может регулироваться токенами или

цифровыми сертификатами, а постоянный мониторинг транзакций позволяет оперативно реагировать на угрозы.

Криптографические методы занимают центральное место, особенно при работе с распределенными реестрами, такими как блокчейн. Эти методы выступают фундаментом для обеспечения конфиденциальности, целостности и подлинности данных. Шифрование, как основной инструмент криптографии, позволяет преобразовывать исходную информацию в нечитаемый формат, доступный для расшифровки только авторизованным лицам, обладающим соответствующим ключом. В контексте блокчейна, шифрование применяется на различных уровнях: от защиты транзакций перед их включением в блок до обеспечения конфиденциальности данных, хранящихся в частных блокчейнах.

Хеширование играет ключевую роль в формировании неизменяемой цепочки блоков. Каждый блок содержит криптографическую хеш-сумму предыдущего блока, что создает криптографическую связь между ними. Любое изменение данных в предыдущем блоке приводит к изменению его хеш-суммы, что, в свою очередь, делает все последующие блоки недействительными. Алгоритмы хеширования, такие как SHA-256, гарантируют, что даже малейшее изменение входных данных приводит к совершенно новой хеш-сумме, делая подмену или модификацию информации практически невозможной без обнаружения.

Цифровые подписи, основанные на асимметричной криптографии (с использованием пары открытого и закрытого ключей), обеспечивают аутентификацию и неотказуемость. При отправке транзакции владелец закрытого ключа подписывает ее, и любой участник сети может проверить подлинность отправителя, используя соответствующий открытый ключ. Это гарантирует, что транзакция действительно исходит от заявленного отправителя и не была изменена в процессе передачи. В блокчейне цифровая подпись подтверждает право собственности на цифровые активы и легитимность операций.

Помимо базовых механизмов защиты, в блокчейн-системах все шире применяются и более сложные криптографические методы. В частности, для обеспечения конфиденциальности используются такие подходы, как гомоморфное шифрование – оно позволяет выполнять вычисления над зашифрованными данными непосредственно, без их расшифровки, – а также доказательства с нулевым разглашением, позволяющие подтвердить корректность утверждения, не раскрывая при этом самого утверждения или каких-либо сопутствующих данных.

Традиционные модели контроля доступа, как правило, опираются на комбинацию идентификатора и секрета. Однако их относительная простота делает такие системы уязвимыми к целому ряду атак – от перебора и фишинга до компрометации целых баз данных. В ответ на эти вызовы современные решения все чаще переходят к многоуровневым и многофакторным схемам аутентификации. В их основе лежит требование предоставления двух или более независимых подтверждений подлинности: знания (например, пароля), владения (токена, смартфона с одноразовым кодом) и биометрических характеристик (отпечаток пальца, лицо и т.п.). Даже при компрометации одного из факторов подобная архитектура значительно повышает порог преодоления защиты.

Блокчейн-технологии открывают новые возможности для модернизации систем аутентификации и управления доступом. Благодаря своей децентрализованной, неизменяемой и прозрачной природе, блокчейн может выступать в роли надежного хранилища криптографических подтверждений личности. Например, вместо хранения паролей или их

хэшей в централизованных базах – цели для злоумышленников – можно использовать децентрализованные идентификаторы (DID), контролируемые самими пользователями. Такие идентификаторы позволяют подтверждать личность без раскрытия персональных данных, а криптографические подписи на основе пар «публичный/приватный ключ» обеспечивают гарантию подлинности каждого действия. Особое значение приобретает применение блокчейн-технологий для соблюдения требований стандарта ISO/IEC 27018, который задает специфические меры контроля для защиты персональных данных в публичных облаках [1].

Кроме того, блокчейн позволяет по-новому подойти к управлению правами доступа. Традиционные списки контроля доступа (ACL) зачастую страдают от сложности администрирования и подверженности ошибкам. В блокчейне же можно фиксировать права доступа в виде неизменяемых записей, распределенных между участниками сети. Это обеспечивает как высокий уровень доверия к данным, так и возможность сквозного аудита: в корпоративной среде, например, можно неоспоримо фиксировать, кто, когда и к каким ресурсам обращался. Особенно актуально это в контексте соблюдения нормативных требований (например, GDPR или HIPAA). Дополнительно, смарт-контракты могут автоматизировать процессы выдачи и отзыва прав на основе заранее заданных условий – что снижает риск ошибок, связанных с человеческим фактором, и ускоряет реакцию на изменения.

Эффективное управление информационной безопасностью невозможно без постоянного мониторинга и регулярного аудита. Мониторинг обеспечивает оперативное обнаружение аномалий: попыток несанкционированного доступа, подозрительной сетевой активности, неожиданных изменений конфигурации и т.д. Инструменты вроде систем обнаружения (IDS) и предотвращения вторжений (IPS) анализируют потоки данных в реальном времени, позволяя быстро реагировать на инциденты.

Аудит, в свою очередь, представляет собой систематическую оценку соответствия системы установленным политикам, стандартам и требованиям. Он проводится периодически и направлен на выявление скрытых уязвимостей – будь то избыточные права доступа, слабые криптографические настройки или нарушения процедур управления инцидентами. Аудиторские проверки могут включать анализ логов, тестирование на проникновение, оценку процессов резервного копирования и восстановления. Комбинация данных мониторинга и результатов аудита формирует целостную картину уровня защищенности, что критически важно для выстраивания многоуровневой и адаптивной стратегии безопасности.

Проведенный анализ подтверждает, что интеграция блокчейн-технологий в архитектуру информационной безопасности обладает значительным потенциалом. Использование распределенного реестра, неизменяемых записей и криптографических примитивов (хэширование, цифровые подписи) позволяет создавать системы, устойчивые к подделке и несанкционированному вмешательству. В то же время, как традиционные, так и блокчейн-системы остаются уязвимыми к целому ряду угроз – от утечек данных и инсайдерских атак до ошибок в реализации смарт-контрактов. Поэтому комплексный подход, сочетающий технические меры (шифрование на стороне клиента, строгий контроль доступа), регулярное тестирование и повышение осведомленности персонала, остается ключевым условием надежной защиты чувствительной информации.Изучение механизмов обеспечения безопасности непосредственно в блокчейн-системах подсветило важность использования проверенных криптографических алгоритмов, применения консенсусных протоколов,

устойчивых к атакам, и разработки безопасных смарт-контрактов с возможностью аудита и обновления.

Рассмотрение конкретных средств и подходов к обеспечению информационной безопасности показало, что интеграция блокчейна не отменяет, а скорее дополняет существующие практики. Криптографические средства, такие как симметричное и асимметричное шифрование, применяемые для защиты данных как в процессе передачи, так и при хранении, остаются важными компонентами. Системы контроля доступа и многофакторной аутентификации становятся еще более актуальными, позволяя гранулированно управлять правами доступа к чувствительной информации, даже в децентрализованных средах. Внедрение систем мониторинга и аудита, способных в реальном времени отслеживать активность в сети и анализировать логи, обеспечивает возможность своевременного выявления аномалий и инцидентов безопасности. Таким образом, интеграция блокчейн-технологий с проверенными методами ИБ представляет собой не просто техническое решение, а стратегический шаг в направлении формирования современной, основанной на международных стандартах (ISO/IEC 27017, 27018) нормативно-методологической базы. Такое изучение и применение мировых практик позволит сократить сроки разработки отечественных документов и повысить их качество, усилить взаимоотношения с мировой практикой [1].

Практическая ценность проделанной работы заключается в формировании понимания того, как синергия блокчейн-технологий и надежных методов информационной безопасности может быть использована для минимизации рисков утечек конфиденциальных данных и персональной информации. Защита информации должна осуществляться комплексно и системно, в рамках определенной политики безопасности [5]. Предлагаемый подход, интегрирующий неизменяемость блокчейна, криптографическую защиту и традиционные средства контроля доступа и мониторинга, представляет собой именно такой системный метод, направленный на создание устойчивой цифровой экосистемы.

Список литературы

1. Бирих Э. В., Виткова Л. А., Левин М. В., Чмутов М. В. Развитие стандартов и руководств в сфере облачных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией Бачевского С.В. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
2. Бирих Э. В., Груздев А. С., Камалова А. О., Сахаров Д. В. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики // Защита информации. Инсайд. 2024. № 1 (115). С. 42–46. EDN RLNHWK.
3. Махмутова Н. Ф., Бирих Э. В., Сахаров Д. В. [и др.] Исследование способов повышения безопасности корпоративных сетей // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 3. С. 110–116. DOI 10.21822/2073-6185-2024-51-3-110-116. EDN HDGBOY.
4. Бирих Э. В., Булова М. Д., Казанцев А. А., Миняев А. А. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН // Актуальные

проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 122-127. – EDN FBPSIL.

5. Бирих, Э. В., Гаврилов А. С., Сацук Е. Н. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией Бачевского С.В. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 104-107. – EDN XSUFFR.
6. Петренко С. А., Балябин А. А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 1 (65). С. 7–17. DOI: 10.21681/2311-3456-2025-1-7-17.
7. Рыспаев Р.С. Интеграция цифровых и физических систем безопасности в инфраструктурных проектах // Актуальные исследования. 2025. № 40 (275). С. 46–48. ISSN 2713-1513.
8. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Электронный ресурс]. URL: https://www.iso.org/standard/43757.html (дата обращения 12.12.2025).
9. Вереховский, О. Л. Разработка методики обеспечения изоляции данных в мультиарендных виртуализированных облачных инфраструктурах / О. Л. Вереховский, М. А. Егоров, И. Е. Пестов // Инновации и инвестиции. – 2025. – № 7. – С. 482-486. – EDN VIXFFI.

References

1. Birikh E. V., Vitkova L. A., Levin M. V., Chmutov M. V. Development of standards and guidelines in the field of cloud technologies // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by Bachevsky S. V. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. - pp. 92-95. - EDN YRPZWJ.
2. Birikh E. V., Gruzdev A. S., Kamalova A. O., Sakharov D. V. Selection of tools for dynamic security analysis of web applications for digital economy tasks // Information Security. Inside. 2024. No. 1 (115). pp. 42–46. EDN RLNHWK.
3. Makhmutova N. F., Birikh E. V., Sakharov D. V. [et al.] Study of ways to improve the security of corporate networks // Bulletin of the Dagestan State Technical University. Technical sciences. 2024. Vol. 51. No. 3. pp. 110–116. DOI 10.21822/2073-6185-2024-51-3-110-116. EDN HDGBOY.
4. Birikh E. V., Bulova M. D., Kazantsev A. A., Minyaev A. A. Development of a software module for automating the determination of the security level in the ISPDN // Actual problems

of infotelecommunications in science and education (APINO 2024): Proceedings of the XIII International scientific-technical and scientific-methodical conference, St. Petersburg, February 27-28, 2024. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2024. - pp. 122-127. - EDN FBPSIL.

5. Birikh, E. V., Gavrilov A. S., Satsuk E. N. Modern problems of ensuring internal security of a distributed network of government agencies // Actual problems of infotelecommunications in science and education (APINO 2018): VII International scientific, technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes, St. Petersburg, February 28 – January 2018 / Edited by Bachevsky S. V. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2018. - pp. 104-107. - EDN XSUFFR.
6. Petrenko S. A., Balyabin A. A. Model of quantum threats to information security for national blockchain ecosystems and platforms // Cybersecurity Issues. 2025. No. 1 (65). pp. 7–17. DOI: 10.21681/2311-3456-2025-1-7-17.
7. Ryspaev R.S. Integration of Digital and Physical Security Systems in Infrastructure Projects // Current Research. 2025. No. 40 (275). pp. 46–48. ISSN 2713-1513.
8. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Electronic resource]. URL: https://www.iso.org/standard/43757.html (accessed 12.12.2025).
9. Verekhovsky, O. L. Development of a methodology for ensuring data isolation in multi-tenant virtualized cloud infrastructures / O. L. Verekhovsky, M. A. Egorov, I. E. Pestov // Innovations and Investments. - 2025. - No. 7. - pp. 482-486. - EDN VIXFFI.

Ткач Г.А. Концепция нулевого доверия как основа современной корпоративной безопасности // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 40–45

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

КОНЦЕПЦИЯ НУЛЕВОГО ДОВЕРИЯ КАК ОСНОВА СОВРЕМЕННОЙ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

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

Работа посвящена концепции нулевого доверия - современному стандарту корпоративной безопасности. Её внедрение необходимо как маленьким компаниям, так и крупным корпорациям для создания комплексной корпоративной защиты, чтобы избежать или минимизировать ущерб. В работе рассматриваются ключевые принципы модели, такие как строгая аутентификация, сегментация сети и методы ее внедрения.

Ключевые слова: Кибербезопасность, концепция нулевого доверия, корпоративная безопасность.

THE CONCEPT OF ZERO TRUST AS THE BASIS OF MODERN CORPORATE SECURITY

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

The work is devoted to the concept of zero trust - a modern standard of corporate security. Its implementation is necessary for both small companies and large corporations to create comprehensive corporate protection to avoid or minimize damage. The paper discusses the key principles of the model, such as strong authentication, network segmentation, and methods of its implementation.

Keywords: Cybersecurity, zero trust concept, corporate security

Введение

Вот совсем недавно корпоративная безопасность строилась на довольно простой и понятной идее: есть внутренняя сеть, которую защищают — брандмауэры, системы обнаружения вторжений. Все что внутри считалось довольно надежным. Но цифровое поле изменилось кардинально. Облака, удаленные должности, личные устройства сотрудников, которые они используют для работы. Атаки стали изощреннее и злоумышленник, проникнув внутрь, получал практически полный набор инструментов и возможностей для реализации своего плана. Именно в этом контексте и родилась концепция Zero Trust - «нулевого доверия», которая по сути своей является не конкретным продуктом, а определенной тактикой. Ее можно описать одной фразой: «никогда не доверяй, всегда проверяй». В этой работе мы рассмотрим, почему эта парадигма стала столь актуальной, из каких ключевых принципов она состоит, как реализуется на практике и с какими вызовами сталкиваются компании при ее внедрении [1-2].

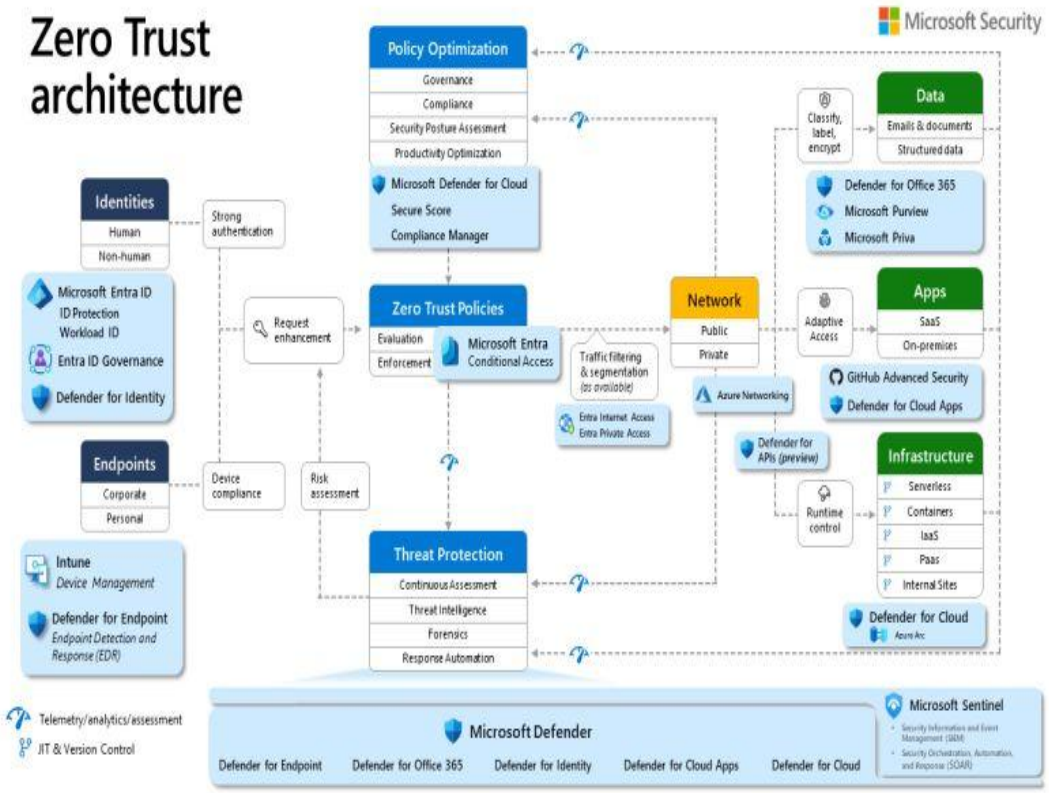

Рисунок 1 - Архитектура Zero-Trust Microsoft

От периметровой безопасности к Zero Trust: эволюция парадигмы

Старая модель безопасности работала во времена, когда данные и приложения находились в пределах физического офиса. Сотрудник, подключившись к корпоративной сети, получал широкий доступ к ресурсам. Проблема в том, что сегодня такого четкого периметра просто не существует. Данные могут храниться в облаке AWS или Microsoft Azure, приложения работать как SaaS-сервисы, а сотрудники подключаться из кафе или своего дома. Традиционная граница стала очень даже ненадежной.

Более того, сама идея «доверия» ко всему внутреннему оказалась фатальной ошибкой. Внутренняя угроза, будь то недовольный сотрудник или просто человек, по неосторожности кликнувший на фишинговую ссылку, демонстрирует, что опасность может исходить и изнутри. Атаки типа «перемещение по цепочке» (lateral movement), когда, получив доступ к одному слабому узлу, злоумышленник движется по сети, стали обыденностью. Концепция Zero Trust предлагает радикальный, но логичный ответ на эти вопросы. Она отрицает саму возможность существования доверенной среды по умолчанию. Каждый пользователь, каждое устройство, каждый запрос на подключение рассматриваются как потенциальная угроза, независимо от их местоположения. Это фундаментальный сдвиг в мышлении — от защиты сети к защите самих ресурсов и данных [3].

Ключевые принципы архитектуры нулевого доверия

Хотя единого жесткого стандарта не существует, можно выделить несколько основополагающих принципов, на которых базируется Zero Trust.

1. *Явная проверка подлинности***.** Это не просто ввод логина и пароля. Речь идет о строгой многофакторной аутентификации (MFA), которая становится практически обязательным минимумом. Система должна проверять личность пользователя, целостность и соответствие его устройства корпоративным политикам, а также контекст запроса (откуда он подключается, в какое время, какое приложение использует). Доступ предоставляется только после успешного прохождения всей этой проверки.
2. *Принцип наименьших привилегий (PoLP).* Пользователь должен получать ровно тот уровень доступа, который необходим ему для выполнения конкретных задач (и на определенное время). Это резко ограничивает потенциальный ущерб в случае компрометации каких-либо данных. Одно подразделение не может ведь иметь доступ к данным другого подразделения (на 2-3 курсе обучения в ВУЗЕ рассказывают как можно элементарно этого избежать – при помощи разделения на те же самые VLAN). Современные системы привилегированного доступа (PAM) позволяют реализовать этот принцип, предоставляя права по требованию и на короткий срок [4].
3. *Микросетевое сегментирование.* Вместо одной большой сети Zero Trust предлагает разбить ее на небольшие, изолированные сегменты или даже отдельные микросети для критически важных ресурсов. Даже если злоумышленник проникнет в один сегмент, он не сможет беспрепятственно перемещаться по всей сети. То есть, получив доступ даже к чему-то одному, то никто не сможет получить доступ к другому. Реализовать это технически непросто, но эффективность такой защиты очень высока.
4. *Непрерывный мониторинг и аналитика.* Проверка не заканчивается в момент входа. Система должна постоянно анализировать поведение пользователей и устройств, выявляя аномалии. Например, если сотрудник, который всегда работает из одного места, внезапно пытается зарегестрироваться уже из другой точки, допустим, в нерабочее время, его сессия должна быть заблокирована для дополнительной проверки. Здесь активно используются технологии машинного обучения и анализа поведения пользователей и объектов (UEBA).

Реализация Zero Trust на практике: технологии и подходы

Переход к Zero Trust — это не одномоментное событие, а долгий технический процесс. Начинается он обычно с аудита и картографирования всех пользователей и потоков данных. Без понимания того, что и от кого нужно защищать, двигаться дальше трудно.

Ключевыми технологическими «кирпичиками» для построения Zero Trust-архитектуры являются:

- *Identity and Access Management (IAM):* становятся центральным элементом безопасности, который управляет аутентификацией и авторизацией.
- *SASE (Secure Access Service Edge):* это облачная архитектура, которая объединяет сетевые и сервисы безопасности (включая Zero Trust Network Access - ZTNA) в единое решение. SASE позволяет безопасно подключать пользователей к приложениям, независимо от их местоположения, что идеально ложится в парадигму Zero Trust.
- *ZTNA (Zero Trust Network Access):* реализация принципа «никогда не доверяй» для доступа к приложениям. Вместо предоставления доступа к всей сети (как в VPN), ZTNA создает зашифрованные микротуннели только к конкретным приложениям, которые нужны пользователю.

- *SIEM-системы и SOAR-платформы:* они собирают данные с тысяч источников и позволяют автоматизировать реагирование на инциденты, что критически важно для непрерывного мониторинга.

Внедрение, лучше начинать с самых критичных активов — например, с систем финансового учета или баз данных с персональной информацией. Это позволяет отработать методику и продемонстрировать быстрый положительный эффект.

Вызовы и критика: насколько реализуема утопия?

Несмотря на всю свою логичность и привлекательность, концепция Zero Trust сталкивается с серьезными препятствиями на пути внедрения. Во-первых, это *высокая стоимость и сложность*. Перестройка устаревшей инфраструктуры под новые принципы требует значительных финансовых вложений и привлечения высококвалифицированных специалистов. Многие компании просто не готовы к таким расходам.

Во-вторых, существует проблема *сопротивления персонала.* Сотрудники могут воспринимать постоянные проверки и строгий контроль как проявление недоверия к себе, что создает негативное психологическое давление. Кроме того, новые процедуры аутентификации могут показаться им излишне громоздкими и мешающими работе. Здесь необходима грамотная работа и обучение [5].

Можно предположить, что существует и определенный *разрыв между теорией и практикой.* Абсолютное Zero Trust — это скорее идеал, к которому нужно стремиться, но которого трудно достичь полностью. Всегда остаются системы, которые невозможно интегрировать в новую модель, или экстренные случаи, требующие быстрого предоставления широких прав. Некоторые критики также указывают на то, что тотальный контроль и сбор данных о поведении пользователей порождают вопросы о приватности и этике.

Заключение

Концепция Zero Trust — это не временный тренд, а закономерный и необходимый ответ на новые реалии цифрового мира, где границы компаний стали прозрачными, а угрозы — более изощренными. Отказ от устаревшей модели «доверенного периметра» в пользу постоянной, контекстно-зависимой проверки каждого запроса является сегодня краеугольным камнем построения устойчивой системы корпоративной безопасности. Конечно, этот путь сопряжен с трудностями — финансовыми, техническими и даже культурными. Полная реализация принципов Zero Trust — сложная и амбициозная задача. Однако уже сам процесс движения в этом направлении, поэтапное внедрение его элементов — от строгой аутентификации до микросетевого сегментирования — значительно повышают уровень защищенности организации. В конечном счете, Zero Trust — это не о том, чтобы создать неприступную крепость, а о том, чтобы сделать среду настолько «неудобной» для потенциального злоумышленника, чтобы стоимость атаки многократно превысила возможную выгоду.

Список литературы

1. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной

научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.

2. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
3. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
4. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН / Э. В. Бирих, М. Д. Булова, А. А. Казанцев, А. А. Миняев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 122-127. – EDN FBPSIL.
5. Бирих, Э. В. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти / Э. В. Бирих, А. С. Гаврилов, Е. Н. Сацук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 104-107. – EDN XSUFFR.

References

1. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017) : Collection of scientific articles of the VI International Scientific and Technical and Scientific and Methodological Conference. In 4 volumes, St. Petersburg, 01–02 March 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 92-95. – EDN YRPZWJ.
2. Selection of tools for dynamic analysis of the security of web applications for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Protection. Inside. – 2024. – № 1(115). – pp. 42-46. – EDN RLNHWK.
3. Study of ways to improve the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [i dr.] // Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Technical Sciences. – 2024. – T. 51, No 3. – pp. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

4. Birikh E. V., Bulova M. D., Kazantsev A. A., Minyaev A. A. Actual Problems of Infotelecommunications in Science and Education (APINO 2024) : Materials of the XIII International Scientific and Technical and Scientific and Methodological Conference, St. Petersburg, February 27–28, 2024. – St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2024. – pp. 122-127. – EDN FBPSIL.
5. Birikh E. V., Gavrilov A. S., Satsuk E. N. Sovremennyye problemy obespecheniya vnutrennoy bezopasnosti raspredelennoy seti organov gosudarstvennogo vlasti [Modern problems of ensuring internal security of the distributed network of state authorities] / E. V. Birikh, A. S. Gavrilov, E. N. Satsuk // Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii (APINO 2018) : VII Mezhdunarodnaya nauchno-tekhnicheskiy i nauchno-metodicheskaya konferentsiya. Collection of scientific articles. In 4 volumes, St. Petersburg, February 28 – 01, 2018 / Edited by S.V. Bachevsky. Volume 1. – St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2018. – pp. 104-107. – EDN XSUFFR.

Кузнецов А.К. Повышение эффективности мониторинга серверных систем на основе технологий искусственного интеллекта// Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 46–51

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.413.2

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ МОНИТОРИНГА СЕРВЕРНЫХ СИСТЕМ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Кузнецов А.К.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия (119454, г. Москва, пр-т Вернадского, д. 78, стр. 4), e-mail: redstarz2002@mail.ru

Современные центры обработки данных и серверные инфраструктуры характеризуются высокой сложностью и динамичностью. Традиционные системы мониторинга, основанные на статических пороговых значениях и реактивных оповещениях, все чаще оказываются неспособны обеспечивать требуемые уровни доступности, производительности и безопасности. Данное исследование посвящено анализу потенциала технологий искусственного интеллекта (ИИ) для трансформации подхода к мониторингу серверов. В статье рассматриваются ключевые проблемы существующих систем, такие как высокий уровень ложных срабатываний, запаздывающее реагирование на инциденты и неспособность прогнозировать сбои. Предложена концептуальная модель интеллектуальной системы мониторинга, интегрирующая методы машинного обучения для прогнозной аналитики, обнаружения аномалий и корреляционного анализа событий. Подчеркивается, что внедрение ИИ позволяет перейти от реактивного к проактивному и предиктивному управлению ИТ-инфраструктурой, что ведет к значительному повышению ее надежности и эффективности.

Ключевые слова: Мониторинг серверов, искусственный интеллект, машинное обучение, предиктивная аналитика, обнаружение аномалий, проактивное управление, ИТ-инфраструктура, центры обработки данных.

IMPROVING THE EFFICIENCY OF SERVER SYSTEM MONITORING BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Kuznetsov A.K.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue Vernadsky, 78, b. 4), e-mail: redstarz2002@mail.ru

Modern data centers and server infrastructures are characterized by high complexity and dynamic behavior. Traditional monitoring systems based on static thresholds and reactive alerts are increasingly unable to ensure required levels of availability, performance, and security. This study analyzes the potential of artificial intelligence (AI) technologies to transform the approach to server monitoring. The article examines key issues with existing systems, such as high false alarm rates, delayed incident response, and the inability to predict failures. A conceptual model of an intelligent monitoring system is proposed, integrating machine learning methods for predictive analytics, anomaly detection, and event correlation analysis. It is emphasized that the implementation of AI enables a transition from reactive to proactive and predictive IT infrastructure management, leading to a significant increase in its reliability and efficiency.

Keywords: Server monitoring, artificial intelligence, machine learning, predictive analytics, anomaly detection, proactive management, IT infrastructure, data centers.

Введение

Стабильность и производительность серверной инфраструктуры являются критически важными факторами для функционирования любого современного предприятия или онлайн-сервиса. Традиционные системы мониторинга, такие как Zabbix, Nagios или Prometheus, основаны на задании статических порогов для ключевых метрик (загрузка процессора,

потребление оперативной памяти, использование дискового пространства и т.д.) [1]. При превышении этих порогов генерируются оповещения для системных администраторов.

Однако данный подход обладает рядом фундаментальных недостатков. Во-первых, статические пороги не учитывают изменчивую природу рабочих нагрузок, что приводит к большому количеству ложных срабатываний или, наоборот, к пропуску реальных проблем. Во-вторых, реактивная модель предполагает, что инцидент уже произошел, и ущерб от простоя или снижения производительности уже наносится. В-третьих, такие системы не способны выявлять сложные, многофакторные аномалии и коррелировать события из различных источников для определения корневой причины сбоя [2].

В связи с этим актуальной задачей является разработка и внедрение интеллектуальных систем мониторинга, способных к самообучению и прогнозированию. Целью данного исследования является анализ возможностей технологий искусственного интеллекта для создания новой парадигмы мониторинга серверных систем, обеспечивающей переход от реактивного к проактивному и предиктивному управлению.

Цель исследования

Целью данного исследования является комплексный анализ возможностей технологий искусственного интеллекта и машинного обучения для создания новой, проактивной парадигмы мониторинга серверных систем. В задачи работы входит: выявление системных недостатков традиционных подходов, разработка расширенной концептуальной модели интеллектуальной системы мониторинга, оценка преимуществ и проблемных аспектов внедрения, а также формулировка практических рекомендаций по ее поэтапной реализации.

Материал и методы исследования

Материалом для исследования послужили современные научные публикации, обзоры и технические отчеты в области мониторинга ИТ-инфраструктуры, искусственного интеллекта и машинного обучения (ML). В работе применялись методы системного анализа для выявления проблем традиционных систем, методы сравнительного анализа алгоритмов ML, а также метод моделирования для проектирования архитектуры интеллектуальной системы. Были проанализированы различные классы алгоритмов: для прогнозирования временных рядов (ARIMA, Prophet, рекуррентные нейронные сети – RNN/LSTM), для обнаружения аномалий без учителя (Isolation Forest, Local Outlier Factor, автоэнкодеры), а также методы анализа графов и алгоритмы с учителем для корреляции событий и анализа корневых причин (RCA) [2].

Особое внимание в ходе исследования было уделено критической оценке применимости рассмотренных алгоритмов в условиях реальных эксплуатационных сред. Для этого анализировались не только теоретические характеристики методов (точность, скорость обучения, чувствительность к параметрам), но и практические аспекты их развертывания, такие как требовательность к вычислительным ресурсам, устойчивость к шуму в данных и возможность инкрементального обучения на поступающих потоках информации. Это позволило сформулировать предварительные рекомендации по выбору алгоритмического инструментария в зависимости от конкретных задач мониторинга (например, долгосрочное

прогнозирование ресурсов versus оперативное обнаружение аномалий в реальном времени) и специфики целевой инфраструктуры [3].

Результаты исследования и их обсуждение

Перспективным направлением является конвергенция интеллектуального мониторинга (AIOps) с технологиями автономных систем и гибридного искусственного интеллекта. Будущие исследования должны быть сосредоточены на создании самообучающихся и самооптимизирующихся платформ, способных не только детектировать и прогнозировать аномалии, но и автоматически инициировать корректирующие действия через интерфейсы оркестрации (например, Kubernetes Operators или Ansible Playbooks) в рамках утвержденных политик безопасности. Особый интерес представляет разработка адаптивных моделей, способных эффективно работать в условиях концептуального дрейфа данных (concept drift), когда паттерны «нормального» поведения инфраструктуры со временем меняются. Кроме того, актуальной задачей остается создание стандартизированных открытых форматов данных и API для обеспечения интероперабельности между разнородными системами мониторинга, анализа и управления различных вендоров. Это позволит строить экосистемы, в которых лучшие в своем классе интеллектуальные модули могут быть легко интегрированы. Исследования в области федерированного машинного обучения также открывают возможности для построения коллективных моделей прогнозирования и обнаружения аномалий на основе агрегированных анонимизированных данных с множества изолированных сред, не нарушая требований к конфиденциальности и безопасности данных каждой отдельной организации. Реализация этих направлений приблизит переход к эпохе truly autonomous IT operations.

Внедрение предложенной модели сулит значительные преимущества: переход к проактивному управлению, радикальное снижение ложных срабатываний, сокращение среднего времени на восстановление (MTTR) за счет автоматизации RCA и оптимизация использования ресурсов через точное прогнозирование нагрузки.

Однако успешная реализация сопряжена с серьезными вызовами:

1. Требования к данным**:** Качество моделей напрямую зависит от объема, полноты и чистки исторических данных. Необходимы стратегии управления данными мониторинга (DataOps для Observability).
2. Экспертиза и сложность: Разработка, обучение и поддержка ML-моделей требуют кросс-функциональной команды, включающей Data Scientists, ML-инженеров и DevOps-специалистов.
3. Вычислительные ресурсы: Обучение и инференс сложных моделей, особенно нейросетевых, потребуют дополнительных ресурсов, что необходимо учитывать в ТЭО.
4. Интерпретируемость (Explainable AI – XAI)**:** Сложные модели часто являются «черным ящиком». Для доверия со стороны эксплуатационных команд необходимо развитие методов XAI, позволяющих объяснить, почему система сгенерировала то или иное предупреждение или прогноз [4].
5. *Интеграционная зрелость***:** Внедрение должно быть совместимо с существующими ITSM-процессами, системами управления (например, ServiceNow) и инструментами оркестрации.

Практический путь внедрения должен быть итеративным: начинаться с консолидации данных и решения конкретной точечной задачи (например, прогноз дискового пространства для конкретного кластера), проходить пилотную эксплуатацию, а затем масштабироваться на новые домены с постоянным дообучением моделей на новых данных.

Ключевые ограничения классических систем мониторинга можно систематизировать следующим образом:

1. Низкая эффективность при динамических нагрузках: Жесткие пороги неадекватны для сервисов с переменной нагрузкой (например, в зависимости от времени суток или дней недели), что ведет к «шуму» в оповещениях и снижению внимания администраторов.
2. Отсутствие прогнозирования: Традиционные системы фиксируют уже случившееся событие, но не могут предсказать потенциальный сбой на основе анализа тенденций.
3. Сложность идентификации корневых причин: При одновременном возникновении множества событий администратору приходится вручную проводить корреляционный анализ для выявления первоначальной проблемы, что отнимает значительное время.
4. Неспособность обнаруживать сложные аномалии: Поведение системы, выходящее за рамки простых метрик, но указывающее на скрытую проблему (например, медленная деградация производительности), часто остается незамеченным.

Предлагаемая модель основана на интеграции модулей машинного обучения в процесс сбора и анализа метрик. Архитектура такой системы включает следующие ключевые компоненты:

1. Сбор и агрегация данных: Система собирает многомерные временные ряды данных с серверов, включая метрики производительности, логи, сетевой трафик и данные о состоянии приложений.
2. Модуль предиктивной аналитики: Используя алгоритмы прогнозирования временных рядов (например, ARIMA, Prophet или рекуррентные нейронные сети – RNN), данный модуль прогнозирует будущие значения ключевых метрик. Это позволяет выявить тенденции, ведущие к исчерпанию ресурсов (например, заполнение диска через 48 часов), и предотвратить инцидент.
3. Модуль обнаружения аномалий: В отличие от статических порогов, этот модуль на основе алгоритмов без учителя (например, Isolation Forest, Local Outlier Factor – LOF или автоэнкодеры) выявляет отклонения в поведении системы, которые не укладываются в нормальные паттерны [3]. Это позволяет обнаруживать ранее неизвестные угрозы, такие как сложные кибератаки или скрытые сбои оборудования.
4. Двигатель корреляции и анализа корневых причин (RCA): На основе методов анализа графов и алгоритмов машинного обучения с учителем этот компонент устанавливает причинно-следственные связи между событиями, автоматически определяя первичную причину сбоя среди множества вторичных симптомов.
5. Система интеллектуального оповещения: Вместо потока одноуровневых оповещений система приоритизирует инциденты, группирует связанные события и предоставляет администраторам не только информацию о проблеме, но и гипотезу о ее причине и возможные рекомендации по устранению.

В контексте трансформации подходов к управлению ИТ-инфраструктурой, внедрение технологий искусственного интеллекта в системы мониторинга представляет собой

качественный скачок, сопряжённый как с существенными операционными выгодами, так и с комплексом технологических и организационных вызовов. Анализ данного перехода требует сбалансированного рассмотрения двух взаимосвязанных сторон: потенциальных преимуществ, которые мотивируют внедрение, и реальных проблемных аспектов, которые необходимо преодолеть для его успешной и устойчивой реализации.

Преимущества:

1. Проактивность: Возможность предотвращать сбои, а не реагировать на них.
2. Снижение количества ложных срабатываний: Адаптивные алгоритмы минимизируют «шум», повышая доверие к системе оповещений.
3. Сокращение времени устранения инцидентов (MTTR): Автоматическое определение корневой причины ускоряет восстановление системы.
4. Оптимизация ресурсов: Прогнозы нагрузки позволяют более эффективно планировать емкость инфраструктуры.

Проблемные аспекты и вызовы:

1. Качество и объем данных: Эффективность моделей ИИ напрямую зависит от объема и релевантности исторических данных, используемых для их обучения.
2. Сложность разработки и настройки: Создание и тонкая настройка моделей машинного обучения требуют привлечения высококвалифицированных специалистов (Data Scientists).
3. Вычислительная стоимость: Обучение и эксплуатация сложных моделей могут потребовать значительных вычислительных ресурсов.
4. Интерпретируемость решений: «Черный ящик» некоторых сложных моделей ИИ может вызывать недоверие у администраторов, поэтому важным направлением является развитие методов объяснимого ИИ (XAI).
5. Интеграция с существующими системами: Развертывание интеллектуальных модулей должно быть совместимо с уже действующими системами мониторинга и управления.

Внедрение системы мониторинга на основе ИИ рекомендуется осуществлять поэтапно:

1. Подготовка данных: Консолидация и очистка исторических данных мониторинга.
2. Выбор и обучение моделей: Начало с решения конкретных задач, например, прогнозирования нагрузки на определенный сервис или обнаружения аномалий в логах веб-сервера.
3. Пилотная эксплуатация: Развертывание прототипа в тестовом контуре или на некритичном сегменте инфраструктуры для валидации эффективности.
4. Интеграция и масштабирование: Постепенное подключение новых систем и сервисов, дообучение моделей на новых данных.
5. Обучение персонала: Подготовка команды эксплуатации к работе с новой системой, интерпретации ее выводов и рекомендаций.

Выводы

Проведенное исследование демонстрирует, что технологии искусственного интеллекта обладают значительным потенциалом для кардинального повышения эффективности мониторинга серверных систем. Переход от реактивных методов к проактивным и

предиктивным, реализуемый за счет применения машинного обучения для прогнозной аналитики и обнаружения аномалий, позволяет не только предотвращать простои и снижать операционные расходы, но и принципиально повышать отказоустойчивость и производительность ИТ-инфраструктуры.

Несмотря на существующие вызовы, связанные со сложностью разработки, требовательностью к данным и необходимостью интеграции, преимущества интеллектуального мониторинга существенно перевешивают риски. Дальнейшие исследования в данной области должны быть сфокусированы на разработке более эффективных и интерпретируемых моделей, создании стандартов интеграции и адаптации решений для облачных и гибридных сред. В перспективе системы мониторинга на основе ИИ станут стандартом де-факто для управления сложной и динамичной ИТ-инфраструктурой.

Список литературы

1. А.Б.Смит, К.Д.Джонсон «Сравнительный анализ традиционных инструментов мониторинга ИТ-инфраструктуры» // Международный журнал компьютерных приложений, 2021.
2. Гарсия М., Ли К., Патель Р. «Машинное обучение для обнаружения аномалий во временных рядах: обзор» // ACM Computing Surveys (CSUR), 2022.
3. Чжан Х., Ван Ю., Чен С. «Подход глубокого обучения для проактивного прогнозирования отказов серверов в центрах обработки данных» // Труды Международной конференции IEEE по большим данным, 2023.
4. Миллер Т., «Объясняемый ИИ — ключ к ИТ-операциям» // IEEE IT Professional, 2022.
5. Робертс С., Чжао П. «Внедрение AIOps в крупном предприятии: проблемы и лучшие практики» «Практики» // Журнал управления сетями и системами, 2021.

References

1. A. B. Smith, C. D. Johnson «Comparative Analysis of Traditional IT Infrastructure Monitoring Tools» // International Journal of Computer Applications, 2021.
2. Garcia, M., Lee, K., & Patel, R. «Machine Learning for Anomaly Detection in Time-Series Data: A Survey» // ACM Computing Surveys (CSUR), 2022.
3. Zhang, H., Wang, Y., & Chen, X. «A Deep Learning Approach for Proactive Server Failure Prediction in Data Centers» // Proceedings of the IEEE International Conference on Big Data, 2023.
4. Miller, T., «Explainable AI is Key for IT Operations» // IEEE IT Professional, 2022.
5. Roberts, S., & Zhao, P. «Implementing AIOps in a Large-Scale Enterprise: Challenges and Best Practices» // Journal of Network and Systems Management, 2021.

Садыков Р.Р. Социальная инженерия: атаки с использованием синтетических личностей и дипфейков // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 52–61

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5:316.6

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: АТАКИ С ИСПОЛЬЗОВАНИЕМ СИНТЕТИЧЕСКИХ ЛИЧНОСТЕЙ И ДИПФЕЙКОВ

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

В данной работе рассматривается анализ методов социальной инженерии, основанных на создании и эксплуатации синтетических личностей в сети Интернет, а также дипфейков, созданных с помощью искусственного интеллекта. Исследование будет опираться на сформированное описание цифрового профиля злоумышленника, что включает в себя поведенческие и коммуникативные характеристики. Подобный анализ позволит оценить уязвимость пользователей к различным формам поддельной айдентики. Показано, что без строгой категоризации уровней пользовательской осведомлённости и сценариев цифрового взаимодействия вероятность успеха реализации атак с участием ИИ-имперсонации и/или дипфейков оказывается существенно завышенной. В работе также представлена типология жертв и сценариев, основанных на использовании методов синтетических личностей и дипфейков, схема методического воздействия злоумышленника на жертву, а также статистические данные, основывающиеся на вышеперечисленных методиках мошенничества. Рассмотрен пример случая мошенничества с использованием искусственного интеллекта и обоснована приоритетность адаптивных стратегий защиты, ориентированных на динамическое выявление подозрительного поведения цифровых субъектов.

Ключевые слова: Искусственный интеллект, социальная инженерия, модель жертвы, синтетическая личность, фишинг, психологическая атака, адаптивные стратегии, информационная безопасность.

SOCIAL ENGINEERING: SYNTHETIC IDENTITY AND DEEPFAKE ATTACKS

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

The article develops an approach to analyzing the techniques of social engineering based on the creation and exploitation of synthetic identities on the Internet, as well as impersonation via AI-generated deepfakes. The proposed approach relies on a formal description of an attacker's digital profile, which includes behavioral and communicative characteristics. This enables the assessment of users' vulnerability to various forms of synthetic identity manipulation. It is shown that, without formalizing user awareness levels and scenarios of digital interaction, the likelihood of successful attacks involving these methods is significantly higher. The article also presents a typology of victims and attack scenarios based on the use of synthetic identities and deepfakes, along with a graphical model of the attacker's methodological influence on the victim, supplemented with statistical data on the aforementioned method of fraud. An example of a fraud case involving the use of artificial intelligence is also presented, and the priority of adaptive defense strategies focused on dynamically detecting suspicious behavior of digital entities is substantiated.

Keywords: Artificial intelligence, social engineering, victim model, synthetic identity, phishing, psychological attack, adaptive strategies, information security.

Современное информационное общество характеризуется тенденцией к расширению области сбора и многоступенчатой обработки персональных данных, что обуславливается стремительным развитием информационных технологий и ростом важности персональных данных как стратегического, в том или ином понимании, ресурса. На фоне развития технологического прогресса и усиленного внедрения информационных технологий в бытовую жизнь человека, в том числе искусственного интеллекта (ИИ), всё более очевидной становится уязвимость со стороны человеческого фактора, которая остаётся фундаментальной основой всех действий злоумышленников. Социальная инженерия, в свою очередь, формируется как совокупность методов психологического воздействия на человека, направленных на изучение его модели поведения и на психо-когнитивное воздействие соответственно, с целью получения доступа к какой-либо чувствительной и/или конфиденциальной информации, ресурсам или инфраструктуре ограниченного доступа. Изучение механизмов подобных воздействий приобретает первостепенную значимость, поскольку именно человек в любом случае остаётся наиболее слабым звеном в цепочке информационной безопасности.

Целью работы является разработка аналитического подхода к оценке уязвимости пользователей к атакам социальной инженерии, основанным на синтетических цифровых личностях и дипфейках, с учетом уровней пользовательской осведомлённости и контекста взаимодействия.

Социальная инженерия, главным образом, состоит из нескольких аспектов. Основными из них являются: разведка (reconnaissanse), легенда (pretexting), взаимодействие/коммуникация (engagement), психологические приемы (psychological methods). Каждый аспект имеет свою основную роль. Так, разведка позволяет собрать информацию о цели: ее положении/роли в обществе/компании, ее контактах, профилях в социальных сетях, структуре организации (при условии атаки на корпоративную личность). Совокупность всего вышеперечисленного зачастую объединяют в понятие OSINT. Ролевая легенда, в свою очередь, позволяет создать ситуационную обстановку и работать над вызовом доверия у жертвы. Психологические приемы позволяют манипулировать эмоциями и чувствами цели для достижения целей, задуманных злоумышленниками.

Взаимодействие с жертвой осуществляется через каналы атак, такими как: электронная почта и социальные сети (phishing), физический (тейлгейтинг, сталкинг), взаимодействие с устройствами (зараженные накопители, устройства).

Как отмечается в работе *Бириха Э.В. «Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6»:*

«злоумышленники активно используют уязвимости современных протоколов связи и методы динамического построения сетей, что позволяет им адаптироваться к защитным мерам компаний. Если раньше социальная инженерия сводилась к относительно примитивным формам фишинга или телефонному выманиванию данных, то сегодня она превратилась в целый комплекс взаимосвязанных стратегий, подкреплённых анализом больших данных, искусственным интеллектом и глубоким знанием поведенческих паттернов целевых аудиторий» [1].

Учитывая стремительное развитие искусственного интеллекта, стоит особенно отметить такие способ социальной инженерии, как «синтетическая цифровая личность» и «дипфейки»

Синтетическая цифровая личность — это цифровая запись о некоторой личности (персоне), содержащая стандартные атрибуты личности (имя, телефон, адрес и т.д.), значения

которых полностью сфабрикованы или скомпилированы из реальных и вымышленных данных. [2][3]

Дипфейк — это форма медиаконтента, например фото или видео, созданного искусственным интеллектом (ИИ) для изображения реальных или несуществующих людей, выполняющих действия, которые они никогда не совершали. [4]

Если говорить о данных методе более обобщенно – подобные атаки, осуществляемые посредством «синтетической цифровой личности» или «дипфейка» можно расценивать как кражу личности. Злоумышленники зачастую подделывают профили известных в обществе людей, устанавливая контакт с фальшивых профилей в социальных сетях с пользователями, не идентифицирующими угрозу, и отправляя им, как пример, те самые «дипфейки» для повышения уровня доверия в их диалогах. Стоит также упомянуть, что не все данные синтетического профиля могут быть сфабрикованными. Некоторые данные вполне могут быть настоящими, например, ИНН (идентификационный номер налогоплательщика), но при этом необязательно соответствовать личности, коей предоставляется злоумышленник, что позволяет ему эффективнее замести следы своих действий/

Формализованная типология жертв атак социальной инженерии с использованием ИИ

В рамках данной работы жертва рассматривается как цифровой субъект, характеристики которого могут быть формализованы и использованы в аналитических моделях риска.

Модель жертвы (формальное описание)

Предлагается описывать пользователей, попавших на влияние мошенников, в виде вектора параметров:

V = ⟨L, A, C, E, R⟩

где:

- **L (Literacy)** — уровень цифровой и ИИ-осведомлённости;
- **A (Authority sensitivity)** — чувствительность к социальному иерархическому давлению;
- **C (Context)** — контекст взаимодействия;
- **E (Emotional state)** — эмоциональное состояние в момент атаки;
- **R (Resources access)** — уровень доступа в инфраструктуре

Данная модель позволяет перейти от субъективных характеристик жертвы к сравнимым параметрам.

Параметры модели жертвы

Таблица 1 - Уровень цифровой осведомлённости (L)

Уровень	Характеристика
L1	Пользователь не осознаёт существования дипфейков и синтетических личностей
L2	Пользователь неполноценно осведомлён теоретически, отсутствие возможности распознания в практических случаях
L3	Пользователь обладает практическими навыками верификации, способен распознать данные виды мошенничества

При L_1 вероятность успешной атаки с использованием ИИ-имперсонации стремится к максимуму: таких пользователей легче всего ввести в заблуждение.

Таблица 2 - Чувствительность к социальному иерархическому давлению (A)

Уровень	Характеристика
A1	Высокая восприимчивость к социальному давлению: высокая подверженность лицам, стоящим выше в социальной иерархии
A2	Умеренная восприимчивость к социальному давлению
A3	Критическое отношение к источнику информации, верификация подлинности сведений

ИИ-дипфейки усиливают воздействие на пользователей уровня A_1, создавая впечатление авторитарности предоставляемой информации, имитируя визуальные и голосовые признаки.

Таблица 3 - Контекст взаимодействия (C) (Таблица 3)

Уровень	Характеристика
C1	Личное общение (близкие люди: родственные связи, друзья и знакомые)
C2	Корпоративная среда
C3	Публичная или анонимная среда (зачастую, незнакомые лица)

Атаки с дипфейками наиболее эффективны в контекстах C_1 и C_2, где запросы выглядят легитимными, т.к. поступают из более доверенных кругов общения пользователя.

Таблица 4 - Эмоциональное состояние (E)

Уровень	Характеристика
E1	Преобладание негативных эмоций: общее стрессовое состояние, страх, ощущение срочности, тревожность
E2	Нейтральный эмоциональный спектр
E3	Хладнокровие и частично повышенная настороженность

Большинство успешных атак происходят при E_1. При E3 могут возникать эмоции разных степеней, которые, тем не менее, не позволяют пользователю стать жертвой мошенничества.

Таблица 5 - Уровень доступа в инфраструктуре (R)

Уровень	Характеристика
R1	Ограниченный
R2	Финансовый
R3	Корпоративный / административный

Максимальная ценность атак достигается при воздействии на субъектов с уровнями доступа R_2–R_3, что приводит к целенаправленному выбору злоумышленниками ролей, связанных с управлением финансовыми и информационными ресурсами.

Типология жертв (сводная классификация)

На основе параметров выделяются типы пользвателей (Таблица 6)

Таблица 6 -Типы пользователей

Тип	Профиль	Описание
V_1	$\langle L_1, A_1, C_1, E_1, R\rangle$	Пользователи с низкой цифровой осведомлённостью
V_2	$\langle L_2, A_1, C_2, E_1, R_2\text{-}R_3\rangle$	Пользователи корпоративных инфраструктур
V_3	$\langle L_3, A_2, C, E_2\text{-}E_3, R\rangle$	Пользователи с высокой цифровой компетентностью

Вероятность успешной атаки

Вероятность успеха атаки может быть представлена как условная функция:

$$\mathbf{P_s = f(V, A_a, T)}$$

где:

- **V** — параметры жертвы;
- $\mathbf{A_a}$ — профиль атакующего;
- **T** — используемые ИИ-технологии (дипфейк, синтетическая личность, голосовая имитация).

При сочетании (L_1, A_1, E_1) вероятность $P_s \rightarrow \max$.

Вероятность успешной атаки с использованием искусственного интеллекта определяется совокупным влиянием параметров жертвы (V), характеристик атакующего (A_a) и применяемых ИИ-технологий (T). В рамках настоящей работы данная зависимость рассматривается не как строго вычисляемая вероятность, а как качественная функция риска, позволяющая сопоставлять различные сценарии атак между собой.

Анализ же, в свою очередь, показывает, что наибольшая вероятность успешной атаки наблюдается при сочетании низкого уровня цифровой осведомлённости жертвы, высокой чувствительности к социально-иерархическому фактору и повышенного эмоционального давления (L_1, A_1, E_1).

Примерная схема взаимодействия представлена на Рисунке 1.

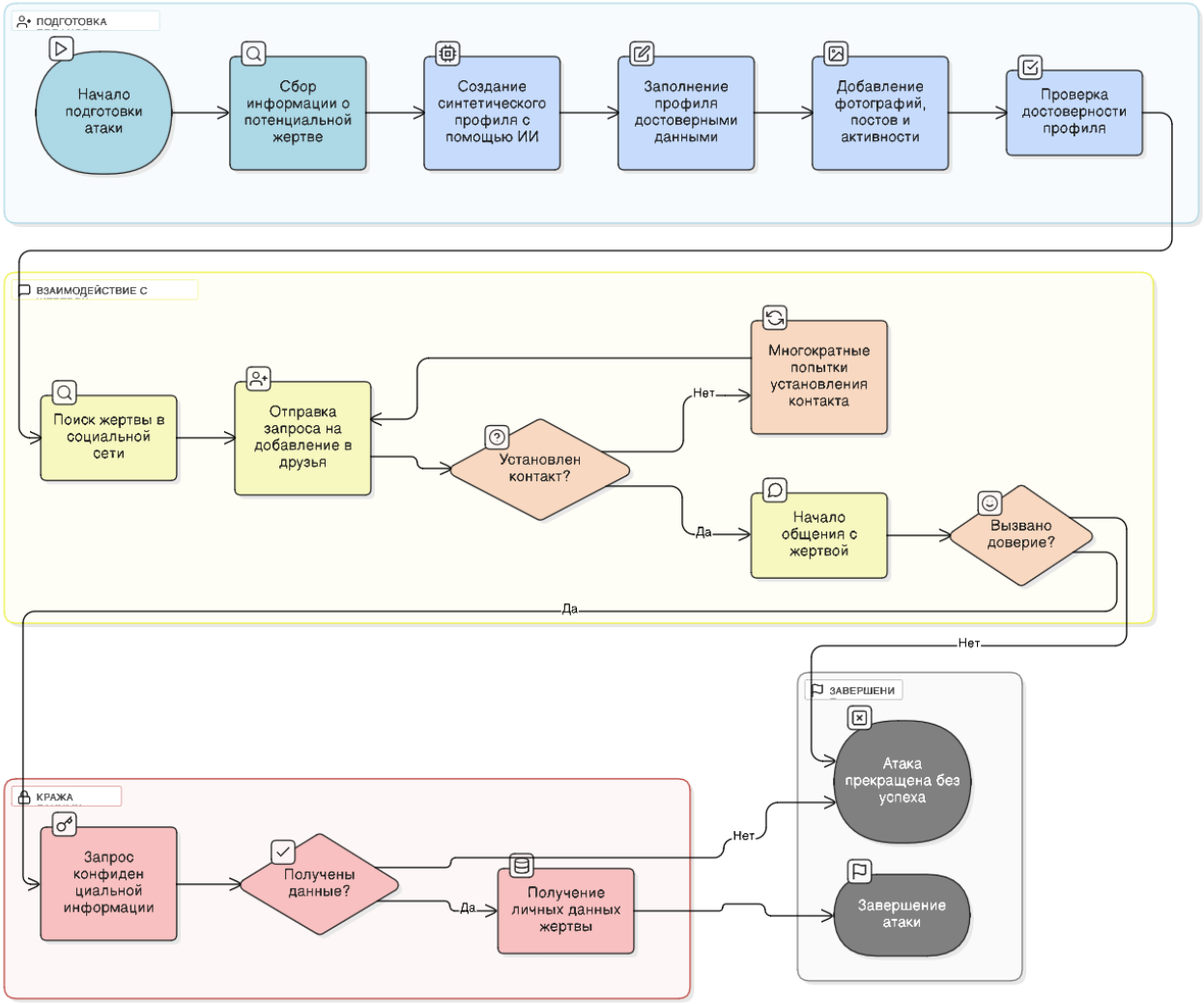

Рисунок 1 – Схема взаимодействия злоумышленника с жертвой

Говоря о поддельных (синтетических) личностях, их можно определить по следующим пунктам:

1. Фотографии, аватар профиля

Синтетические цифровые учетные записи имеют фотографии/рисунки, сгенерированные искусственным интеллектом. Рисунки, например, имеют характерное размытие диффузии: мягкие границы объектов, «заплывшие» текстуры, нечеткость деталей. До сей поры нейросети могут ошибаться и в анатомии: лишние пальцы, неправдоподобные изгибы конечностей и их сращивание, неверные пропорции. Некоторые модели нейросетевых технологий уже обучены работе с фотореалистичными изображениями и большинство подобных ошибок встречаются реже.

2. Биография профиля, данные о человеке

Зачастую, подобные данные будут также сгенерированы при помощи нейросети, с возможностью ручного редактирования.

3. История записей в социальных сетях

Злоумышленнику нужно создать имитацию социальной жизни, из-за чего создается череда публикаций, комментариев и различных репостов. Зачастую данные публикации не имеют глубокого контекста и четкой связи между собой.

4. Список контактов/друзей

Зачастую список друзей подобных личностей состоит из аналогичных профилей, специализированных ботов, а в крайних случаях – из взломанных аккаунтов настоящих людей.

5. Поведение

В зависимости от типа технологий нейросетей можно проследить паттерн имитации поведения: ответы одного стиля, излишне формальные и вежливые приветствия, «моментальные» ответы в точную секунду отправки жертвой собственного сообщения, и так далее.

Если же говорить о дипфейках, то создаются они либо с помощью GAN (Generative Adversarial Network), либо с использованием автокодировщика. [4]. Дипфейки же имеют гораздо более широкую область использования, и, соответственно, влияния. Они могут использоваться для следующих целей:

1. Дезинформационные кампании

Широкое распространение дезинформационных кампаний происходит в социальных сетях, особенно во время каких-либо важных общественных событий (выборы, катастрофы, резонансные события), для воздействия на широкий слой общественности.

2. Шантаж

Шантаж является одной из ключевых целей использования дипфейков. Если противостоять «краже личности», где примером выступает случай когда на контакт с пользователем выходит личность, широко известная в различных кругах, или некое государственное лицо – достаточно просто, то при подделке личности самой жертвы ситуация осложняется. Шантажисты могут «наложить» лицо человека на любое фото либо видео, чем и угрожают жертве, грозясь разослать этот контент его близким людям и родственникам, требуя выкуп.

3. Фишинг

Нечто похожее на шантаж, но подделывается личность близкого жертве человека. Зачастую это просьба о помощи в реальном времени, просьба перечислить денежные средства, либо получить какие-либо иные конфиденциальные данные.

Если говорить о признаках дипфейка и компрометации видео-контента, можно отметить следующие пункты:

1. Мимика лица

Так как нейросети все еще обучаются, они, как уже было указано ранее, могут допускать ошибки в анатомии лица в фотографиях, и «не успевать» за видеорядом в вопросе рендера лица. Изображение может быть дерганым, взгляд может быть «стеклянным», а кожа лица максимально гладкой.

2. Обстановка и освещение

Зачастую, визуальные артефакты происходят и на заднем фоне. Смазанные надписи, «дергающиеся» объекты, характерная искусственному интеллекту «рябь».

По реальным случаям можно привести пример того, как еще в 2023 году сотрудник из финансового отдела компании Arup, предоставляющей профессиональные услуги в области проектирования, архитектуры, планирования и консалтинга, филиал которой базировался в

Гонконге, перечислил злоумышленникам $25.000.000 после приглашения на видеозвонок якобы «старшим менеджером» компании. В видеозвонке также была симуляция других сотрудников и финансового директора компании, что сделало обстановку еще более убедительной для сотрудника. [6][7]

Чтобы защититься от подобных методов, достаточно быть осведомленным об отличительных особенностях сгенерированного контента и синтетических личностей, которые уже были описаны в тексте ранее, а также перепроверять подлинность предоставляемых людьми данных.

В корпоративных же сетях, взяв как пример ту же защиту баз данных, можно существуют дополнительные средства защиты информации помимо основных, что привязано к отдельно разработанной системе безопасности [8]. Подобные методы защиты подбираются компаниями соответственно.

Для вычисления вероятности успешной атаки и калькуляции ее факторов в работе были приведены характеристики, а также соответствующая им формула.

Таким образом, угроза мошенничества с использованием искусственного интеллекта в нынешнее время является в высшей степени актуальной. Предполагается, что с дальнейшим развитием информационных технологий и нейросетей всецелом возрастет и количество случаев мошенничества с использованием ИИ. Рекомендуется усилить комплекс мер по предотвращению подобных преступлений: повысить цифровую грамотность населения, развить технологии аутентификации, а также внести соответствующие законопроекты.

Список литературы

1. Бирих Э.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Э.В. Бирих // Вестник Санкт-Петербургского государственного университета телекоммуникаций. – 2024. – № 1. – С. 45-53.
2. Кузьмин А.М., Свичкарь Д.А., Хенкин П.В. Мошенничество с использованием синтетических цифровых личностей / Современные информационные технологии и ИТ-образование, [S.l.], v. 19, n. 2, p. 251-261, june 2023. ISSN 2411-1473.
3. Кузьмин А.М., Свичкарь Д.А., Хенкин П.В. Синтезированные цифровые личности / Сбер. – URL: https://www.sberbank.ru/ru/person/kibrary/experts/sintezirovannye-cifrovye-lichnosti
4. Как защищаться от дипфейков / Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake
5. Ashley D’Andrea, Kaylee Palak, Darren Guccione. What are deepfakes? / Keeper. URL - https://www.keepersecurity.com/blog/ru/2024/09/19/what-are-deepfakes/
6. Heather Chen, Kathleen Magramo / CNN. – URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
7. Cheng Leng, Chan Ho-him. Arup lost $25mn in Hong Kong deepfake video conference scam / Financial Times. – URL: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea?\
8. Защита информации в базах данных / Э. В. Бирих, Л. А. Виткова, В. В. Гореленко, Д. Б. Казаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и

научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 89-92. – EDN YRQKPJ.

9. Методология формирования модели угроз безопасности информационных систем / Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 103-107. – EDN NSLUFH.
10. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
11. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
12. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

References

1. Birikh E.V. Modeling a Secure Scalable Enterprise Network with Dynamic Routing Based on IPv6 / E.V. Birikh // Bulletin of the St. Petersburg State University of Telecommunications. - 2024. - No. 1. - pp. 45-53.
2. Kuzmin A.M., Svichkar D.A., Henkin P.V. Fraud Using Synthetic Digital Identities / Modern Information Technologies and IT Education, [S.l.], v. 19, n. 2, pp. 251-261, June 2023. ISSN 2411-1473.
3. Kuzmin A.M., Svichkar D.A., Henkin P.V. Synthesized Digital Identities / Sber. – URL: https://www.sberbank.ru/ru/person/kibrary/experts/sintezirovannye-cifrovye-lichnosti
4. How to protect yourself from deepfakes / Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake
5. Ashley D’Andrea, Kaylee Palak, Darren Guccione. What are deepfakes? / Keeper. URL - https://www.keepersecurity.com/blog/ru/2024/09/19/what-are-deepfakes/
6. Heather Chen, Kathleen Magramo / CNN. – URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
7. Cheng Leng, Chan Ho-him. Arup lost $25mn in Hong Kong deepfake video conference scam / Financial Times. – URL: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea?\

8. Information security in databases / E. V. Birikh, L. A. Vitkova, V. V. Gorelenko, D. B. Kazakov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 89–92. – EDN YRQKPJ.
9. Methodology for Forming a Model of Information System Security Threats / E.V. Birikh, E.Yu. Ryabov, D.V. Sakharov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of scientific articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 103-107. – EDN NSLUFH.
10. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 92-95. – EDN YRPZWJ.
11. Selection of tools for dynamic analysis of web application security for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Security. Inside. - 2024. - No. 1 (115). - Pp. 42-46. - EDN RLNHWK.
12. Research of ways to improve the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University. Technical sciences. - 2024. - Vol. 51, No. 3. - pp. 110-116. - DOI 10.21822/2073-6185-2024-51-3-110-116. - EDN HDGBOY.

Семеняка И.А. Метрики, логи и трейсы как основа мониторинга виртуализированной инфраструктуры // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 62–69

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

МЕТРИКИ, ЛОГИ И ТРЕЙСЫ КАК ОСНОВА МОНИТОРИНГА ВИРТУАЛИЗИРОВАННОЙ ИНФРАСТРУКТУРЫ

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

В статье рассматриваются подходы к мониторингу виртуальной инфраструктуры на основе триады наблюдаемости: метрик, логов и трейсов. Анализируется роль каждого типа данных в обеспечении прозрачности работы распределённых систем, а также особенности их формирования и интерпретации в операционных системах семейства Linux. Отдельное внимание уделяется источникам системных метрик, механизмам журналирования и принципам распределённой трассировки запросов. Рассматриваются современные инструменты мониторинга Prometheus, Loki и Grafana, их архитектурные особенности и области применения. Результаты работы ориентированы на практическое использование при проектировании и эксплуатации виртуализированных и контейнерных сред.

Ключевые слова: Мониторинг, наблюдаемость, виртуальная инфраструктура, метрики, логи, трейсы, Linux, Prometheus, Loki, Grafana.

THE CONCEPT OF ZERO TRUST AS THE BASIS OF MODERN CORPORATE SECURITY

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

The article discusses approaches to monitoring virtual infrastructure based on the triad of observability: metrics, logs and traces. The role of each type of data in ensuring the transparency of the operation of distributed systems is analyzed, as well as the features of their formation and interpretation in operating systems of the Linux family. Special attention is paid to the sources of system metrics, logging mechanisms and the principles of distributed request tracing. Modern monitoring tools Prometheus, Loki and Grafana, their architectural features and areas of application are considered. The results of the work are focused on practical use in the design and operation of virtualized and container environments.

Keywords: Monitoring, observability, virtual infrastructure, metrics, logs, traces, Linux, Prometheus, Loki, Grafana.

Введение

Современные информационные системы становятся всё более распределёнными, динамичными и нагруженными, что существенно повышает требования к их надёжности и предсказуемости. На помощь приходит мониторинг, который выступает основным механизмом обеспечения стабильности и наблюдаемости вычислительных сред. [1] Он позволяет своевременно выявлять отклонения в работе сервисов, анализировать

производительность и собирать важную информацию для принятия инженерных решений. В практиках DevOps мониторинг является неотъемлемой частью культуры непрерывной доставки (CI/CD) и концепции Observability, предназначенной повысить прозрачность поведения систем и дать понимание их внутреннего состояния.

Особое значение мониторинг приобретает в виртуальных инфраструктурах. Виртуализация усложняет интерпретацию метрик: гипервизор распределяет ресурсы между машинами динамически, контейнеризация изолирует приложения с помощью namespaces и cgroups, а вычислительные узлы часто работают в мультитенантной модели. Эти особенности изменяют характер наблюдаемых параметров и требуют учёта дополнительных уровней абстракции. Источники данных в Linux — такие как псевдофайловые системы /proc и /sys, механизмы контроля ресурсов и подсистемы ядра — предоставляют лишь частичное представление о состоянии системы, которое необходимо корректно соотносить с контекстом виртуализации.[2]

Цель данной работы — провести системный анализ собираемых при мониторинге трёх основных типов данных: метрик, логов и трейсов, а также показать их роль в обеспечении наблюдаемости виртуальной инфраструктуры. В статье рассматриваются механизмы формирования и интерпретации этих данных в Linux, анализируются современные инструменты сбора и визуализации (Prometheus, Loki, Grafana).

Типы данных, собираемые при мониторинге, и их значение

В практиках мониторинга принято выделять три основных типа данных — метрики, логи и трейсы. Совместное использование метрик, логов и трейсов даёт возможность анализировать систему с разных точек зрения. [3] Такой подход упрощает оценку как количественных характеристик работы сервисов, так и особенностей их поведения в различных режимах нагрузки.

Метрики представляют собой числовые значения, отражающие текущее состояние ресурсов и сервисов во времени. На практике они используются для оценки загрузки процессора, потребления памяти, активности операций ввода-вывода и других параметров производительности. За счёт компактного и строго структурированного формата метрики удобны для хранения и автоматической обработки, однако в большинстве случаев они не дают прямого ответа на вопрос о причинах возникновения сбоев.

Логи содержат записи о событиях, происходящих в операционной системе и прикладных сервисах. За счёт высокой детализации они позволяют восстановить ход выполнения операций, выявить ошибки и проанализировать поведение приложений. При этом с ростом объёма журналов возрастает сложность их анализа, что делает необходимым использование средств структурирования и индексирования данных.

Трейсы — это по сути история того, как запрос проходит через разные части распределённой системы. Они позволяют увидеть, кто кого вызывает, где именно появляется задержка и какая часть цепочки начинает «сыпаться». В отличие от обычных логов или сухих метрик, трейсы дают более цельную картину: видно не только факт ошибки или рост времени ответа, но и почему это произошло. Из-за сложности настройки их внедряют не так часто, как хотелось бы, но когда они всё-таки есть, диагностировать проблемы и разбираться в реальной производительности становится значительно проще.

В данной работе рассматриваются три популярныхых решения выполняют взаимодополняющие роли.

Метрики

Метрики лежат в основе большинства современных систем мониторинга, поскольку позволяют количественно оценивать состояние ресурсов и сервисов.

В системах мониторинга принято выделять четыре основные категории метрик. Счётчики (counters) представляют собой неубывающие величины, увеличивающиеся в процессе накопления событий, например количество байтов, переданных сетевым интерфейсом, или число обработанных запросов. Они удобны для вычисления скоростей изменения (rate). Gauge-метрики фиксируют мгновенное состояние системы: объём используемой памяти, текущую загрузку процессора, количество активных соединений. Такие значения могут как увеличиваться, так и уменьшаться, что делает их ключевыми при мониторинге изменяющихся ресурсов. Гистограммы (histograms) используются для анализа распределений, прежде всего задержек или размеров запросов.[4]

К основным требованиям к метрикам относятся точность, агрегируемость и корректный выбор интервала опроса. Слишком частый сбор данных увеличивает нагрузку на систему и хранилище, а слишком редкий — делает невозможным выявление быстрых аномалий.

Метрики в Linux формируются главным образом через виртуальные файловые системы ядра — /proc и /sys, предоставляющие структурированный интерфейс к внутреннему состоянию ОС.

Подсистема /proc содержит множество файлов, динамически формируемых ядром. Файл /proc/stat предоставляет данные о времени работы CPU. Файл /proc/meminfo описывает состояние памяти, включая общий объём, свободную память, буферы, кэш и использование swap. Метрики, связанные с сетевыми интерфейсами, публикуются в /proc/net/dev. Эти данные позволяют анализировать входящий и исходящий трафик, а также потери пакетов.

Интерфейс sysfs (/sys) дополняет эти данные сведениями об устройствах, драйверах и параметрах ядра, что особенно важно в виртуализированных средах, где часть оборудования представлена виртуальными компонентами.

Дополнительный уровень детализации обеспечивают cgroups, применяемые для ограничения и учёта потребления ресурсов контейнерами. Они позволяют отслеживать использование CPU, памяти и операций ввода-вывода в пределах заданных лимитов, что делает их ключевым источником метрик в контейнерных платформах.

Логи

Логи — это текстовые или бинарные записи, фиксирующие события, происходящие в операционной системе, приложениях или сервисах. Они служат ключевым источником детализированной диагностической информации. Благодаря чтению журнала можно восстановить последовательность операций, выявить ошибки.

По структуре логи могут быть неструктурированными и структурированными. Неструктурированные логи представляют собой свободный текст, который легко генерировать, но сложнее автоматически обрабатывать. Структурированные логи используют поля фиксированного формата (например, JSON), что облегчает автоматический разбор, индексирование и дальнейший анализ. Современные системы мониторинга и лог-агрегации

стремятся переходить к структурированным данным, поскольку они позволяют проводить более точные поисковые запросы и корреляцию событий.

Уровни логирования определяют важность или критичность сообщения. Примерами таких уровней являются debug, info, warning, error и critical. Они помогают администраторам фильтровать сообщения, определять тип произошедшего события и быстрее реагировать на реально важные события. [5] Правильная настройка уровней логирования особенно важна в высоконагруженных системах, поскольку избыток диагностических сообщений может приводить к переполнению дискового пространства и затруднять анализ.

В Linux традиционно используются две взаимосвязанные системы логирования: syslog и journald.

Syslog является классической подсистемой журналирования, широко использующейся в различных Unix-подобных системах. Архитектура syslog предполагает наличие демона (например, rsyslog или syslog-ng), принимающего сообщения от приложений через unix-сокет /dev/log или по сети. Сообщения syslog имеют стандартизованный формат, включающий метку времени, имя хоста, идентификатор процесса и текст сообщения. Каждая запись в syslog содержит facility (источник события) и severity (критичность события). Это может быть удобным для фильтрации и поиска сообщений. Syslog поддерживает отправку журналов по сети, что открывает возможности на организации централизированного мониторинга.

Современные дистрибутивы Linux используют journald, входящий в состав systemd. Он предоставляет бинарный журнал, содержащий расширенный набор метаданных: идентификаторы процессов, cgroups, имена юнитов systemd, дополнительные параметры среды. Journald поддерживает структурированный формат хранения данных, что облегчает фильтрацию и обеспечивает повышенную эффективность работы. С помощью утилиты journalctl администратор может выполнять фильтрацию по времени, юнитам, приоритетам и другим критериям. Важной особенностью journald является возможность ограничения размера журналов в соответствии с заданными правилами.

Объём логов в системах высокой нагрузки может расти чрезвычайно быстро, поэтому важнейшей задачей является корректное управление.

Утилита logrotate обеспечивает ротацию логов. Это происходит в соответствии с заданной политикой: ежедневной, недельной или по достижению определённого размера. Ротация делает возможным эффективное удаление устаревших записей, а также архивирование и сжатие старых журналов.

Индексация — это способ организовать логи так, чтобы их можно было быстро фильтровать. При этом можно опираться на временные промежутки, уровни сообщений, нужные процессы и т. д. Благодаря индексам доступ к данным остаётся быстрым даже тогда, когда хранилище разрастается до ощутимых размеров.

Трейсы

Трейсы используются для анализа того, как конкретный запрос проходит через распределённую систему. В отличие от метрик и логов, которые фиксируют состояние или отдельные события, трассировка позволяет восстановить последовательность вызовов между компонентами и увидеть, на каких этапах обработки возникают задержки.

Каждый трейс состоит из набора связанных между собой участков выполнения (span), описывающих отдельные операции. Для каждого такого участка фиксируются временные

характеристики и контекст выполнения, что позволяет проследить путь запроса от точки входа до формирования ответа. На основе этих данных формируется граф выполнения, отражающий реальные взаимодействия между сервисами.

Практическая ценность трейсов особенно заметна в распределённых и микросервисных архитектурах. Когда обработка одного запроса включает обращение к нескольким сервисам, базам данных и промежуточным компонентам, традиционных метрик и логов часто оказывается недостаточно. Трассировка в таких случаях позволяет локализовать источник задержек и понять, какой именно компонент влияет на общее время отклика.

При этом использование трейсов связано с дополнительными сложностями. Для их сбора требуется инструментирование приложений и поддержка передачи контекста между компонентами. По этой причине в небольших инфраструктурах трассировка применяется реже и, как правило, используется выборочно. Тем не менее при анализе производительности сложных систем трейсы остаются одним из наиболее информативных источников данных и эффективно дополняют метрики и логи.

Современные инструменты мониторинга

Современные системы мониторинга виртуальной инфраструктуры широко используют специализированные инструменты, ориентированные на высокую масштабируемость, гибкость и глубокий аналитический потенциал. В данной работе рассматриваются три популярныхых решения: Prometheus, предназначенный для сбора и анализа метрик; Loki, обеспечивающий эффективную обработку логов; и Grafana, выполняющая роль универсальной платформы визуализации.

Prometheus

Prometheus — это система мониторинга, основанная на сборе метрик во временных рядах (time-series). Её архитектура строится вокруг модели pull, при которой сервер Prometheus самостоятельно опрашивает целевые узлы по протоколу HTTP. Такой подход снижает зависимость от внешних агентов и позволяет централизованно контролировать частоту опроса и состояние источников данных.

Основные инструменты сбора метрик называются экспортеры. Это небольшие программы, предоставляющие метрики в формате, совместимом с Prometheus. Существуют стандартные экспортеры для операционных систем, баз данных, веб-серверов и сетевых устройств, а также возможность разработки собственных.

Хранение данных организовано в формате time-series, где каждая метрика представляет собой набор точек «значение-время», дополненный набором меток (labels), определяющих источник и контекст данных.

Prometheus предоставляет мощный язык запросов PromQL, позволяющий выполнять различные операции над метриками. Базовые запросы включают выборку временных рядов по имени метрики и фильтрацию по меткам.

Язык запросов PromQL позволяет выполнять выборку и агрегацию метрик по заданным меткам и временным интервалам, что даёт возможность анализировать состояние ресурсов и динамику их изменения. С его помощью можно оценивать загрузку процессора, использование памяти и другие показатели производительности без привязки к конкретной реализации источника данных.

PromQL предоставляет набор агрегирующих функций, которые позволяют работать с данными более гибко. Например:

1. sum() собирает значения по указанным меткам;
2. avg() рассчитывает среднее;
3. rate() показывает скорость изменения счётчиков во времени;

Такие выражения позволяют быстро оценить текущую нагрузку системы и понять, где именно могут возникать узкие места.

Loki

Loki — это система для хранения и обработки логов, созданная по тем же архитектурным принципам, что и Prometheus, но адаптированная под текстовые данные. Ключевое отличие Loki в том, что она не индексирует сами сообщения. В индекс попадают только метки (labels), описывающие источник и контекст логов, а полный текст помещается в последовательные chunks. Такой подход уменьшает объём хранилища и заметно ускоряет поиск.

Передача логов в Loki обычно выполняется через агент promtail. Он читает локальные файлы, добавляет необходимые метки и отправляет потоки данных на сервер. При необходимости promtail может разбирать формат сообщений (парсинг) и приводить их к единому виду.

Для запросов Loki использует свой язык — LogQL. Он объединяет фильтрацию по меткам и полнотекстовый поиск в сообщениях. Например, чтобы найти строки с ошибками в системном журнале, можно выполнить запрос {job="system"} |= "error".

Помимо поиска, LogQL умеет строить метрики на основе логов — фактически он играет ту же роль, что PromQL, только для текстовых данных.

Grafana

Grafana — это платформа для визуализации и анализа данных мониторинга. Она поддерживает множество источников, среди которых Prometheus, Loki, Elasticsearch, InfluxDB и другие системы. Grafana позволяет собирать дашборды, строить графики, работать с таблицами и настраивать оповещения, обеспечивая единое окно для наблюдения за состоянием инфраструктуры.

Платформа предоставляет широкий набор визуальных компонентов:

1. Графики временных рядов для отображения динамики метрик;
2. Таблицы, подходящие для анализа логов и агрегированных данных;
3. Алерты, автоматически генерируемые на основе пороговых значений PromQL/LogQL-запросов;
4. Панели корреляции, позволяющие сопоставлять метрики и логи в едином интерфейсе.

Grafana играет ключевую роль в интегрированной мониторинговой системе, объединяя телеметрию различного типа и обеспечивая удобные средства анализа состояния виртуальной инфраструктуры.

Заключение

Мониторинг виртуальной инфраструктуры является ключевым элементом обеспечения стабильности, производительности и предсказуемости современных распределённых систем.

Использование метрик, логов и трейсов в совокупности дает целостное представление о состоянии инфраструктуры и поведении сервисов на разных уровнях абстракции. В статье показано, что каждый тип данных решает собственный класс задач и наиболее эффективен при комплексном применении в рамках концепции наблюдаемости.

Рассмотренные инструменты Prometheus, Loki и Grafana формируют гибкую и масштабируемую экосистему мониторинга, адаптированную под особенности виртуализированных и контейнерных сред. Их совместное использование упрощает сбор, анализ и визуализацию телеметрии, а также способствует более быстрому выявлению и диагностике инцидентов. Полученные выводы могут быть использованы при построении систем мониторинга в инфраструктурах различного масштаба и назначения.

Список литературы

1. Развитие стандартов и руководств в сфере облачных технологий/Э.В.Бирих, Л.А. Виткова, М.В.Левин, М.В.Чмутов//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
2. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
3. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
4. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН / Э. В. Бирих, М. Д. Булова, А. А. Казанцев, А. А. Миняев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 122-127. – EDN FBPSIL.
5. Бирих, Э. В. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти / Э. В. Бирих, А. С. Гаврилов, Е. Н. Сацук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 104-107. – EDN XSUFFR.

References

1. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Current problems of information telecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International Scientific-Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 01–02, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2017. – pp. 92-95. – EDN YRPZWJ.
2. Selection of tools for dynamic analysis of web application security for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Protection. Insider – 2024. – No. 1(115). – pp. 42-46. – EDN RLNHWK.
3. Research on ways to improve the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [etc.] // Bulletin of the Dagestan State Technical University. Technical Sciences. – 2024. – T. 51, No. 3. – P. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
4. Development of a software module for automating the determination of the level of security in IPDN / E. V. Birikh, M. D. Bulova, A. A. Kazantsev, A. A. Minyaev // Current problems of information telecommunications in science and education (APINO 2024): Proceedings of the XIII International Scientific-Technical and Scientific-Methodological Conference, St. Petersburg, February 27–28 2024. – St. Petersburg: St. Petersburg State University of Telecommunications named after. prof. M.A. Bonch-Bruevich, 2024. – pp. 122-127. – EDN FBPSIL.
5. Birikh, E. V. Modern problems of ensuring internal security of a distributed network of public authorities / E. V. Birikh, A. S. Gavrilov, E. N. Satsuk // Current problems of information telecommunications in science and education (APINO 2018): VII International scientific-technical and scientific-methodological conference. Collection of scientific articles. In 4 volumes, St. Petersburg, February 28 – 01, 2018 / Edited by S.V. Bachevsky. Volume 1. – St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2018. – pp. 104-107. – EDN XSUFFR.

Воронов Д.С., Ачкасова В.А. (научный руководитель). Роль технологий искусственного интеллекта в электоральных проектах // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 70–81

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8:324:316.77.

РОЛЬ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭЛЕКТОРАЛЬНЫХ ПРОЕКТАХ

[1]Воронов Д.С., **Ачкасова В.А**. (научный руководитель)
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Санкт-Петербург, Россия (199034, город Санкт-Петербург, Университетская наб., д.7/9), e-mail: [1]voronovd2002@gmail.com

Развитие нейросетевых технологий как тренд XXI века оказывает заметное влияние на социальное пространство в целом и коммуникационные паттерны в частности. Генеративный искусственный интеллект (ChatGPT, Midjourney, GigaChat, Kandinsky) имеет большой потенциал влияния на медиаландшафт, трансформацию общественного и политического дискурса. Обладая значительным функционалом в области анализа и генерации контента, нейросети с каждым годом играют все большую роль в коммуникационной деятельности в целом и в коммуникационном сопровождении политических проектов в частности. В ближайшие годы ожидается дальнейшее развитие и распространение нейросетевых технологий в коммуникационной деятельности, повышение их значимости в политических проектах с перспективой полной замены традиционных инструментов и даже специалистов по политическому консультированию, политическому PR через 7-10 лет.

В статье изучаются генеративные нейросети, применяемые для создания текстового и визуального контента как актор коммуникации. На основе метода кейс-стади и вторичного анализа социологических исследований авторы анализируют роль ИИ в формировании и трансформации политического дискурса, а также паттерны организации коммуникационного сопровождения политических проектов с применением ИИ, перспективы и ограничения применения искусственных нейронных сетей в политической коммуникации.

Ключевые слова: Генеративный искусственный интеллект, нейросети, коммуникация, дискурс, политическая коммуникация, контент.

THE ROLE OF GENERATIVE NEURAL NETWORKS IN ELECTORAL PROJECTS

[1]Voronov D.S., **Achkasova V.A**. (supervisor)
"ST. PETERSBURG STATE UNIVERSITY", St. Petersburg, Russia (199034, Saint-Petersburg, Universitetskaya nab., 7/9), e-mail: [1]voronovd2002@gmail.com

The development of neural network technologies as a trend of the 21st century has a noticeable impact on social space in general and communication patterns in particular. Generative artificial intelligence (ChatGPT, Midjourney, GigaChat, Kandinsky) has a great potential to influence the media landscape, transforming social and political discourse. Having a significant functionality in the field of analysis and content generation, neural networks play an increasingly important role every year in communication activities in general and in the communication support of political projects in particular. In the coming years, it is expected that the development and dissemination of neural network technologies in communication activities will continue, increasing their importance in political projects with the prospect of complete replacement of traditional tools and even specialists in political advice, political PR in 7-10 years.

The article studies generative neural networks, used to create text and visual content as a communication actor. On the basis of the method of case-study and secondary analysis of sociological studies, authors analyze the role of AI in the formation and transformation of political discourse, as well as patterns of organization of communication support of political projects with the use of AI, The prospects and limitations of artificial neural networks in political communication.

Keywords: Generative artificial intelligence, neural networks, communication, discourse, political communication, content.

Введение

Актуальность исследования роли искусственного интеллекта (ИИ) в политических проектах обусловлена стремительным развитием и внедрением нейросетей во многие сферы жизни общества. Так, направление, связанное с технологиями искусственного интеллекта, по оценкам аналитиков, будет одним из самых быстрорастущих в будущем. Согласно прогнозам экспертов компьютерной области, за десятилетие (2022-2032) доходы в направлениях, связанных с генеративным ИИ вырастут в 30 раз [1].

Умные технологии активно внедряются и в политические проекты. За последние годы тема распространения ИИ звучала в рамках саммита G7 в Хиросиме в 2023 г [2]., стала центральной темой международного Саммита в Лондоне (2023г.) [3], а также одного из специальных заседаний Совета безопасности ООН [4].

ИИ уже активно используется в политических проектах, при анализе общественного мнения, создании и распространении политического контента в социальных сетях и медиа. Эти процессы трансформируют традиционные формы политического дискурса и ставят новые вопросы о роли ИИ в формировании общественного сознания и принятии людьми политических решений.

В числе проблем, связанных с влиянием технологий ИИ на политический дискурс, можно выделить:

1. Трансформацию публичной сферы и политического дискурса.
2. Анализ данных и персонализация коммуникации.
3. Создание и распространение контента.
4. Вызовы для демократических институтов.

Изучение этих проблем требует междисциплинарного подхода и проведения исследований на стыке коммуникационных наук, политологии, теории коммуникации, социологии и компьютерных наук.

Уникальность ИИ как инструмента в коммуникационных проектах заключается в его способности к обучению, анализу больших объемов данных, персонализации взаимодействия и автоматизации процессов. Эти возможности делают ИИ мощным и гибким инструментом по сравнению с традиционными технологиями, позволяя организациям более эффективно взаимодействовать с аудиторией и адаптироваться к быстро меняющемуся миру.

Если говорить о значимости ИИ в политической коммуникации, очевидно, что искусственный интеллект играет все более важную роль в коммуникационном сопровождении политических проектов, трансформируя способы взаимодействия с избирателями и оптимизируя процессы управления кампаниями.

Данная работа будет посвящена изучению роли искусственных нейронных сетей в политических проектах, теоретических и практических аспектах его применения при реализации коммуникационных задач, а также перспектив и ограничений технологий ИИ как нового инструмента в политическом PR.

Результаты данного исследования могут иметь практическое применение в разработке политических стратегий и регулировании использования ИИ в политической сфере, а также в повышении медиаграмотности и критического мышления пользователей в отношении политического контента, создаваемого с помощью ИИ. Кроме того, исследование может

способствовать развитию междисциплинарного диалога о социальных и политических последствиях внедрения ИИ и выработке этических принципов его использования. В долгосрочной перспективе нейросети могут стать важным фактором изменения политических институтов и процессов, изменения форм политического участия и представительства, а также переосмысления самих основ демократии в условиях «алгоритмической» медиаполитики. Трансформация политического дискурса в результате применения и распространения генеративных технологий ИИ – очередной признак «новой нормальности». Могут ли нейросети стать полноценным субъектом его формирования? Какие качества создают перспективы и ограничения применения ИИ в политических проектах? Ответы на эти вопросы даст человек 21-го века.

Теория

Исследователи искусственного интеллекта отмечают, что развитие нейросетевых технологий провоцирует ряд социально-политических изменений. Так, например, увеличивается «цифровой разрыв» [5] - разница между практиками цифрового взаимодействия и применения технологий разными поколениями. Изменяется и соотношение сил на рынке медиауслуг – крупный медиабизнес, имеющий возможность инвестировать в технологии ИИ и внедрять их в свою работу начинает опережать небольшие компании еще быстрее, увеличивая разрыв и трансформируя медиаландшафт [6].

Эксперты отмечают, что повсеместное распространение технологий искусственного интеллекта, и, в частности, генеративных нейросетей в первую очередь затронет представителей интеллектуальных, творческих и креативных профессий, составляющих группу так называемых «белых воротничков», к которым относятся и маркетологи, PR-специалисты, политологи и политические консультанты.

При этом на сегодняшний день очевидно, что технологии эти глубоко проникли в нашу действительность. Несмотря на существенные ограничения, вызванные внедрением санкций, в России существует ряд субъектов, формирующих медиапространство и цифровую экосистему в соответствии с мировыми трендами. К ним относятся «Сбер», VK, «Яндекс», Telegram. Каждая из названных компаний активно внедряет технологии искусственного интеллекта, в том числе генеративные нейросети, в повседневную жизнь. Согласно исследованию, проведенному в августе 2024 года «Яков и Партнеры» совместно с «Ромир», 84% жителей России осведомлены о существовании и функциях ИИ [7], а 24% пользуются нейросетями в повседневной жизни или профессиональной деятельности.

При этом внедрение технологий искусственного интеллекта в повседневную жизнь трансформирует и сами представления людей о сути коммуникации. В данном случае нейросети выступают в качестве «медиатора действительности», все более явно изменяя политические, социальные, научные и творческие процессы. Важнейший вопрос в определении роли технологий искусственного интеллекта в формировании дискурса – может ли формировать дискурс актор, лишенный таких качеств, как креативность и рефлексия?

На сегодняшний день мы можем выделить ключевые научные подходы к дискурсу в социальных науках:

1. Лингвистический (Бенвенист);
2. Социально-философский (Фуко);
3. Социокогнитивный (Ван Дейк);

4. Теория коммуникативного действия (Хабермас);
5. Критический дискурс анализ (Фэркло, Водак).

Общими признаками дискурса в этих подходах являются:

- Наличие субъекта;
- Наличие сообщения;
- Возможность передачи через речь и текст;
- Наличие позиции и обстоятельств в сообщении.

Перечисленные концепции дискурса дают нам целостное понимание механизмов формирования и изменения социальной действительности через коммуникацию. При этом, в зависимости от специфики этой коммуникации, мы можем прогнозировать коммуникативный результат, строить модели донесения информации в зависимости от цели, аудитории, социальных условий. Можно предположить, что на основе перечисленных концепций можно и создавать алгоритмы для генерации и анализа эффективности контента в рамках политических проектов. Теории дискурса как основа для выстраивания политической коммуникации могут быть актуальны для таких задач, как:

1. Проведение электоральных кампаний (Бенвенист);
2. Формирование общественного мнения (Фуко);
3. Политическая риторика и пропаганда (Рут, Фэркло);
4. Публичная политика и обсуждение социальных проблем (Хабермас);
5. Социальные движения (Ван Дейк).

Таким образом, концепции дискурса в политической коммуникации дают инструментарий для анализа коммуникативных практик, правил, норм, и их влияния на формирование, распределение и сопротивление власти в конкретном обществе. В рамках политических проектов теоретические положения данных теорий можно использовать для разработки наиболее эффективных моделей коммуникации в рамках политической борьбы, создания механизмов производства контента, написания и распространения политических текстов, речей, для достижения политических целей.

Для понимания работы сервисов ИИ и возможностей манипулирования ими, целенаправленного применения в рамках трансформации дискурса и изменения общественного мнения нам необходимо хотя бы базово изучить технико-технические характеристики и механизмы работы нейросетевых алгоритмов.

История становления и развития технологий искусственного интеллекта описана в работе В. Н. Авдонина и В. Л. Силаевой «Нейросети нового поколения в контексте технологий искусственного интеллекта, философии и социально-политических наук» [8]. Как отмечают авторы, разработка искусственных нейронных сетей началась еще в середине XX века. Первые математические модели нейронных сетей и первые программы обучения искусственных нейросетей возникли в 1940-е годы, появление нейросетей с различной архитектурой и рост разнообразия типов их обучения относят к 1980-м годам, а выход на рынок и широкое распространение языковых программ, сервисов и алгоритмов на базе нейросетей произошло лишь с 2010-х годов [9].

В основу развития нейросетей в современном их понимании легли инновационные математические и статистические подходы (байесовская статистика, «нечеткая логика», роевой интеллект, исследования естественных языков и др.), которые позволили справляться с неопределенностью и сложностью вычислительных процессов и создали преимущества

перед классическими компьютерными моделями, основанными на символических вычислениях. Так, ядром современных ИИ стали нейронные сети, основанные на вероятностно-статистическом методе.

Генеративный же искусственный интеллект, который является предметом данной работы, относится к классу искусственных нейросетей нового поколения. Его уникальность заключается в возможности создавать понятные человеку продукты (коды, тексты, изображения, видео) и модифицировать их согласно указаниям и подсказкам пользователя. Кроме того, новые генеративные нейросети способны выполнять широкий круг задач и создавать разнообразный высококачественный контент, что стало возможным благодаря их глубокому обучению и сложной структуре. Сети этого класса реализуют новейшие Большие языковые модели (LLM), состоящие из миллиардов параметров и прошедшие через «глубокое обучение» на миллиардах слов/символов [10].

Для того, чтобы оценить релевантность применения искусственных нейронных сетей в политической коммуникации и политических проектах, разберем типичные этапы политического проекта и задачи, возникающие в рамках его реализации. Стоит отметить, что большинство классических работ по тематике публичных коммуникаций, коммуникационного проектирования и политического проектирования были написаны до повсеместного распространения нейросетей, а значит и принципы подготовки и реализации политических проектов были сформулированы без учета возможностей искусственного интеллекта. Безусловно, внедрение новых умных технологий может значительно изменить механику и алгоритм разработки и реализации коммуникационного проекта в будущем, однако в рамках данного исследования мы рассмотрим релевантность технологий ИИ в существующей парадигме коммуникационного проектирования.

В общем виде коммуникационный проект состоит из нескольких этапов, в рамках каждого из которых выполняется ряд задач. Этими этапами и задачами, соответствующими этапам, являются [11]:

1. Аналитический этап. В рамках этапа выполняются такие процедуры, как ситуационный анализ, анализ рынка, конкурентный анализ, анализ аудитории, анализ стейкхолдеров, коммуникативный аудит, SWOT-анализ, PEST- или PESTLE-анализ.
2. Креативный этап. Этап предполагает разработку ключевых сообщений под разные целевые аудитории, креативных форматов и каналов для трансляции этих сообщений, подбор референсов и примеров визуального и текстуального оформления контента.
3. Этап планирования. На данном этапе формируется контент-план, SMM-план, бюджетный план, прописываются сроки реализации проекта и разделение проекта на этапы в соответствии с избранной методологией управления.
4. Этап реализации. В рамках данного этапа происходит непосредственный запуск коммуникационной кампании (реализация всех запланированных мероприятий, включая публикацию контента, запуск рекламных акций и активное взаимодействие с аудиторией), отслеживается выполнение всех запланированных действий, контроль за соблюдением сроков и бюджета, корректируется формат и содержание контента и сообщений в зависимости от откликов аудитории и текущих событий, производится сбор обратной связи, отзывов от целевой аудитории и стейкхолдеров для оценки текущей реакции на кампанию.
5. Этап оценки эффективности. На этом этапе происходит сбор данных и аналитика, анализ KPI, оценка ROI (анализ возврата инвестиций), проводится сравнительный анализ

(сравнение полученных результатов с предыдущими кампаниями или с плановыми показателями), подготавливаются отчеты (составляется итоговый отчет о результатах проекта, включая выводы и рекомендации по улучшению будущих кампаний) и производится презентация результатов команде и клиенту или руководству организации.

Таким образом, в ключевых теоретических работах (Азарова, Ачкасова, Иванова и др., 2009; Ачкасова, Борисова, Быков и др., 2022; Ачкасова, Минтусов, Филатова и др., 2021; Чередов, 2016), посвященных коммуникационному проектированию в целом и коммуникационной деятельности в сфере политики в частности сформулированы этапы коммуникационного проекта, выделены ключевые задачи на каждом из этапов. При реализации таких проектов специалист зачастую применяет множество методов, использование которых требует высокой квалификации, значительного опыта и серьезного временного ресурса. Как видно из технических характеристик, алгоритма работы и функционала технологий ИИ на сегодняшний день они способны взять на себя часть функций специалиста, значительно сократив при этом время на их выполнение. Единственная функция, которую не может взять на себя искусственный интеллект – офлайн-коммуникация, которая является важнейшим аспектом, например, в электоральных проектах и GR-деятельности. Существующие попытки реализовать эту задачу пока носят примитивный характер [12].

Наиболее же релевантным применение технологий ИИ будет при реализации стратегических и аналитических задач – обработка больших массивов информации, обзор источников, анализ социологических данных, подготовка бюджетного и календарного планов, ситуационный анализ, анализ аудитории, формулирование ключевых сообщений, и пр. В будущем, по мере усложнения нейросетевых алгоритмов и увеличения мощности нейросетей ожидается и развитие их креативных функций – возможности самостоятельного творчества без опоры на существующие примеры.

Таким образом, ряд уникальных возможностей генеративного искусственного интеллекта могут быть использованы при реализации коммуникационных задач в политических проектах.

Результаты и обсуждение

Помимо теоретической части, в научном сообществе расширяется и корпус исследований, посвященных практическому применению технологий ИИ в маркетинге, PR, политическом консалтинге и стратегических коммуникациях. В рамках этого направления акцент делается на изучении функционала приложений и сервисов на базе ИИ, оценке их релевантности и перспектив со стороны специалистов.
Между тем, работ, в которых бы проводился обзор существующих технологий и видов нейросетей, была проведена понятная классификация и типологизация до сих пор нет. Это является проблемной областью в изучении ИИ с точки зрения формирования фундаментальной научной теории.

Для оценки перспектив и ограничений применения новых искусственных нейронных сетей и сервисов на их основе в политических проектах помимо теории необходимо проанализировать и широкий корпус эмпирического материала на основе метода вторичного анализа социологических исследований и кейс-стади. В последние годы все больше работ охватывают область практического использования умных технологий в области

коммуникации, выделяются преимущества и недостатки сервисов на базе ИИ перед специалистами, формулируются прогнозы и рекомендации.

В исследовании Оксфордского университета в 2020 году было зафиксировано применение технологий ИИ в политической сфере в 81 стране. Если рассматривать основные технологии искусственных нейросетей подробнее, то ими были [13]:

1. Базы данных для распознавания лиц;
2. Дипфейки (сервисы для создания и копирования человеческого голоса, а также генерации изображения реального человека в формате фото или видео);
3. Микротаргетинг;
4. Чат-боты;
5. Сервисы для генерации контента (тексты, изображения, видео, аудио, и др.).

В рамках обзорной работы Российского Совета по международным делам (РСМД) исследователи выделили основные направления применения нейросетевых технологий в политике [14]:

1. Создание контента для политической агитации (изображения, фото, видео, аудио, тексты);
2. Применение чат-ботов для коммуникации с избирателями;
3. Анализ big data для оценки предпочтений избирателей;
4. Создание прогнозов, развитие предсказательных моделей на основе анализа big data;
5. Сегментирование аудитории, подготовка и рассылка таргетированных сообщений;
6. Анализ и выявление фейков в кампаниях конкурентов;
7. Проведение социологических исследований (опросов и интервью) и анализ результатов.

В сообщениях крупнейших отечественных и мировых СМИ и научных работах, посвященных применению ИИ в реальных политических кампаниях, наиболее часто упоминаются следующие нейросетевые технологии:

1. Дипфейки;
2. Чат-боты;
3. Генеративные модели;
4. Модели для анализа больших данных (big data);
5. Модели для анализа аудитории, разработки и рассылки таргетированных сообщений.

Современные работы в области теории и практики применения ИИ в политической коммуникации (Gacanin, Di Renzo, 2020; Karnouskos, 2020; Kerr, Barry, Kelleher, 2020) подтверждают возможность повышения точности данных, получаемых при анализе, качества создаваемого контента, более глубокой персонализации политических сообщений, оптимизации временных и трудовых затрат при реализации кампании.

Среди наиболее перспективных направлений внедрения ИИ в сферу политического управления по результатам исследования РЭУ им. Г. В. Плеханова стали [15]:

1. Аналитика данных;
2. Прогнозирование;
3. Мониторинг;
4. Политическая коммуникация;
5. Демократизация политических процессов;

В 2023 году было опубликовано исследование коллектива авторов из НИУ ВШЭ и МГУ им. М. В. Ломоносова, посвященное использованию технологий искусственного интеллекта в российской индустрии медиа и коммуникаций (Давыдов, Лукина, Замков, Крашенинникова, 2023). Работа состояла из двух частей – качественного (15 глубинных интервью с экспертами) и количественного (анкетирование 176 респондентов) социологических исследований [16].

Результаты показали, что применение нейросетевых технологий в коммуникационных профессиях имеет широкую распространенность. Так, более 70% респондентов отметили, что используют нейросети в профессиональной деятельности.

Результаты исследования свидетельствуют о том, что представители медиа индустрии позитивно оценивают перспективы внедрения ИИ в отечественную сферу коммуникаций – об этом сообщили более 90% респондентов (91,5%). При этом близкое число опрошенных (86,9%) отметили, что по данному направлению Россия отстает от ведущих экономик мира. Наиболее популярными технологиями ИИ в медиакоммуникациях, согласно результатам исследования, являются персонализация новостных лент (27%), рекомендательные сервисы (24%), текстовая расшифровка аудиозаписей (19%). Наиболее же перспективными технологиями для внедрения в редакционную практику респонденты считают персонализацию новостных лент (41%), автоматическое генерирование текстов (39%), аналитика текстов (32%) – то есть, по мнению специалистов, ожидается переход от автоматизации рутинных процессов к более сложным аналитическим и генеративным моделям ИИ в области медиакоммуникаций.

Основными барьерами при внедрении ИИ в медиакомпании были названы нехватка средств (51%), недостаток опыта у сотрудников (42%), нехватка информации о передовом опыте применения ИИ (31%). Нехватка данных, по мнению опрошенных, не является ключевой проблемой – о ней сообщили лишь 13% участников.

Один из ведущих российских политологов, президент Фонда «Петербургская политика» Михаил Виноградов отмечает типичные ошибки при использовании нейросетей [17] в политических проектах:

1. Невозможность применения ChatGPT в качестве поисковика по традиционным, аналогичным с браузером схемам;
2. Подстраивание ответов под ожидания пользователя или социально одобряемые представления, заложенные в сервис;
3. Необходимость формирования дополнительных вопросов для получения релевантной информации;
4. Невозможность обработки любого нетекстового контента;
5. Отставание ChatGPT от текущих событий.

При этом уникальными возможностями применения генеративных технологий искусственного интеллекта в политических проектах можно считать:

1. Возможность получения гипотез, размышлений и предположений;
2. Возможность адаптации научного языка, научных фактов для публичного выступления и формулирование на их основе лозунгов, речей и публицистических текстов;
3. Возможность подготовки черновиков и набросков, которые в дальнейшем можно отправлять на доработку специалистам;
4. Подготовка технических документов;
5. Возможность получения объективной критики.

Таким образом, по результатам кейс-стади можно с уверенностью сказать, что в политических проектах сложился алгоритм применения ИИ в рамках решения коммуникационных задач. Как видно из результатов эмпирических исследований, технологии ИИ на сегодняшний день широко применяются во всех гуманитарных областях. Опыт показывает, что искусственные нейронные сети используются в случаях, когда они позволяют выполнить задачу без потери качества и, при этом, экономя временные и человеческие ресурсы.

В рамках коммуникационной деятельности (маркетинг, PR, политические коммуникации, политконсалтинг) технологии ИИ используются при выполнении как аналитических, так и креативных задач.

Выводы

В ходе выполнения работы были сделаны следующие выводы:

В политологии, социологии и теории коммуникации активно развивается направление, связанное с изучением влияния ИИ на социальную действительность, социальные нормы и практики. Исследования в этой области затрагивают роль ИИ в усилении разрыва между поколениями, место ИИ в демократических процессах, GR-деятельности, электоральных проектах, изменении медиаландщафта, возможности манипулирования общественным мнением. Ключевыми научными концепциями при оценке влияния технологий искусственного интеллекта на коммуникационное пространство являются концепции дискурса и дискурсного анализа. Исследование показало, что искусственные нейронные сети при отсутствии таких качеств, как рефлексия и креативность в человеческом понимании обладают достаточным функционалом для трансформации дискурсов путем их усиления или блокировки. Тем самым ИИ становится субъектом формирования дискурса, что делает его важным актором коммуникационной деятельности и повышает потенциал его применения в рамках политических проектов.

Обзор фундаментальных работ в области коммуникационного проектирования и политической коммуникации позволил выявить ключевые задачи специалистов в коммуникационных и политических проектах. При изучении технических характеристик искусственных нейронных сетей, их функционала и возможностей, а также проведении сравнительного анализа авторы пришли к выводу о высоком потенциале применения умных технологий в коммуникационной деятельности и политических проектах в частности. Так, помимо оффлайн-среды, практически все задачи специалиста в области политической коммуникации может взять на себя ИИ.

Для выявления основных технологий ИИ, применяемых в политических проектах, были проанализированы известные кейсы, проведен вторичный анализ масштабных исследований, посвященных использованию искусственных нейронных сетей в мировой политике за последние годы. Наиболее часто используемыми технологиями стали:

1. Дипфейки;
2. Генеративные нейросети;
3. Чат-боты;
4. Предсказательные модели;
5. Алгоритмы для создания таргетированных сообщений.

Анализ опыта применения технологий ИИ показал высокую эффективность нейронных сетей при реализации политических проектов. В ряде случаев они сыграли решающую роль во всей кампании.

При изучении перспектив и ограничений применения технологий ИИ в политических проектах были выявлены сильные и слабые стороны ИИ по сравнению со специалистом. По результатам анализа эмпирических исследований, выполненных с участием профессионалов коммуникационной сферы (PR-специалистов, маркетологов, политических консультантов) можно с уверенностью сказать, что на сегодняшний день искусственный интеллект не способен заменить специалиста и может выступать лишь в роли помощника, который может выполнять ряд рутинных задач и взять на себя практически все аналитические функции, но нуждается в постоянном контроле. По оценкам экспертов, 5-7 лет необходимо для усложнения нейросетей до уровня человека, с его аналитическими способностями, критическим мышлением, рефлексией. Основным преимуществом человека перед ИИ, по мнению специалистов, и будущем останется креативность и творческие способности, возможность генерировать идеи без опоры на опыт предыдущих поколений.

Список литературы

1. Рынок генеративного ИИ на горизонте 10 лет вырастет в 30 раз Bloomberg // RB.RU. URL: https://rb.ru/news/generative-ai-market/ (дата посещения: 12.01.2025).
2. Страны G7 договорились о пяти принципах ответственного использования ИИ // ТАСС URL: https://tass.ru/mezhdunarodnaya-panorama/17648739 (дата обращения: 10.12.2025).
3. В Британии открылся первый международный саммит по безопасности ИИ // ТАСС URL: https://tass.ru/mezhdunarodnaya-panorama/19172611 (дата обращения: 10.01.2025).
4. Генсек ООН – об искусственном интеллекте: «Это еще только начало...» //Новости ООН. URL: https://news.un.org/ru/story/2023/07/1442977 (дата обращения: 10.01.2025).
5. Шомова С. А., Качкаева А. Г. Между очарованием и испугом: диалог с «другим». Опыт анали-за практик использования ИИ в профессиональной и повседневной жизни // Мониторинг общественного мнения: экономические и социальные перемены. 2024. No 5. С. 3—17. https:// doi.org/10.14515/monitoring.2024.5.2766/ (дата обращения 23.11.2024).
6. Аналитики оценили опыт и перспективы использования ИИ в медиа и коммуникациях // РАЭК URL: https://raec.ru/live/branch/14034/ (дата обращения: 10.01.2025).
7. Россияне и искусственный интеллект // Яков и партнеры. 2024. Август. URL:https://www.yakovpartners.ru/publications/russian-citizens-and-ai/ (дата обращения 23.11.2024).
8. Авдонин В.С., Силаева В.Л. Нейросети нового поколения в контексте технологий искусственного интеллекта, философии и социально-политических наук // Политическая наука. - 2023. - №4. - С. 127-154.
9. Russell S.J., Norvig P. Artificial intelligence: a modern approach (4 th ed.). Hoboken: Pearson, 2021, 1136 p.
10. Best language models and their implications // OpenAI. – Mode of access: https://openai.com/research/better-language-models (дата обращения: 10.01.2025).

11. Азарова Л.В., Ачкасова В.А., Иванова К.А, Кривоносов А.Д., Филатова О.Г. Ситуационный анализ в связях с общественностью: учебник. – СПб.: Питер, 2009.
12. Нейрополитические технологии // Коммерсантъ URL: https://www.kommersant.ru/amp/5939887 (дата обращения: 08.01.2025).
13. Industrialized Disinformation. 2020 Global Inventory of Organized Social Media Manipulation // University of Oxford URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf (дата обращения: 10.12.2025).
14. Искусственный интеллект идет в политику // РСМД URL: https://russiancouncil.ru/amp/analytics-and-comments/columns/cybercolumn/iskusstvennyy-intellekt-idet-v-politiku/ (дата обращения: 11.12.2025).
15. Давыдова Ю. А., Матюхин А. В., Ананьевская Е. А. Искусственный интеллект в политическом управлении: тенденции и перспективы // ЖУРНАЛ ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ. - 2023. - №4. - С. 100-113.
16. РАЭК. Искусственный интеллект в медиа и коммуникациях. Практики российского медиабизнеса // ICT. Moscow. 2023. 19 июля.
URL: https://ict.moscow/projects/ai/research/iskusstvennyi-intellekt-v-media-i-kommunikatsiiakh-praktiki-rossiiskogo-mediabiznesa/.
17. ChatGPT и потенциал выживаемости политконсалтинга // Социодиггер URL: https://sociodigger.ru/articles/articles-page/chatgpt-i-potencial-vyzhivaemosti-politkonsaltinga (дата обращения: 09.01.2025).

References

1. The market of generative AI on the horizon 10 years will grow 30 times Bloomberg // RB.RU. URL: https://rb.ru/news/generative-ai-market/ (date of visit: 12.01.2025).
2. G7 countries have agreed on five principles for the responsible use of AI // TASS URL: https://tass.ru/mezhdunarodnaya-panorama/17648739 (date of application: 10.12.2025).
3. The first international AI security summit has opened in Britain // TASS URL: https://tass.ru/mezhdunarodnaya-panorama/19172611 (date of issue: 10.01.2025).
4. UN Secretary-General - about artificial intelligence: «It's just the beginning...» //UN News. URL: https://news.un.org/ru/story/2023/07/ 1442977 (date of application: 10.01.2025).
5. Shomova S. A., Kachkaeva A. G. Between charm and fear: dialogue with «others». Experience of the use of AI in professional and everyday life // Monitoring public opinion: economic and social change. 2024. No 5. C. 3—17. https:// doi.org/10.14515/monitoring.2024.5.2766/ (date of application 23.11.2024).
6. Analysts assessed the experience and prospects of using AI in media and communications // RAEC URL: https://raec.ru/live/branch/14034/ (date of application: 10.01.2025).
7. Russians and artificial intelligence // Yakov and partners. 2024. August. URL:https://www.yakovpartners.ru/publications/russian-citizen-and-ai/ (date of application 23.11.2024).

8. Avdonin V.S., Silaeva V.L. New generation neural networks in the context of artificial intelligence technologies, philosophy and socio-political sciences // Political science. -2023. - 4. - pp. 127-154.
9. Russell S.J., Norvig P. Artificial intelligence: a modern approach (4th ed.). Hoboken: Pearson, 2021, 1136 p.
10. Best language models and their implications // OpenAI. - Mode of access: https://openai.com/research/better-language-models (date of application: 10.01.2025).
11. Azarova L.V., Achkasova V.A., Ivanova K.A, Krivonosov A.D., Filatova O.G. Situational analysis in public relations: textbook. - PP: Peter, 2009.
12. Neuro-political technologies // Commerce URL: https://www.kommersant.ru/amp/5939887 (date of address: 08.01.2025).
13. Industrialized Disinformation. 2020 Global Inventory of Organized Social Media Manipulation // University of Oxford URL: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf (Date of Issue: 10.12.2025).
14. Artificial intelligence goes to politics // RSS URL: https://russiancouncil.ru/amp/analytics-and-comments/columns/cybercolumn/iskusstvennyy-intellekt-idet-v-politiku/ (date of circulation: 11.12.2025).
15. Davydova Y. A., Matyuhin A. V., Ananyevskaya E. A. Artificial intelligence in political management: trends and prospects // JOURNAL OF POLITICAL STUDIES. - 2023. - 4. - pp. 100-113.
16. RAEC. Artificial intelligence in media and communications. Russian media industry practices // ICT. Moscow. 2023. 19 July. URL: https://ict.moscow/projects/ai/research/iskusstvennyi-intellekt-v-media-i-kommunikatsiiakh-praktiki-rossiiskogo-mediabiznesa/.
17. ChatGPT and the potential of survival of political consulting // Sociologiger URL: https://sociodigger.ru/articles/articles-page/chatgpt-i-potencial-vyzhivaemosti-politkonsaltinga (date of request: 09.01.2025).

Зюзин А.О. Вероятностная методика оценки риска нарушения стабильности банковских информационных систем при выпуске релиза на основе имитационного моделирования (MONTE CARLO) // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 82–87

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.4

ВЕРОЯТНОСТНАЯ МЕТОДИКА ОЦЕНКИ РИСКА НАРУШЕНИЯ СТАБИЛЬНОСТИ БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ВЫПУСКЕ РЕЛИЗА НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ (MONTE CARLO)

Зюзин А.О.
ФГАОУ ВО "САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П.КОРОЛЕВА" , Самара, Россия (443086, Самарская область, город Самара, Московское ш., д. 34), e-mail: yuzin.ao@ya.ru

В статье предложена вероятностная методика количественной оценки риска нарушения стабильности банковских информационных систем при выпуске релиза программного обеспечения. Методика основана на факторной модели релиза, включающей параметры объема и сложности изменений, качества тестирования, дефектности до выпуска, сжатия релизного окна, репрезентативности тестовых сред, наличия нерешенных замечаний информационной безопасности и готовности процедур отката. Для каждого фактора задаются распределения вероятностей с учетом ограничений области допустимых значений и формируется правило наступления неблагоприятного исхода. Интегральная оценка риска вычисляется методом имитационного моделирования Монте-Карло как доля реализаций, в которых фиксируется нарушение стабильности. Рассмотрены подходы к параметризации и калибровке распределений по экспертным оценкам и историческим данным, а также предложена интерпретация вероятности риска в виде управленческой метрики релизного гейта. Показан демонстрационный расчет для трех сценариев релиза и выполнен анализ чувствительности, позволяющий ранжировать факторы по влиянию на итоговую вероятность. Полученные результаты подтверждают применимость методики для риск-ориентированного управления релизами и обосновывают необходимость калибровки модели под контекст конкретной информационной системы.

Ключевые слова: Релиз программного обеспечения, операционный риск, банковские информационные системы, имитационное моделирование, метод Монте-Карло, калибровка модели, управление качеством, анализ чувствительности.

PROBABILISTIC METHOD FOR ASSESSING THE RISK OF BANKING INFORMATION SYSTEM STABILITY VIOLATION DURING A SOFTWARE RELEASE USING MONTE CARLO SIMULATION

Zyuzin A.O.
"SAMARA NATIONAL RESEARCH UNIVERSITY NAMED AFTER ACADEMICIAN S.P. KOROLEV" , Samara, Russia (443086, Samara region, city of Samara, Moskovskoye sh., d. 34), e-mail: yuzin.ao@ya.ru

The paper proposes a probabilistic method for quantifying the risk of stability violation in banking information systems during a software release. The method relies on a release factor model that captures the scale and complexity of changes, testing quality, pre-release defectiveness, release window compression, representativeness of test environments, unresolved information security remarks, and rollback readiness. For each factor, probability distributions are specified within feasible bounds, and an adverse outcome rule is defined. The integrated risk is estimated by Monte Carlo simulation as the share of trials in which a stability violation is observed. The paper outlines a reproducible procedure for distribution parameterization and calibration based on expert elicitation and historical release data, and interprets the resulting probability as a managerial metric for release gating. A demonstration experiment for three release scenarios is presented along with a sensitivity analysis

used to rank the most influential drivers. The results indicate that the approach is suitable for risk-oriented release governance, provided that calibration is performed for each system context.

Keywords: Software release, operational risk, banking information systems, simulation modeling, Monte Carlo method, model calibration, quality management, sensitivity analysis.

Введение

Банковские информационные системы относятся к критически важным элементам инфраструктуры, а выпуск релизов программного обеспечения является одним из основных источников операционного риска. Практика релиз-менеджмента традиционно опирается на регламенты, чек-листы и экспертные согласования, однако такие инструменты слабо выражают неопределенность и затрудняют сопоставление релизов между собой. [1] В результате управленческое решение о выпуске, переносе или расширении мер контроля часто принимается без количественной оценки вероятности неблагоприятного исхода. Дополнительным фактором сложности является многопричинность инцидентов: нарушения стабильности обусловлены комбинацией объема и сложности изменений, качества тестирования, характеристик релизного окна, репрезентативности тестовых сред и организационных условий внедрения. В этих условиях целесообразен вероятностный подход, который позволяет формализовать инженерные факторы и получать интегральную оценку риска, пригодную для внедрения в релизную политику.

Цель исследования

Целью исследования является разработка воспроизводимой вероятностной методики количественной оценки риска нарушения стабильности банковской информационной системы при выпуске релиза, основанной на методе имитационного моделирования Монте-Карло, а также определение правил интерпретации получаемой вероятности как управленческой метрики релизного гейта. Для достижения цели решаются следующие задачи:

1) формирование факторной модели релиза и определение доменов факторов;

2) выбор семейств распределений и правил ограничения (усечения) значений;

3) разработка алгоритма расчета интегральной вероятности риска и доверительного интервала;

4) описание процедуры параметризации и калибровки модели;

5) демонстрация расчетов на типовых сценариях и выполнение анализа чувствительности.

Материал и методы исследования

Материал исследования включает:

а) сведения о релизах, извлекаемые из системы учета задач и изменений, системы управления тестированием и ITSM/мониторинга;

б) экспертные оценки, используемые при отсутствии достаточной статистики;

в) синтетические сценарии, позволяющие продемонстрировать работу модели в условиях ограниченного набора наблюдений. [2]

Методологически работа опирается на риск-ориентированную постановку задачи: требуется оценить вероятность события S, где S означает нарушение стабильности в пострелизном окне наблюдения. Под нарушением стабильности в статье понимается

наступление хотя бы одного из событий: критический инцидент в заданном окне, выполнение отката, либо нарушение регламентного окна внедрения. Факторная модель задается в виде набора случайных величин $F = F_{size}, F_{complex}, F_{test}, F_{def}, F_{window}, F_{env}, F_{is}, F_{rb}$, соответствующих объему релиза, сложности изменений, качеству тестирования, дефектности до релиза, сжатию релизного окна, репрезентативности тестовых сред, наличию нерешенных замечаний информационной безопасности и готовности отката.

Для вычисления вероятности P(S) используется имитационное моделирование Монте-Карло. На k-й итерации (k = 1..N) генерируется реализация факторов $F^{(k)}$, далее вычисляется риск-скор $R^{(k)}$ и индикатор события $I^{(k)} = 1R^{(k)} \geq \tau$. Интегральная оценка риска определяется как:

$p_{risk} = (1/N) * \Sigma_{k=1..N} I^{(k)}.$	*(0.1)*

Для p_{risk} вычисляется доверительный интервал по биномиальной модели, что позволяет количественно учитывать статистическую неопределенность оценки.

Риск-скор R рассчитывается как нормированная взвешенная сумма факторных вкладов:

$R = \Sigma w_i * g_i(F_i),$	*(0.2)*

где $g_i(\dots)$ – функции приведения факторов к единой шкале [0;1] (например, линейная нормализация или кусочно-линейные функции), w_i – веса факторов. В качестве альтернативы применяется логистическая модель:

$P(S\|F) = 1/\left(1 + exp\left(-\left(a + \Sigma b_i * g_i(F_i)\right)\right)\right),$	*(0.3)*

в которой параметры a, b_i калибруются на исторических релизах. В обоих случаях порог τ или уровень вероятности P(S|F) служит релизным гейтом.[3]

Параметризация распределений факторов выполняется в два этапа. На первом этапе формируются априорные распределения на основе экспертной элицитации, включая указание ожидаемого значения, диапазона и формы распределения (например, Triangular для объема релиза, Beta для долевых характеристик в интервале [0;1], Poisson для счетных величин). На втором этапе проводится калибровка по данным: параметры уточняются путем минимизации ошибки вероятностного прогноза (например, по Brier score) и проверки калибровки (reliability).[4]

Результаты исследования и их обсуждение

Демонстрационный эксперимент выполнен на трех сценариях релиза, отражающих типовые условия внедрения:

- S1 – малый релиз с высокой репрезентативностью сред и достаточным релизным окном;
- S2 – средний релиз при умеренном сжатии окна;
- S3 – крупный релиз с повышенной сложностью, умеренно сниженным качеством тестирования и более выраженным сжатием окна. [5]

В Таблице 1 приведен пример параметризации ключевых факторов для сценария S3.

Таблица 1 – Пример параметризации распределений для ключевых факторов

Фактор	**Обозначение**	**Распределение (ограничения)**	**Смысл / интерпретация**
Размер релиза (число задач)	F_{size}	Triangular(70; 95; 130)	Объем изменений; прокси нагрузки и разнообразия
Сложность изменений	$F_{complex}$	Poisson(λ=6), ограничение 0,.10	Техническая сложность и интеграционность
Качество тестирования	F_{test}	Beta(6;4), диапазон 0..1	Доля обеспеченности тестированием/покрытием
Дефектность до релиза	F_{def}	Poisson(λ=3), ограничение 0..10	Нагрузка дефектов, выявленных до выпуска
Сжатие релизного окна	F_{window}	Normal(μ=0,25; σ=0,08), усечение [0;0,40]	Относительное сжатие окна по сравнению с планом
Репрезентативность сред	F_{env}	Beta(18;2), диапазон 0..1	Сходство тестовой/предпрод среды с продуктивом
Нерешенные замечания ИБ	F_{is}	Bernoulli(p=0,25)	Наличие критических/значимых замечаний безопасности
Готовность отката	F_{rb}	Beta(8;2), диапазон 0..1	Готовность плана отката и технических процедур

Источник: разработано автором.

В ходе моделирования выполнено N = 100 000 прогонов для каждого сценария. Полученные оценки вероятности нарушения стабильности представлены на Рисунке 1.

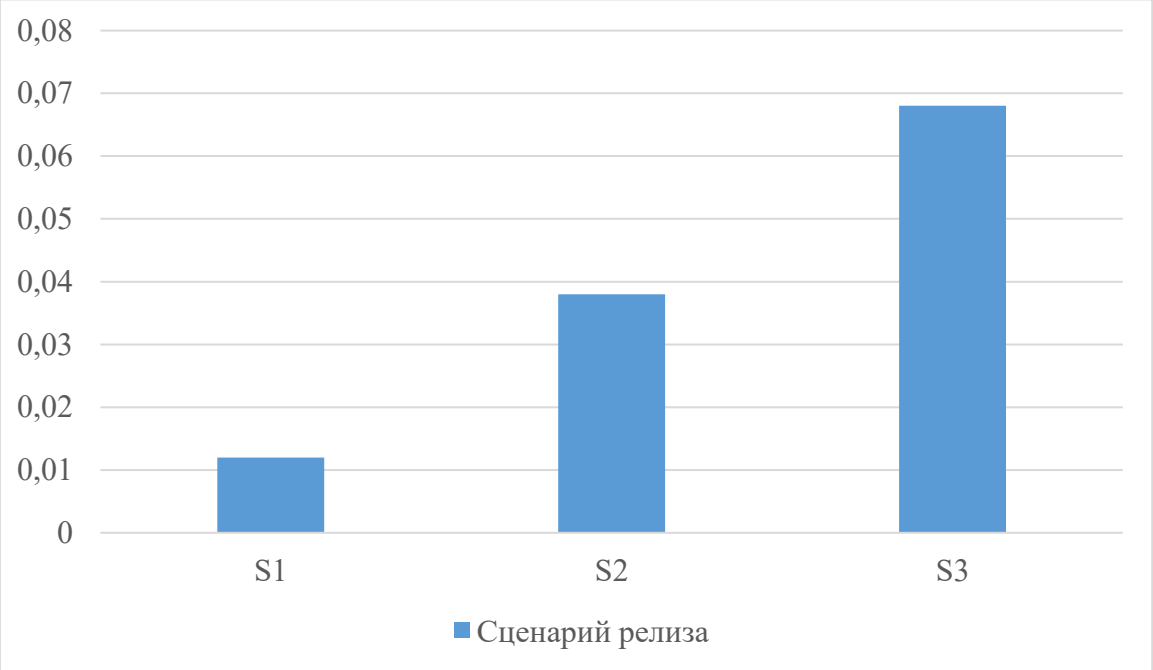

Рисунок 1- Оценка вероятности нарушения стабильности по сценариям релиза

Источник: расчеты автора.

Для сценариев S1–S3 получены следующие демонстрационные оценки p_{risk}: 0,012, 0,038 и 0,068 соответственно. Интерпретационно значение 0,068 означает, что при сопоставимых условиях примерно один из пятнадцати релизов может завершиться нарушением стабильности в заданном пострелизном окне. Для систем высокой критичности такая частота может быть признана неприемлемой и требует либо усиления мер контроля, либо переноса релиза.

Анализ чувствительности выполнялся методом последовательной вариации факторов при фиксировании остальных параметров на медианном уровне. Наибольшее влияние на p_{risk} в демонстрационном эксперименте показали репрезентативность сред F_{env}, качество тестирования
F_{test} и готовность отката F_{rb}. Рост объема и сложности релиза (F_{size}, $F_{complex}$) усиливал риск прежде всего через ухудшение распределения F_{test} и увеличение дефектности F_{def} в сценарных настройках. Наличие нерешенных замечаний информационной безопасности ($F_{is} = 1$) выступало как фактор с дискретным скачком риска, что отражает практику запретов/ограничений на внедрение при неустраненных замечаниях.

Отдельно отмечается роль ограничений распределений. Усечение нормального распределения для F_{window} на интервале [0; 0,40] предотвращает получение нефизичных значений и стабилизирует итоговую оценку p_{risk} при небольших изменениях параметров. Таким образом, ограниченная параметризация повышает воспроизводимость и интерпретируемость модели, что особенно важно при ограниченном объеме исторических данных.

Выводы

1) Предложена вероятностная методика оценки риска нарушения стабильности банковской информационной системы при выпуске релиза, основанная на моделировании Монте-Карло и факторной параметризации условий релиза.

2) Сформирован воспроизводимый порядок задания распределений факторов, включая домены и ограничения, позволяющий применять методику при дефиците статистики за счет экспертных априорных оценок и последующей калибровки по данным.

3) Показано, что интегральная вероятность риска может использоваться как управленческая метрика релизного гейта и как основание для выбора мер снижения риска, а анализ чувствительности позволяет ранжировать приоритетные направления улучшений (тестирование, репрезентативность сред, готовность отката).

4) Для практического внедрения методики необходимы: формализация целевого события нарушения стабильности, обеспечение качества данных о релизах и инцидентах, а также регулярная перекалибровка параметров с учетом изменения процессов и технологического ландшафта.

Список литературы

1. ISO/IEC 25010:2023. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.

2. Brier G.W. Verification of forecasts expressed in terms of probability. Monthly Weather Review, 1950.
3. Goessling H.F., Jung T. A probabilistic verification score for contours: methodology and application to ensemble forecasts. Quarterly Journal of the Royal Meteorological Society, 2018.
4. Janssen H. Monte-Carlo based uncertainty analysis: Sampling efficiency and error. Reliability Engineering & System Safety, 2013.
5. Lysytsia D.O., Bulba S.S. Classification of methods assessment and management risk development software. (UDC 004.422), 2016.

References

1. ISO/IEC 25010:2023. Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models.
2. Brier G.W. Verification of forecasts expressed in terms of probability. Monthly Weather Review, 1950.
3. Goessling H.F., Jung T. A probabilistic verification score for contours: methodology and application to ensemble forecasts. Quarterly Journal of the Royal Meteorological Society, 2018.
4. Janssen H. Monte-Carlo based uncertainty analysis: Sampling efficiency and error. Reliability Engineering & System Safety, 2013.
5. Lysytsia D.O., Bulba S.S. Classification of methods assessment and management risk development software. (UDC 004.422), 2016.

Немчинов А.В. Методы обнаружения аномалий в информационной инфраструктуре на основе статистического анализа и корреляции трафика // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 88–94

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.57

МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ НА ОСНОВЕ СТАТИСТИЧЕСКОГО АНАЛИЗА И КОРРЕЛЯЦИИ ТРАФИКА

Немчинов А.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: sasha01082004@gmail.com

Статья посвящена методам обнаружения аномалий в информационной инфраструктуре на основе статистического анализа и корреляции сетевого трафика. В статье описываются факторы нормальной работы сети и ее активность, метрики важные для анализа состояния сети, какие закономерности обычно их распределения используются для выявления отклонений.

Ключевые слова: Статистический анализ, корреляция трафика, мониторинг, аномалии, обнаружение угроз, информационная инфраструктура.

METHODS FOR DETECTING ANOMALIES IN THE INFORMATION INFRASTRUCTURE BASED ON STATISTICAL ANALYSIS AND TRAFFIC CORRELATION

Nemchinov A.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: sasha01082004@gmail.com

The article is devoted to methods for detecting anomalies in the information infrastructure based on statistical analysis and correlation of network traffic. The article describes the factors of the normal operation of the network and its activity, metrics important for analyzing the state of the network, which patterns of their distribution are usually used to identify deviations.

Keywords: Statistical analysis, traffic correlation, monitoring, anomalies, threat detection, information infrastructure.

Введение

Современные методы обнаружения кибератак на основе шаблонов или сигнатур позволяют успешно выявлять только известные типы атак. По мере расширения сети и увеличения трафика многие неизвестные угрозы становятся невидимыми или могут обходить традиционные механизмы защиты. Поведенческие методы не всегда подходят к конкретной сети и оценивают ее характеристики, а сигнатурные методы не успевают за новыми и усовершенствованными атаками. Соответственно, необходимо внедрять подходы, которые фокусируются не на содержании трафика, а на его статистических характеристиках и отклонениях от нормального поведения.[1]

Несмотря на огромное количество информации для анализа, трафик всегда имеет свои закономерности, и они различны для каждой сети. Определение нормального поведения сети может показаться сложной задачей, но достаточно проанализировать определенный период времени и принять во внимание, какие отклонения от нормы допустимы. После этого будут известны "правила", по которым работает сеть, это динамическая информация, поэтому важно учитывать любые изменения в сети, чтобы избежать ложных срабатываний и постоянно обновлять эти "правила".

Обычный сетевой трафик характеризуется стабильными статистическими закономерностями, включая распределение объема передаваемых данных, количество активных подключений, временные интервалы между пакетами, а также использование портов и протоколов. Значительные отклонения этих параметров от типичных значений могут указывать на сбои, ошибки конфигурации или попытки вмешательства в работу сети. Например, резкое увеличение числа кратковременных подключений может указывать на сканирование портов, а изменение корреляции между объемом трафика и количеством активных узлов может указывать на аномалии маршрутизации или появление нежелательного трафика.

Для выявления таких отклонений целесообразно использовать комбинацию статистического и корреляционного анализа. [2] Статистический анализ позволяет определить границы нормального поведения сети, в то время как корреляционный анализ позволяет выявить нарушения устойчивых взаимосвязей между параметрами трафика. Совместное использование этих методов обеспечивает более полное понимание происходящих изменений и упрощает локализацию источников аномальной активности.

Практическая реализация этого подхода может быть основана на сборе статистики сетевого трафика с маршрутизаторов и других сетевых устройств, анализе ее с фиксированными интервалами и сравнении текущих значений с эталонной моделью нормального поведения. Особенно важно учитывать не только средние значения показателей, но и форму их распределения, а также взаимосвязь между различными параметрами.[3]

Для построения модели нормального поведения сети используются такие параметры, как объем данных, передаваемых за единицу времени, количество активных подключений, распределение трафика по протоколам и портам, средняя и максимальная длины пакетов, а также интервалы между пакетами. Во многих случаях эти параметры подчиняются хорошо известным статистическим законам, включая экспоненциальное распределение и распределение Пуассона, и проявляют выраженную суточную периодичность.

Для оценки отклонений используются такие методы, как вычисление среднего значения и стандартного отклонения, квантильный анализ, скользящие окна и контрольные карты. Превышение заранее определенных пороговых значений, рассчитанных на основе исторических данных, позволяет обнаружить потенциальную аномалию без анализа содержимого трафика.

Корреляционный анализ и выявление взаимосвязей

Анализа только отдельных показателей часто бывает недостаточно, так как многие атаки маскируются под обычную активность по отдельным показателям. В этом случае важную роль играет корреляционный анализ, который позволяет выявить взаимосвязи между различными параметрами трафика.

При нормальной работе сети существует устойчивая корреляция между рядом показателей. Например, увеличение объема передаваемых данных обычно сопровождается увеличением количества активных подключений, а изменение нагрузки на один сегмент сети влияет на соседние узлы. Нарушение этих связей может указывать на скрытые проблемы: туннелирование трафика, распределенные атаки или несанкционированное использование ресурсов.

Для анализа используются коэффициенты корреляции Пирсона или Спирмена, а также корреляционные матрицы, позволяющие оценить общее состояние сети. Значительное снижение или увеличение корреляции между ключевыми параметрами рассматривается как потенциальный признак аномалии и требует дополнительного анализа.

Обнаружение аномалий при конкретных типах атак

Статистический и корреляционный анализ сетевого трафика позволяет выявлять признаки ряда распространенных сетевых атак без использования сигнатурных методов. При сканировании портов, как правило, наблюдается резкое увеличение количества кратковременных подключений при относительно небольшом объеме передаваемых данных. Статистически это проявляется как сдвиг в распределении количества подключений при постоянных или незначительно изменяющихся значениях объема трафика, а также нарушение характерной корреляции между этими параметрами. Такие отклонения могут быть выявлены с помощью пороговых значений и анализа временных рядов.[4]

Атаки типа «отказ в обслуживании» (DoS и DDoS-атаки) характеризуются значительным увеличением интенсивности сетевого трафика, увеличением количества пакетов в единицу времени и уменьшением вариабельности их параметров. В таких условиях распределение объема трафика и количества подключений становится ярко выраженным асимметричным, а отдельные значения выходят за пределы доверительных интервалов, сформированных на основе модели нормального поведения сети. Статистический анализ позволяет выявлять такие выбросы на ранних стадиях атаки, до начала критического ухудшения качества услуг.

Атаки, направленные на скрытую утечку данных или туннелирование трафика, являются одними из наиболее труднодоступных для обнаружения, поскольку отдельные параметры сетевой активности могут оставаться в пределах допустимых значений. В таких случаях основным признаком аномалии является нарушение устоявшихся «правил», включая объем передаваемых данных, количество активных узлов, используемые протоколы и временные характеристики соединений. Например, увеличение исходящего трафика при постоянном количестве активных подключений или использовании нетипичного протокола может указывать на скрытую передачу данных.

Статистические методы могут выявлять аномалии, связанные с ошибками конфигурации и несанкционированным использованием сетевых ресурсов. Появление нетипичных периодических пиков активности, изменений в ежедневных профилях нагрузки или сбоев в нормальном распределении трафика по портам и службам может указывать как на технические сбои, так и на попытки замаскировать вредоносную активность.[5]

Таким образом, использование статистического и корреляционного анализа обеспечивает идентификацию широкого спектра сетевых аномалий, включая как явные, так и скрытые формы воздействий. Этот подход дополняет традиционные меры безопасности и

повышает эффективность мониторинга информационной инфраструктуры за счет выявления отклонений от нормального поведения сети.

Выявление атак типа отказа в обслуживании по интенсивности событий

На Рисунке 1 показано изменение количества событий с течением времени во время атаки типа «отказ в обслуживании». В отличие от кратковременных аномалий, характерных для сканирования портов, атаки DoS и DDoS-атак сопровождаются устойчивым и значительным увеличением интенсивности событий в течение длительного периода времени. В то же время значения временных рядов выходят за пределы доверительных интервалов, основанных на модели нормального поведения сети.

Такие аномалии могут быть обнаружены с помощью методов скользящего среднего, дисперсионного анализа и контрольных карт, что позволяет обнаруживать атаки на ранней стадии и принимать своевременные меры для защиты инфраструктуры.

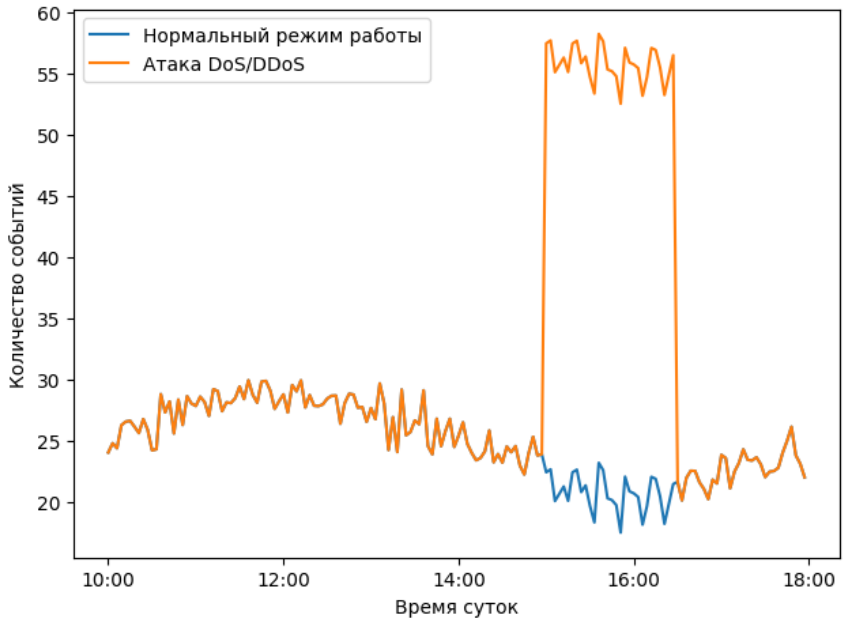

Рисунок 1 - Временной ряд количества событий

Статистический анализ распределения количества событий

Дополнительную информацию о характере сетевой активности можно получить, проанализировав распределение количества событий в единицу времени. На Рисунке 2 показано сравнение распределений количества событий в обычном режиме и в период аномальной активности. Нормальная работа сети характеризуется компактным распределением значений с ограниченной вариабельностью, тогда как во время атаки происходит сдвиг в распределении и появление значений, значительно превышающих типичные уровни.

Изменение формы распределения и увеличение дисперсии позволяют выявлять аномалии даже в тех случаях, когда средние значения показателей незначительно отличаются от нормальных. Такой подход повышает устойчивость системы обнаружения к маскировке атак под законную сетевую активность.

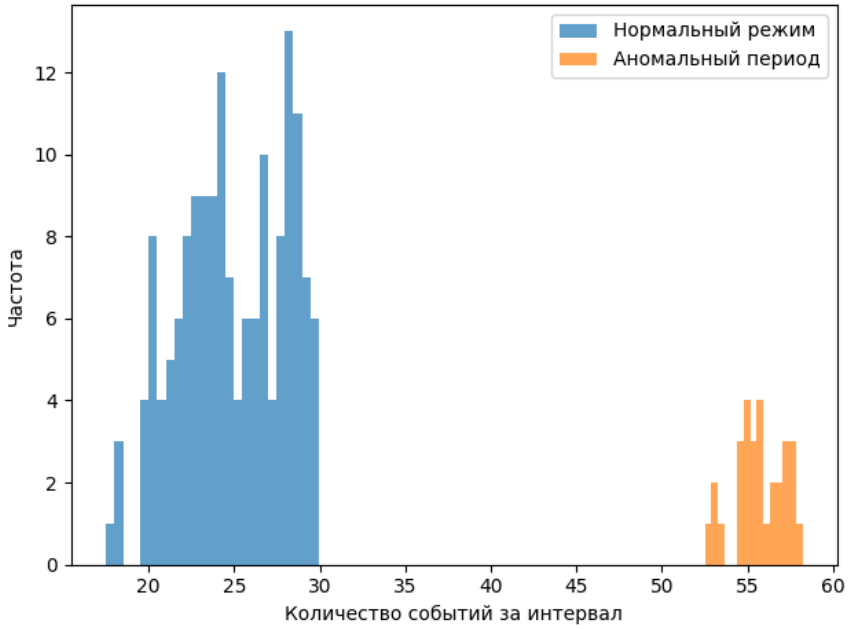

Рисунок 2 - Распределение количества событий

Применение методов в системах мониторинга

Интеграция статистических и корреляционных методов в системы мониторинга позволяет создать многоуровневый механизм обнаружения аномалий. На первом уровне регистрируются отклонения отдельных показателей от нормы, а на втором - анализируются изменения взаимосвязей между ними. Такой подход сокращает количество ложных срабатываний и повышает точность обнаружения реальных угроз.

Важным аспектом является адаптивность модели. Информационная инфраструктура со временем меняется: добавляются новые сервисы, меняется профиль нагрузки и модернизируется оборудование. Поэтому модели нормального поведения должны регулярно обновляться с учетом новых данных, а пороговые значения должны пересматриваться.

Заключение

В ходе работы рассматриваются методы обнаружения аномалий в информационной инфраструктуре, основанные на статистическом анализе и корреляции сетевого трафика и событий. Показано, что нормальное функционирование сети характеризуется стабильными статистическими закономерностями и устойчивыми корреляциями между ключевыми параметрами, такими как количество сетевых событий, интенсивность подключений и временные характеристики активности.

Анализ показывает, что отклонения от модели нормального поведения, выраженные в виде кратковременных всплесков, устойчивого превышения пороговых значений или нарушения корреляций, могут служить надежными индикаторами различных типов сетевых атак. В частности, сканирование портов проявляется в виде резкого кратковременного увеличения количества событий, атаки типа «отказ в обслуживании» характеризуются длительным увеличением интенсивности событий, а скрытая утечка данных и туннелирование трафика обнаруживаются путем нарушения стабильных взаимосвязей между параметрами сетевой активности.

Использование анализа временных рядов и распределения количества событий позволяет выявлять аномалии без анализа содержимого пакетов и использования сигнатурных методов, что особенно важно для высоконагруженных и распределенных инфраструктур. Рассмотренные подходы помогают обнаружить как явные, так и скрытые сетевые воздействия, а также помогают снизить зависимость систем мониторинга от заранее известных схем атак.

Таким образом, статистический и корреляционный анализ трафика и событий является хорошим дополнением к традиционным методам обнаружения угроз. Внедрение этих методов в системы мониторинга повышает надежность и стабильность систем, обеспечивая своевременное обнаружение аномалий и более быстрое реагирование на инциденты.

Список литературы

1. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
2. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
3. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
4. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН / Э. В. Бирих, М. Д. Булова, А. А. Казанцев, А. А. Миняев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 122-127. – EDN FBPSIL.
5. Бирих, Э. В. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти / Э. В. Бирих, А. С. Гаврилов, Е. Н. Сацук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 104-107. – EDN XSUFFR.

References

1. 1. Research of methods for increasing the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University.

Technical sciences. - 2024. - Vol. 51, No. 3. - pp. 110-116. - DOI 10.21822/2073-6185-2024-51-3-110-116. - EDN HDGBOY.

2. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S.V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2017. – pp. 92–95. – EDN YRPZWJ.
3. Selecting Tools for Dynamic Security Analysis of Web Applications for Digital Economy Tasks / E.V. Birikh, A.S. Gruzdev, A.O. Kamalova, D.V. Sakharov // Information Security. Inside. – 2024. – No. 1(115). – pp. 42–46. – EDN RLNHWK.
4. Development of a software module for automating the determination of the security level in the information system for personal data protection / E. V. Birikh, M. D. Bulova, A. A. Kazantsev, A. A. Minyaev // Actual problems of infotelecommunications in science and education (APINO 2024): Proceedings of the XIII International scientific-technical and scientific-methodical conference, St. Petersburg, February 27-28, 2024. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2024. - pp. 122-127. - EDN FBPSIL.
5. Birikh, E. V. Modern problems of ensuring internal security of a distributed network of government bodies / E. V. Birikh, A. S. Gavrilov, E. N. Satsuk // Actual problems of infotelecommunications in science and education (APINO 2018): VII International scientific-technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes, St. Petersburg, February 28 – January 01, 2018 / Edited by S. V. Bachevsky. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2018. - pp. 104-107. - EDN XSUFFR.

Захарова М.М. Сравнительный анализ эффективности стратегий ZTNA и традиционных VPN для защиты гибридной ИТ-инфраструктуры предприятия // Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 95–98

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ СТРАТЕГИЙ ZTNA И ТРАДИЦИОННЫХ VPN ДЛЯ ЗАЩИТЫ ГИБРИДНОЙ ИТ-ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Захарова М.М.
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: efizmor@gmail.com

В статье проводится сравнительный анализ двух доминирующих архитектур безопасного удаленного доступа в условиях распределенной гибридной ИТ-инфраструктуры: традиционных виртуальных частных сетей (VPN) и модели Zero Trust Network Access (ZTNA). Анализ базируется на критериях безопасности, производительности, масштабируемости и соответствия требованиям современных гибридных рабочих сред. Рассматриваются базовые принципы, преимущества и ограничения каждой модели. Предлагается методика поэтапной миграции с VPN-ориентированной инфраструктуры на архитектуру Zero Trust.

Ключевые слова: Zero Trust, ZTNA, виртуальная частная сеть, гибридная инфраструктура, безопасность, периметровая модель, микросегментация, гранулярный доступ.

A COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF ZTNA AND TRADITIONAL VPN STRATEGIES FOR SECURING HYBRID ENTERPRISE IT INFRASTRUCTURE

Zakharova M.M.
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: efizmor@gmail.com

The article presents a comparative analysis of the two dominant secure remote access architectures in a distributed hybrid IT infrastructure: traditional Virtual Private Networks (VPN) and the Zero Trust Network Access (ZTNA) model. The analysis is based on security, performance, scalability, and compliance criteria with the requirements of modern hybrid work environments. The basic principles, advantages, and limitations of each model are considered. A methodology for a phased migration from a VPN-centric infrastructure to a Zero Trust architecture is proposed.

Keywords: Zero Trust, ZTNA, virtual private network, hybrid infrastructure, security, perimeter model, microsegmentation, granular access.

Введение

Распространение облачных сервисов, переход к гибридному формату работы и увеличение количества удаленных точек доступа обострили недостатки периметровой модели безопасности, к которой относятся традиционные VPN. Классические VPN, предоставляя избыточный уровень доверия после аутентификации, увеличивают риски латерального перемещения злоумышленника при компрометации учетных данных, что противоречит

требованиям защиты от целевых и APT-атак. В этих условиях концепция Zero Trust, основанная на принципе «никогда не доверяй, всегда проверяй», и её практическая реализация в виде ZTNA становятся объектом пристального внимания.[1]

Традиционные VPN-решения создают зашифрованный туннель между устройством пользователя и корпоративной сетью, предоставляя после успешной аутентификации доступ к сегменту сети. Данный подход отличается относительной простотой внедрения для базового удаленного доступа и широкой поддержкой на различных устройствах. [2] Однако модель характеризуется существенными недостатками: широкой поверхностью атаки после установления соединения, сложностями реализации гранулированного доступа и микросегментации, проблемами масштабирования в распределенных средах, а также потенциальным снижением производительности из-за туннелирования всего трафика через единый шлюз.

Архитектура ZTNA реализует принцип нулевого доверия, предоставляя доступ не к сети, а непосредственно к конкретным приложениям или сервисам на основе динамической оценки контекста: идентичности пользователя, состояния устройства, местоположения и других параметров. Ключевыми компонентами являются центральный контроллер (ZTNA Broker), осуществляющий авторизацию, и коннекторы, размещаемые рядом с защищаемыми ресурсами. Основные преимущества ZTNA включают минимальную площадь атаки за счет гранулированного доступа, постоянную проверку доверия, скрытие приложений от публичной сети, а также улучшенную производительность за счет установления прямых оптимизированных соединений, особенно с облачными ресурсами.[3]

Сравнительный анализ эффективности моделей проводится по следующим критериям: безопасность, производительность и пользовательский опыт, операционная эффективность.

В аспекте безопасности ZTNA демонстрирует стратегическое преимущество, устраняя неявное доверие, присущее VPN. Если VPN предоставляет доступ к сетевому сегменту после однократной аутентификации, то ZTNA реализует явное, постоянное доверие с проверкой каждого запроса. Это обеспечивает точный гранулированный контроль доступа к конкретным приложениям (микросегментация) вместо горизонтального расширения прав в сети. Как следствие, площадь атаки при компрометации конечной точки в модели ZTNA минимальна, в то время как при компрометации VPN-клиента злоумышленник потенциально получает доступ ко всей внутренней сети. Кроме того, ZTNA обеспечивает более высокую манёвренность и меньшее время на парирование инцидентов благодаря мгновенному применению изменений в политиках доступа.

С точки зрения производительности и пользовательского опыта ZTNA также предлагает более современный подход. Традиционное VPN-туннелирование всего трафика через корпоративный шлюз может создавать задержки, особенно при доступе к облачным приложениям (эффект backhauling). ZTNA устанавливает прямое безопасное соединение пользователя с приложением по оптимальному маршруту, что улучшает скорость отклика для распределенных ресурсов. Управление доступом в ZTNA централизовано через политики, не зависящие от сетевой топологии, что упрощает администрирование и масштабирование в динамичных гибридных средах по сравнению со сложным управлением большим количеством VPN-правил и шлюзов.[4]

На основе анализа предлагается 4-этапная модель миграции для типовой корпоративной инфраструктуры:

1. Инвентаризация и сегментация: каталогизация пользователей, устройств, приложений и данных; применение внутренней сегментации сети для снижения рисков на переходном этапе.

2. Внедрение сильной аутентификации: обязательное использование многофакторной аутентификации (MFA) для привилегированных пользователей и доступа к критичным активам.

3. Пилотное внедрение ZTNA для отдельных приложений: выбор низкорисковых, публичных или новых облачных приложений для развертывания ZTNA; параллельная работа с VPN.

4. Расширение и отказ от VPN: постепенный перевод сервисов на модель ZTNA с последующим мониторингом; финальный отказ от VPN для большинства сценариев.[5]

Таким образом, ZTNA демонстрирует стратегические преимущества для современных гибридных инфраструктур, обеспечивая более высокий уровень безопасности за счет отказа от концепции «доверенной внутренней сети» и реализации принципа минимальных привилегий. Традиционные VPN сохраняют актуальность для специфических задач, таких как доступ к legacy-системам, или в качестве резервного канала. Для новых проектов и облачных сервисов целесообразно сразу внедрять принципы Zero Trust. Для существующей инфраструктуры рекомендован плановый переход по предложенной модели с фокусом на сильную аутентификацию и детальную сегментацию ресурсов.

Список литературы

1. Защита информации в базах данных / Э. В. Бирих, Л. А. Виткова, В. В. Гореленко, Д. Б. Казаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 89-92.
2. Э. В. Бирих, Е. Ю. Рябов, Д. В. Сахаров / Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 103-107.
3. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.

4. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
5. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

References

1. Information Security in Databases /E.V.Birikh, L. A. Vitkova, V. V. Gorelenko, D. B. Kazakov // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 89–92.
2. E. V. Birikh, E. Yu. Ryabov, D. V. Sakharov / Methodology for Forming a Model of Information System Security Threats // Actual Problems of Infotelecommunications in Science and Education (APINO 2017): Collection of Scientific Articles from the VI International Scientific, Technical and Scientific-Methodological Conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. – pp. 103–107.
3. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. - pp. 92-95. - EDN YRPZWJ.
4. Selection of tools for dynamic security analysis of web applications for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information Security. Inside. – 2024. – No. 1(115). – pp. 42-46. – EDN RLNHWK.
5. Research of methods for improving the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University. Technical sciences. – 2024. – Vol. 51, No. 3. – pp. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.

Гордеева А. М. Влияние отключения протокола SMB в Windows на безопасность корпоративных сетей // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 99–104

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.53

ВЛИЯНИЕ ОТКЛЮЧЕНИЯ ПРОТОКОЛА SMB В WINDOWS НА БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Гордеева А. М.
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА», Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: ardeeva1920@gmail.com

В статье рассматривается влияние отключения протокола SMB в Windows на безопасность корпоративных сетей. Обосновывается актуальность этой меры, анализируются ключевые угрозы, связанные с использованием протокола, и демонстрируется, как его отключение способствует выполнению требований нормативных документов Российской Федерации в области информационной безопасности.

Ключевые слова: информационная безопасность, протокол smb, эксплойт, уязвимость, нормативная документация.

IMPACT OF DISABLING THE SMB PROTOCOL IN WINDOWS ON CORPORATE NETWORK SECURITY

Gordeeva A. M.
SAINT PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROF. M.A. BONCH-BRUEVICH, St. Petersburg, Russia (3232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: ardeeva1920@gmail.com

The article discusses the impact of disabling the SMB protocol in Windows on the security of corporate networks. The relevance of this measure is substantiated, the key threats associated with the use of the protocol are analyzed, and it is demonstrated how disabling it contributes to meeting the requirements of regulatory documents of the Russian Federation in the field of information security.

Keywords: Cybersecurity, SMB protocol, exploit, vulnerability, regulatory documentation.

Введение

Протокол SMB (Server Message Block) является сетевым протоколом прикладного уровня, который обеспечивает удаленный доступ к файлам и принтерам по локальной сети. Изначально был разработан американской компанией IBM (International Business Machines Corporation) в 1980-х годах, впоследствии стал основным инструментом для совместного использования ресурсов в операционных системах Windows и продолжает использоваться в современных корпоративных сетях. Однако устаревшая версия протокола SMBv1, о которой далее и пойдет речь, содержит критические уязвимости, которые делают ее опасной для использования в наши дни.

Цель исследования

Целью исследования в данной работе является протокол SMBv1 – его основные уязвимости и причины использования его по сей день. На основании выявленных недостатков проводится оценка соответствия использования данного протокола требованиям нормативных документов в области информационной безопасности и формулируются практические рекомендации по снижению потенциальных рисков.

1. Уязвимости SMBv1 и последствия их эксплуатации

Протокол SMBv1, выпущенный еще в 1984 году, имеет серьезные для современных угроз недоработки в системе безопасности: отсутствие шифрования передаваемых данных, слабые механизмы аутентификации и уязвимости, позволяющие осуществлять удаленное выполнение кода. Эти недостатки в совокупности и позволяют злоумышленникам проводить масштабные атаки. Наиболее наглядным примером является эксплуатация уязвимости CVE-2017-0144, известной как «EternalBlue», которая позволяла выполнять произвольный код на удаленной системе без каких-либо прав доступа. В мае 2017 года эта уязвимость стала причиной глобальной эпидемии шифровальщика-вымогателя «WannaCry», который за короткое время парализовал работу сотен тысяч компьютеров по всему миру, включая больницы, компании и государственные учреждения. Уже через месяц тот же эксплойт был использован в еще более разрушительной атаке «NotPetya», которая нанесла многомиллионный ущерб крупным международным корпорациям.

Также в протоколе присутствует уязвимость CVE-2017-0143, известная как «Уязвимость удаленного выполнения кода SMB в Windows». Она возникает из-за недостаточной проверки входных данных при обработке специально сформированных пакетов и позволяет получить несанкционированный доступ к системе.

Выявление вышеперечисленных эксплойтов стало моментом, после которого даже сама Microsoft официально признала протокол небезопасным и начала процесс его поэтапного исключения.

2. Почему протокол используется до сих пор

Несмотря на свою давно доказанную небезопасность, протокол SMBv1 до сих пор используется, и его полное отключение часто связано с рядом сложностей. Причины для этого связаны со спецификой устаревшего оборудования, которое продолжает использоваться в государственных и частных учреждениях.

Прежде всего, использование протокола объясняется его глубоким внедрением в инфраструктуру предприятий. Он продолжает работать на критически важном оборудовании, которое либо физически не способно поддерживать новые протоколы, либо его модернизация экономически нецелесообразна или технически невозможна. Примерами такого оборудования являются старые промышленные компьютеры и медицинские аппараты (например, МРТ-сканеры), которые работают на Windows XP и имеют закрытое, необновляемое ПО, а также сетевые накопители (NAS), выпущенные много лет назад. Полное отключение SMBv1 в таком случае равносильно остановке производства или оказания медицинских услуг, что неприемлемо.

Кроме того, существуют практические и экономические причины. Модернизация или замена множества устаревшего оборудования требует огромных затрат, которые многие

организации, особенно в государственном секторе или на промышленных предприятиях, не могут себе позволить. [1-2]

Именно по вышеперечисленным причинам компания Microsoft хоть и отключила SMBv1 по умолчанию начиная с Windows 10 версии 1709 и Windows Server 2019, но продолжает предоставлять администраторам возможность вручную установить его обратно через специальный пакет.

Таким образом, сохраняя функциональность критически важных систем, учреждения одновременно принимают на себя осознанный риск. Однако здесь вступают в силу требования нормативных документов в области информационной безопасности.

3. Как использование SMBv1 нарушает требования регуляторов Российской Федерации

Отключение SMBv1 напрямую способствует выполнению ключевых требований российского законодательства в области защиты информации, что особенно актуально для государственных информационных систем и объектов критической информационной инфраструктуры (КИИ) [3-5].

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обязывает операторов информационных систем принимать технические меры для защиты данных от целого ряда угроз, включая неправомерный доступ, изменение, блокировку или уничтожение. Архитектурные недостатки протокола делают его использование несовместимым с выполнением этих требований. Вместо обеспечения защиты SMBv1 создает в информационной системе готовый канал, который может быть использован злоумышленниками [6].

Федеральный закон № 187-ФЗ «О безопасности КИИ» обязывает субъектов КИИ принимать организационные и технические меры для защиты значимых объектов. Использование протокола с известными критическими уязвимостями, эксплуатируемыми в атаках в прошлом, является очевидным пренебрежением этим требованием [7].

Приказ ФСТЭК России № 239 (требования по безопасности значимых объектов КИИ) предписывает проводить выявление и анализ уязвимостей, обновлять программное обеспечение и нейтрализовывать актуальные угрозы. ФСТЭК прямо указывал на уязвимости SMBv1 в своих информационных сообщениях, так что отключение протокола является прямым исполнением предписаний регулятора по устранению выявленной уязвимости [8].

Приказ ФСТЭК России № 17 (требования к защите информации в государственных информационных системах) содержит положение о необходимости реализации мер, направленных на нейтрализацию актуальных угроз безопасности информации. Сохранение в системе компонента, который является каналом для реализации ранее обсуждаемых угроз, делает невозможным выполнение этого требования [9].

Отключение неиспользуемых и небезопасных сетевых служб является базовым принципом построения защищенных систем, который ФСТЭК также активно продвигает в своих рекомендациях, как и необходимость сегментации сети.

4. Практические шаги по минимизации рисков в корпоративной сети

Таким образом, чтобы минимизировать риски и максимально выполнить все предписания, изложенные в пункте 3, необходимо первым шагом провести тщательный аудит

сети для выявления всех устройств, использующих SMBv1. Далее следует оценить возможность обновления прошивки или замены такого оборудования. Если это невозможно по причинам, описанным в пункте 2, уязвимые устройства должны быть строго изолированы в отдельный сегмент сети с помощью VLAN и межсетевых экранов, а трафик SMB должен быть заблокирован на границе этого сегмента [10].

Заключение

Проведенный в статье анализ позволяет утверждать, что отключение протокола SMBv1 оказывает прямое и крайне положительное влияние на безопасность корпоративных сетей. Эта мера позволяет превентивно заблокировать вероятность использования опасных векторов атак, сильно уменьшая возможности для потенциального вторжения в систему.

С правовой же точки зрения отключение протокола является не просто рекомендацией, а обязательным условием в случаях, когда это реализуемо. Во всех остальных настоятельно рекомендуется использовать дополнительные меры, перечисленные в пункте 4, для минимизации потенциальных рисков..

Список литературы

1. Развитие стандартов и руководств в сфере облачных технологий / Э. В. Бирих, Л. А. Виткова, М. В. Левин, М. В. Чмутов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 92-95. – EDN YRPZWJ.
2. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики / Э. В. Бирих, А. С. Груздев, А. О. Камалова, Д. В. Сахаров // Защита информации. Инсайд. – 2024. – № 1(115). – С. 42-46. – EDN RLNHWK.
3. Исследование способов повышения безопасности корпоративных сетей / Н. Ф. Махмутова, Э. В. Бирих, Д. В. Сахаров [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
4. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН / Э. В. Бирих, М. Д. Булова, А. А. Казанцев, А. А. Миняев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024) : Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 122-127. – EDN FBPSIL.
5. Бирих, Э. В. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти / Э. В. Бирих, А. С. Гаврилов, Е. Н. Сацук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. Том 1. – Санкт-Петербург: Санкт-

Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 104-107. – EDN XSUFFR.
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
8. Банк данных угроз безопасности информации ФСТЭК. BDU:2017-01099 [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2017-01099 (дата обращения 19.11.2025).
9. Банк данных угроз безопасности информации ФСТЭК. BDU:2017- 01100 [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2017-01100 (дата обращения 19.11.2025).
10. Официальный сайт компании Microsoft. SMBv1 не установлен по умолчанию в Windows Server и Windows [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows (дата обращения 19.11.2025).

References

1. Development of standards and guidelines in the field of cloud technologies / E. V. Birikh, L. A. Vitkova, M. V. Levin, M. V. Chmutov // Actual problems of infotelecommunications in science and education (APINO 2017): Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, March 1–2, 2017 / Edited by S. V. Bachevsky. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2017. - Pp. 92-95. - EDN YRPZWJ.
2. Selection of tools for dynamic security analysis of web applications for digital economy tasks / E. V. Birikh, A. S. Gruzdev, A. O. Kamalova, D. V. Sakharov // Information security. Insider. – 2024. – No. 1(115). – P. 42-46. – EDN RLNHWK.
3. Research of ways to improve the security of corporate networks / N. F. Makhmutova, E. V. Birikh, D. V. Sakharov [et al.] // Bulletin of the Dagestan State Technical University. Technical sciences. – 2024. – Vol. 51, No. 3. – P. 110-116. – DOI 10.21822/2073-6185-2024-51-3-110-116. – EDN HDGBOY.
4. Development of a software module for automating the determination of the security level in the information system for personal data protection / E. V. Birikh, M. D. Bulova, A. A. Kazantsev, A. A. Minyaev // Actual problems of infotelecommunications in science and education (APINO 2024): Proceedings of the XIII International scientific-technical and scientific-methodical conference, St. Petersburg, February 27-28, 2024. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2024. - P. 122-127. - EDN FBPSIL.
5. Birikh, E. V. Modern Problems of Ensuring Internal Security of a Distributed Network of Government Bodies / E. V. Birikh, A. S. Gavrilov, E. N. Satsuk // Actual Problems of Infotelecommunications in Science and Education (APINO 2018): VII International Scientific, Technical and Scientific-Methodological Conference. Collection of Scientific Articles. In 4 volumes, St. Petersburg, February 28 – January 2018 / Edited by S. V. Bachevsky. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2018. - pp. 104-107. - EDN XSUFFR.

6. Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection".
7. Federal Law of July 26, 2017 No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation."
8. FSTEC Information Security Threat Database. BDU:2017-01099 [Electronic resource]. URL: https://bdu.fstec.ru/vul/2017-01099 (accessed on November 19, 2025).
9. FSTEC Information Security Threat Database. BDU:2017-01100 [Electronic resource]. URL: https://bdu.fstec.ru/vul/2017-01100 (accessed on November 19, 2025).
10. /Official Microsoft website. SMBv1 is not installed by default on Windows Server and Windows [Electronic resource]. URL: https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows (accessed 19.11.2025).

Кайралапов А.М. Эволюция оптических измерений на конечном участке траектории: от регистрации координат к интеллектуальному анализу физических процессов // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с.105–112

Международный журнал информационных технологий и энергоэффективности

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

УДК 681.7.068: 535.8:53.082.5:004.8:004.93

ЭВОЛЮЦИЯ ОПТИЧЕСКИХ ИЗМЕРЕНИЙ НА КОНЕЧНОМ УЧАСТКЕ ТРАЕКТОРИИ: ОТ РЕГИСТРАЦИИ КООРДИНАТ К ИНТЕЛЛЕКТУАЛЬНОМУ АНАЛИЗУ ФИЗИЧЕСКИХ ПРОЦЕССОВ

Кайралапов А.М.
ФГБУ "16 ЦЕНТРАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ОРДЕНА КРАСНОЙ ЗВЕЗДЫ ИНСТИТУТ ИМЕНИ МАРШАЛА ВОЙСК СВЯЗИ А.И.БЕЛОВА" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, Мытищи, Россия (141006, Московская область, Мытищи г.о., город Мытищи, Рупасовский 1-й пер.), e-mail: alexandr_trir@mail.ru

В статье проводится детальный анализ трансформации функционального назначения и архитектуры оптических траекторно-измерительных комплексов (ОТИК) в ответ на появление новых классов гиперзвуковых и высокоманевренных целей. Рассматривается исторический контекст развития оптических методов контроля и обозначается фундаментальный разрыв между возможностями традиционных систем и требованиями современных испытаний. Основной акцент сделан на комплексном, двухуровневом подходе к модернизации, включающем революционные изменения в аппаратной части (переход к спектрально-селективным и активным оптико-локационным методам) и создание принципиально новых алгоритмических систем на основе искусственного интеллекта для обработки данных. Впервые в рамках данной тематики детально обсуждаются перспективы создания распределённых сетей интеллектуальных оптических датчиков (свармов) и концепция «цифрового двойника» цели в реальном времени. Делается вывод о необходимости перехода от роли пассивного регистратора к статусу активного аналитического центра, обеспечивающего не траекторные, а физико-технические характеристики испытываемых объектов.

Ключевые слова: Оптический траекторно-измерительный комплекс (ОТИК), конечный участок траектории, гиперзвуковые летательные аппараты (ГЗЛА), измерения в условиях плазменного образования, спектральная селекция, активная лазерная подсветка, компьютерное зрение, глубокое обучение, распределённая сеть датчиков, цифровой двойник, обработка данных в реальном времени, испытания перспективных вооружений.

EVOLUTION OF OPTICAL MEASUREMENTS ON THE FINAL TRAJECTORY SEGMENT: FROM REGISTRATION TO INTELLIGENT ANALYSIS

Kayralapov A.M.
16TH CENTRAL RESEARCH AND TESTING INSTITUTE OF THE ORDER OF THE RED STAR NAMED AFTER MARSHAL OF THE SIGNAL CORPS A.I. BELOV OF THE MINISTRY OF DEFENSE OF THE RUSSIAN FEDERATION, Mytishchi, Russia (141006, Moscow region, Mytishchi, city of Mytishchi, Rupasovsky 1st lane), e-mail: alexandr_trir@mail.ru

The article provides a detailed analysis of the transformation in the functional purpose and architecture of Optical Trajectory Measurement Complexes (OTMC) in response to the emergence of new classes of hypersonic and high-maneuverability targets. The historical context of the development of optical monitoring methods is considered, and a fundamental gap between the capabilities of traditional systems and the requirements of modern testing is

identified. The main emphasis is placed on a comprehensive, two-level approach to modernization. This approach includes revolutionary changes in hardware (the transition to spectrally-selective and active optico-location methods) and the creation of fundamentally new algorithmic systems based on artificial intelligence for data processing. For the first time within this subject area, the prospects for creating distributed networks of intelligent optical sensors (swarms) and the concept of a real-time target "digital twin" are discussed in detail. A conclusion is drawn on the necessity of transitioning from the role of a passive recorder to the status of an active analytical center, providing not just trajectory, but physical and technical characteristics of the objects under test.

Keywords: Optical Trajectory Measurement System (OTMS), final trajectory segment, terminal phase, hypersonic vehicles, measurements in plasma environment, spectral selection, multispectral imaging, active laser illumination, LIDAR, computer vision, deep learning, distributed sensor network, sensor swarm, digital twin, real-time data processing, advanced weapons testing.

Введение

Конечный участок полёта боевых блоков баллистических и планирующих крылатых ракет представляет собой уникальный и критически важный полигон для верификации их боевой эффективности, живучести и соответствия расчётным характеристикам. Именно в этой финальной фазе, на этапе гиперзвукового планирования или баллистического снижения в плотных слоях атмосферы, абстрактные математические модели и результаты стендовых испытаний сталкиваются с комплексной и нелинейной реальностью. Здесь доминируют экстремальные физические явления, такие как интенсивный аэродинамический нагрев, приводящий к абляции материалов теплозащиты [1], а также формирование неравновесной плазменной оболочки, радикально меняющей условия радиолокационного и оптического наблюдения [2]. Традиционная роль оптических траекторно-измерительных комплексов, десятилетиями развёрнутых на полигонах, сводилась к высокоточной регистрации пространственных координат и параметров движения с помощью кинотеодолитов и фотограмметрии [3]. Однако появление и активные испытания новейших гиперзвуковых комплексов обозначили качественный скачок в требованиях [4]. Современный ОТИК уже не может ограничиваться функцией «фотографа», фиксирующего положение точки в пространстве. От него требуется стать «диагностом» и «физиком-экспериментатором», способным в режиме, близком к реальному времени, не просто наблюдать, но и интерпретировать сложнейшие физические процессы, происходящие с объектом, оценивать целостность его конструкции и идентифицировать его состояние среди множества ложных целей.

Вызовы современности и системные ограничения классических ОТИК

Классические оптические системы, основанные на принципах плёночной или ранней цифровой кинотеодолитной съёмки, сталкиваются с рядом фундаментальных ограничений при работе с новейшими целями [5]. Эти ограничения носят системный характер и затрагивают все этапы получения информации. Прежде всего, гиперзвуковые скорости порождают колоссальные угловые скорости при наблюдении с наземных пунктов. Механические системы азимутально-угломестного сопровождения с сервоприводами имеют конечное быстродействие и инерционность, что приводит к отставанию оси визирования от цели и потере её из поля зрения [6]. Даже использование современных матричных приёмников не решает проблему полностью, так как сверхзвуковое движение всё ещё может вызывать смазывание изображения, делая невозможным анализ мелких деталей конструкции [7].

Другой фундаментальной проблемой являются опто-физические помехи. Интенсивное свечение плазменной оболочки создаёт не помеху в классическом радиоэлектронном понимании, а мощный мешающий фон. Этот фон не только снижает общий контраст изображения, но и действует как динамическая маска [2]. Плазма, обладающая сложной пространственно-временной структурой, визуально искажает и скрывает истинные геометрические контуры боевого блока, делая традиционные методы фотограмметрии и визуальной оценки состояния малоэффективными или вовсе неприменимыми [8]. Кроме того, на конечном участке испытаний полигонный измерительный комплекс имеет дело не с изолированной точечной целью. Это сложная динамическая сцена, включающая основной боевой блок, элементы последней ступени ракеты-носителя, ложные тепловые цели, дипольные отражатели и прочие средства преодоления ПРО [9]. В таких условиях ручной или полуавтоматический захват оператором ключевого объекта становится задачей, требующей недопустимо больших временных затрат и чреватой критическими ошибками, а традиционные алгоритмы сопровождения по контрасту или яркости теряют эффективность [10].

Комплексный подход к модернизации: революция в аппаратной части

Ответом на указанные вызовы не может быть эволюционное улучшение существующих компонентов — требуется пересмотр физических принципов получения оптической информации. Модернизация должна носить комплексный характер, затрагивая всю измерительную цепь от приёмника излучения до метода освещения цели. Одним из ключевых направлений является переход к матрицам с глобальным затвором и внедрение спектральной селекции. Замена устаревших приёмников на современные КМОП-матрицы устраняет геометрические искажения быстродвижущихся объектов. Однако подлинный качественный скачок связан с интеграцией спектрального анализа непосредственно в процесс формирования изображения [11]. Реализуется это путём оснащения оптических каналов ОТИК быстросменными или перестраиваемыми узкополосными интерференционными фильтрами, настроенными на строго определённые длины волн, соответствующие линиям излучения ключевых химических элементов в плазме или в продуктах абляции [12]. Таким образом, система переходит от получения интегрального «яркостного портрета» к созданию набора спектральных каналов, каждый из которых несёт информацию о конкретных физических процессах: температуре плазмы в определённой зоне, интенсивности абляции, химическом составе продуктов разрушения. Это позволяет «вычесть» мешающее свечение плазмы и получить контрастное изображение самой конструкции [13].

Параллельно для кардинального снижения зависимости от естественной освещённости и повышения информативности данных необходимо развитие активных оптико-локационных гибридных систем [14]. Речь идёт о создании мощных лазерных систем, работающих в глазобезопасных для наземной аппаратуры диапазонах. Лазерный луч, направленный на цель, создаёт на её поверхности яркое освещённое пятно, а приёмный телескоп регистрирует отражённый сигнал. Ключевые преимущества такого подхода заключаются в следующем: система получает высококонтрастное изображение цели на тёмном фоне независимо от времени суток; по времени задержки отражённого импульса можно с высочайшей точностью определять дальность, что критически важно для прецизионной триангуляции [15]; анализируя доплеровское смещение и спектр отражённого

сигнала, можно оценивать не только радиальную скорость, но и вибрационные характеристики объекта [16]. Гибридизация пассивных и активных методов формирует основу для всепогодного и всесуточного высокоточного измерительного комплекса нового поколения, что подтверждается и патентными разработками в данной области [17].

Перспективы: интеллектуализация как ключевой драйвер развития

Усовершенствование аппаратной части создаёт поток данных беспрецедентного объёма и сложности. Их эффективная обработка и интерпретация возможны только за счёт принципиальной интеллектуализации всего измерительного процесса. На первый план здесь выходит внедрение алгоритмов компьютерного зрения и глубокого обучения. Современные нейросетевые архитектуры способны решать задачи, выходящие за рамки человеческих возможностей [18]. На этапе обучения такие алгоритмы «пропускают» через себя десятки тысяч синтезированных и реальных исторических кадров, учась выделять целевые признаки в условиях сильных помех. В реальном времени обученная нейросеть может автоматически обнаруживать и классифицировать все объекты в кадре, с высокой достоверностью идентифицируя боевой блок среди ложных целей, осуществлять устойчивое автоматическое сопровождение выбранной цели, компенсируя смазывание и засветы, а также мгновенно детектировать и сигнализировать о нештатных событиях, таких как начало нерасчётного вращения или отделение фрагментов [19]. Это превращает ОТИК из инструмента пост-обработки в систему оперативного ситуационного реагирования.

Логическим развитием идеи интеллектуализации является отказ от концепции нескольких крупных, дорогих и уязвимых стационарных пунктов. Ей на смену может прийти распределённая сеть из множества компактных, мобильных и максимально автоматизированных оптических постов, формирующих так называемый оптический сварм [20]. Каждый такой пост представляет собой автономный модуль с собственной вычислительной мощностью и каналом защищённой связи. Посты, развёрнутые на местности с оптимальным перекрытием полей зрения, обмениваются данными между собой, формируя единое адаптивное информационное поле. Такая архитектура обеспечивает высочайшую отказоустойчивость, возможность применения методов многобазовой стереоскопии для восстановления полной пространственной ориентации и деформаций конструкции цели с субсантиметровой точностью, а также гибкость и быстроту развёртывания под конкретную трассу испытаний [21].

На основе потока данных от модернизированной аппаратной части и их обработки алгоритмами ИИ становится возможным реализация концепции «цифрового двойника» цели в реальном времени [22]. Эта виртуальная модель будет интегрировать в себе не только кинематические параметры, но и оценённые физические состояния: температурное поле поверхности, интенсивность абляции, динамику изменения геометрии, параметры плазменного образования. Такой комплексный цифровой слепок, сравниваемый с расчётными моделями, предоставляет инженерам-разработчикам беспрецедентно глубокое понимание реального поведения изделия в экстремальных условиях, открывая путь к итеративному совершенствованию конструкций [23].

Кроме того, эволюционировавший ОТИК не должен оставаться изолированной системой. Его необходимо интегрировать в единый информационно-измерительный контур

полигона совместно с радиолокационными станциями, радиотелеметрическими системами и акустическими датчиками [24]. Алгоритмы объединения данных датчиков смогут коррелировать оптические данные о визуальных проявлениях нештатной ситуации с телеметрическими сигналами о внутренних параметрах систем блока и радиолокационной картиной [25]. Это позволит устанавливать причинно-следственные связи между внешними воздействиями, отказами внутренней аппаратуры и наблюдаемыми эффектами, значительно повышая достоверность и аналитическую ценность результатов всего цикла испытаний, что отражено в актуальных концептуальных документах [26].

Заключение

Таким образом, обеспечение технологического лидерства в области испытаний перспективных гиперзвуковых и высокоманевренных комплексов требует не модернизации, а концептуальной перезагрузки подхода к оптическим траекторным измерениям на конечном участке. Стратегическое развитие отечественных ОТИК должно идти по пути глубокой синергии двух направлений: революционного обновления аппаратного парка на основе спектрально-селективных и активных гибридных методов и тотальной интеллектуализации процессов сбора и анализа данных с использованием передовых алгоритмов ИИ. Реализация рассмотренных направлений, включая создание распределённых сетей интеллектуальных датчиков и интеграцию в единый измерительный контур, позволит трансформировать ОТИК из пассивного инструмента регистрации координат в активный, интеллектуальный аналитический центр. Такой центр будет в режиме, близком к реальному времени, предоставлять не просто траекторную информацию, а комплексную физико-техническую картину состояния и поведения испытываемого объекта. Это является безальтернативным условием для ускорения цикла разработки, повышения надёжности новейших систем вооружения и гарантированного обеспечения национальной безопасности в условиях жёсткой технологической конкуренции, что соответствует долгосрочным стратегическим установкам [27].

Список литературы

1. Теплов Ф.И., Леонтьев А.К. Термомеханика абляционных композитов в гиперзвуковом потоке. М.: Физматлит, 2019. 288 с.
2. Захаров Ю.В., Петров А.А. Радиофизические характеристики плазменного чехла гиперзвукового объекта // Радиотехника и электроника. 2020. Т. 65, № 3. С. 234-245.
3. Смирнов Г.И. Оптические траекторные измерения в ракетно-космической технике. М.: Машиностроение, 2005. 408 с.
4. Воскресенский Д.Н. Современные тенденции развития гиперзвуковых технологий и их влияние на полигонный измерительный комплекс // Известия высших учебных заведений. Приборостроение. 2021. Т. 64, № 6. С. 45-57.
5. Кузнецов В.П. Методы и средства оптико-электронных измерений в испытаниях авиационно-космической техники. СПб.: Политехника, 2017. 512 с.
6. Белов А.М., Гришин В.Н. Динамика систем точного сопровождения быстродвижущихся объектов // Оптический журнал. 2019. Т. 86, № 2. С. 12-19.
7. Гордеев А.С. Особенности регистрации изображений быстроизменяющихся процессов цифровыми камерами // Автометрия. 2018. Т. 54, № 4. С. 112-120.
8. Мельников В.М. Фотограмметрия в экстремальных условиях: проблемы и решения. Новосибирск: Наука, 2016. 275 с.
9. Андреев С.К. Средства преодоления противоракетной обороны: физические принципы и моделирование. М.: Физматлит, 2018. 332 с.
10. Коробейников А.В. Алгоритмы сопровождения точечных и протяжённых объектов в сложной помеховой обстановке // Информационные процессы. 2020. Т. 20, № 3. С. 301-315.
11. Прохоров М.Е., Семёнова Л.В. Мультиспектральные и гиперспектральные методы в технической диагностике. М.: Техносфера, 2016. 198 с.
12. Соколов Д.Л., Орлов А.В. Спектральный анализ излучения плазмы гиперзвукового потока // Письма в ЖТФ. 2022. Т. 48, вып. 4. С. 18-22.
13. Лисицын В.Н., Коробейников В.П. Спектральные методы выделения слабого сигнала на фоне интенсивных помех. М.: Радио и связь, 2001. 189 с.
14. Капустин В.В. Лазерные локационные системы для контроля быстродвижущихся объектов. Томск: Томский госуниверситет, 2013. 210 с.
15. Дмитриев А.С., Попов Г.М. Лазерная дальнометрия с миллиметровой точностью в задачах траекторных измерений // Квантовая электроника. 2017. Т. 47, № 8. С. 765-770.
16. Селиванов В.В., Тарасов С.П. Лазерная доплеровская виброметрия в задачах диагностики механических конструкций. М.: Физматлит, 2009. 304 с.
17. Патент RU 2689876 C1. Способ оптико-локационного контроля гиперзвукового объекта и система для его осуществления. Опубл. 27.05.2019.
18. Куржанский А.Б., Максимов Е.А. Глубокое обучение и нейросетевые модели в задачах обработки изображений // Труды СПИИРАН. 2020. Вып. 62. С. 150-179.
19. Чугунов А.С., Борисов Р.А. Метод детектирования нештатных ситуаций при визуальном сопровождении летательных аппаратов на основе сверточных нейронных сетей // Искусственный интеллект и принятие решений. 2020. № 4. С. 76-85.

20. Ренев О.Ю., Степанов К.А. Архитектура распределённой сети оптико-электронных сенсоров для аэрокосмического полигона // Датчики и системы. 2021. № 5. С. 34-41.
21. Злобин В.К., Матвеев А.А. Теория и алгоритмы многовидовой фотограмметрии. М.: Изд-во МГТУ им. Н.Э. Баумана, 2014. 376 с.
22. Семёнов И.В., Фролов К.В. Цифровые двойники в жизненном цикле высокотехнологичных изделий // Информационные технологии. 2021. Т. 27, № 11. С. 678-689.
23. Гаврилов А.Н., Тихонов Д.В. Применение цифровых двойников для анализа результатов натурных испытаний сложных технических систем // Вестник компьютерных и информационных технологий. 2022. № 3. С. 12-20.
24. Николаев Е.П., Шестаков А.Л. Интегрированные информационно-измерительные системы полигонного комплекса. М.: Горячая линия – Телеком, 2012. 496 с.
25. Архипов В.И., Беляев М.Г. Алгоритмы комплексной обработки разнородной информации в системах мониторинга // Системный анализ, управление и обработка информации. 2019. № 1. С. 89-100.
26. Доклад «Концепция развития единого информационного пространства полигонного измерительного комплекса на период до 2030 года». ЦНИИ «Центр», 2022. 120 с.
27. Стратегия развития средств измерений, испытаний и контроля в оборонно-промышленном комплексе Российской Федерации на 2024-2035 гг. Утверждена распоряжением Правительства РФ от 15.12.2023 № 1245-р.

References

1. Teplov F.I., Leontiev A.K. Thermomechanics of Ablative Composites in Hypersonic Flow. M.: Fizmatlit, 2019. p. 288
2. Zakharov Y.V., Petrov A.A. Radiophysical Characteristics of the Plasma Sheath of a Hypersonic Vehicle // Radiotekhnika i Elektronika. 2020. Vol. 65, No. 3. pp. 234-245.
3. Smirnov G.I. Optical Trajectory Measurements in Rocket and Space Technology. M.: Mashinostroenie, 2005. p.408
4. Voskresensky D.N. Modern Trends in the Development of Hypersonic Technologies and Their Impact on the Test Range Measurement Complex // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2021. Vol. 64, No. 6. pp. 45-57.
5. Kuznetsov V.P. Methods and Means of Optoelectronic Measurements in Testing Aerospace Equipment. SPb.: Politekhnika, 2017. p.512
6. Belov A.M., Grishin V.N. Dynamics of Precision Tracking Systems for Fast-Moving Objects // Opticheskii Zhurnal. 2019. Vol. 86, No. 2. pp. 12-19.
7. Gordeev A.S. Features of Imaging Registration for Fast-Transient Processes by Digital Cameras // Avtometriya. 2018. Vol. 54, No. 4. pp. 112-120.
8. Melnikov V.M. Photogrammetry in Extreme Conditions: Problems and Solutions. Novosibirsk: Nauka, 2016. p.275
9. Andreev S.K. Means of Overcoming Missile Defense: Physical Principles and Modeling. M.: Fizmatlit, 2018. p.332
10. Korobeinikov A.V. Algorithms for Tracking Point and Extended Objects in Complex Jamming Environments // Informatsionnye Protsessy. 2020. Vol. 20, No. 3. pp. 301-315.

11. Prokhorov M.E., Semenova L.V. Multispectral and Hyperspectral Methods in Technical Diagnostics. M.: Tekhnosfera, 2016. p.198
12. Sokolov D.L., Orlov A.V. Spectral Analysis of Hypersonic Flow Plasma Radiation // Pis'ma v Zhurnal Tekhnicheskoi Fiziki. 2022. Vol. 48, Issue 4. pp. 18-22.
13. Lisitsyn V.N., Korobeinikov V.P. Spectral Methods for Weak Signal Extraction Against Intense Noise. M.: Radio i Svyaz', 2001. p.189.
14. Kapustin V.V. Laser Ranging Systems for Monitoring Fast-Moving Objects. Tomsk: Tomsk State University, 2013. p.210
15. Dmitriev A.S., Popov G.M. Laser Ranging with Millimeter Accuracy for Trajectory Measurement Problems // Kvantovaya Elektronika. 2017. Vol. 47, No. 8. pp. 765-770.
16. Selivanov V.V., Tarasov S.P. Laser Doppler Vibrometry for Problems of Mechanical Structures Diagnostics. M.: Fizmatlit, 2009. p.304
17. Patent RU 2689876 C1. Method of Optico-Locational Monitoring of a Hypersonic Object and System for Its Implementation. Publ. 27.05.2019.
18. Kurzhanski A.B., Maksimov E.A. Deep Learning and Neural Network Models in Image Processing Tasks // Trudy SPIIRAN. 2020. Issue 62. pp. 150-179.
19. Chugunov A.S., Borisov R.A. A Method for Detecting Anomalous Situations During Visual Tracking of Aircraft Based on Convolutional Neural Networks // Iskusstvennyi Intellekt i Prinyatie Reshenii. 2020. No. 4. pp. 76-85.
20. Renev O.Y., Stepanov K.A. Architecture of a Distributed Network of Optoelectronic Sensors for an Aerospace Test Range // Datchiki i Sistemy. 2021. No. 5. pp. 34-41.
21. Zlobin V.K., Matveev A.A. Theory and Algorithms of Multi-View Photogrammetry. M.: Izd-vo MGTU im. N.E. Baumana, 2014. p. 376
22. Semenov I.V., Frolov K.V. Digital Twins in the Lifecycle of High-Tech Products // Informatsionnye Tekhnologii. 2021. Vol. 27, No. 11. pp. 678-689.
23. Gavrilov A.N., Tikhonov D.V. Application of Digital Twins for Analysis of Field Test Results of Complex Technical Systems // Vestnik Komp'yuternykh i Informatsionnykh Tekhnologii. 2022. No. 3. pp. 12-20.
24. Nikolaev E.P., Shestakov A.L. Integrated Information-Measurement Systems of the Test Range Complex. M.: Goryachaya Liniya – Telekom, 2012. p. 496
25. Arkhipov V.I., Belyaev M.G. Algorithms for Integrated Processing of Heterogeneous Information in Monitoring Systems // Sistemnyi Analiz, Upravlenie i Obrabotka Informatsii. 2019. No. 1. pp. 89-100.
26. Report "Concept for the Development of a Unified Information Space for the Test Range Measurement Complex for the Period Until 2030". TsNII "Tsentr", 2022. p.120
27. Strategy for the Development of Measurement, Testing and Control Means in the Defense-Industrial Complex of the Russian Federation for 2024-2035. Approved by the Decree of the Government of the Russian Federation dated 15.12.2023 No. 1245-r.

Белов М.Э. Алгоритмическое управление в государственных цифровых платформах: архитектура, данные и интеллектуальные модели // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 113–117

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.03:004.6:004.8:35.07

АЛГОРИТМИЧЕСКОЕ УПРАВЛЕНИЕ В ГОСУДАРСТВЕННЫХ ЦИФРОВЫХ ПЛАТФОРМАХ: АРХИТЕКТУРА, ДАННЫЕ И ИНТЕЛЛЕКТУАЛЬНЫЕ МОДЕЛИ

Белов М.Э.
ФГБОУ ВО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ», Донецк, Россия (283001, Донецкая народная республика, г. Донецк, Университетская ул., д. 24), e-mail: mark_1998boss@mail.ru

В статье рассматриваются государственные цифровые платформы как сложные информационные системы, в которых ключевые управленческие функции реализуются с использованием алгоритмов интеллектуальной обработки данных. Показано, что внедрение технологий машинного обучения, анализа больших данных и обработки естественного языка приводит к формированию архитектур алгоритмического управления, в которых данные, модели и вычислительные контуры образуют единый управленческий цикл.Особое внимание уделяется архитектурным принципам построения государственных цифровых платформ, включая микросервисную организацию, доменно-ориентированное проектирование, централизованные хранилища данных и интеграционные шины. Обосновывается тезис о том, что именно архитектура платформы во многом определяет свойства алгоритмических систем — их прозрачность, воспроизводимость и устойчивость, а также характер возникающих системных ограничений. В работе предложена классификация алгоритмических моделей, используемых в государственных информационных системах, и показано, как они встраиваются в управленческий цикл цифровых платформ. Делается вывод о том, что архитектурные решения цифровых платформ являются ключевым фактором, влияющим на возможности контроля и управления алгоритмическими процессами, что имеет принципиальное значение для дальнейшего развития интеллектуальных государственных информационных систем.

Ключевые слова: Цифровые государственные платформы, архитектура информационных систем, интеллектуальная обработка данных, алгоритмическое управление, машинное обучение, цифровое государство.

ALGORITHMIC MANAGEMENT IN GOVERNMENT DIGITAL PLATFORMS: ARCHITECTURE, DATA, AND INTELLIGENT MODELS

Belov M.E.
DONETSK NATIONAL UNIVERSITY, Donetsk, Russia (283001,Donetsk People's Republic Donetsk, Universitetskaya St., 24), e-mail: mark_1998boss@mail.ru

This article examines government digital platforms as complex information systems in which key management functions are implemented using intelligent data processing algorithms. It is shown that the implementation of machine learning, big data analysis, and natural language processing technologies leads to the development of algorithmic management architectures in which data, models, and computational circuits form a single management cycle. Particular attention is paid to the architectural principles of building government digital platforms, including microservices, domain-specific design, centralized data warehouses, and integration buses. The paper substantiates the thesis that it is the platform architecture that largely determines the properties of algorithmic systems—their transparency, reproducibility, and sustainability—as well as the nature of emerging systemic constraints. The paper proposes a classification of algorithmic models used in government information systems and demonstrates how they fit into the management cycle of digital platforms. It concludes that the architectural solutions of digital platforms are a key factor influencing the ability to monitor and manage algorithmic processes, which is of fundamental importance for the further development of intelligent government information systems.

Keywords: digital government platforms, information system architecture, intelligent data processing, algorithmic management, machine learning, digital government.

Государственные цифровые платформы стремительно усложняются, внедряя алгоритмы искусственного интеллекта для обработки больших данных и автоматизации решений. Это приводит к появлению феномена алгоритмического управления – ситуации, когда ключевые управленческие функции выполняются с опорой на алгоритмы. Возникает проблема «чёрного ящика»: решения, принимаемые ИИ, становятся непонятными и непредсказуемыми для людей, что подрывает традиционные механизмы подотчётности. Юристы отмечают, что без обеспечения прозрачности и объяснимости алгоритмов ИИ их применение угрожает самому институту юридической ответственности [1]. Действительно, прозрачность и нейтральность алгоритмов выявляются как центральная проблема – платформы и их сервисы выступают посредниками между государством и гражданами, но часто работают непрозрачно [2]. Опираться на «чёрные ящики» опасно: если государственные органы не понимают логику алгоритма, они не могут гарантировать соблюдение прав граждан и законности решений. Таким образом, усложнение цифровых платформ порождает рост регуляторных рисков: от случайного несоответствия решений ИИ требованиям закона до систематического уклонения от правовых норм и принципов справедливости [3].

Методологическую основу исследования составляет междисциплинарный подход, сочетающий элементы правового анализа, теории публичного управления и анализа архитектуры информационных систем. Используется структурно-функциональный анализ для выявления роли алгоритмических компонентов в системе государственного управления, а также институциональный подход, позволяющий рассмотреть алгоритмы как новые квазиинституты принятия управленческих решений.

В рамках работы применяется аналитическая классификация алгоритмических систем, основанная на их функциональном назначении в государственных информационных системах, а также сравнительный анализ архитектурных решений цифровых платформ с точки зрения их влияния на прозрачность, подотчётность и соблюдение прав граждан. Такой подход позволяет преодолеть ограниченность сугубо технического или сугубо юридического анализа и рассматривать алгоритмическое управление как социотехнический феномен.

Предложенный междисциплинарный подход сочетает анализ архитектурных решений цифровых платформ и правовых аспектов функционирования алгоритмических систем [4]. Данная работа стремится объединить технический анализ (вопрос «как устроены и работают алгоритмические платформы») с юридическим анализом (то есть вопрос «как эти системы вписываются в существующие правовые рамки или требуют их обновления»). В рамках работы выявлены и классифицированы ключевые классы моделей ИИ, используемые в государственных цифровых платформах. Каждый класс моделей обладает своими рисками с точки зрения прозрачности: например, глубокие нейросети особенно трудно объяснить, а рекомендационные алгоритмы могут создавать эффект «фильтрующего пузыря». К ним относятся:

• Предиктивные модели машинного обучения (классификация, регрессия, нейросетевые модели) для прогнозирования событий и поддержки принятия решений в управлении – например, системы оценки рисков (финансовых, социальных) или прогнозирования потребностей в услугах.

• Аналитические модели для больших данных (кластеризация, факторный анализ) – применяются для выявления скрытых зависимостей в массиве государственных данных, что позволяет формировать доказательную базу для политики.

• Алгоритмы обработки естественного языка (NLP) – используются при анализе обращений граждан, нормативных актов, судебных решений; позволяют автоматически извлекать смысл из текстов и даже отвечать на запросы (чат-боты в госуслугах).

• Рекомендательные системы – персонализируют предоставление государственных услуг, подсказывая гражданам релевантные сервисы или информацию на основе их профиля и предыдущих взаимодействий.

Алгоритмические системы в государственных цифровых платформах следует рассматривать не изолированно, а в контексте полного управленческого цикла. На этапе сбора и агрегации данных алгоритмы обеспечивают предварительную фильтрацию и структурирование информации. На аналитическом этапе модели машинного обучения используются для выявления закономерностей и прогнозирования сценариев развития. Далее алгоритмические рекомендации могут напрямую или опосредованно влиять на принятие управленческих решений, включая распределение ресурсов, приоритизацию обращений граждан и формирование управленческих воздействий. В целом, алгоритмическое управление представляет собой замкнутый контур, в котором данные, модели и управленческие решения взаимно усиливают друг друга. Это повышает эффективность государственного управления, но одновременно усиливает значимость рисков, связанных с ошибками моделей, смещениями данных и непрозрачностью процедур принятия решений.

Кроме этого, был проведен анализ архитектурных принципов цифровых платформ. Он показал, что эффективная государственная платформа строится на принципах модульности, устойчивости и безопасности. Микросервисная архитектура стала де-факто стандартом: системы разбиваются на отдельные сервисы, отвечающие за конкретные функции (например, сервис аутентификации, сервис аналитики данных и т.д.), что повышает их управляемость и масштабируемость. Доменно-ориентированный подход (использованный, например, при создании платформы «ГосТех» – облачной цифровой платформ для федеральных и региональных органов власти в России, которая служит для быстрого создания, развития и эксплуатации государственных информационных систем) обеспечивает унификацию решений в масштабах государства за счёт разделения по предметным областям и стандартизации интерфейсов между ними. Обязательным элементом архитектуры является единое хранилище данных (или интеграционная шина), связывающее различные ведомства: это позволяет алгоритмам получать доступ к большим массивам государственных данных для обучения и работы. Уделяется особое внимание встроенной безопасности и соответствию требованиям регуляторов: платформы включают сертифицированные средства защиты информации и инструменты мониторинга, чтобы соблюсти законодательство о персональных данных и гостайне. Указанные архитектурные принципы повышают прозрачность и управляемость. Например, модульные алгоритмические компоненты легче подвергать аудиту, а единые стандарты обмена данными облегчают контроль за тем, как и какие данные используются.

Архитектура государственных цифровых платформ не является нейтральной по отношению к правовым рискам, а напротив — напрямую влияет на степень прозрачности и контролируемости алгоритмических решений. Так, микросервисная архитектура, с одной стороны, повышает управляемость и масштабируемость систем, но с другой — приводит к

фрагментации ответственности, когда принятие итогового управленческого решения распределяется между несколькими автономными сервисами. В таких условиях затрудняется установление источника ошибки или дискриминационного эффекта алгоритма.

С точки зрения правового анализа особое значение приобретает многоуровневая структура архитектуры государственных цифровых платформ. На уровне инфраструктуры (облачные среды, центры обработки данных, интеграционные шины) формируются риски, связанные с концентрацией данных и зависимостью от технических операторов. На уровне прикладных сервисов возникают вопросы распределения ответственности между различными компонентами системы, особенно в условиях микросервисной архитектуры. Наконец, на уровне аналитических и рекомендательных модулей сосредоточены ключевые риски алгоритмической непрозрачности, поскольку именно здесь происходит трансформация данных в управленческие решения. Такое расслоение архитектуры осложняет применение традиционных правовых механизмов контроля, ориентированных на линейные и иерархически организованные системы. В результате алгоритмическое управление приобретает распределённый характер, при котором ни один из отдельных элементов платформы не может быть однозначно идентифицирован как источник управленческого решения, что требует переосмысления подходов к юридической ответственности и подотчётности.

Централизованные хранилища данных и интеграционные шины создают предпосылки для обучения более точных моделей машинного обучения, однако одновременно усиливают риски вторичного использования персональных данных и нарушения принципа минимизации данных. Алгоритмическая непрозрачность в данном случае возникает не только на уровне модели, но и на уровне потоков данных, их агрегации и повторного использования. Таким образом, архитектурные решения цифровых платформ следует рассматривать как самостоятельный объект правового регулирования, а не исключительно как технический аспект. Эти ограничения алгоритмического управления в государственных информационных системах могут быть классифицированы по нескольким основаниям. Во-первых, это ограничения, связанные с качеством и происхождением данных, включая требования к достоверности, актуальности и правомерности источников данных. Во-вторых, ограничения, касающиеся самих алгоритмических моделей, в том числе требования к объяснимости, воспроизводимости результатов и недопущению дискриминационных эффектов.

В-третьих, особую группу составляют институциональные ограничения, связанные с распределением ответственности между государственными органами, разработчиками и операторами цифровых платформ. В условиях алгоритмического управления традиционные механизмы юридической ответственности оказываются недостаточно адаптированными к многоуровневым социотехническим системам. Наконец, следует выделить процедурные ограничения, предполагающие обязательность алгоритмического аудита, документирования логики принятия решений и возможности внешнего контроля со стороны надзорных органов и общества. Такая типология позволяет перейти от абстрактных требований «прозрачности» и «этичности» к конкретным объектам регулирования, что имеет принципиальное значение для развития правовых режимов цифрового государства.

Озвученная проблема носит комплексный характер – затрагивает и технологию, и власть, и права людей – а потому и ответ должна быть комплексным. Прозрачность алгоритмов и их подконтрольность нельзя обеспечить лишь техническими средствами,

поскольку они затрагивают баланс интересов и властные отношения [5]. Необходима интеграция инженерных подходов с правовыми рамками: только так государственные цифровые платформы смогут реализовать потенциал интеллектуальной обработки данных и алгоритмического управления без ущемления прав и свобод, сохраняя доверие общества. В перспективе необходим синтез технических и правовых решений: разработка стандартов и ГОСТов на прозрачность и качество данных, этические кодексы для разработчиков госалгоритмов, создание постоянно действующих междисциплинарных комитетов по надзору за алгоритмическим управлением. Научная новизна исследования заключается в комплексном рассмотрении алгоритмического управления в государственных информационных системах через призму архитектурных решений цифровых платформ. В отличие от работ, фокусирующихся преимущественно на правовых или технических аспектах, в данной статье показано, что именно архитектура цифровых платформ формирует условия возникновения регуляторных рисков и определяет возможности обеспечения прозрачности и подотчётности алгоритмических решений.

Список литературы

1. Зубарев С.М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. – 2020. – № 6 (115). – С. 23–32.
2. Володенков С.В., Федорченко С.Н. Цифровые инфраструктуры гражданско-политического активизма: актуальные вызовы, риски и ограничения // Мониторинг общественного мнения: экономические и социальные перемены. – 2021. – № 6. – С. 97–118.
3. Томин Л.В., Балаян А.А. Политические эффекты государственных цифровых платформ и сервисов в автократиях // Публичная политика. – 2023. – Т. 7, № 1–2. – С. 108–117.
4. Мухаметов Д.Р. Прозрачность алгоритмов в государственном секторе: основные аспекты // Креативная экономика. – 2024. – Т. 18, № 12. – С. 3867–3880.
5. Талапина Э.В. Прозрачность алгоритмов искусственного интеллекта // Право. Журнал Высшей школы экономики. – 2025. – Т. 18, № 3. – С. 4–27.

References

1. Zubarev S.M. Legal Risks of Digitalization of Public Administration // Current Issues of Russian Law. - 2020. - No. 6 (115). - Pp. 23-32.
2. Volodenkov S.V., Fedorchenko S.N. Digital Infrastructures of Civil and Political Activism: Current Challenges, Risks, and Limitations // Public Opinion Monitoring: Economic and Social Changes. - 2021. - No. 6. - Pp. 97-118.
3. Tomin L.V., Balayan A.A. Political Effects of State Digital Platforms and Services in Autocracies // Public Policy. - 2023. - Vol. 7, No. 1-2. - Pp. 108-117.
4. Mukhametov D.R. Transparency of Algorithms in the Public Sector: Key Aspects // Creative Economy. – 2024. – Vol. 18, No. 12. – Pp. 3867–3880.
5. Talapina E.V. Transparency of Artificial Intelligence Algorithms // Law. Journal of the Higher School of Economics. – 2025. – Vol. 18, No. 3. – Pp. 4–27.

Белов М.Э. Персональные данные: локализация «первичной записи» и архитектура комплаенса // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с.118–132

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056:342.721:004.6:004.03.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЛОКАЛИЗАЦИЯ «ПЕРВИЧНОЙ ЗАПИСИ» И АРХИТЕКТУРА КОМПЛАЕНСА

Белов М.Э.
ФГБОУ ВО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ», Донецк, Россия (283001, Донецкая народная республика, г. Донецк, Университетская ул., д. 24), e-mail: mark_1998boss@mail.ru

В статье анализируется требование локализации «первичной записи» персональных данных в условиях современных распределённых IT-архитектур. Показано, что отсутствие легального определения первичной записи и расхождение между юридическим и техническим пониманием фиксации данных формируют системные риски несоблюдения требований локализации даже при формальном размещении баз данных на территории Российской Федерации. На основе анализа нормативного регулирования, правоприменительной практики и типовых архитектур цифровых платформ предложена техническая модель архитектуры комплаенса, обеспечивающая контролируемую точку первичной записи, управление потоками персональных данных и проверяемость соответствия требованиям законодательства. Модель ориентирована на практическое применение в IT-аудите, regtech-инструментах и проектировании информационных систем.

Ключевые слова: LegalTech, локализация, первичная запись, ч.5 ст.18 152-ФЗ, трансграничная передача, ст.12 152-ФЗ, архитектура комплаенса, ИСПДн, 1119, ФСТЭК-21, риск-ориентированный подход.

PERSONAL DATA: LOCALIZATION OF THE "PRIMARY RECORD" AND COMPLIANCE ARCHITECTURE

Belov M.E.
DONETSK NATIONAL UNIVERSITY, Donetsk, Russia (283001,Donetsk People's Republic Donetsk, Universitetskaya St., 24), e-mail: mark_1998boss@mail.ru

This article analyzes the requirement to localize the "primary record" of personal data in the context of modern distributed IT architectures. It is shown that the lack of a legal definition of the primary record and the discrepancy between the legal and technical understanding of data recording create systemic risks of non-compliance with localization requirements, even when databases are formally located within the Russian Federation. Based on an analysis of regulatory frameworks, law enforcement practices, and typical digital platform architectures, a technical model of compliance architecture is proposed that ensures a controlled primary record point, management of personal data flows, and verifiability of compliance with legal requirements. The model is designed for practical application in IT audits, regulatory technology tools, and information system design.

Keywords: LegalTech, localization, primary recording, Part 5 of Article 18 of Federal Law No. 152, cross-border transfer, Article 12 of Federal Law No. 152, compliance architecture, ISPDN, 1119, FSTEC-21, risk-oriented approach.

Введение

Актуализация требований к локализации персональных данных в 2025 году обозначила качественный сдвиг в правовом регулировании обработки данных, сместив фокус с формального контроля места хранения к регулированию архитектуры процессов их сбора и первичной фиксации. Усиление акцента на локализацию «первичной записи» выявило

системное противоречие между юридическим пониманием момента начала обработки персональных данных и технической логикой функционирования современных распределённых IT-систем. В научной литературе отмечается, что действующее правовое регулирование персональных данных исторически ориентировано преимущественно на централизованные модели обработки информации и в ограниченной степени учитывает специфику распределённых архитектур и микросервисных систем [5],[8]. В результате формируется разрыв между нормативным толкованием «записи» персональных данных и фактическими процессами их фиксации и передачи в IT-системах, что порождает риски формального соблюдения требований локализации при их фактическом нарушении. Настоящая статья направлена на анализ данного противоречия и обоснование перехода от декларативного комплаенса к архитектурно ориентированному подходу. В работе предлагается авторская модель архитектуры комплаенса, обеспечивающая проверяемую локализацию первичной записи персональных данных и синхронизацию нормативных требований с реальной технической организацией процессов обработки данных.

1. Теоретико-нормативные основания локализации персональных данных

1.1. Эволюция требований к локализации персональных данных

Требования к локализации персональных данных сформировались как часть более общего процесса развития правового регулирования в сфере защиты информации и обеспечения цифрового суверенитета. На первоначальном этапе регулирование было ориентировано преимущественно на обеспечение конфиденциальности и безопасности данных как объекта правовой охраны, без жёсткой привязки к месту их физического размещения [5, с. 42,].

С развитием цифровых платформ и трансграничных информационных потоков акцент регулирования сместился в сторону территориального контроля обработки персональных данных. В российском праве данный подход был закреплён во введении требования локализации персональных данных граждан Российской Федерации, установленного в с. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», согласно которому запись, систематизация, накопление и хранение персональных данных должны осуществляться с использованием баз данных, расположенных на территории Российской Федерации [1, с. 18].

Изначально указанное требование в правоприменительной практике трактовалось преимущественно как требование к месту хранения и систематизации данных. Однако усложнение архитектуры информационных систем и переход к распределённым моделям обработки выявили ограниченность такого подхода, поскольку территориальный контроль исключительно над базами данных не охватывает этапы сбора и первоначальной фиксации персональных данных [6, с. 117].

Указанное противоречие было нормативно устранено в результате изменений, внесённых **Федеральным законом от 30.11.2024 № 420-ФЗ**, вступивших в силу с **1 января 2025 года**, которыми в с. 18 152-ФЗ был прямо усилен акцент на локализацию **первичной записи персональных данных** при их сборе [2, с. 18]. Тем самым законодатель зафиксировал, что соблюдение требования локализации должно обеспечиваться уже на этапе первоначальной фиксации данных, а не только на стадии их последующего хранения. Данное

изменение знаменует переход от формального территориального контроля к содержательному регулированию архитектуры процессов обработки персональных данных.

1.2. Понятие «первичной записи» персональных данных

В юридическом смысле под первичной записью персональных данных понимается момент первоначальной фиксации персональных данных оператором, с которого начинается их обработка и возникают предусмотренные законодательством обязанности по обеспечению локализации и защиты данных [1, с. 3]. В правоприменительной практике именно данный момент рассматривается как юридически значимый для определения применимой юрисдикции и объёма обязанностей оператора.

В техническом смысле первичная запись представляет собой первое персистентное сохранение персональных данных в устойчивом компоненте информационной системы — базе данных, журнале событий, event-store или очереди сообщений, — допускающем восстановление, воспроизведение и использование данных в бизнес- или аналитических процессах [9, с. 45]. Такое сохранение принципиально отличается от временного нахождения данных в оперативной памяти или транзитной передаче.

В юридической доктрине первичная запись традиционно связывается с возникновением правовых последствий и началом обработки персональных данных [7, с. 64]. Однако данный подход носит абстрактный характер и не учитывает архитектурную специфику современных распределённых информационных систем, в которых персональные данные могут фиксироваться поэтапно и в различных компонентах инфраструктуры [8, с. 89]. Это затрудняет однозначное определение момента и места первичной записи и формирует зону правовой неопределённости.

В целях устранения указанного разрыва в рамках настоящего исследования предлагается авторское комплексное определение:
первичная запись персональных данных — это первый юридически значимый и технически персистентный акт фиксации персональных данных в контролируемом компоненте информационной системы оператора, с которого данные становятся доступными для последующей обработки, воспроизведения или анализа и с которого должны обеспечиваться **требования локализации и защиты персональных данных**.

Данное определение позволяет синхронизировать нормативное и техническое понимание первичной записи и использовать его как основу для архитектурного проектирования и оценки соответствия требованиям законодательства.

1.3. Аспекты противоречия между нормативным и техническим пониманием момента «первичной записи»

В технической архитектуре информационных систем фиксация персональных данных носит принципиально иной характер и представляет собой распределённый процесс, включающий приём запросов, временное хранение данных в памяти, буферизацию, кэширование, логирование и асинхронную обработку [9, с. 134]. В результате момент, который в праве рассматривается как единичный акт записи, в IT-системах распадается на последовательность технических операций, не всегда очевидных для оператора и юридической функции.

В распределённых архитектурах персональные данные могут быть зафиксированы в логах, аналитических модулях или инфраструктуре внешних сервисов до их поступления в основное хранилище, которое оператор формально считает локализованным. Это приводит к ситуации, при которой фактическая первичная фиксация персональных данных осуществляется за пределами контролируемой юрисдикции при формальном соблюдении требований законодательства [10, с. 98].

Таким образом, выявляемое противоречие указывает на ограниченность трактовки локализации персональных данных исключительно как требования к месту хранения информации. В условиях современных IT-архитектур локализация приобретает характер архитектурного свойства системы, зависящего от проектных решений, определяющих маршруты данных и точки их фиксации. Указанное обстоятельство обосновывает необходимость перехода от формального нормативного подхода к архитектурно ориентированному пониманию локализации «первичной записи», что и определяет дальнейшую логику исследования.

2. Архитектура современных IT-систем обработки персональных данных

2.1. Типовая цепочка обработки персональных данных

Современные IT-системы обработки персональных данных, как правило, строятся на принципах распределённой архитектуры и включают несколько функциональных уровней, каждый из которых участвует в процессе фиксации и передачи данных. Типовая цепочка обработки начинается с пользовательского интерфейса — веб- или мобильного приложения, через которое субъект персональных данных вводит информацию. На данном этапе данные формируются в виде структурированных запросов и могут временно сохраняться в памяти устройства или браузера [11, с. 56].

Далее данные передаются через API-шлюзы, выполняющие функции маршрутизации, аутентификации и предварительной обработки запросов. API-шлюзы нередко осуществляют логирование входящих запросов, что уже на этом этапе создает дополнительную точку фиксации персональных данных [12, с. 143]. Серверы приложений обеспечивают бизнес-логику обработки данных, их валидацию и последующую передачу в хранилища.

Отдельное место в архитектуре занимают аналитические и логирующие сервисы, предназначенные для мониторинга, сбора метрик и анализа пользовательского поведения. Такие сервисы могут обрабатывать идентификаторы пользователей, IP-адреса и иные сведения, относящиеся к персональным данным, зачастую в автоматическом режиме [13, с. 211]. Дополнительно в цепочку обработки включаются внешние сервисы и SDK, предоставляемые третьими лицами, что существенно усложняет контроль над потоками данных и местом их первичной фиксации.

2.2. Точки возникновения и фиксации персональных данных

В рамках описанной архитектуры персональные данные могут возникать и фиксироваться на различных уровнях системы. Уже на уровне пользовательского интерфейса и API-шлюзов формируются потенциальные точки первичной записи, что требует их рассмотрения не только как элементов передачи данных, но и как архитектурных компонентов, критичных для соблюдения требований локализации. На клиентской стороне фиксация данных происходит в момент их ввода пользователем и формирования сетевого

запроса. Несмотря на то, что такие данные часто рассматриваются как «необработанные», они уже могут быть сохранены в логах браузера, мобильного приложения или инструментов отладки.

На серверной стороне фиксация персональных данных осуществляется при приёме запросов, их обработке и записи в базы данных. Однако помимо основного хранилища данные могут сохраняться во временных буферах, очередях сообщений и логах серверных компонентов, что создает дополнительные точки записи [15, с. 98].

Особую категорию составляют сторонние сервисы аналитики и мониторинга, которые могут получать персональные данные параллельно с основной обработкой. Такие сервисы нередко функционируют в иной юрисдикции и используют собственную инфраструктуру хранения данных [16, с. 162]. В результате «первичная запись» персональных данных может происходить до того, как данные поступят в локализованную базу оператора, что противоречит его представлениям о контролируемой точке фиксации.

2.3. Проблема распределённой фиксации данных

Ключевой архитектурной особенностью современных IT-систем является распределённый характер фиксации персональных данных. Использование механизмов буферизации и кэширования приводит к временному сохранению данных в различных компонентах системы, не всегда находящихся под прямым контролем оператора [17, с. 121]. Асинхронная передача данных, характерная для микросервисных архитектур, дополнительно размывает границы между моментом сбора и моментом окончательной записи данных.

Значительную роль в распределённой фиксации играют журналы событий и системные логи, которые предназначены для диагностики и обеспечения отказоустойчивости. В таких журналах могут содержаться персональные данные или их производные, что фактически образует самостоятельные точки первичной записи [18, с. 87]. При этом данные журналы зачастую не рассматриваются оператором как элементы системы обработки персональных данных.

Таким образом, архитектура современных IT-систем создает ситуацию, при которой фиксация персональных данных осуществляется множественно и распределённо, а момент «первичной записи» может предшествовать осознанной обработке данных оператором. Это, в свою очередь, формирует существенные риски несоблюдения требований локализации, которые рассмотрены в следующем разделе.

3. Риски несоблюдения локализации «первичной записи» персональных данных

3.1. Архитектурные риски обработки персональных данных

Распределённая архитектура современных IT-систем формирует совокупность архитектурных рисков, связанных с неконтролируемой фиксацией персональных данных. Одним из ключевых рисков является наличие множественных точек записи данных, не учитываемых оператором при проектировании системы. Такие точки могут возникать в API-шлюзах, промежуточных сервисах, очередях сообщений и логирующих компонентах, которые изначально не рассматриваются как элементы обработки персональных данных [12, с. 146].

Использование облачных инфраструктур и внешних SDK дополнительно усиливает данные риски. Персональные данные могут временно или постоянно фиксироваться в инфраструктуре третьих лиц, что затрудняет определение юрисдикции первичной записи и

контроль за соблюдением требований локализации [8, с. 91]. В условиях микросервисной архитектуры оператор нередко утрачивает целостное представление о потоках данных, поскольку отдельные компоненты системы разрабатываются и обслуживаются независимо друг от друга [17, с. 129].

Следствием указанных архитектурных особенностей становится ситуация, при которой фактическая первичная фиксация персональных данных происходит вне локализованного контура, несмотря на размещение основной базы данных на территории требуемой юрисдикции. Это создает структурный риск несоответствия требованиям законодательства, не связанный с умышленными действиями оператора.

3.2. Правовые и комплаенс-риски

В соответствии с законодательством о персональных данных ответственность за соблюдение требований обработки возлагается на оператора независимо от используемых технических решений и привлечения третьих лиц [1, с. 18].

В правоприменительной практике это означает, что формальное размещение баз данных на территории соответствующей юрисдикции не освобождает оператора от ответственности в случае выявления фактов первичной фиксации данных за её пределами. При этом доказательство архитектурной добросовестности оператора осложняется отсутствием документированной модели потоков данных и явных точек первичной записи [6, с. 121].

Дополнительным комплаенс-риском является разрыв между юридической и технической интерпретацией обработки персональных данных. Юридическая функция, как правило, опирается на договоры, политики и реестры процессов, тогда как реальные точки фиксации данных определяются архитектурными решениями, принятыми на уровне разработки и эксплуатации системы [10, с. 102]. В результате комплаенс приобретает декларативный характер и не отражает фактическое состояние системы.

3.3. Практика регуляторного и судебного толкования первичной записи персональных данных

Практика Роскомнадзора и судебных органов Российской Федерации свидетельствует о расширительном толковании требования локализации персональных данных, при котором ключевое значение придаётся не только месту хранения баз данных, но и архитектуре процессов их сбора и первичной фиксации. В рамках контрольно-надзорной деятельности регулятор исходит из того, что первичная запись персональных данных может осуществляться на ранних этапах обработки, включая момент их передачи в сторонние сервисы и программные компоненты.

Показательным является дело LinkedIn Corporation (дело № А40-18827/2016). В решении Московского городского суда от 10.11.2016 указано, что сбор и обработка персональных данных пользователей осуществлялись с использованием серверной инфраструктуры, расположенной за пределами Российской Федерации, что образует нарушение требований с. 18 Федерального закона № 152-ФЗ. Суд фактически связал нарушение не только с хранением данных, но и с архитектурой их первичного сбора, признав юридически значимым момент первоначальной фиксации персональных данных пользователей.

Аналогичный подход отражён в практике Таганского районного суда г. Москвы по делам о привлечении к ответственности Twitter Inc. и Meta Platforms Inc. (Facebook) (дела № 05-

1927/2021, № 05-1196/2022). В указанных делах суд исходил из того, что персональные данные российских пользователей фиксируются и обрабатываются в зарубежной инфраструктуре на этапе их сбора, что свидетельствует о несоблюдении требований локализации независимо от последующего хранения отдельных массивов данных.

Практика Роскомнадзора в отношении российских операторов также подтверждает архитектурный характер толкования первичной записи. В ходе проверок и разъяснений 2021–2023 гг. регулятор указывал на недопустимость использования сервисов веб-аналитики Google Analytics без обеспечения локализации первичной фиксации пользовательских данных, включая IP-адреса и идентификаторы, передаваемые в инфраструктуру Google LLC в момент взаимодействия пользователя с сайтом.

В научной литературе подобный подход объясняется объективным усложнением архитектуры обработки данных и направлен на предотвращение формального соблюдения требований локализации при фактическом выведении процессов первичной фиксации за пределы национальной юрисдикции.

4. Архитектура комплаенса как ответ на регуляторные требования

4.1. Понятие архитектуры комплаенса

Таким образом, усложнение цифровых систем и распределённый характер обработки персональных данных выявили ограниченность традиционного понимания комплаенса как совокупности формальных документов, регламентов и договорных обязательств. Такой подход не отражает фактические процессы фиксации и передачи данных в современных IT-архитектурах и не позволяет обеспечить проверяемое соблюдение требований законодательства. В этой связи в научной и прикладной литературе используется понятие архитектуры комплаенса, под которой понимается совокупность архитектурных решений, обеспечивающих встроенное соответствие информационной системы нормативным требованиям [9, с. 37].

Архитектура комплаенса предполагает рассмотрение правовых требований не как внешних ограничений, а как проектных параметров системы, учитываемых при формировании её структуры и логики функционирования. Такой подход соответствует концепции *compliance by design*, согласно которой соблюдение правовых норм обеспечивается архитектурой системы, а не исключительно последующим контролем или аудитом [16, с. 174]. В сфере персональных данных это означает, что требования локализации и контроля первичной записи должны быть реализованы на уровне архитектуры обработки данных.

Таким образом, архитектура комплаенса может быть определена как способ формализации правовых требований в виде устойчивых архитектурных свойств информационной системы. Вне такой формализации комплаенс носит декларативный характер и не оказывает влияния на фактическую организацию процессов обработки персональных данных [6, с. 127].

4.2. Компоненты архитектуры комплаенса и их соответствие НПА

Под компонентами архитектуры комплаенса в рамках настоящего исследования понимаются **структурно и функционально выделенные элементы IT-архитектуры**, через которые реализуются требования законодательства о персональных данных и подзаконного регулирования. В отличие от формального подхода, при котором требования 152-ФЗ, ПП РФ

№ 1119 и приказа ФСТЭК № 21 фиксируются в документации, архитектурный подход предполагает их прямую реализацию в конкретных технических контурах обработки данных.

Регуляторную основу данных компонентов составляют положения Федерального закона № 152-ФЗ «О персональных данных», а также подзаконные акты, конкретизирующие его требования: Постановление Правительства РФ от 01.11.2012 № 1119, устанавливающее уровни защищённости ИСПДн, и приказ ФСТЭК России от 18.02.2013 № 21, определяющий обязательные меры защиты информации. С 2025 года данные требования дополняются усиленным акцентом на локализацию **первичной записи персональных данных**, что требует явного архитектурного закрепления соответствующих этапов обработки.

Ключевым компонентом архитектуры комплаенса является **Primary Data Ingress (PDI)** — архитектурно выделенная точка приёма персональных данных. В нормативном смысле данный компонент реализует требования с. 18 152-ФЗ и ПП РФ № 1119 в части контроля этапа сбора данных. В практической реализации PDI, как правило, представляет собой API Gateway или backend-for-frontend, совмещённый с механизмами фильтрации и контроля трафика. Его основная функция заключается в предотвращении несанкционированной первичной фиксации персональных данных в сторонних сервисах и обеспечении того, чтобы момент первичной записи происходил исключительно в контролируемом локализованном контуре.

Primary Storage Layer (PSL) отвечает за выполнение требований законодательства, связанных с локализацией, хранением и защитой персональных данных. Данный компонент реализуется в виде локализованного устойчивого хранилища (база данных или event-store), размещённого на территории Российской Федерации и защищённого в соответствии с приказом ФСТЭК № 21. С практической точки зрения PSL является технически и юридически значимой точкой начала обработки персональных данных, поскольку именно в нём осуществляется их первичное персистентное сохранение, подлежащее контролю и аудиту.

Функции **Data Classification Middleware (DCM)** соотносятся с требованиями ПП РФ № 1119 о необходимости классификации ИСПДн и определения уровня их защищённости. В практической архитектуре DCM реализуется в виде middleware или policy-engine, автоматически присваивающего данным и операциям обработки соответствующий статус. Значение данного компонента заключается в формализации регуляторных требований и снижении риска ошибочной или избыточной передачи персональных данных за пределы допустимого контура.

Outbound Control Layer (OCL) реализует положения приказа ФСТЭК № 21, касающиеся контроля сетевых взаимодействий и предотвращения утечек информации. На практике OCL внедряется на уровне сетевой инфраструктуры или service mesh и обеспечивает контроль всех исходящих потоков данных. Его роль заключается в техническом обеспечении запрета передачи персональных данных за пределы локализованного контура до момента их допустимой трансформации, что имеет ключевое значение для соблюдения требований локализации первичной записи.

Таким образом, архитектурное выделение и согласованная реализация компонентов PDI, PSL, DCM и OCL позволяет трансформировать требования законодательства и подзаконных актов в устойчивые технические свойства информационной системы. Учет данных компонентов формирует основу для построения авторской модели архитектуры комплаенса, ориентированной на проверяемое и доказуемое соблюдение обновлённых требований о локализации первичной записи персональных данных, вступивших в силу с 2025 года.

5. Техническая модель обеспечения локализации первичной записи персональных данных

5.1. Формализация архитектурной модели первичной записи

В целях практической реализации требований локализации «первичной записи» персональных данных предлагается техническая архитектурная модель, основанная на **жёстком разграничении этапов фиксации данных и их последующей обработки**.

В рамках настоящего исследования под архитектурной моделью первичной записи персональных данных понимается **формализованная последовательность технических и логических операций обработки данных**, выстроенная таким образом, что момент и место первичной записи персональных данных однозначно фиксируются в пределах территории Российской Федерации, а последующие операции обработки допускаются только после завершения данной записи и в нормативно допустимой конфигурации потоков данных.

В рамках данной модели первичная запись трактуется не абстрактно, а как конкретная операция записи данных в устойчивое хранилище или журнал событий, обладающее следующими признаками:

1. возможность восстановления данных после сбоя;
2. возможность их последующего воспроизведения;
3. использование в бизнес- или аналитических процессах.

Таким образом, первичная запись приравнивается к первому персистентному сохранению персональных данных в архитектуре системы [9, с. 45].

5.2. Совокупная модель архитектуры первичной записи персональных данных

Предлагаемая модель архитектуры первичной записи персональных данных основана на жёстко заданной и технически детерминированной последовательности этапов обработки данных, при которой каждый последующий этап логически и архитектурно невозможен без завершения предыдущего. Модель исключает параллельные, опережающие либо неявные операции записи и передачи персональных данных за пределы первичного контура до момента их нормативно корректной фиксации, что обеспечивает однозначное определение момента и места первичной записи.

Этап 1. Инициация сбора персональных данных (pre-collection stage). На первом этапе субъект персональных данных инициирует взаимодействие с информационной системой (заполнение формы, обращение к сервису, использование функционала приложения). На данном этапе допускается обработка исключительно неидентифицирующих технических данных, необходимых для установления соединения и функционирования протоколов передачи информации (например, параметры сетевого соединения, служебные заголовки запросов).
Любая фиксация данных, позволяющих прямо или косвенно идентифицировать субъекта персональных данных, на данном этапе архитектурно исключается и не рассматривается как первичная запись.

Этап 2. Первичная запись идентифицируемых данных (PDI/PSL stage). На втором этапе осуществляется первая и единственная первичная запись персональных данных, позволяющих идентифицировать субъекта. Данный этап реализуется исключительно через компонент Primary Data Ingress (PDI) с последующей записью данных в Primary Storage Layer (PSL), развернутые в пределах инфраструктуры, физически и логически расположенной

на территории Российской Федерации. Юридически именно этот момент квалифицируется как «сбор персональных данных» в смысле части 5 статьи 18 Федерального закона № 152-ФЗ. Технически он выражается в операции персистентного сохранения персональных данных в устойчивом хранилище или журнале событий без предварительной передачи, репликации или обработки данных во внешних сервисах, аналитических SDK или вспомогательных контурах.

Этап 3. Формирование псевдонимизированных идентификаторов (post-record stage).

Только после завершения первичной записи персональных данных система формирует устойчивые технические идентификаторы (токены, session ID, client ID), используемые для последующей обработки данных и взаимодействия между компонентами системы. Указанные идентификаторы логически связаны с первичной записью, однако не содержат персональных данных в явном виде и не позволяют идентифицировать субъекта без обращения к первичному контуру хранения.

Этап 4. Классификация данных и управление потоками (DCM stage). На данном этапе осуществляется контролируемая маршрутизация и дальнейшая обработка данных с использованием Data Classification Middleware (DCM). Архитектура модели обеспечивает, что:

- идентифицируемые персональные данные не покидают первичный контур без наличия правового основания;
- псевдонимизированные и агрегированные данные могут использоваться для аналитических и сервисных целей;
- любые попытки отклонения от установленной последовательности обработки блокируются на уровне маршрутизации и политик передачи данных.

Тем самым реализуется нормативно обусловленный поток данных (data flow), при котором направление, содержание и допустимость передачи данных определяются не функциональной целесообразностью, а требованиями законодательства о персональных данных.

Этап 5. Фиксация и подтверждение корректности обработки (OCL stage). Заключительный этап модели направлен на фиксацию и подтверждение соблюдения установленной архитектурной последовательности обработки персональных данных. В рамках данного этапа формируются журналы первичной записи, метаданные маршрутизации, логи сетевых и прикладных операций, а также реестр интеграций и технических зависимостей, контролируемых через Outbound Control Layer (OCL). Наличие данного слоя позволяет воспроизвести полную цепочку обработки персональных данных и подтвердить, что первичная запись была осуществлена до любых операций последующей обработки, логирования, аналитики или передачи данных во внешние сервисы, что устраняет архитектурную неопределённость момента фиксации персональных данных [12, с. 158].

5.3. Критерии аудита и проверки реализации модели

Для практического применения предложенная архитектурная модель допускает формализованную проверку соответствия, ориентированную на воспроизводимый IT-аудит и доказуемость соблюдения требований локализации первичной записи. В отличие от

документального комплаенса, который фиксирует намерения оператора, техническая верификация модели должна подтверждать фактическое поведение системы: где именно происходит первичная запись, какие компоненты получают доступ к данным и в какой последовательности выполняются операции обработки.

Критерий 1. Наличие единственной точки первичной записи. Верификация включает подтверждение того, что в архитектуре существует ровно одна контролируемая точка, в которой идентифицируемые персональные данные впервые сохраняются персистентно (PSL), а любые альтернативные маршруты (прямой доступ клиента к сервисам, запись через обходные эндпоинты, «теневые» очереди или журналы) исключены. На практике данный критерий проверяется через анализ конфигураций API, сетевых политик и фактических маршрутов запросов.

Критерий 2. Отсутствие логов и метрик, содержащих персональные данные, до PSL.

Проверка предусматривает анализ логирования на всех этапах до первичной записи: на уровне клиентских SDK, API Gateway, middleware, балансировщиков и систем мониторинга. Требование означает, что до PSL допускается фиксация только технических параметров, не позволяющих идентифицировать субъекта, а персональные данные должны быть исключены из логов и метрик либо замещены безопасными маркерами. Это снижает риск неявной первичной записи в логирующем контуре.

Критерий 3. Документированная и актуальная схема data flow. Модель предполагает наличие архитектурно утверждённой схемы потоков данных, отражающей последовательность этапов обработки: от пользовательского интерфейса до первичного хранилища и далее до контуров аналитики и внешних интеграций. Для аудита значима не только наличие схемы, но и её подтверждаемость наблюдаемыми техническими артефактами (маршрутизация, политики egress, конфигурации сервисов).

Критерий 4. Технические ограничения на SDK и внешние API. Доказуемость модели обеспечивается не декларативными запретами, а техническими ограничениями: контролем исходящего трафика, запретом прямых вызовов внешних сервисов до PSL, а также регламентом допустимых данных, которые могут покидать локализованный контур (только псевдонимизированные или агрегированные). В рамках аудита проверяется наличие механизма принудительного исполнения этих ограничений.

Критерий 5. Трассируемость данных от интерфейса до хранилища. Критически важным элементом является возможность воспроизвести цепочку обработки персональных данных и показать, что первичная запись предшествует любой дальнейшей обработке или передаче. Трассируемость достигается за счёт корреляционных идентификаторов, журналов событий, метаданных маршрутизации и контроля доступа, что позволяет проводить расследования инцидентов и подтверждать соответствие модели [10, с. 109].

Перечисленные критерии позволяют использовать предложенную модель как практическую основу для **IT-аудита**, **регуляторных проверок** и **regtech-инструментов автоматизированного контроля**, в которых соответствие проверяется по наблюдаемым техническим признакам, а не по декларативным документам.

5.4. Границы применимости модели

Предложенная архитектурная модель локализации первичной записи персональных данных ориентирована на практическое применение в информационных системах, архитектура которых допускает выделение контролируемого первичного контура обработки данных. Наибольшую эффективность модель демонстрирует в системах с централизованным backend-контуром, в рамках которого возможно архитектурно зафиксировать единственную точку первичной записи и обеспечить нормативно обусловленную последовательность обработки данных. В таких системах компоненты PDI, PSL, DCM и OCL могут быть чётко разграничены и поддаются техническому аудиту и трассировке, что позволяет реализовать проверяемый комплаенс.

Дополнительным условием применимости модели является наличие контролируемого набора внешних интеграций. Архитектура предполагает, что все взаимодействия с аналитическими, мониторинговыми и сторонними сервисами осуществляются через формализованные каналы передачи данных, допускающие техническое ограничение состава и статуса передаваемой информации. При таком подходе становится возможным исключить неявную первичную фиксацию персональных данных во внешних компонентах и обеспечить соответствие требованиям локализации первичной записи.

В высоко-распределённых системах, использующих событийно-ориентированные архитектуры, большое количество автономных микросервисов и внешних SDK, реализация модели сталкивается с дополнительными ограничениями. В таких условиях контроль последовательности обработки и предотвращение несанкционированной фиксации данных требуют внедрения дополнительных уровней orchestration, централизованного управления событиями и расширенных механизмов event-control. Это приводит к росту архитектурной сложности, увеличению эксплуатационных затрат и повышенным требованиям к управлению конфигурациями и политиками безопасности [8, с. 104].

Таким образом, предложенная модель не претендует на универсальное применение во всех типах информационных систем, однако она задаёт архитектурный ориентир и набор проектных принципов, которые могут быть адаптированы и масштабированы в зависимости от уровня распределённости системы и требований к контролю обработки персональных данных.

Заключение

Проведённое исследование показало, что усиление требования локализации «первичной записи» персональных данных с 2025 года обусловлено не столько расширением объёма обязанностей операторов, сколько необходимостью устранения системного разрыва между юридическим и техническим пониманием процессов обработки данных. Анализ нормативных источников и правоприменительной практики подтвердил, что формальное размещение баз данных на территории Российской Федерации не гарантирует соблюдение требований законодательства в условиях распределённых IT-архитектур, в которых фиксация персональных данных может происходить множественно и асинхронно.

В рамках работы предложено авторское комплексное определение первичной записи персональных данных как первого юридически значимого и технически персистентного акта фиксации данных в контролируемом компоненте информационной системы оператора. Данное определение позволяет синхронизировать абстрактные правовые категории с

реальными архитектурными решениями и устранить неопределённость момента начала обработки персональных данных.

Существенным результатом исследования является анализ компонентов архитектуры комплаенса (PDI, PSL, DCM, OCL) и их соотнесение с требованиями Федерального закона № 152-ФЗ и подзаконного регулирования. Показано, что нормативные требования могут быть реализованы не декларативно, а в виде устойчивых архитектурных свойств информационной системы, поддающихся технической верификации и аудиту.

На основе проведённого анализа разработана авторская модель архитектуры локализации первичной записи персональных данных, основанная на жёстко детерминированной последовательности этапов обработки и исключающая неявную фиксацию данных за пределами локализованного контура. Предложенная модель формирует практическую основу для проверяемого комплаенса, IT-аудита и regtech-инструментов и может быть использована операторами персональных данных при проектировании и модернизации информационных систем в условиях обновлённого регулирования.

Список литературы

1. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ
2. «О персональных данных» (ред. действующая на 2025 г.) // Собрание законодательства РФ. — 2006. — № 31 (ч. 1). — С. 3451.
3. Российская Федерация. Законы. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 ноября 2024 г. № 420-ФЗ // Официальный интернет-портал правовой информации.
4. Российская Федерация. Правительство. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Постановление Правительства РФ от 01 ноября 2012 г. № 1119
5. Федеральная служба по техническому и экспортному контролю. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 14.05.2020) : зарегистрировано в Минюсте России 14.05.2013 № 28375 // КонсультантПлюс.
6. Бачило И. Л. Право информационных технологий : учебник для вузов. — 2-е изд., перераб. и доп. — М. : Юрайт, 2020. — 419 с.
7. Кучерена А. Г. Информационная безопасность и защита персональных данных. — М. : Норма, 2019. — 304 с.
8. Лопатин В. Н. Правовые основы защиты персональных данных в цифровой среде // Журнал российского права. — 2021. — № 3. — С. 58–71.
9. Kuner C. Transborder Data Flows and Data Privacy Law. — Oxford : Oxford University Press, 2017. — 392 p.
10. Bass L., Clements P., Kazman R. Software Architecture in Practice. — 3rd ed. — Boston : Addison-Wesley, 2012. — 624 p.
11. Черников Б. В. Архитектура информационных систем : учебное пособие. — М. : ИНФРА-М, 2020. — 256 с.

12. Tanenbaum A. S., Van Steen M. Distributed Systems: Principles and Paradigms. — 2nd ed. — Upper Saddle River : Pearson, 2017. — 686 p.
13. Newman S. Building Microservices: Designing Fine-Grained Systems. — 2nd ed. — Sebastopol : O’Reilly Media, 2021. — 600 p.
14. Zuboff S. The Age of Surveillance Capitalism. — New York : PublicAffairs, 2019. — 704 p.
15. Mozilla Foundation. Web Application Security Guide. — Mozilla Developer Network, 2023. — URL: developer.mozilla.org (дата обращения: 2025-01-03).
16. Fowler M. Patterns of Enterprise Application Architecture. — Boston : Addison-Wesley, 2003. — 533 p.
17. Kuner C., Bygrave L., Docksey C. The EU General Data Protection Regulation (GDPR): A Commentary. — Oxford : Oxford University Press, 2020. — 1920 p.
18. Kleppmann M. Designing Data-Intensive Applications. — Sebastopol : O’Reilly Media, 2017. — 616 p.
19. Черняк Л. Журналы событий и логирование в распределённых системах // Открытые системы. СУБД. — 2020. — № 4. — С. 82–90.

References

1. Federal Law of the Russian Federation of July 27, 2006, No. 152-FZ
2. "On Personal Data" (as amended as of 2025) // Collected Legislation of the Russian Federation. — 2006. — No. 31 (Part 1). — p. 3451.
3. Russian Federation. Laws. On Amendments to the Code of the Russian Federation on Administrative Offenses: Federal Law of November 30, 2024, No. 420-FZ // Official Internet Portal of Legal Information.
4. Russian Federation. Government. On Approval of Requirements for the Protection of Personal Data When Processed in Personal Data Information Systems: Resolution of the Government of the Russian Federation of November 1, 2012, No. 1119
5. Federal Service for Technical and Export Control. On approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data When Processing them in Personal Data Information Systems: Order of the FSTEC of Russia dated February 18, 2013 No. 21 (as amended on May 14, 2020): registered with the Ministry of Justice of Russia on May 14, 2013 No. 28375 // ConsultantPlus.
6. Bachilo I. L. Information Technology Law: textbook for universities. — 2nd ed., revised and enlarged. — Moscow: Yurait, 2020. — p.419
7. Kucherena A. G. Information Security and Personal Data Protection. — Moscow: Norma, 2019. — 304 p.
8. Lopatin V. N. Legal Foundations for Personal Data Protection in the Digital Environment // Journal of Russian Law. — 2021. — No. 3. — pp. 58–71.
9. Kuner C. Transborder Data Flows and Data Privacy Law. — Oxford : Oxford University Press, 2017. — p.392
10. Bass L., Clements P., Kazman R. Software Architecture in Practice. — 3rd ed. — Boston : Addison-Wesley, 2012. — p.624
11. Chernikov B. V. Architecture of Information Systems: A Tutorial. — Moscow : INFRA-M, 2020. — p.256

12. Tanenbaum A. S., Van Steen M. Distributed Systems: Principles and Paradigms. — 2nd ed. — Upper Saddle River : Pearson, 2017. — p.686
13. Newman S. Building Microservices: Designing Fine-Grained Systems. — 2nd ed. — Sebastopol: O'Reilly Media, 2021. — p. 600
14. Zuboff S. The Age of Surveillance Capitalism. — New York: PublicAffairs, 2019. — p.704
15. Mozilla Foundation. Web Application Security Guide. - Mozilla Developer Network, 2023. - URL: developer.mozilla.org (accessed 2025-01-03).
16. Fowler M. Patterns of Enterprise Application Architecture. - Boston: Addison-Wesley, 2003. - p.533
17. Kuner C., Bygrave L., Docksey C. The EU General Data Protection Regulation (GDPR): A Commentary. — Oxford : Oxford University Press, 2020. — p.1920
18. Kleppmann M. Designing Data-Intensive Applications. — Sebastopol : O'Reilly Media, 2017. — p.616
19. Chernyak L. Event logs and logging in distributed systems // Open Systems. DBMS. — 2020. — No. 4. — pp. 82–90.

Ким А.С., Крепак И.П. Эволюция APT-атак: применение обфускации и ИИ для обхода от средств защиты информации // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 133–138

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ЭВОЛЮЦИЯ APT-АТАК: ПРИМЕНЕНИЕ ОБФУСКАЦИИ И ИИ ДЛЯ ОБХОДА ОТ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

[1]Ким А.С., [2]Крепак И.П.
ФГОБУ ВО «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ», Москва, Россия (125167, г. Москва, Ленинградский просп., 55), e-mail: [1] archikim1441@gmail.com, [2] krepak.2311@yandex.ru

Статья посвящена анализу современных тенденций в области целевых компьютерных атак повышенной сложности. Рассматривается эволюция тактик, техник и процедур злоумышленников, уделяя особое внимание двум ключевым аспектам: усложнению методов обфускации вредоносного кода и активному внедрению технологий искусственного интеллекта для повышения скрытности и адаптивности компьютерных атак. На основе актуальных данных и исследований 2025 года проанализированы этапы типичной APT-атаки, методы противодействия классическим средствам защиты, а также случаи компьютерных атак на российские компании. Цель статьи — систематизировать новые угрозы и предложить направления для усиления стратегии защиты, включая переход к предиктивной аналитике и комплексному подходу, сочетающему технологические и организационные меры.

Ключевые слова: APT-атака, обфускация кода, искусственный интеллект, генеративный ИИ, машинное обучение, SOC, поведенческий анализ.

EVOLUTION OF APT ATTACKS: THE USE OF OBFUSCATION AND AI TO EVADE SECURITY MEASURES

[1]Kim A.S., [2]Krepak I.P.
FINANCIAL UNIVERSITY UNDER THE GOVERNMENT OF THE RUSSIAN FEDERATION, Moscow, Russia (125167, Moscow, Leningradsky Prospekt, 55), e-mail: [1]archikim1441@gmail.com, [2] krepak.2311@yandex.ru

The article is devoted to the analysis of current trends in advanced targeted cyberattacks. It examines the evolution of adversaries' tactics, techniques, and procedures, with particular attention to two key aspects: the increasing sophistication of malware obfuscation methods and the active adoption of artificial intelligence technologies to enhance the stealth and adaptability of cyberattacks. Based on up-to-date data and studies from 2025, the paper analyzes the stages of a typical APT attack, methods of countering traditional security solutions, as well as cases of cyberattacks against Russian companies. The aim of the article is to systematize emerging threats and propose directions for strengthening defense strategies, including a transition to predictive analytics and a comprehensive approach that combines technological and organizational measures.

Keywords: APT attack, code obfuscation, artificial intelligence, generative AI, machine learning, SOC, behavioral analysis.

Введение

Современные APT-атаки стремительно эволюционируют, становясь более скрытными и адаптивными. Ключевыми факторами этой трансформации являются усложнение методов обфускации кода и внедрение технологий искусственного интеллекта (ИИ). Эти технологии позволяют злоумышленникам эффективно маскировать вредоносную активность под

легитимную, а также автоматизировать создание персонализированных фишинговых атак и полиморфного кода, что значительно усложняет их обнаружение.

Особую опасность представляет использование генеративного ИИ, которое сокращает время на подготовку атаки и повышает её точность, позволяя злоумышленникам анализировать защитные системы и адаптироваться к ним в реальном времени. Это создаёт серьёзный вызов для традиционных средств кибербезопасности и требует пересмотра стратегий защиты. В данной статье рассматриваются новые TTP (тактики, техники и процедуры) APT-группировок и необходимые изменения в подходах к противодействию интеллектуальным угрозам.

Классические методы обфускации в APT-атаках: эволюция и современные техники

Обфускация кода — базовый инструмент APT-группировок для сокрытия вредоносной логики и продления жизненного цикла компьютерной атаки. Её развитие отражает непрерывное противостояние с создателями защитных решений. Изначально методы обхода сигнатурного анализа, такие как шифрование полезной нагрузки и упаковщики, оставались уязвимыми для эвристического анализа из-за оставляемых поведенческих паттернов.

Эволюционным скачком стало внедрение полиморфных и метаморфных технологий. Полиморфный код мог изменяться при каждом цикле заражения, сохраняя функциональность, а метаморфный — полностью перестраивать алгоритм работы. Это сделало статические сигнатуры неэффективными и стимулировало развитие динамического анализа, включая песочницы и эмуляторы.

В современных условиях обфускация стала комплексной стратегией, где доминируют файлесс-атаки, при которых вредоносный код существует только в оперативной памяти и использует легитимные процессы [5]. Параллельно развивается сетевая маскировка, когда трафик управления имитирует легитимные HTTPS-сессии, DNS-запросы или данные облачных сервисов, что серьёзно затрудняет его обнаружение [4]. Эти методы уже интегрированы во все этапы APT-атак, превращая обфускацию в ключевой компонент обеспечения скрытности и устойчивости целевых операций.

Роль искусственного интеллекта в автоматизации и усилении целевых атак

Искусственный интеллект и машинное обучение стали ключевыми технологиями APT-группировок, превращая целевые атаки в высокоавтоматизированные и адаптивные операции. ИИ выступает силовым множителем на всех этапах — от подготовки до исполнения, кардинально повышая эффективность и скрытность атак.

Генеративные модели ИИ трансформируют социальную инженерию, создавая фишинг сообщения и голосовые подделки с беспрецедентным уровнем персонализации на основе анализа открытых источников. Это значительно повышает успешность целевого фишинга — основного вектора начальной компрометации [4]. Одновременно ИИ революционизирует автоматизацию разведки: алгоритмы сканируют цифровой периметр организаций, анализируют базы уязвимостей и сопоставляют их с обнаруженными сервисами, сокращая время от разведки до атаки до минимума [2].

В области разработки вредоносного ПО нейросетевые модели создают полиморфный код нового поколения, способный адаптироваться под конкретные системы защиты.

Алгоритмы автоматически тестируют образцы на детектирование и отбирают наиболее скрытные варианты [1]. Наиболее сложным направлением становится применение состязательного машинного обучения для уклонения от обнаружения, когда специально сконструированные воздействия обходят системы защиты, заставляя их классифицировать атаку как нормальную активность. ИИ-агенты атакующих анализируют реакцию защитных систем и динамически корректируют свое выполнение.

Таким образом, ИИ преобразует APT-атаки в самообучающиеся и адаптивные угрозы, что требует от специалистов информационной безопасности разработки принципиально новых подходов к системам защиты, устойчивых к интеллектуальному противодействию.

Тактика противодействия: интеграция поведенческого анализа и предиктивных моделей

Противодействие современным APT-атакам требует перехода от реактивных к предиктивным и поведенческим моделям защиты. Традиционные методы часто оказываются неэффективными против адаптивных угроз, использующих обфускацию и ИИ.

Основу новой стратегии составляет поведенческий анализ. Вместо поиска известных сигнатур эти системы выстраивают базовые профили нормального поведения пользователей, устройств и процессов. Любое значимое отклонение — например, аномальный доступ к данным или подозрительные сетевые соединения из служебных учетных записей — становится поводом для расследования. Такой подход позволяет выявлять атаки на этапе перемещения по сети или эксфильтрации, даже если начальное внедрение осталось незамеченным.

Критически важной является интеграция предиктивных моделей на основе ИИ. Современные платформы (XDR) агрегируют телеметрию с конечных точек, сетевого оборудования и облачных сред. Алгоритмы машинного обучения анализируют эти данные, выявляя сложные корреляции и слабые сигналы, которые могут указывать на подготовку компьютерной атаки. Система способна связать, например, использование легитимного инструмента администрирования с последующими попытками отключить журналирование, предсказав развитие инцидента по известным тактикам [2].

Необходимым элементом становится автоматизация реагирования. При обнаружении угрозы автоматические сценарии могут изолировать зараженные узлы, блокировать вредоносные IP-адреса и отключать скомпрометированные учётные записи. Это сокращает время реагирования до минут, что критически важно для минимизации ущерба [3].

Организационной основой эффективной защиты выступает архитектура «недоверия по умолчанию». Каждый запрос на доступ должен проходить строгую проверку, а микросетевое сегментирование ограничивает возможности злоумышленника для перемещения внутри сети даже после первоначальной компрометации.

Таким образом, противостояние современным APT-угрозам требует комплексного подхода, объединяющего поведенческую аналитику, предиктивные модели ИИ, автоматизированное реагирование и принципы Zero Trust.

Будущее индустрии информационной безопасности: стратегии и технологии для отражения адаптивных угроз

Будущее противостояния APT-угрозам лежит в переходе от реактивных к проактивным и самообучающимся системам защиты. Против атак, использующих искусственный интеллект, традиционные методы реагирования становятся неэффективными, что требует фундаментального пересмотра стратегий безопасности.

Ключевым направлением станет развитие систем ИИ нового поколения, способных не только анализировать данные, но и предсказывать действия злоумышленников, моделируя их поведение на основе известных тактик. Это позволит перейти от пассивного реагирования к упреждающему противодействию. Технологии генеративно-состязательных сетей будут использоваться для создания реалистичных тренировочных данных, что улучшит и ускорит обучение алгоритмов без риска для реальных систем. Параллельно, важную роль сыграет глубокая консолидация и контекстуализация данных, где защитные платформы будущего будут агрегировать информацию из внутренних и внешних источников, включая актуальные базы угроз, создавая единую оперативную картину для оценки каждого инцидента в контексте глобальной киберобстановки.

Перспективной технологией станут конфиденциальные вычисления, позволяющие обрабатывать зашифрованные данные без их расшифровки. Это может кардинально улучшить совместный анализ угроз, поскольку организации смогут безопасно обмениваться информацией об атаках, не раскрывая конфиденциальные детали, что ускорит коллективное противодействие сложным APT-кампаниям [1]. На организационном уровне произойдет переход к полностью автоматизированным центрам безопасности, где роль человека сместится к стратегическому управлению и расследованию сложных случаев, в то время как ИИ-системы будут автономно оценивать риски, принимать решения и запускать контрмеры в реальном времени.

Таким образом, устойчивость к адаптивным APT-угрозам будет обеспечиваться симбиозом трех элементов: продвинутых автономных систем ИИ, глубоко интегрированной телеметрии и доверительного отраслевого сотрудничества.

Заключение

Эволюция APT-атак демонстрирует качественный сдвиг в ландшафте киберугроз. От сравнительно простых методов обфускации кода злоумышленники перешли к комплексному использованию искусственного интеллекта, что превратило целевые атаки в высокоадаптивные, скрытные и интеллектуальные операции. Способность вредоносных программ динамически изменяться, использовать социальную инженерию нового уровня и анализировать среду для уклонения от обнаружения создает беспрецедентные вызовы для традиционных систем безопасности.

Ответом на такие вызовы не может быть простое обновление сигнатур или ужесточение правил. Требуется стратегический пересмотр самой парадигмы защиты. Будущее кибербезопасности лежит в предиктивных и поведенческих моделях, где технологии искусственного интеллекта работают на стороне защитников. Интеграция расширенной аналитики поведения, автоматизации реагирования и архитектуры нулевого доверия формирует основу для создания устойчивых систем.

Ключ к успеху — в опережающем развитии. Защита должна не просто реагировать на известные угрозы, а предвосхищать методы будущих атак, обучаясь и адаптируясь с той же скоростью, что и противник. Это предполагает не только инвестиции в передовые технологии,

но и улучшение отраслевой кооперации, развитие кадрового потенциала и построение организационной культуры, в которой безопасность является непрерывным процессом, а не разовой задачей.

В конечном итоге, противостояние современным APT-угрозам — это непрерывная динамичная борьба, где технологическое превосходство должно подкрепляться стратегическим мышлением, глубоким пониманием тактик противника и готовностью к постоянной эволюции. Только комплексный и проактивный подход позволит организациям не просто выявлять атаки постфактум, а эффективно предотвращать их, обеспечивая надежную защиту критически важных активов в условиях постоянно меняющейся киберсреды.

Список литературы

1. Эволюция массовых атак и стратегия защиты // Positive Technologies [Электронный ресурс]. – 2025. – URL: https://www.ptsecurity.com/research/analytics/evolution-of-mass-attacks-and-defense-strategy/ (дата обращения: 12.12.2025).
2. APT-атака: что это такое и как их предотвратить // IT-Grad [Электронный ресурс]. – 2025. – URL: https://it-grad.kz/blog/bezopasnost/apt-ataka-chto-eto-takoe-i-kak-ikh-predotvratit?ysclid=mj4fj7i1ee402252345 (дата обращения: 12.12.2025).
3. APT-группировки и глобальная кибервойна — кто против кого, как и почему // SecurityLab.ru [Электронный ресурс]. – 2025. – URL: https://www.securitylab.ru/blog/personal/xiaomite-journal/356240.php?ysclid=mj4f9sijcm757052172 (дата обращения: 13.12.2025).
4. APT-атаки на российские компании в 2025 году: что рассказали на SOC Forum 2025 // Anti-Malware [Электронный ресурс]. – 2025. – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/APT-attacks-on-Russian-companies-in-2025?ysclid=mj4fbrr9j9862972518 (дата обращения: 13.12.2025).
5. APT и целевые атаки: признаки, этапы, детект и практический план реагирования // ИнфраТех [Электронный ресурс]. – 2025. – URL: https://blog.infra-tech.ru/apt-ataki/?ysclid=mj4fdfgdmi43426158 (дата обращения: 13.12.2025).

References

1. The Evolution of Mass Attacks and Defense Strategy // Positive Technologies [Electronic resource]. – 2025. – URL: https://www.ptsecurity.com/research/analytics/evolution-of-mass-attacks-and-defense-strategy/ (date of access: 12.12.2025).
2. APT Attack: What is it and how to prevent it // IT-Grad [Electronic resource]. – 2025. – URL: https://it-grad.kz/blog/bezopasnost/apt-ataka-chto-eto-takoe-i-kak-ikh-predotvratit?ysclid=mj4fj7i1ee402252345 (date of access: 12.12.2025).
3. APT groups and global cyberwarfare – who is fighting whom, how, and why // SecurityLab.ru [Electronic resource]. – 2025. – URL: https://www.securitylab.ru/blog/personal/xiaomite-journal/356240.php?ysclid=mj4f9sijcm757052172 (accessed: 13.12.2025).
4. APT attacks on Russian companies in 2025: what was revealed at SOC Forum 2025 // Anti-Malware [Electronic resource]. – 2025. – URL: https://www.anti-malware.ru/analytics/Threats_Analysis/APT-attacks-on-Russian-companies-in-2025?ysclid=mj4fbrr9j9862972518 (accessed: 13.12.2025).

5. APT and targeted attacks: signs, stages, detection and a practical response plan // InfraTech [Electronic resource]. – 2025. – URL: https://blog.infra-tech.ru/apt-ataki/?ysclid=mj4fdfgdmi43426158 (accessed: 13.12.2025)

Маркевич Д.В. Методика оценки систем безопасности микросервисов с учётом ложных срабатываний и концептуального дрейфа // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 139–151

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056:004.7:004.416:004.85.

МЕТОДИКА ОЦЕНКИ СИСТЕМ БЕЗОПАСНОСТИ МИКРОСЕРВИСОВ С УЧЁТОМ ЛОЖНЫХ СРАБАТЫВАНИЙ И КОНЦЕПТУАЛЬНОГО ДРЕЙФА

Маркевич Д.В.
ФГБОУ ВО «ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА I», Санкт-Петербург, Россия (190031, г.Санкт-Петербург, Московский просп., 11А), e-mail: dmarkevich811@mail.ru

Статья анализирует применение методов интеллектуального мониторинга для выявления инцидентов безопасности в микросервисной архитектуре, где распределенность компонентов и разнообразие протоколов взаимодействия (gRPC/REST, очереди сообщений, service mesh) формируют сложные профили нормального поведения и повышают вероятность «шумных» уведомлений. Рассматриваются классы средств обнаружения вторжений и предотвращения атак, а также переход от знаний-ориентированных правил к поведенческим моделям и алгоритмам машинного обучения, позволяющим учитывать многомерные телеметрические сигналы и контекст выполнения. Обсуждаются критерии качества детектирования, практическая значимость баланса false positives/false negatives для SOC-процессов и влияние ограничений по задержкам на выбор вычислительных схем. Существенное внимание уделено проблеме concept drift, проявляющейся при изменении API, конфигураций и нагрузочных режимов, и описываются стратегии поддержания работоспособности моделей: пакетное переобучение, online-обучение, ансамбли, перенос обучения и fine-tuning. Проанализированы угрозы надежности ML-компонентов, включая adversarial attacks и poisoning, а также методы повышения robustness в условиях целенаправленного воздействия. Отмечается роль человеко-машинного контура (human-in-the-loop), активного обучения и корреляции алертов для снижения alert fatigue и повышения интерпретируемости решений, включая подходы Explainable AI.

Ключевые слова: Микросервисы, SOC, обнаружение вторжений, устойчивость моделей, concept drift.

METHODOLOGY FOR EVALUATING MICROSERVICE SECURITY SYSTEMS BASED ON FALSE ALARMS AND CONCEPTUAL DRIFT

Markevich D.V.
EMPEROR ALEXANDER I ST. PETERSBURG STATE TRANSPORT UNIVERSITY, St. Petersburg, Russia (190031, St. Petersburg, Moskovsky Prospekt, 11A), e-mail: dmarkevich811@mail.ru

The article analyzes the use of intelligent monitoring methods to identify security incidents in a microservice architecture, where the distribution of components and a variety of interaction protocols (gRPC/REST, message queues, service mesh) form complex profiles of normal behavior and increase the likelihood of "noisy" notifications. Classes of intrusion detection and attack prevention tools are considered, as well as the transition from knowledge-based rules to behavioral models and machine learning algorithms that take into account multidimensional telemetry signals and the execution context. Detection quality criteria, the practical significance of the false positives/false negatives balance for SOC processes, and the impact of latency constraints on the choice of computing circuits are discussed. Significant attention is paid to the problem of concept drift, which manifests itself when changing APIs, configurations, and load modes, and describes strategies for maintaining model performance: batch retraining, online training, ensembles, learning transfer, and fine-tuning. Threats to the reliability of ML components, including adversarial attacks and poisoning, as well as methods for increasing robustness under targeted conditions, are analyzed. The role of the human-machine loop (human-in-the-loop), active learning, and alert correlation is noted to reduce alert fatigue and increase interpretability of solutions, including Explicable AI approaches.

Keywords: Microservices, SOC, intrusion detection, model resilience, concept drift.

Введение

Современная парадигма разработки программного обеспечения, характеризующаяся повсеместным переходом от монолитных архитектур к микросервисным, кардинально изменила ландшафт информационной безопасности, создав новые векторы угроз и значительно усложнив процессы мониторинга и защиты периметра, который в условиях распределенных систем фактически размывается и перестает существовать в классическом понимании. Микросервисная архитектура, обеспечивающая беспрецедентную гибкость, масштабируемость и скорость развертывания функционала, одновременно порождает сложную сеть межсервисного взаимодействия, где каждый отдельный компонент может стать точкой входа для злоумышленника или источником компрометации всей системы, что требует пересмотра традиционных подходов к обнаружению аномалий и вторжений. В условиях высокой динамики изменения трафика, обусловленной как легитимными обновлениями сервисов, так и вариативностью пользовательского поведения, статические правила безопасности [3] и сигнатурные методы демонстрируют критическую неэффективность, приводя к недопустимо высокому уровню ложных срабатываний, которые не только дезориентируют операторов центров мониторинга безопасности (SOC), но и создают условия для пропуска реальных целенаправленных атак, маскирующихся под легитимную активность в общем потоке "шума" предупреждений. Проблема усугубляется явлением концептуального дрейфа (concept drift), при котором статистические свойства целевой переменной, которую модель пытается предсказать, меняются с течением времени непредвиденным образом, что ведет к деградации качества работы предиктивных моделей безопасности, обученных на исторических данных, которые перестают отражать текущее состояние защищаемой среды.

Критический анализ существующих методыик оценки эффективности систем защиты показывает, что большинство из них фокусируется на моментальных метриках точности, игнорируя темпоральную динамику и адаптивность алгоритмов к изменяющимся условиям среды, что является фундаментальным недостатком при работе с микросервисами, где жизненный цикл контейнеров может исчисляться минутами, а паттерны взаимодействия меняются с каждым релизом. Внедрение механизмов машинного обучения для выявления аномалий представляется безальтернативным вектором развития, однако оно сопряжено с необходимостью решения проблем интерпретируемости решений, устойчивости к атакам на сами модели (adversarial attacks) и, что наиболее важно, управления жизненным циклом моделей в условиях непрерывного дрейфа данных [12]. Ложные срабатывания в таких системах не являются просто статистической погрешностью, а представляют собой значимый экономический и операционный фактор, истощающий ресурсы команд безопасности и снижающий доверие к автоматизированным системам защиты. Следовательно, разработка комплексной методики оценки, которая учитывала бы не только способность системы обнаруживать известные и неизвестные угрозы, но и ее устойчивость к дрейфу концепций, а также эффективность механизмов фильтрации ложных тревог, является актуальной научно-технической задачей, требующей глубокого теоретического осмысления и практической верификации. Отсутствие стандартизированных подходов к тестированию устойчивости алгоритмов безопасности к дрейфу данных в контексте микросервисной архитектуры создает вакуум в методологическом обеспечении, который данное исследование призвано заполнить [8].

Необходимость учета специфики микросервисного взаимодействия, включающего использование различных протоколов (gRPC, REST, message queues), динамическую оркестрацию и service mesh, накладывает дополнительные ограничения на применимость классических методов обнаружения аномалий, требуя разработки адаптивных механизмов, способных обучаться в режиме реального времени или с минимальной задержкой. Традиционные метрики, такие как точность (accuracy) или полнота (recall), взятые в изоляции, не способны дать адекватную оценку надежности системы в долгосрочной перспективе, поскольку высокая точность на статической выборке может быстро смениться полной неработоспособностью при изменении профиля нагрузки или логики работы сервиса. В этом контексте особое значение приобретает анализ природы концептуального дрейфа — будь то внезапный, постепенный или переодический сдвиг — и способность защитных механизмов классифицировать его не как атаку, а как легитимное изменение состояния системы [5], что требует внедрения интеллектуальных контуров обратной связи и контекстуального анализа. Таким образом, проблематика исследования лежит на стыке кибербезопасности, системного анализа и науки о данных, требуя интегрального подхода к формированию критериев оценки и методологии тестирования защищенности распределенных вычислительных сред.

Материалы и методы исследования

Методологическую основу данного исследования составляет системный подход к анализу безопасности распределенных информационных систем, базирующийся на теории сложных систем и методах интеллектуального анализа данных, что позволяет рассматривать микросервисную архитектуру не как совокупность разрозненных компонентов, а как единый организм с эмерджентными свойствами, где безопасность является интегральной характеристикой всей совокупности взаимодействий. В качестве теоретического базиса для классификации типов концептуального дрейфа и аномалий использовались таксономии, принятые в области машинного обучения и адаптивных систем [1], адаптированные с учетом специфики сетевого трафика и журналов событий микросервисов, что позволило выделить ключевые паттерны изменений, критически влияющие на эффективность детектирования угроз. Для сравнительного анализа эффективности различных подходов к обеспечению безопасности применялся метод синтетического моделирования атак и генерации трафика, имитирующего реальную нагрузку высоконагруженных систем электронной коммерции и финансовых платформ, что позволило воспроизвести сценарии "чистого" трафика, трафика с внедренными атаками и трафика с искусственно индуцированным дрейфом концепций различной природы. Особое внимание уделялось формализации понятийного аппарата, описывающего метрики устойчивости алгоритмов к изменениям среды, что потребовало синтеза подходов из области статистики, теории надежности и кибернетики.

В рамках исследования был проведен детальный обзор и сравнительный анализ существующих архитектурных паттернов построения систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS), адаптированных для облачных сред, с акцентом на их способность обрабатывать потоковые данные и адаптироваться к изменяющимся условиям без необходимости полной перестройки моделей. Использовались методы декомпозиции задач обнаружения аномалий на составляющие элементы: сбор метрик, предварительная обработка, извлечение признаков и принятие решений, что позволило выявить узкие места, ответственные за генерацию ложных срабатываний при возникновении дрейфа данных [15]. Для оценки механизмов управления ложными срабатываниями применялся метод экспертных

оценок в сочетании с анализом чувствительности алгоритмов к пороговым значениям классификации, что дало возможность сформулировать требования к адаптивным порогам, динамически изменяющимся в зависимости от текущего контекста работы системы. Анализ литературы и существующих практических реализаций позволил выделить основные стратегии переобучения моделей — от полного периодического переобучения до инкрементального обучения и ансамблевых методов, которые были подвергнуты критическому осмыслению с точки зрения их вычислительной сложности и применимости в условиях жестких ограничений на задержку обработки запросов (latency constraints).

Особое место в методологии исследования занимает анализ механизмов обратной связи и участия человека (human-in-the-loop) в процессе валидации инцидентов, поскольку в условиях высокой неопределенности и сложности атак полностью автоматизированные решения часто демонстрируют недостаточную гибкость. Были изучены подходы к активному обучению (active learning), где система самостоятельно выбирает наиболее информативные примеры для маркировки экспертом, тем самым ускоряя адаптацию к новым видам дрейфа и снижая нагрузку на операторов [7]. Для верификации предложенных теоретических положений использовался метод сравнительного анализа качественных характеристик различных классов алгоритмов обнаружения аномалий — статистических, основанных на обучении с учителем и без учителя, а также гибридных подходов. Исследование опирается на предположение, что эффективность системы безопасности в микросервисной среде определяется не столько статическими показателями качества обнаружения на фиксированном наборе данных, сколько скоростью восстановления целевых показателей качества после наступления события дрейфа и способностью минимизировать операционные потери, связанные с расследованием ложных инцидентов.

Результаты и обсуждение

Проблема оценки эффективности систем безопасности в динамических средах микросервисов выходит далеко за рамки простого подсчета корректно отраженных атак, поскольку сама природа "нормального" поведения системы является подвижной, зависящей от множества факторов, включая сезонность, маркетинговые активности, обновление функционала и изменение пользовательской базы. Статические модели угроз, эффективные в монолитных системах с редкими циклами обновлений, в условиях CI/CD пайплайнов, доставляющих изменения в продакшн несколько раз в день, становятся источником постоянных помех, генерируя поток предупреждений на легитимные изменения в структуре запросов или топологии сети [9]. Это приводит к феномену, известному как "усталость от тревог" (alert fatigue), когда реальные инциденты игнорируются на фоне сотен ложных, вызванных, например, изменением формата JSON в ответе одного из микросервисов. Следовательно, ключевым аспектом анализа становится способность системы различать вредоносные аномалии и аномалии, вызванные эволюцией системы, что требует глубокого понимания механизмов дрейфа данных и концепций.

Анализ механизмов безопасности требует четкого разграничения подходов к обнаружению аномалий, так как выбор базовой технологии определяет предельную эффективность системы в условиях неопределенности и способность адаптироваться к новым видам угроз без ручного вмешательства. Существующие методы можно условно разделить на классы в зависимости от наличия априорных знаний об атаках и способа построения эталонной модели поведения, причем каждый из классов обладает уникальным набором

характеристик в контексте устойчивости к дрейфу и склонности к ложным срабатываниям [2]. Важно понимать, что универсального алгоритма не существует, и выбор конкретного механизма всегда представляет собой компромисс между чувствительностью к атакам и толерантностью к изменениям среды, что диктует необходимость использования гибридных архитектур. Для систематизации существующих подходов и выявления их концептуальных ограничений был проведен сравнительный анализ, результаты которого представлены в таблице (Таблица 1).

Таблица 1 – Сравнительный анализ концептуальных подходов к обнаружению аномалий в микросервисах

Критерий сравнения	Сигнатурный подход (Knowledge-based)	Поведенческий подход (Behavior-based)	Гибридный адаптивный подход
Базовый принцип функционирования	Сопоставление паттернов трафика с базой известных сигнатур атак и правил	Формирование профиля нормального поведения и поиск отклонений от него	Комбинация сигнатур для известных угроз и ML-моделей для неизвестных с механизмом обратной связи
Реакция на концептуальный дрейф	Индифферентность (не реагирует на изменения легитимного профиля, если они не совпадают с сигнатурами)	Высокая чувствительность (интерпретирует дрейф как аномалию, вызывая ложные срабатывания)	Адаптивная (способность перестраивать профиль нормы при подтверждении легитимности изменений)
Уровень ложных срабатываний (False Positives)	Низкий (только при совпадении легитимного трафика с сигнатурой атаки)	Высокий (любое отклонение от исторической нормы считается подозрительным)	Умеренный (снижается за счет механизмов корреляции и контекстуального анализа)
Способность обнаруживать атаки "нулевого дня"	Отсутствует (требуется обновление базы сигнатур вендором или администратором)	Высокая (атака проявляется как статистическое отклонение от нормы)	Высокая (за счет поведенческого компонента и эвристического анализа)
Механизм обновления модели знаний	Ручное или автоматическое обновление базы статических правил	Периодическое переобучение модели на новых исторических данных	Непрерывное дообучение (Online Learning) или активное обучение с участием эксперта

Анализ представленных в таблице подходов демонстрирует, что классический сигнатурный метод, несмотря на низкий уровень ложных срабатываний, является тупиковым для защиты микросервисов от новых угроз, так как он реактивен по своей природе и не способен защитить от атак, использующих уязвимости логики приложения или "нулевого дня", тогда как поведенческий подход, будучи проактивным, страдает от

гиперчувствительности к любым изменениям среды. Главная проблема поведенческих систем заключается в сложности формализации границы между "аномалией-атакой" и "аномалией-новизной", что в условиях микросервисной архитектуры, где новизна является нормой, приводит к параличу системы мониторинга [11]. Гибридные адаптивные подходы представляются наиболее перспективными, так как они пытаются объединить детерминизм сигнатур с гибкостью машинного обучения, однако их реализация сопряжена с высокой технической сложностью построения контуров обратной связи. Важным аспектом является то, что эффективность гибридного подхода напрямую зависит от качества реализации механизма разрешения конфликтов между подсистемами и скорости адаптации к новым профилям нормальности.

Следующим шагом в понимании проблематики является глубокий анализ природы изменений, происходящих в данных, циркулирующих между микросервисами, поскольку не всякое изменение является дрейфом в классическом понимании машинного обучения, и не всякий дрейф одинаково опасен для целостности системы безопасности. Различение типов дрейфа позволяет выбирать соответствующие стратегии адаптации моделей: в одних случаях требуется немедленное полное переобучение, в других — достаточно коррекции весов или обновления пороговых значений, а в третьих — изменение вообще должно быть проигнорировано как временный шум [6]. Отсутствие дифференциации между типами изменений ведет к нерациональному использованию вычислительных ресурсов на постоянное переобучение моделей или, наоборот, к использованию устаревших моделей, пропускающих атаки, что делает критически важным классификацию видов концептуального дрейфа применительно к задачам информационной безопасности (таблица 2).

Рассмотрение классификации дрейфа позволяет сделать вывод, что единая монолитная модель безопасности неспособна эффективно справляться со всем спектром изменений, так как стратегии реакции на внезапный и постепенный дрейф являются взаимоисключающими: первый требует быстрой реакции и забывания старого опыта, второй — консервативного накопления нового знания при сохранении стабильности. Это наблюдение подтверждает необходимость перехода к ансамблевым методам и архитектурам, поддерживающим версионность моделей в привязке к версиям микросервисов, что на практике реализуется через интеграцию процессов обучения моделей безопасности (MLOps) в процессы доставки приложений (DevOps/DevSecOps). Игнорирование циклической природы многих процессов в микросервисах (бэкапы, пиковые нагрузки) является одной из основных причин ложных срабатываний в ночное время или выходные дни, что решается не переобучением, а контекстуализацией модели [4]. Осознание природы дрейфа позволяет перейти от реактивного "латания дыр" к предиктивному управлению состоянием системы защиты.

Таблица 2 – Классификация видов концептуального дрейфа и их влияние на системы безопасности

Тип концептуального дрейфа	Характеристика проявления в микросервисной среде	Влияние на прогностическую модель безопасности	Необходимая стратегия реакции системы
Внезапный дрейф (Sudden Drift)	Резкое изменение структуры трафика или логики приложения (например, развертывание новой версии сервиса, изменение API)	Мгновенная деградация метрик качества; старая модель становится полностью неактуальной	Детектирование точки изменения, сброс контекста и инициация процедуры экстренного переобучения или переключения на новую модель
Постепенный дрейф (Gradual Drift)	Плавное изменение характеристик (например, рост пользовательской базы, постепенное изменение профиля использования функций)	Медленное снижение уверенности классификатора; старые и новые паттерны сосуществуют некоторое время	Использование взвешенных окон (наблюдений), где новые данные имеют больший приоритет; инкрементальное дообучение
Возвратный (циклический) дрейф (Recurring Drift)	Повторяющиеся изменения паттернов, связанные с временными циклами (сезонность, время суток, регулярные регламентные работы)	Ложные срабатывания в моменты смены циклов, если модель не учитывает темпоральные признаки	Использование ансамбля моделей, переключаемых в зависимости от контекста времени или внешних триггеров
Инкрементальный дрейф (Incremental Drift)	Непрерывная эволюция признакового пространства, добавление новых типов запросов при сохранении старых	Постепенное размывание границ классов; устаревание признаков, которые ранее были дискриминантными	Динамический отбор признаков, непрерывное обучение с механизмом забывания старых данных

Ключевым фактором, определяющим применимость той или иной методики в реальных условиях эксплуатации, является механизм обработки ложных срабатываний, который должен не просто фильтровать шум, но и служить источником данных для совершенствования системы, превращая ошибки первого рода в обучающие примеры. В условиях, когда стоимость пропуска атаки (False Negative) несоизмеримо выше стоимости ложной тревоги, системы традиционно настраиваются на высокую чувствительность, что неизбежно приводит к перегрузке аналитиков, поэтому современные методики должны включать инструменты автоматической валидации и приоритизации инцидентов. Необходимо анализировать не только технические метрики моделей, но и организационно-технические механизмы, позволяющие снижать негативное влияние ложных срабатываний на бизнес-процессы и операционную эффективность [10]. Сравнение различных стратегий управления ложными

срабатываниями позволяет выявить их сильные и слабые стороны в контексте автономности и требуемых ресурсов (Таблица 3).

Таблица 3 – Стратегии минимизации и обработки ложных срабатываний (False Positives)

Стратегия	Механизм реализации	Преимущества	Недостатки и ограничения
Корреляция событий (Alert Correlation)	Объединение множества низкоуровневых алертов в один высокоуровневый инцидент на основе логических связей и времени	Существенное снижение информационного шума; повышение контекстной осведомленности	Сложность настройки правил корреляции; риск группировки атаки с легитимным шумом (маскировка)
Динамическое профилирование (Dynamic Profiling)	Автоматическая корректировка порогов срабатывания для каждого микросервиса индивидуально на основе истории его поведения	Высокая точность для стабильных сервисов; адаптивность к локальным особенностям	Инерционность при обучении; уязвимость к "отравлению" модели (poisoning attacks) на этапе профилирования
Активное обучение с участием эксперта (Active Learning)	Система запрашивает подтверждение у человека только для наиболее спорных случаев, используя ответ для дообучения	Быстрое улучшение качества модели в пограничных случаях; использование экспертных знаний	Зависимость от доступности и квалификации эксперта; невозможность полной автоматизации
Контекстуальная фильтрация (Context-aware Filtering)	Использование внешних данных (планы релизов, статус инфраструктуры) для подавления алертов во время известных изменений	Исключение срабатываний, вызванных легитимными работами; интеграция с процессами управления изменениями	Требует глубокой интеграции с инструментами CI/CD и оркестрации; риск пропуска атак, проведенных во время "окна обслуживания"

Анализ стратегий управления ложными срабатываниями показывает, что наиболее эффективным является подход, сочетающий технические алгоритмы корреляции с глубокой интеграцией в процессы управления ИТ-инфраструктурой, поскольку значительная часть "аномалий" в микросервисах является следствием штатных процедур (деплой, масштабирование, рестарт), информация о которых доступна в смежных системах. Изолированные системы безопасности, не имеющие доступа к контексту оркестратора (например, Kubernetes), обречены на генерацию ложных тревог при каждом изменении конфигурации подов или перестроении маршрутов в service mesh. Внедрение активного обучения создает петлю положительной обратной связи, где система становится умнее с каждым разобранным инцидентом, однако это требует изменения регламентов работы SOC и выделения ресурсов на постоянное взаимодействие с алгоритмами [13]. Таким образом,

проблема ложных срабатываний трансформируется из чисто алгоритмической задачи в задачу архитектурной интеграции и процессного управления.

Четвертым важным аспектом анализа является выбор стратегии обновления моделей безопасности, так как в условиях дрейфа концепций статичная модель — это уязвимая модель, а процесс обновления должен быть бесшовным и не создавать перерывов в защите. Существуют различные подходы к поддержке актуальности знаний системы обнаружения вторжений, варьирующиеся от полного пересоздания моделей до непрерывной микрокоррекции весов в реальном времени, каждый из которых накладывает свои требования на вычислительную инфраструктуру и архитектуру хранения данных [14]. Выбор стратегии зависит от баланса между необходимостью учитывать самые последние данные и риском катастрофического забывания (catastrophic forgetting), когда модель, адаптируясь к новому, теряет способность распознавать старые угрозы. Сравнительная характеристика механизмов адаптации позволяет определить оптимальные сценарии их применения (Таблица 4).

Таблица 4 – Сравнительный анализ механизмов адаптации и обновления моделей безопасности

Механизм адаптации	Описание процесса обновления	Требования к ресурсам	Устойчивость к манипуляциям (Robustness)
Пакетное переобучение (Batch Retraining)	Периодическое обучение новой модели с нуля на скользящем окне исторических данных	Высокие пиковые нагрузки; требует хранения больших архивов данных	Высокая (за счет валидации на отложенной выборке), но есть лаг между изменением среды и обновлением модели
Инкрементальное (Online) обучение	Обновление параметров модели с каждым новым поступающим образцом данных или мини-батчем	Равномерная низкая нагрузка; не требует хранения всей истории	Низкая; высокий риск моментального отравления модели вредоносными данными
Ансамблевое обучение (Ensemble Learning)	Использование набора моделей, обученных на разных временных интервалах, с голосованием	Высокие постоянные вычислительные затраты; сложность управления	Очень высокая; позволяет нивелировать ошибки отдельных моделей и сглаживать дрейф
Трансферное обучение (Transfer Learning)	Использование предобученной базовой модели с дообучением (fine-tuning) на специфике конкретного микросервиса	Средние затраты; ускоряет развертывание защиты для новых сервисов	Средняя; зависит от качества базовой модели и релевантности исходного домена

Интерпретация данных о механизмах адаптации подводит к выводу, что для критически важных микросервисов наиболее надежным решением является использование ансамблевых методов, которые позволяют демпфировать резкие колебания статистики и обеспечивают плавный переход при смене концепций, сохраняя знания о прошлых паттернах атак. Инкрементальное обучение, несмотря на свою привлекательность с точки зрения скорости реакции, представляет собой значительный вектор атаки, так как злоумышленник может

постепенно "приучить" модель к вредоносному поведению, осуществляя атаку методом "варки лягушки", что делает чистые online-методы рискованными без дополнительных механизмов валидации. Пакетное переобучение остается золотым стандартом для обеспечения стабильности, но его дискретность создает окна уязвимости, что вынуждает искать компромиссные архитектуры, сочетающие стабильные "медленные" модели с адаптивными "быстрыми" компонентами.

Обобщая полученные результаты анализа концептуальных подходов, типов дрейфа, стратегий управления ложными срабатываниями и механизмов обновления моделей, можно констатировать, что построение эффективной системы безопасности микросервисов невозможно в рамках одной изолированной парадигмы или технологии. Наблюдается четкая тенденция к усложнению архитектур защиты, которые эволюционируют от простых классификаторов к сложным экосистемам, включающим элементы обучения с подкреплением, экспертные системы и глубокую интеграцию с инфраструктурным слоем. Фактор изменчивости среды становится не помехой, а фундаментальным свойством, которое должно быть заложено в архитектуру системы безопасности на этапе проектирования. Адаптивность и контекстуальная осведомленность становятся более важными метриками качества, чем абстрактная точность на тестовых датасетах, что требует смены всей парадигмы оценки эффективности средств защиты информации в облачных средах. Успешность системы определяется ее способностью сопровождать микросервис на протяжении всего его жизненного цикла, трансформируясь вместе с ним и обеспечивая непрерывность защиты в условиях перманентной турбулентности данных.

Выводы

Проведенное исследование методик оценки систем безопасности микросервисов позволяет заключить, что традиционные статические подходы к обеспечению защиты информации исчерпали свой потенциал в условиях динамических распределенных сред, демонстрируя неспособность эффективно противостоять угрозам на фоне концептуального дрейфа и генерируя неприемлемый уровень ложных срабатываний. Разработанная концептуальная модель оценки подчеркивает необходимость перехода от бинарных метрик "пропуск/обнаружение" к комплексным показателям адаптивности, которые характеризуют скорость сходимости алгоритмов к новым нормам поведения системы и устойчивость к деградации качества при изменении статистических свойств трафика. Доказано, что ключевым элементом современной системы безопасности является не только сам алгоритм детектирования, но и механизм управления его жизненным циклом, включающий стратегии обнаружения дрейфа и автоматизированного переобучения, что позволяет поддерживать актуальность моделей без существенного вмешательства человека.

Научная значимость полученных результатов заключается в систематизации типов концептуального дрейфа применительно к специфике микросервисной архитектуры и обосновании дифференцированных стратегий реакции на каждый из выявленных типов, что позволяет минимизировать ресурсные затраты на адаптацию защитных механизмов. Сравнительный анализ технических приемов показал преимущество гибридных и ансамблевых архитектур, которые обеспечивают необходимый баланс между пластичностью (способностью к обучению) и стабильностью (сохранением знаний об угрозах), снижая риск катастрофического забывания и повышая робастность системы к состязательным атакам.

Особое внимание следует уделить интеграции процессов обеспечения безопасности с процессами DevOps, так как именно метаданные о развертывании и конфигурации сервисов являются ключом к контекстуальной фильтрации ложных срабатываний и корректной интерпретации аномалий.

В перспективе дальнейшее развитие методологии оценки должно быть направлено на создание стандартизированных наборов данных (бенчмарков), содержащих реалистичные сценарии дрейфа концепций в микросервисных средах, что позволит проводить более объективное сравнение различных алгоритмических решений. Также критически важным направлением является исследование применимости методов объяснимого искусственного интеллекта (Explainable AI) для интерпретации причин срабатывания адаптивных моделей, что необходимо для повышения доверия к автоматизированным системам принятия решений и ускорения расследования инцидентов. Таким образом, обеспечение безопасности микросервисов требует смены парадигмы от построения "непробиваемых стен" к созданию "иммунной системы", способной к самообучению, регенерации и адаптации к постоянно меняющемуся ландшафту угроз.

Список литературы

1. Каляев И.А., Мельник Э.В. Доверенные системы управления // Мехатроника, автоматизация, управление. 2021. Т. 22. № 5. С. 227-236.
2. Грушо А.А., Грушо Н.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е., Шоргин С.Я. О безопасной архитектуре вычислительной системы на основе микросервисов // Информатика и ее применения. 2022. Т. 16. № 4. С. 87-92.
3. Савельев А.С., Неретин Е.С., Дяченко С.А., Берсуцкая О.Д., Иванов А.С. Метод определения подхода отказобезопасности критического оборудования на этапе системного проектирования // Crede Experto: транспорт, общество, образование, язык. 2020. № 4. С. 32-45.
4. Ефимов А.О., Рогозин Е.А. Оценка уровня защищенности (безопасности функционирования) автоматизированных систем на основе их уязвимостей, формализованная при помощи теории систем массового обслуживания // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 2. С. 83-89.
5. Бесогонов В.В., Костылев А.Г. О необходимости разработки многофакторной методики оценки уровня безопасности полетов // Проблемы летной эксплуатации и безопасность полетов. 2021. № 15. С. 192-193.
6. Кожанков В.Н., Иванов И.И., Бондаренко Е.Ю., Нагих Т.С. Подход к обеспечению безопасности в системах с микросервисной архитектурой // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2021. № 1 (14). С. 211-214.
7. Ефимов А.О., Рогозин Е.А. Перспективные направления оценки уровня защищенности автоматизированных систем органов внутренних дел // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2023. № 9. С. 40-45.
8. Тельный А.В., Монахов М.Ю., Николаев А.В., Матвеева Е.А. Методика оценки защищенности человеко-машинного интерфейса для автоматизированного рабочего места

интегрированной системы безопасности // Современные наукоемкие технологии. 2025. № 1. С. 67-77.
9. Куклев Е.А. Применение модели "спящей катастрофы" при определении рисков возникновения аварийных ситуаций воздушных судов на этапах снижения // Вестник Санкт-Петербургского государственного университета гражданской авиации. 2024. № 4 (45). С. 26-33.
10. Ефимов А.О. Методика количественной оценки уровня защищенности автоматизированных систем с учетом их уязвимости // Охрана, безопасность, связь. 2024. № 9-3. С. 20-25.
11. Золотых В.И. Применение нормативно-эквивалентного метода при оценке обеспечения безопасности авиационной системы средствами ее подсистем // Воздушно-космические силы. Теория и практика. 2021. № 18. С. 46-54.
12. Бестемьянов П.Ф. Методы обеспечения безопасности аппаратных средств микропроцессорных систем управления движением поездов // Электротехника. 2020. № 9. С. 2-8.
13. Крахмальный И.О. Разработка модели прогнозирования кибератак // Академический исследовательский журнал. 2025. Т. 3. № 5. С. 180-184.
14. Золотых В.И. Оценка состояния безопасности полетов в авиационном формировании // Военная мысль. 2022. № 2. С. 59-66.
15. Вееводин В.А., Черняев В.С., Нуценок Ц.М., Виноградов И.В. Методика оценки защищенности автоматизированной системы управления критической информационной инфраструктуры от DDOS-атак на основе имитационного моделирования методом Монте-Карло // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 1. С. 62-74.

References

1. Kalyaev I.A., Melnik E.V. Trusted management systems // Mechatronics, automation, control. 2021. Vol. 22. No. 5. pp. 227-236.
2. Grusho A.A., Grusho N.A., Zabezhailo M.I., Smirnov D.V., Timonina E.E., Shorgin S.Ya. On the secure architecture of a computing system based on microservices // Informatics and its applications. 2022. Vol. 16. No. 4. pp. 87-92.
3. Savelyev A.S., Neretin E.S., Dyachenko S.A., Bersutskaya O.D., Ivanov A.S. A method for determining the approach of fault safety of critical equipment at the stage of system design // Crede Experto: transport, society, education, language. 2020. No. 4. pp. 32-45.
4. Efimov A.O., Rogozin E.A. Assessment of the level of security (operational safety) of automated systems based on their vulnerabilities, formalized using the theory of queuing systems // Bulletin of Dagestan State Technical University. Technical sciences. 2023. Vol. 50. No. 2. pp. 83-89.
5. Besogonov V.V., Kostylev A.G. On the need to develop a multifactorial methodology for assessing the level of flight safety // Problems of flight operation and flight safety. 2021. No. 15. pp. 192-193.
6. Kozhenkov V.N., Ivanov I.I., Bondarenko E.Yu., Nagikh T.S. An approach to ensuring safety in systems with microservice architecture // Information security is an urgent problem of our time. Improvement of educational technologies for training specialists in the field of information security. 2021. No. 1 (14). pp. 211-214.

7. Efimov A.O., Rogozin E.A. Promising areas for assessing the level of security of automated systems of law enforcement agencies // Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes. 2023. No. 9. pp. 40-45.
8. Telny A.V., Monakhov M.Yu., Nikolaev A.V., Matveeva E.A. Methodology for assessing the security of a human-machine interface for an automated workplace of an integrated security system // Modern science-intensive technologies. 2025. No. 1. pp. 67-77.
9. Kuklev E.A. Application of the "sleeping disaster" model in determining the risks of aircraft accidents at the stages of reduction // Bulletin of the St. Petersburg State University of Civil Aviation. 2024. No. 4 (45). pp. 26-33.
10. Efimov A.O. Methodology for quantifying the security level of automated systems, taking into account their vulnerability // Security, safety, communications. 2024. No. 9-3. pp. 20-25.
11. Zolotykh V.I. Application of the normative equivalent method in assessing the safety of an aviation system by means of its subsystems // Aerospace forces. Theory and practice. 2021. No. 18. pp. 46-54.
12. Bestemyanov P.F. Methods of ensuring the safety of hardware for microprocessor-based train control systems // Electrical Engineering. 2020. No. 9. pp. 2-8.
13. Krakhmalny I.O. Development of a model for predicting cyber attacks // Academic Research Journal. 2025. Vol. 3. No. 5. pp. 180-184.
14. Zolotykh V.I. Assessment of the state of flight safety in aviation education // Military thought. 2022. No. 2. pp. 59-66.
15. Veevodin V.A., Chernyaev V.S., Nutsenok Ts.M., Vinogradov I.V. Methodology for assessing the security of an automated critical information infrastructure management system against DDOS attacks based on Monte Carlo simulation // Bulletin of Dagestan State Technical University. Technical sciences. 2023. Vol. 50. No. 1. pp. 62-74

Дудин В.Д. Общеканальная система сигнализации объекта информатизации как элемент защиты информационно-телекоммуникационной сети // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с.152–156

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.53

ОБЩЕКАНАЛЬНАЯ СИСТЕМА СИГНАЛИЗАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ КАК ЭЛЕМЕНТ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Дудин В.Д.
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА», Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: slava_4944@mail.ru

В работе обоснована актуальность развития общеканальных систем сигнализации. Рассмотрены теоретические основы построения систем с общим каналом сигнализации, включающие архитектурные принципы, механизмы функционирования и особенности применения единого защищённого канала передачи сигналов. Представлена типовая модель, описывающая процессы сбора, обработки и доставки сигнальных сообщений. Проанализированы преимущества предлагаемого подхода по сравнению с традиционными. Показана роль общеканальных систем сигнализации как элемента комплексной защиты информационно-телекоммуникационных сетей и приведены направления дальнейшего совершенствования механизмов корреляции и обработки сигнального трафика.

Ключевые слова: информационная безопасность, объект информатизации, система сигнализации, общеканальная архитектура, мониторинг, несанкционированное воздействие, корреляция событий.

CHANNEL-WIDE ALARM SYSTEM FOR AN INFORMATION FACILITY AS AN ELEMENT OF INFORMATION AND TELECOMMUNICATION NETWORK PROTECTION

Dudin V.D.
SAINT PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROF. M.A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: slava_4944@mail.ru

This paper substantiates the relevance of developing common-channel signaling systems. It examines the theoretical foundations of building systems with a common signaling channel, including architectural principles, operational mechanisms, and the specifics of using a single secure signaling channel. A standard model describing the processes of collecting, processing, and delivering signaling messages is presented. The advantages of the proposed approach compared to traditional approaches are analyzed. The role of common-channel signaling systems as an element of comprehensive protection for information and telecommunications networks is demonstrated, and directions for further improvement of signaling traffic correlation and processing mechanisms are outlined.

Keywords: information security, information technology object, alarm system, common-channel architecture, monitoring, unauthorized impact, event correlation.

Введение

Информационно-телекоммуникационные сети являются основой функционирования большинства современных объектов информатизации, включая критически важные. Усложнение сетевой инфраструктуры, распределённый характер вычислительных ресурсов и рост количества взаимодействующих элементов способствуют формированию новых угроз, в

том числе внутренних, направленных на нарушение штатной работы и компрометацию информации.

Для своевременного выявления подобных воздействий необходимы системы, обеспечивающие оперативное получение сведений о событиях безопасности. Применяемые на практике раздельные каналы сигнализации создают избыточность инфраструктуры и приводят к разрыву информационных потоков, что затрудняет анализ событий и замедляет реагирование.

В этих условиях целесообразно применение общеканальной системы сигнализации (далее - ОСС), объединяющей передачу всех типов сигналов в едином защищённом коммуникационном контуре.

Целью работы является определение принципов построения ОСС и анализ её роли в обеспечении защищённости информационно-телекоммуникационных сетей от несанкционированных воздействий.

Понятие и назначение общеканальной системы сигнализации

Общеканальная система сигнализации представляет собой совокупность аппаратных и программных средств, обеспечивающих централизованный приём, обработку и передачу сообщений о событиях безопасности по защищённому каналу связи. [4, с. 30]

Основные функции ОСС включают сбор сведений о состоянии подсистем и компонентов сети, обеспечение своевременной и достоверной доставки сообщений, интеграцию данных различной природы — физических, сетевых и логических, а также автоматизированное оповещение операторов и подсистем реагирования.

ОСС является элементом комплексной системы защиты информации и выполняет задачи мониторинга, первичной аналитики и корреляции событий.

Концепция общего канала.

Общеканальный подход в контексте системы сигнализации предусматривает передачу всех сигналов по единому защищенному каналу, в отличие от традиционных решений, которые, в свою очередь, используют выделенные каналы для каждой из подсистем.

Предложенный подход упрощает инфраструктуру и исключает возможное дублирование информации, что повышает согласованность данных. Подход основан на идее переноса принципов общеканальной сигнализации из области телекоммуникаций на сферу обеспечения безопасности информационно-телекоммуникационных сетей общего назначения. [3, с. 115]

Архитектурные принципы построения ОСС

Предлагаемая архитектура общеканальной системы сигнализации включает в себя следующие положения:

- **единый коммуникационный контур**, передающий все типы сигналов по защищённому каналу;
- **модульное построение**, включающее блоки сбора сообщений, маршрутизации, обработки и визуализации;
- **централизованное управление**, позволяющее выполнять анализ и принятие решений на выделенном сервере сигнализации;

• **криптографическая защита коммуникаций**, предусматривающая защищённые протоколы передачи данных, взаимную аутентификацию и контроль целостности;

• **интеграция с существующими подсистемами** — вышеупомянутая модульность позволяет интегрировать другие средства защиты систем.

Подобная модель построения общеканальной системы сигнализации обеспечивает согласованность данных, повышение надежности защищаемой инфокоммуникационной системы и снижение времени реакции при инцидентах безопасности. ОСС становится центральным элементом инфраструктуры мониторинга, объединяющим разнородные подсистемы в единый защищённый канал обмена. [5, с. 20]

Роль общеканальной сигнализации при несанкционированных воздействиях

При нарушении штатной работы сети возможны угрозы, связанные с перехватом и модификацией управляющих сообщений, подменой сигналов, генерацией ложных уведомлений и блокировкой каналов передачи данных.

Общеканальная система сигнализации должна обеспечивать выявление аномалий в сигнальном трафике, резервирование маршрутов передачи данных, а также автоматическую корреляцию событий на различных уровнях информационно-телекоммуникационной сети, осуществляя защиту от подмены и перехвата сообщений. [4, с. 34] ОСС выступает как механизм раннего обнаружения нарушений, позволяющий свести к минимуму последствия несанкционированных воздействий на инфраструктуру.

Сравнение общеканального подхода с современно используемыми методами организации инфраструктуры сигнализации

Современные ИТ-инфраструктуры, как правило, используют раздельный подход к организации каналов сигнализации, при котором различные подсистемы безопасности функционируют изолированно. [1, с. 92]. Так, системы пожарной и охранной сигнализации, СКУД, IDS/IPS, средства мониторинга технического состояния оборудования и сетевые анализаторы передают данные по собственным каналам и применяют специализированные протоколы обмена. Этот подход исторически сформирован как следствие различий в функциональных требованиях, регламентах и стандартах отраслей.

Однако фрагментированная модель обладает рядом недостатков, особенно в условиях усложнения ИТКС и роста количества источников событий безопасности:

• **Отсутствие единой картины событий** — информация поступает в различные центры мониторинга и обрабатывается разными программными комплексами, что требует ручной корреляции и увеличивает время анализа инцидентов.

• **Разрозненность протоколов и инфраструктуры связи** приводит к избыточности каналов, усложняет сопровождение и повышает вероятность ошибок конфигурации.

• **Возможность обхода систем безопасности** за счёт того, что события на одном уровне (например, физическом) могут не учитываться подсистемами, работающими на логическом или сетевом уровнях.

• **Снижение оперативности реагирования** при одновременном возникновении событий в нескольких подсистемах, что характерно для мультивекторных атак.

Общеканальный подход, реализуемый в ОСС, принципиально отличается от традиционных архитектур.

Во-первых, описанный подход обеспечивает консолидацию всех потоков событий в едином защищённом канале, позволяя синхронно доставлять сообщения от различных подсистем, что упрощает инфраструктуру за счёт отказа от множества потоков сигнальных сообщений.

Во-вторых, такая модель позволяет реализовать более глубокую корреляцию физических, сетевых и логических событий, повышая качество аналитики и точность выявления источников угроз.

В-третьих, сокращается время реакции за счёт исключения промежуточных этапов обработки и передачи данных.

Дополнительным преимуществом является повышение уровня защищённости, поскольку единый коммуникационный канал проще контролировать и защищать, чем разнородный набор распределённых линий связи.

Заключение

Общеканальная система сигнализации выступает ключевым элементом архитектуры защиты информационно-телекоммуникационных сетей. В работе обоснованы принципы построения ОСС, разработана теоретическая модель её функционирования, а также выделены преимущества общеканального подхода по сравнению с традиционными решениями на основе раздельных каналов сигнализации. Перспективными направлениями дальнейших исследований являются создание математических моделей корреляции сигналов и оптимизация параметров передачи данных в распределённых защищённых сетях..

Список литературы

1. Бирих Э.В., Виткова Л.А., Левин М.В., Чмутов М.В. Развитие стандартов и руководств в сфере облачных технологий // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 26. URL: https://www.sut.ru/doci/nauka/6apino/programm2017apino.pdf
2. Ворона В.А. Комплексные (интегрированные) системы обеспечения безопасности / В.А. Ворона В.А., Тихонов В.А. // М:Горячая Линия–Телеком. 2013. С. 5-121. URL: https://www.techbook.ru/book.php?id_book=569
3. Езерская А. Б. Автоматизированная интегрированная система управления комплексной безопасностью научного центра // Научный альманах. 2017. №9-1(35). С. 34-35. URL: https://elib.pnzgu.ru/files/eb/TfB1FuoCi2G5.pdf
4. Махмутова Н.Ф., Бирих Э.В., Сахаров Д.В., Кривец А.С., Дегтярев М.А. Исследование способов повышения безопасности корпоративных сетей // Вестник Дагестанского гос. техн. ун-та. — 2024;51(3): `С. 110–116. URL: https://doi.org/10.21822/2073-6185-2024-51-3-110-116
5. Рыжова В.А. Проектирование и исследование комплексных систем безопасности // С: НИУ ИТМО. 2013. С. 8–149. URL: https://books.ifmo.ru/book/837/proektirovanie_i_issledovanie_kompleksnyh_sistem_bezopasnosti.htm.

References

1. Birikh E.V., Vitkova L.A., Levin M.V., Chmutov M.V. Development of standards and guidelines in the field of cloud technologies // In the collection: Actual problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes. Edited by S.V. Bachevsky. 2017. P. 26. URL: https://www.sut.ru/doci/nauka/6apino/programm2017apino.pdf
2. Vorona V.A. Comprehensive (integrated) security systems / V.A. Vorona V.A., Tikhonov V.A. // M: Goryachaya Liniya-Telecom. 2013. P. 5-121. URL: https://www.techbook.ru/book.php?id_book=569
3. Ezerskaya A. B. Automated integrated management system for complex security of a scientific center // Scientific Almanac. 2017. No. 9-1 (35). P. 34-35. URL: https://elib.pnzgu.ru/files/eb/TfB1FuoCi2G5.pdf
4. Makhmutova N. F., Birikh E. V., Sakharov D. V., Krivets A. S., Degtyarev M. A. Study of ways to improve the security of corporate networks // Bulletin of the Dagestan State Technical University. - 2024; 51 (3): `P. URL: https://doi.org/10.21822/2073-6185-2024-51-3-110-116
5. Ryzhova V.A. Design and Research of Integrated Security Systems // NRU ITMO. 2013. pp. 8–149. URL: https://books.ifmo.ru/book/837/proektirovanie_i_issledovanie_kompleksnyh_sistem_bezopasnosti.htm.

Погорова М.А., Фаргиева З.С. (научный руководитель) Методические и практические рекомендации к использованию ИИ в образовании // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 157–162

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.42

МЕТОДИЧЕСКИЕ И ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ К ИСПОЛЬЗОВАНИЮ ИИ В ОБРАЗОВАНИИ

[1]Погорова М.А., Фаргиева З.С. (научный руководитель)
ФГБОУ ВО «ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Магас, Россия (386001, Республика Ингушетия, г.Магас, просп. Идриса Зязикова, 7), e-mail: 1 marem.pogorova05@mail.ru

В статье рассматриваются современные подходы к внедрению искусственного интеллекта в образовательную практику. На основе анализа передовых российских и зарубежных исследований выделены ключевые методические принципы, способствующие успешной интеграции ИИ-инструментов в учебный процесс. Особое внимание уделено обсуждению этических аспектов, ролей преподавателя и обучающегося в новой цифровой образовательной среде, а также изменениям в педагогических стратегиях. Статья обосновывает необходимость формирования цифровой грамотности у всех участников образовательного процесса, предлагая практические рекомендации по созданию адаптивных учебных траекторий, использованию интеллектуальных платформ и систем автоматической оценки знаний. Материал статьи иллюстрируется примерами успешных кейсов и содержит обсуждение возникающих рисков и способов их минимизации. В заключении подчеркивается значимость развивающихся компетенций как у педагогов, так и у обучающихся для эффективного и этичного использования ИИ в образовании.

Ключевые слова: искусственный интеллект, цифровая грамотность, образовательные технологии, этика, педагогика, адаптивное обучение, автоматизация, образовательная среда.

METHODOLIGICAL AND PRACTICAL RECOMMEDATIONS FOR THE USE OF AI IN EDUCATION

[1]Pogorova M.A., Fargieva Z.S. (supervisor)
INGUSH STATE UNIVERSITY, Magas, Russia (386001, Republic of Ingushetia, Magas, Idris Zyazikov Avenue, 7), e-mail: [1]marem.pogorova05@mail.ru

This article examines contemporary approaches to the integration of artificial intelligence (AI) in educational practice. Based on the analysis of leading Russian and international research, key methodological principles that contribute to the successful incorporation of AI tools into the learning process are identified. Special attention is paid to ethical issues, the evolving roles of teachers and students within the new digital learning environment, and shifts in pedagogical strategies. The article substantiates the necessity of digital literacy formation among all educational participants and provides practical recommendations for creating adaptive educational pathways, utilizing intelligent learning platforms, and applying automated knowledge assessment systems. The material is illustrated by successful case studies and discusses potential risks and strategies for their mitigation. The conclusion emphasizes the critical role of emerging competencies for both educators and learners to achieve effective and ethical AI application in education.

Keywords: artificial intelligence, digital literacy, educational technologies, ethics, pedagogy, adaptive learning, automation, educational environment.

Введение

Резкое развитие технологий искусственного интеллекта (ИИ) в последние годы неизбежно влияет на образование. Ведущие мировые университеты и школы, а также

инновационные образовательные платформы всё чаще обращаются к ИИ-инструментам, способным коренным образом менять традиционные педагогические практики [1, с. 5–7]. Однако наряду с прекрасными возможностями, ИИ приносит новые вызовы и риски, требующие не только технологической грамотности, но и качественного пересмотра методических оснований образовательного процесса. Возникает задача выработки комплексных рекомендаций, позволяющих системно и безопасно внедрять ИИ в учебное пространство.

Цель исследования

Цель настоящей статьи — обобщение теоретических и эмпирических данных современных работ и формулирование методических и практических рекомендаций по использованию ИИ в образовательной практике, учитывающих российский и международный опыт.

Материал и методы исследования

Материал исследования включил научные публикации по педагогике, психологии образования и информатике [2, p. 116–130; 3, с. 40–51], а также аналитические отчёты ведущих образовательных центров (Harvard Graduate School of Education, Институт образования НИУ ВШЭ) и результаты экспертных опросов среди педагогов [4, p. 89–101]. Применён комплексный метод: сравнительный анализ, эмпирическое изучение кейсов внедрения ИИ, структурно-содержательный и этический анализ. Особое место занимает синтез данных практических экспериментов и апробации ИИ-систем (рисунки 1-3).

Обсуждение результатов

Методические принципы внедрения ИИ в образовательную среду

Современное образование переходит от формальной передачи знаний к формированию компетенций, где ИИ может выступать не только как инструмент автоматизации, но и как полноценный участник образовательного взаимодействия. Включение ИИ-технологий диктует новые подходы к проектированию образовательных программ: обучение становится нелинейным, ориентированным на индивидуальные учебные траектории [2, p. 118–120]. Методологически эффективны такие принципы, как гибкость, адаптация, цифровая этика и технологическая прозрачность [3, с. 45–47].

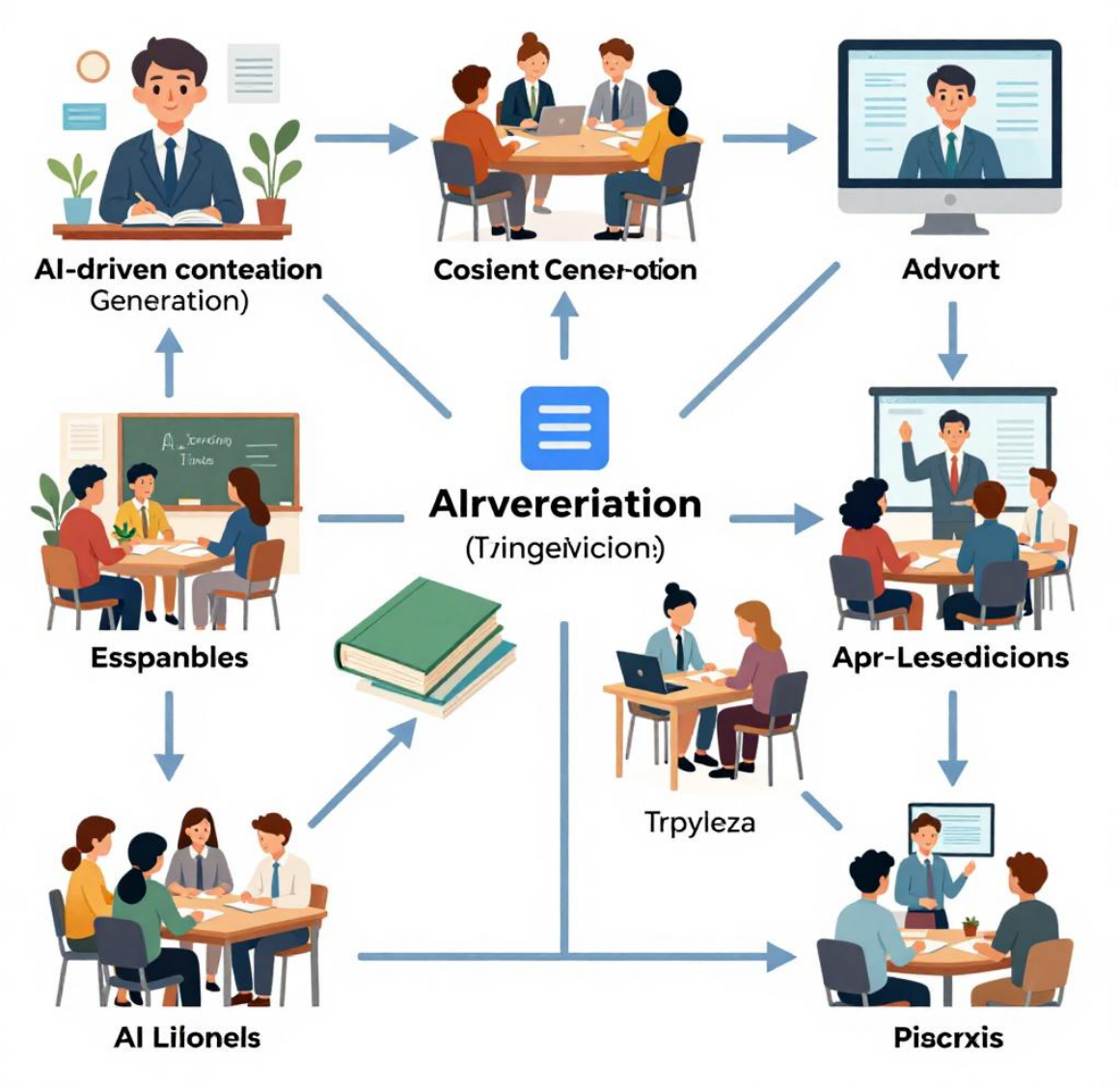

Рисунок 1 – Схема интеграции ИИ-инструментов в традиционный учебный процесс

Практические аспекты использования ИИ в обучении

ИИ может выполнять функции рекомендательных систем, автоматической проверки, интеллектуального поиска и диагностики дефицита знаний [5, p. 75–86]. На практике результативность связана с правильной постановкой целей: использование ИИ для создания сценариев адаптивного обучения, формирования персонализированных рекомендаций и автоматизации повторяемых рутинных операций (проверка тестов, генерация вариантов заданий) [3, с. 48–49].

Однако успешная апробация подобных систем требует постоянного педагогического контроля и корректировки “чёрного ящика” ИИ (рисунок 2).

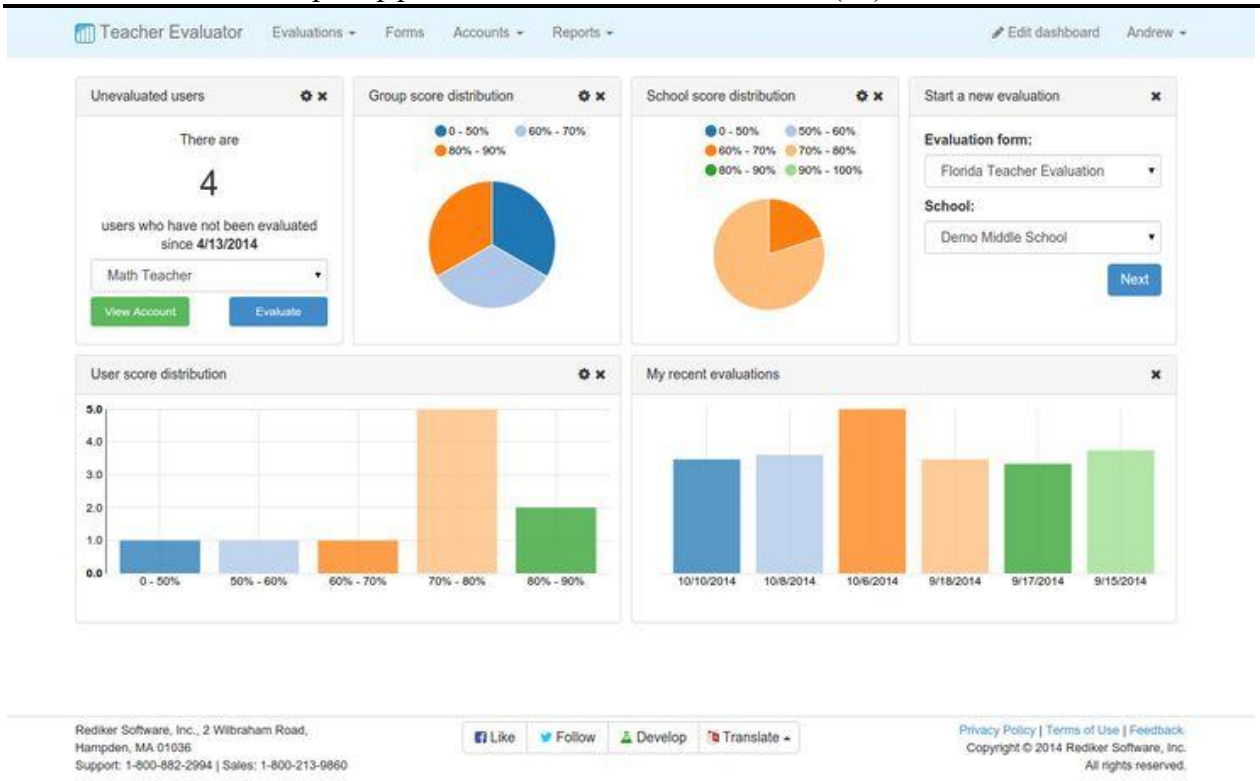

Рисунок 2 – Пример панели учителя по мониторингу работы ИИ-системы

Кроме того, ИИ открывает возможности для новых видов диагностики и прогнозирования образовательных результатов [6, с. 274–277]. Применение интеллектуального анализа больших данных позволяет выявлять скрытые сложности усвоения материала и индивидуальные потребности обучающихся, что ранее было недоступно [7, p. 43–44].

Этические вызовы и педагогические роли

Важнейшим открытым вопросом остается этика применения ИИ в образовании [8, с. 16–18]. Речь идет о необходимости соблюдения баланса между автоматизацией и уважением к личности обучающегося. Не менее значим контроль алгоритмов принятия решений, прозрачность механизмов оценивания, а также защита персональных данных. Роль учителя претерпевает трансформацию: педагог становится фасилитатором, аналитиком и наставником, координирующим работу гибридных (человек–ИИ) команд [1, с. 12–14].

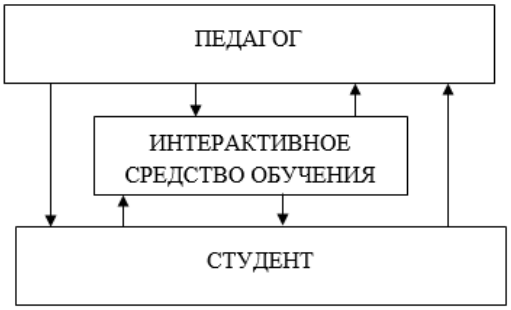

Рисунок 3 – Этический контур взаимодействия в ИИ-ориентированной образовательной системе

Актуальные проблемы и риски, пути минимизации

Одним из наиболее серьёзных рисков является низкая цифровая грамотность части педагогов и студентов, что может приводить к некорректному использованию даже лучших ИИ-сервисов [9, p. 322–324]. Не менее опасны “алгоритмические предвзятости” и слепое доверие рекомендациям цифровых систем. Практика показывает, что успешное внедрение ИИ неизбежно сопровождается многоуровневой подготовкой, проектированием курсов по цифровой компетентности и вовлечением студентов в экспертизу/оценку работы ИИ [10, с. 89–93].

Выводы

Обобщая результаты, можно отметить, что системное и ответственное использование ИИ в образовании требует осознанного подхода, инвестиции в цифровую грамотность и переосмысления педагогических функций. Практическая значимость разработанных рекомендаций заключается в их применимости не только для экспертов в области образования, но и для широкой аудитории преподавателей, заинтересованных в повышении эффективности и качества учебного процесса в условиях цифровой трансформации. Значимость данных находок заключается в формировании новых базовых компетенций XXI века и поиске оптимального баланса между человекоцентрированным и цифровым подходами.

Литература

1. Кузьмина О.В. Искусственный интеллект в системе образования: вызовы и возможности // Педагогика. — 2022. — №8. — С. 5–18.
2. Selwyn N. Should robots replace teachers? AI and the future of education. — Cambridge: Polity Press, 2019. — 207 p. — P. 116–130.
3. Семенова Т.В., Дмитриева С.Г. Методические аспекты внедрения цифровых технологий в школу // Информатика и образование. — 2023. — №3. — С. 40–51.
4. Greenhow C., Lewin C. Online social networks and AI tools: New opportunities for teaching and student learning. // British Journal of Educational Technology. — 2021. — Vol. 52, no. 1. — P. 89–101.
5. Woolf B.P. Building Intelligent Interactive Tutors: Student-Centered Strategies for Revolutionizing E-Learning. — Burlington: Morgan Kaufmann, 2009. — 405 p. — P. 75–86.
6. Иванов Д.А. Диагностика цифровых компетенций студентов с помощью ИИ-сервисов // Вопросы образования. — 2023. — №4. — С. 271–279.
7. Bainbridge W.S., Roco M.C. Handbook of Science and Technology Convergence. — Cham: Springer, 2016. — 540 p. — P. 43–44.
8. Зинченко В.П., Королёв С.А. Этические проблемы цифровизации образования // Вестник РАН. — 2020. — Т. 90, №1. — С. 13–21.
9. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education. — Boston: Center for Curriculum Redesign, 2019. — 362 p. — P. 321–324.
10. Волкова И.В. Практика формирования цифровой грамотности педагогов // Современное образование. — 2022. — №11. — С. 87–93.

References

1. Kuzmina, O.V. “Artificial Intelligence in the Education System: Challenges and Opportunities” // Pedagogy. — 2022. — No. 8. — pp. 5–18.
2. Selwyn, N. “Should Robots Replace Teachers? AI and the Future of Education” // Cambridge: Polity Press, 2019. — 207 p. — pp. 116–130.
3. Semenova, T.V., Dmitrieva, S.G. “Methodological Aspects of Implementing Digital Technologies in School” // Computer Science and Education. — 2023. — No. 3. — pp. 40–51.
4. Greenhow, C., Lewin, C. “Online Social Networks and AI Tools: New Opportunities for Teaching and Student Learning” // British Journal of Educational Technology. — 2021. — Vol. 52, no. 1. — pp. 89–101.
5. Woolf B.P. Building Intelligent Interactive Tutors: Student-Centered Strategies for Revolutionizing E-Learning. — Burlington: Morgan Kaufmann, 2009. — 405 p. — P. 75–86.
6. Ivanov D.A. Diagnostics of Students’ Digital Competencies Using AI Services // Voprosy obrazovaniya. — 2023. — No. 4. — P. 271–279.
7. Bainbridge W.S., Roco M.C. Handbook of Science and Technology Convergence. — Cham: Springer, 2016. — 540 p. — P. 43–44.
8. Zinchenko V.P., Korolev S.A. Ethical Issues in the Digitalization of Education // Vestnik RAS. — 2020. — Vol. 90, No. 1. — P. 13–21.
9. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education. — Boston: Center for Curriculum Redesign, 2019. — 362 p. — P. 321–324.
10. Volkova I.V. Practice of Developing Teachers’ Digital Literacy // Modern Education. — 2022. — No. 11. — P. 87–93.

Нестерова В.А., Дробкова О.С. Обзор использования технологий искусственного интеллекта в бизнес-аналитике: навигатор BI как кейс ИИ-трансформации // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 163–170

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

ОБЗОР ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БИЗНЕС-АНАЛИТИКЕ: НАВИГАТОР BI КАК КЕЙС ИИ-ТРАНСФОРМАЦИИ

[1]Нестерова В.А., [2]Дробкова О.С.
ФГАОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия (105005, г.Москва, 2-я Бауманская ул., 7), e-mail: [1]nest@valleria.ru, [2] drobkova.os@bmstu.ru

Статья посвящена обзору бизнес-аналитики под влиянием искусственного интеллекта (ИИ), с акцентом на интеграцию ИИ-решений в современные аналитические платформы. Рассматриваются ключевые преимущества ИИ-аналитики, включая обработку естественного языка (NLP), предиктивное моделирование и автоматизацию процессов. Рассмотрен кейс внедрения ИИ-ассистента в Навигатор BI, демонстрирующему функционал семантического поиска, голосового ввода и генерации интерактивных отчетов.

Ключевые слова: Бизнес-Аналитика, BI, искусственный интеллект, обработка естественного языка (NLP), предиктивная аналитика, автоматизация, Навигатор BI, большая языковая модель (LLM), демократизация данных, дэшборд.

A REVIEW OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN BUSINESS ANALYTICS: BI NAVIGATOR AS A CASE STUDY OF AI TRANSFORMATION

[1]Nesterova V.A., [2]Drobkova O.S.
"BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY)", Moscow, Russia (105005, Moscow, 2nd Baumanskaya, 7), e-mail: [1]nest@valleria.ru, [2] drobkova.os@bmstu.ru

The article is devoted to the transformation of business intelligence (BI) under the influence of artificial intelligence (AI), with an emphasis on the integration of AI solutions into modern analytical platforms. The key advantages of AI analytics, including natural language processing (NLP), predictive modeling, and process automation, are discussed. The case of implementing an I-assistant in a BI Navigator is considered, demonstrating the functionality of semantic search, voice input and generation of interactive reports..

Keywords: Business analytics, BI, artificial intelligence, natural language processing (NLP), predictive analytics, automation, BI Navigator, large language model (LLM), data democratization, dashboard.

Целью работы является обосновать необходимость интеграции искусственного интеллекта (ИИ) в BI-платформы и продемонстрировать, как такие решения повышают эффективность, упрощают взаимодействие пользователя с платформой и расширяют функционал.

Бизнес-аналитика (BI – Business Intelligence) направлена на преобразование больших объемов данных в идеи для принятия обоснованных решений [1]. Типичный рабочий процесс BI включает в себя несколько этапов, таких как подготовка, анализ и визуализация данных. Это требует совместной работы инженеров, ученых и аналитиков, работающих с данными с использованием различных специализированных инструментов (например, Visual Studio Code,

Power BI, Tableau), что может быть очень утомительным и отнимать много времени [2]. Поэтому современным организациям требуются передовые методы для автоматизации и оптимизации этого рабочего процесса.

Аналитика на основе искусственного интеллекта подразумевает интеграцию технологий искусственного интеллекта в процессы бизнес-аналитики, что позволяет предприятиям анализировать огромные и сложные наборы данных, вникать в их закономерности и вырабатывать действия при ограниченном участии человека.

Анализ данных на основе ИИ открывает новые перспективы в развитии аналитики, существенно отличаясь от традиционных подходов, ограниченных ручным сбором статичных данных и составлением отчетов. Аналитика, управляемая ИИ, означает автоматизацию процессов обработки данных, которые позволяют компаниям получать в реальном времени как прогнозные, так и предписывающие решения [3].

Актуальные разработки в области автономных агентов, функционирующих на базе больших языковых моделей (LLM – Large Language Model) [4] предлагают потенциал для рационализации рабочего процесса BI. Получая инструкции на естественном языке (NL – Natural Language), агенты на основе LLM могут выполнять планирование задач, рассуждения и действия в исполняемых средах. Это решение может значительно снизить сложность многих BI-задач, таких как генерация кода [5], перевод текста в визуализацию [6] и автоматизированное обнаружение инсайтов [7].

Например, интеграция искусственного интеллекта в BI-систему Power BI расширила возможности последнего [8]. Использование искусственного интеллекта в Power BI оптимизирует процесс обработки данных, усиливает предиктивные функции платформы и делает углублённую аналитику доступной для пользователей без специализированных навыков. Это объединяет бизнес-аналитику и искусственный интеллект, отвечая на растущую потребность в инструментах, которые могут визуализировать данные и в то же время предлагать интеллектуальные рекомендации по принятию решений [9].

Появление аналитики, основанной на искусственном интеллекте, стало важным поворотным моментом в революции BI. Появление машинного обучения, обработки естественного языка (NLP) и автоматизации привело к переводу акцента с описательной на предиктивную и предписывающую аналитику [3]. Данные инструменты обеспечивают агрегацию больших объемов данных, обработку неструктурированной информации и генерацию аналитических выводов в режиме реального времени для последующей визуализации и оперативного принятия решений.

Сила таких технологий, как ML и NLP, когда они начинают управляться искусственным интеллектом, превращает статичные приборные панели в динамичные и интерактивные системы, поддерживающие принятие решений. Например, в Power BI возможности Smart Narratives и Key Influencers, основанные на искусственном интеллекте, позволяют задавать запросы на естественном языке, предоставляяи в считанные секунды получать полезную информацию. Не только сделать BI удобным для пользователей, но и в большей степени демократизировать его – это BI на основе искусственного интеллекта.

Принятие решений на основе ИИ приобретает важное значение, поскольку позволяет преодолеть разрыв между сложными данными и человеческим познанием.

Навигатор BI - российская платформа бизнес-аналитики и визуализации данных. Навигатор помогает быстрее принимать оптимальные решения, оперативно визуализировать

показатели деятельности на интерактивных дэшбордах [10]. Платформа разработана компанией Сбер и ориентирована на топ-менеджмент, руководителей различных уровней и аналитиков. Внедрение платформы осуществляется как в Группе Сбер, так и среди крупных корпоративных клиентов и организаций государственного сектора. "Навигатор" отмечен рядом международных наград, включая премии The Banker, Global Finance и EFMA. Важным конкурентным преимуществом платформы является запатентованный графический интерфейс. [11] Навигатор BI является отечественным решением, функционально замещающим зарубежные системы бизнес-аналитики, такие как QlikSense, Tableau и Power BI, также программный продукт включен в Реестр отечественного программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Платформа "Навигатор" реализована как омниканальный продукт, обеспечивающий кросс-платформенную совместимость (веб-интерфейс, мобильные приложения для iOS и Android), что позволяет пользователям получать актуальные данные в любом месте и с любого устройства. Ключевым преимуществом системы является BI-аналитика в режиме реального времени, обеспечивающая мгновенную обработку и визуализацию данных. Платформа демонстрирует высокую производительность, обрабатывая сотни миллионов транзакций ежедневно, что делает ее применимой в высоконагруженных корпоративных средах. Кроме того, система предоставляет функционал для онлайн-мониторинга эффективности маркетинговых и управленческих кампаний, позволяя оперативно корректировать стратегии на основе актуальных метрик [12].

Интеграция искусственного интеллекта в платформу Навигатор BI трансформирует традиционные возможности визуализации данных в полноценную интеллектуальную систему поддержки принятия решений. Реализованный ИИ-ассистент предлагает следующие ключевые функции:

1. Запрос на естественном языке позволяет формулировать аналитические запросы на разговорном языке с мгновенным получением структурированных результатов, исключая необходимость написания сложных формализованных запросов.

2. Улучшенный семантический поиск - благодаря внедрению векторного представления данных и обработке синонимии существенно повышена точность поиска дашбордов с учётом применённых фильтров.

3. Голосовой ввод вопросов и вывод ответов - реализована голосовая коммуникация на базе технологии Salute speech, обеспечивающая голосовой ввод запросов и озвучивание результатов анализа [13].

Таким образом, функции искусственного интеллекта в Навигатор BI включают обработку данных на естественном языке, которая позволяет пользователям запрашивать наборы данных, используя разговорный язык.

Пользователю достаточно ввести текстовый запрос (например, "Финансы") в диалоговое окно помощника, после чего система автоматически предлагает релевантные дашборды из библиотеки Навигатора. Важно отметить, что переход к нужной информационной панели возможен непосредственно из интерфейса диалога, что значительно сокращает время доступа к данным. При получении ответа от ИИ-помощника система предлагает интеллектуальный превью-виджет для настроенных дашбордов. Пользователь может непосредственно из диалогового окна добавить соответствующий виджет на свой обзорный экран, что значительно ускоряет процесс работы с аналитическими данными.

Для повышения точности выборки система поддерживает расширенный синтаксис запросов. Пользователь может уточнять параметры поиска, добавляя в запрос:

– временные периоды (месяц, квартал, текущая дата);
– бизнес-сегменты;
– каналы взаимодействия и др.

На рисунке 1 представлен пример запроса ИИ-помощнику.

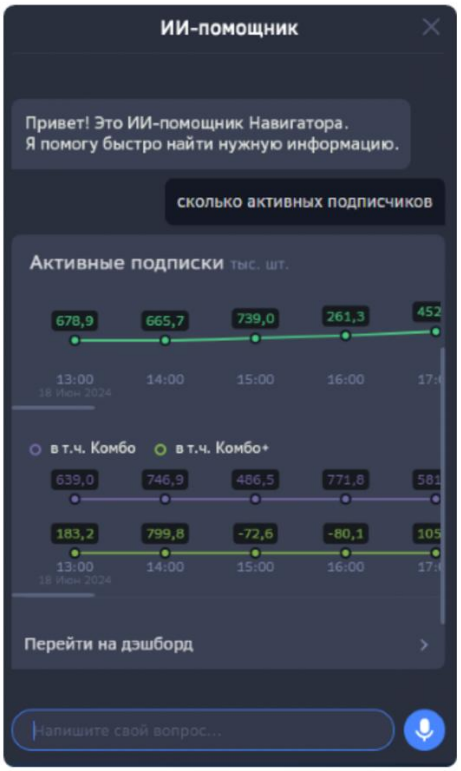

Рисунок 1 – Запрос на естественном языке ИИ-помощнику на платформе

Например, аналитик или менеджер, работающий с дэшбордом, сталкивается с необходимостью получить данные в конкретном разрезе, но испытывает сложности с применением соответствующих фильтров или навигацией по интерфейсу. Вместо ручного конфигурирования параметров пользователь может сформулировать запрос на естественном языке и обратиться с ним к ИИ-помощнику, например:

«Мне необходимо получить информацию по показателю EBIDTA по компании X за последний закрытый квартал текущего года». ИИ-помощник выполняет семантический разбор запроса, идентификацию целевого показателя (EBIDTA), определяет временной период и сопоставляет с доступными источниками данных. На выходе система либо перенаправляет пользователя на соответствующий дэшборд с предустановленными фильтрами, либо выдает интерактивный ответ с виджетом по запрошенным метрикам.

Такая демократизация анализа данных устраняет разрыв между техническими и нетехническими пользователями, способствуя формированию культуры принятия решений на основе данных на всех уровнях организации [14].

Также система способна анализировать содержимое документов и предоставлять точные ответы на пользовательские запросы, извлекая релевантную информацию из файлов. Система обеспечивает автоматическое создание саммари для документов в формате PDF: новые и

существующие документы помещаются в очередь обработки после установки соответствующего признака. Сформированные саммари становятся доступными в разделе "Документы" (см. рисунок 2).

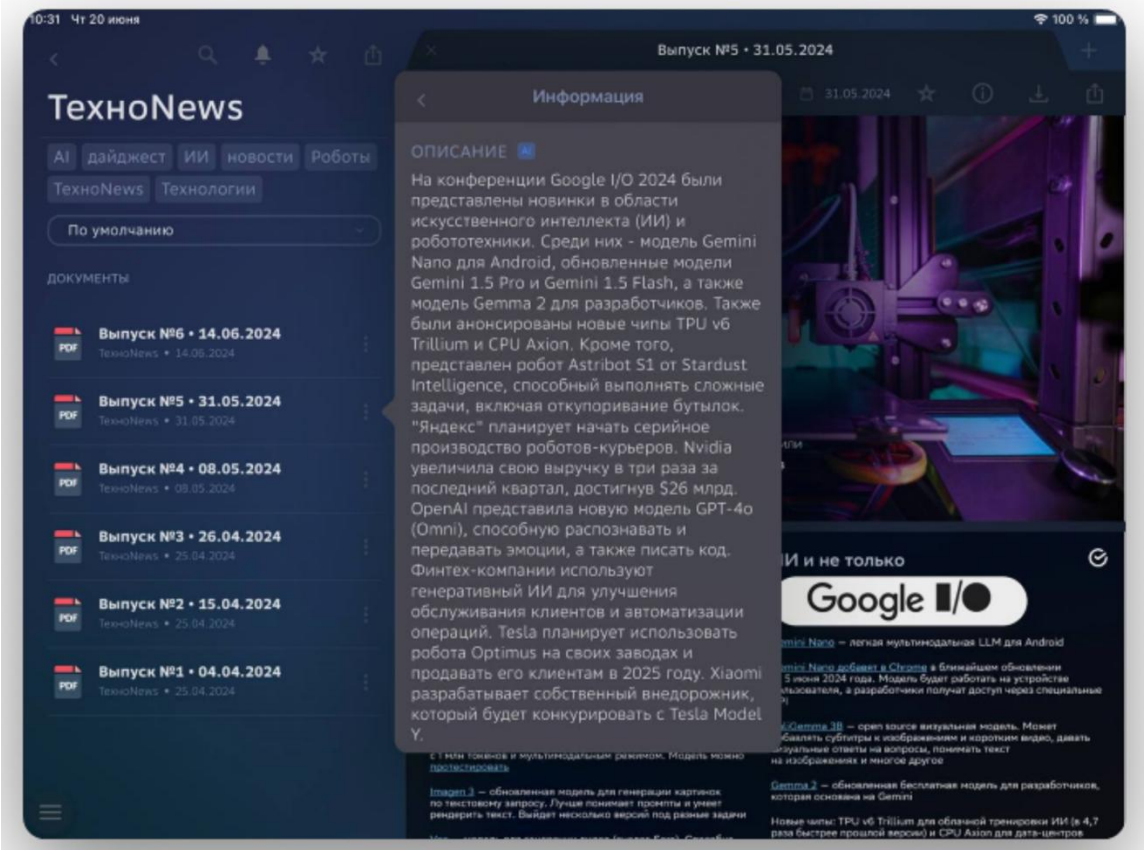

Рисунок 2 – Саммари документа с помощью ИИ в «Навигаторе»

Несмотря на большой список улучшений и преимуществ, добавление искусственного интеллекта в Навигатор BI имеет ряд недостатков. Например, время генерации саммари (до 40 минут) может быть недостаточным для сценариев, требующих мгновенного доступа к информации. Также стоит отметить, что модели ИИ очень требовательны к данным. Если данные непоследовательны или неточны, это может привести к неправильному результату [15].

Подводя итог, аналитика на основе искусственного интеллекта больше не является делом будущего и существует в действительности. Машинное обучение, обработка естественного языка, автоматизация, предиктивное моделирование и многое другое – все это обеспечивает доступ к передовым аналитическим инструментам [16]. Обработка естественного языка в Навигаторе BI обеспечивает более эффективное получение нужных результатов, которые соответствуют целям и стратегиям организации.

Один из самых значительных вкладов ИИ в Навигатор BI – это объединение технических и нетехнических пользователей, что способствует сотрудничеству и расширяет возможности заинтересованных сторон на всех уровнях организаций.

Список литературы

1. Quamar A., Ozcan F., Miller D. Conversational BI: онтологически управляемая система диалога для приложений бизнес-аналитики // Proceedings of the VLDB Endowment. 2020. Т. 13, № 12. С. 3369–3381.
2. Cao R., Lei F., Wu H. Spider2-V: насколько далеки мультимодальные агенты от автоматизации рабочих процессов в области науки о данных и инженерии? [Электронный ресурс] // arXiv. 2024. URL: https://arxiv.org/abs/2407.10956
3. Liu X., Zhang J., Wang H. Передовые методы искусственного интеллекта для улучшения систем бизнес-аналитики [Электронный ресурс] // IEEE Xplore. 2022. URL: https://ieeexplore.ieee.org/document/10696409
4. Xie T., Zhou F. OpenAgents: открытая платформа для языковых агентов в реальных условиях [Электронный ресурс] // arXiv. 2024. URL: https://arxiv.org/abs/2310.10634
5. Lai Y., Li C., Wang Y. DS-1000: естественный и надежный бенчмарк для генерации кода в области науки о данных // Proceedings of the 40th International Conference on Machine Learning (ICML). Proceedings of Machine Learning Research. 2023. Т. 202. С. 18319–18345.
6. Wu Y., Wan Y., Zhang H. Автоматизированная визуализация данных из естественного языка с помощью больших языковых моделей: исследовательское исследование [Электронный ресурс] // Proceedings of the ACM on Management of Data. 2024. Т. 2, № 3. С. 115. URL: https://dl.acm.org/doi/10.1145/3654992
7. Weng L., Wang X., Lu J. InsightLens: обнаружение и исследование инсайтов из контекстов диалога в анализе данных с использованием больших языковых моделей [Электронный ресурс] // arXiv. 2024. URL: https://arxiv.org/abs/2404.01644
8. Zwingmann T. Бизнес-аналитика с поддержкой ИИ. С.: O'Reilly Media, Inc., 2022.
9. Syed W. K., Mohammed A., Reddy J. K., Dhanasekaran S. Биометрические системы аутентификации в банковской сфере: техническая оценка мер безопасности // Proceedings of the 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC). 2024. С. 1331–1336.
10. Платформа Navigator // SberAnalytics [Электронный ресурс]. 2025. URL: https://navigator.sberanalytics.ru/#platform
11. Russian BI: Обзор платформы "Навигатор"[Электронный ресурс] // Russian BI. URL: https://russianbi.ru/vendors/detail.php?ID=633
12. Платформа "Навигатор" [Электронный ресурс]// SberTech. URL: https://platformv.sbertech.ru/products/analitika-dannyh/navigator
13. Release Notes. Navigator [Электронный ресурс] // SberTech. 2025. URL: https://platformv.sbertech.ru/strapi/api/media/Release_Notes_5e15a0358d.pdf
14. Ravichandran P., Machireddy J. R., Rachakatla S. K. Улучшенная ИИ аналитика данных для бизнес-аналитики в реальном времени: приложения и вызовы // Journal of AI in Healthcare and Medicine. 2022. Т. 2, № 2. С. 168–195.
15. Mohammed A.K. Boosting Decision-Making with LLM-Powered Prompts in PowerBI [Электронный ресурс] // ResearchGate. 2023. URL: https://www.researchgate.net/profile/Abdul-Khaleeq-Mohammed/publication/388653726_Boosting_Decision-Making_with_LLM-Powered_Prompts_in_PowerBI/links/67a12603207c0c20fa749fde/Boosting-Decision-Making-with-LLM-Powered-Prompts-in-PowerBI.pdf

16. Shamnad M. S. AI-управляемая аналитика: будущее бизнес-аналитики. [Электронный ресурс] // IJRES. 2024. URL: https://d1wqtxts1xzle7.cloudfront.net/122205409/AI_DrivenAnalytics_TheFutureofBusinessIntelligence.pdf

References

1. Quamar A., Ozcan F., Miller D. Conversational BI: An Ontology-Driven Dialogue System for Business Intelligence Applications // Proceedings of the VLDB Endowment. 2020. Vol. 13, No. 12. pp. 3369–3381.
2. Cao R., Lei F., Wu H. Spider2-V: How Far Are Multimodal Agents from Automating Workflows in Data Science and Engineering? [Electronic resource] // arXiv. 2024. URL: https://arxiv.org/abs/2407.10956
3. Liu X., Zhang J., Wang H. Advanced Artificial Intelligence Techniques for Improving Business Intelligence Systems [Electronic resource] // IEEE Xplore. 2022. URL: https://ieeexplore.ieee.org/document/10696409
4. Xie T., Zhou F. OpenAgents: An Open Framework for Real-World Language Agents [Electronic resource] // arXiv. 2024. URL: https://arxiv.org/abs/2310.10634
5. Lai Y., Li C., Wang Y. DS-1000: A Natural and Robust Benchmark for Code Generation in Data Science // Proceedings of the 40th International Conference on Machine Learning (ICML). Proceedings of Machine Learning Research. 2023. Vol. 202. pp. 18319–18345.
6. Wu Y., Wan Y., Zhang H. Automated Visualization of Natural Language Data with Large Language Models: An Exploratory Study [Electronic resource] // Proceedings of the ACM on Management of Data. 2024. Vol. 2, No. 3. P. 115. URL: https://dl.acm.org/doi/10.1145/3654992
7. Weng L., Wang X., Lu J. InsightLens: Discovering and Exploring Insights from Dialogue Contexts in Data Analysis Using Large Language Models [Electronic resource] // arXiv. 2024. URL: https://arxiv.org/abs/2404.01644
8. Zwingmann T. AI-Enabled Business Analytics. S.: O'Reilly Media, Inc., 2022.
9. Syed W. K., Mohammed A., Reddy J. K., Dhanasekaran S. Biometric Authentication Systems in Banking: A Technical Assessment of Security Measures // Proceedings of the 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC). 2024. pp. 1331–1336.
10. Navigator Platform // SberAnalytics [Electronic resource]. 2025. URL: https://navigator.sberanalytics.ru/#platform
11. Russian BI: Navigator Platform Review [Electronic resource] // Russian BI. URL: https://russianbi.ru/vendors/detail.php?ID=633
12. Navigator Platform [Electronic resource] // SberTech. URL: https://platformv.sbertech.ru/products/analitika-dannyh/navigator
13. Release Notes. Navigator [Electronic resource] // SberTech. 2025. URL: https://platformv.sbertech.ru/strapi/api/media/Release_Notes_5e15a0358d.pdf
14. Ravichandran P., Machireddy J. R., Rachakatla S. K. AI-Enhanced Data Analytics for Real-Time Business Intelligence: Applications and Challenges // Journal of AI in Healthcare and Medicine. 2022. Vol. 2, No. 2. pp. 168–195.
15. Mohammed A.K. Boosting Decision-Making with LLM-Powered Prompts in PowerBI [Electronic resource] // ResearchGate. 2023. URL:

https://www.researchgate.net/profile/Abdul-Khaleeq-Mohammed/publication/388653726_Boosting_Decision-Making_with_LLM-Powered_Prompts_in_PowerBI/links/67a12603207c0c20fa749fde/Boosting-Decision-Making-with-LLM-Powered-Prompts-in-PowerBI.pdf

16. Shamnad M. S. AI-Driven Analytics: The Future of Business Intelligence. [Electronic resource] // IJRES. 2024. URL: https://d1wqtxts1xzle7.cloudfront.net/122205409/AI_DrivenAnalytics_TheFutureofBusinessIntelligence.pdf

Нестерова В.А. Влияние внешних факторов на предприятия авиастроительного комплекса России: систематический обзор литературы // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 171–176

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

ВЛИЯНИЕ ВНЕШНИХ ФАКТОРОВ НА ПРЕДПРИЯТИЯ АВИАСТРОИТЕЛЬНОГО КОМПЛЕКСА РОССИИ: СИСТЕМАТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ

Нестерова В.А.
ФГАОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия (105005, г.Москва, 2-я Бауманская ул., 7), e-mail: nest@valleria.ru

Статья посвящена систематическому обзору научных и аналитических работ, исследующих влияние внешних факторов (геополитических, санкционных, макроэкономических, рыночных) на функционирование предприятий авиационно-промышленного комплекса России, с акцентом на деятельность ОАК и положение на российском рынке в период 2013–2025 гг. Рассматриваются ключевые подходы к анализу, включая оценку санкционных рисков, SWOT и сценарное прогнозирование, моделирование экономических эффектов, а также эволюция от традиционных методов (ERP/MRP) к современным BI-системам, способным учитывать внешние шоки. На основе обзора сформулированы выводы о критическом воздействии ограничений на цепочки поставок, вызовах импортозамещения и определяющей роли государственной поддержки для устойчивости отрасли.

Ключевые слова: авиационная промышленность России, Объединенная авиастроительная корпорация (ОАК), внешние факторы, экономические санкции, импортозамещение, геополитические риски, цепочки поставок, бизнес-аналитика (BI), сценарное прогнозирование, отраслевая устойчивость.

INFLUENCE OF EXTERNAL FACTORS ON ENTERPRISES OF THE RUSSIAN AIRCRAFT MANUFACTURING COMPLEX: A SYSTEMATIC REVIEW OF THE LITERATURE

Nesterova V.A.
"BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY)", Moscow, Russia (105005, Moscow, 2nd Baumanskaya, 7), e-mail: nest@valleria.ru

The article is devoted to a systematic review of scientific and analytical works investigating the impact of external factors (geopolitical, sanctions, macroeconomic, market) on the functioning of enterprises in the Russian aircraft industry, with a focus on the activities of the United Aircraft Corporation (UAC) and the situation on the Russian market in the period 2013–2025. Key analytical approaches are considered, including sanctions risk assessment, SWOT and scenario forecasting, modeling of economic effects, as well as the evolution from traditional methods (ERP/MRP) to modern BI systems capable of accounting for external shocks. Based on the review, conclusions are formulated about the critical impact of restrictions on supply chains, the challenges of import substitution, and the determining role of state support for the industry's resilience.

Keywords: Russian aircraft industry, United Aircraft Corporation (UAC), external factors, economic sanctions, import substitution, geopolitical risks, supply chains, business intelligence (BI), scenario forecasting, industry resilience.

Цель настоящего литературного обзора – систематизировать и обобщить результаты научных и аналитических работ, посвящённых влиянию внешних факторов (геополитических, санкционных, макроэкономических, рыночных) на функционирование предприятий авиационно-промышленного комплекса России, с акцентом на деятельность ОАК и положение на российском рынке. Обзор охватывает период с 2013 по 2025 год, что позволяет отследить динамику изменений, связанных с началом санкций, изменением международной

конъюнктуры, запуском программ импортозамещения и усиливающимся давлением на отрасль. Географический фокус – Россия, с учётом её связей с зарубежными поставщиками, но также с учётом глобальных цепочек поставок и внешнеэкономических условий.

Для формирования базы литературы использовались академические и открытые ресурсы: базы данных (eLibrary, CyberLeninka), Google Scholar, а также официальные документы и аналитические отчёты (включая данные от государственных структур и отраслевых организаций). Основными ключевыми словами и фразами были: «влияние внешних факторов на авиационную промышленность России», «санкции авиация Россия», «ОАК импортозамещение», «развитие гражданского авиапрома при санкциях», «макроэкономические факторы авиапром» и др.

В работах по российскому авиапрому и ОАК чаще всего применяются следующие подходы:

- Анализ санкций и геополитических рисков: исследования, посвящённые тому, как западные санкции и международное давление влияют на цепочки поставок, доступ к технологиям, лизинг, техническое обслуживание, экспорт/импорт комплектующих. [**Ошибка! Источник ссылки не найден.**]
- SWOT анализ и сценарное прогнозирование: в условиях санкций как метод оценки сильных и слабых сторон отрасли, возможностей и угроз, а также планирования дальнейших шагов. [**Ошибка! Источник ссылки не найден.**]
- Моделирование экономических эффектов санкций и импортозамещения – оценка, как санкции и потеря доступа к иностранным компонентам влияют на производственный потенциал, себестоимость, способность к серийному выпуску, нужную долю инвестиций. Например, в работе Forecasting the impact of economic sanctions on the development of Russia’s aircraft industry (Klochkov & Kritskaya, 2017) сделан прогноз на развитие отрасли при санкциях, анализируются требования к инвестициям и снижение производительности. [**Ошибка! Источник ссылки не найден.**]
- Анализ цепочек поставок и зависимости от импортных компонентов – оценка проблем, связанных с прекращением поставок, необходимостью импортозамещения, перестройкой производственных цепочек. [**Ошибка! Источник ссылки не найден.**]
- Статистический и эмпирический анализ отраслевых данных – анализ реальных темпов производства, объёмов поставок, графиков выполнения планов выпуска самолетов, состояния флота, инвестиций, влияния макроэкономических условий (финансирование, курс валют, кредитные ставки). [**Ошибка! Источник ссылки не найден.**]

Таким образом, литература предлагает комбинацию качественных стратегических оценок (SWOT, сценарии), экономико-аналитических моделей и отраслевой эмпирики.

На основании проанализированных работ можно выделить несколько ключевых выводов:

- Внешние факторы – санкции, ограничение международной кооперации, прекращение поставок комплектующих, лизинга, технического обслуживания – стали критическим вызовом для российского гражданского авиапрома [**Ошибка! Источник ссылки не найден.**].
- Попытки импортозамещения и локализации производства (компонентов, двигателей, оборудования) часто сталкиваются с проблемами – нехватка ресурсов, технологий, квалифицированных кадров, длительный срок сертификации, высокая себестоимость [**Ошибка! Источник ссылки не найден.**].

- Продолжающаяся зависимость от импорта – даже через «параллельные» схемы или через посредников – свидетельствует о сложности достижения полной технологической независимости [**Ошибка! Источник ссылки не найден.**].
- Внутренняя экономическая и организационная устойчивость – инвестиции, политика импортозамещения, модернизация производственных мощностей, развитие отечественной базы поставщиков – становится главным фактором, определяющим выживаемость отрасли. [**Ошибка! Источник ссылки не найден.**].

Исторически период, который охватывает обзор, характеризуется следующими этапами:

2014 год и далее (санкции после кризиса 2014 г.) – первые сигналы риска: ограничение зарубежных инвестиций, рост психологии «госбезопасности», переосмысление стратегии развития авиапрома. Работы этого периода прогнозировали необходимость локализации цепочек поставок [**Ошибка! Источник ссылки не найден.**].

2018–2021 годы – период подготовки к импортозамещению, постепенного планирования, попыток вложений в собственные мощности, диверсификации поставщиков, подготовки нормативной базы и программ поддержки [**Ошибка! Источник ссылки не найден.**].

2022 год и далее – кризис: полномасштабные санкции, прекращение поставок, лизинга, технического обслуживания от западных партнёров; форсированные попытки импортозамещения; снижение объёмов выпуска, проблемы с комплектующими, дефицит ресурсообеспечения [**Ошибка! Источник ссылки не найден.**].

2024–2025 годы – текущая фаза: усилия по локализации, государственные программы поддержки, но значительные задержки, нехватка комплектующих, необходимость «параллельных импортов», устойчивые проблемы с производительностью и темпами выпуска [**Ошибка! Источник ссылки не найден.**]

Эта эволюция отражает переход от глобальной кооперации к попытке автономного производства в условиях жёстких внешних ограничений.

В литературе по анализу внешних факторов для предприятий промышленности и авиационного комплекса прослеживается явная эволюция подходов – от простых схем и ручных учётов до сложных BI-систем и аналитики на основе больших данных. Ниже – сравнительный анализ сильных и слабых сторон основных подходов и рекомендации, исходя из этого анализа.

Традиционные и ранние методы (блок-схемы, MRP / ERP) удобны для описания и учёта бизнес-процессов, управления ресурсами и планирования – что критично для производственных предприятий. Однако при внешних шоках (санкции, сбои цепочек поставок, макроэкономическая нестабильность, политический риск) такие системы часто оказываются недостаточными: они не предназначены для анализа внешней среды, не дают представления о возможных рисках и последствиях, не способны предсказывать сценарии. Более того, ERP и MRP ориентированы на внутренних регламентированных процессах – они не учитывают внешние факторы, что снижает их стратегическую ценность в условиях непредсказуемости.

BI-системы и BI Analytics (BI&A, Big Data, прогнозирование) дают возможность интегрировать данные из разных источников – финансовые, операционные, производственные, внешние – и получать аналитическую картину предприятия в целом [**Ошибка! Источник ссылки не найден.**]. BI&A, с элементами Data Science, статистики,

машинного обучения, позволяют прогнозировать последствия внешних изменений, строить сценарии, оценивать риски, что особенно важно для отраслей, подверженных внешним воздействиям (геополитика, спрос, санкции, поставки). Тем не менее, внедрение таких систем требует значительных ресурсов, что может быть сложно для предприятий с ограниченными ресурсами. Также есть риски: прогнозы могут быть неточными, модели – ошибочными, особенно при недостаточных или неполных данных; требуется постоянное обновление и поддержка данных, моделей и систем.

Современные тенденции, на которые указывают последние исследования и аналитика:

- Активное стремление к импортозамещению и локализации производства: как стратегическая цель для обеспечения технологической и производственной независимости авиационной отрасли [**Ошибка! Источник ссылки не найден.**].
- Рост роли государства – финансирования, поддержки, регулирования: бюджетные программы, субсидии, государственные заказы, централизованное управление как условие сохранения авиационного производства [**Ошибка! Источник ссылки не найден.**].
- Увеличение зависимости от «параллельных импортов», серых схем поставок, альтернативных маршрутов поставки комплектующих – как вынужденная мера при недоступности легальных каналов [**Ошибка! Источник ссылки не найден.**]
- Технологические и ресурсные ограничения: нехватка квалифицированных кадров, технологической базы, времени и средств на сертификацию и производство комплектующих, которые ранее поставлялись извне [4].
- Нестабильность планов и сроков: снижение темпов выпуска, срывы сроков, пересмотр планов производства – что подрывает уверенность в способности отрасли обеспечить обновление флота и модернизацию [**Ошибка! Источник ссылки не найден.**]

Вызовы, отмечаемые в литературе:

- Невозможность в короткие сроки заменить весь импортный компонентный базис – требует десятилетий и значительных инвестиций [9].
- Повышенная себестоимость, снижение конкурентоспособности продукции (по цене, эффективности, срокам) [**Ошибка! Источник ссылки не найден.**].
- Риски дефицита комплектующих, технологий, человеческих ресурсов – что может привести к снижению качества, отказам, задержкам, проблемам с безопасностью [7].

Обзор литературы показывает, что в условиях санкционного давления основную роль в ухудшении операционной эффективности и финансовых результатов отрасли играют перебои в поставках критичных комплектующих и затраты на импортозамещение. На этой основе формулируется рабочая гипотеза эксперимента: негативные информационные шоки (новости о санкциях, приостановках поставок) опережают ухудшение финансовых показателей ОАК и могут быть использованы в качестве предиктора краткосрочных колебаний выручки, дебиторской задолженности и ликвидности.

Список литературы

1. Особенности и перспективы развития российского гражданского авиастроения в условиях санкционного давления со стороны стран Запада [Электронный ресурс] // Лапушкин В.В. URL: https://cyberleninka.ru/article/n/osobennosti-i-perspektivy-razvitiya-rossiyskogo-grazhdanskogo-aviastroeniya-v-usloviyah-sanktsionnogo-davleniya-so-storony-stran

2. Promising directions for the development of Russian civil aircraft in the context of sanctions pressure [Электронный ресурс] // Lapushkin B. I. URL: https://statecounsellor.wordpress.com/wpcontent/uploads/2025/08/pdf_240204.pdf
3. Forecasting the impact of economic sanctions on the development of the Russian aircraft industry [Электронный ресурс] // Springer Nature . URL: https://link.springer.com/article/10.1134/S107570071706003X
4. Россия на мировом рынке авиадвигателей: проблемы и перспективы [Электронный ресурс] // РУДН / Пинчук В.Н. Занчев Д.А. URL: https://journals.rudn.ru/economics/article/view/36233
5. Industrial Collapse: Crippled by Sanctions, Russia's Aviation Industry Produces Only One Commercial Aircraft in 2025 [Электронный ресурс] // Aviacioline. URL: https://www.aviacionline.com/industrial-collapse-crippled-by-sanctions-russias-aviation-industry-produces-only-one-commercial-aircraft-in-2025
6. Политика санкций западных стран против России и ее влияние на гражданскую авиацию [Электронный ресурс] // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/columns/sanctions/politika-sanktsiy-zapadnykh-stran-protiv-rossii-i-ee-vliyanie-na-grazhdanskuyu-aviatsiyu
7. Farewell, Boeing and Airbus: Russian Aircraft Industry Goes Fully Domestic [Электронный ресурс] // Sputnik International. URL: https://www.themoscowtimes.com/2025/07/14/russian-aircraft-industry-struggles-to-replace-western-parts-amid-sanctions-a89814
8. Import Substitution in High-Tech Industries under External Sanctions [Электронный ресурс] // URL: https://managementscience.fa.ru/jour/article/download/384/322
9. https://www.wilsoncenter.org/blog-post/sanctions-are-spoiling-russias-plans-make-its-own-airplanes
10. 150 years of business intelligence: A brief history [Электронный ресурс] // URL: https://www.cio.com/article/221963/history-of-business-intelligence.html
11. Гражданская авиация в эпоху санкций [Электронный ресурс] // ВЦИОМ Новости. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/grazhdanskaja-aviacija-v-ehpokhu-sankcii
12. Wings Still Clipped? Russia's Airpower after Three Years of Conflict and Embargo [Электронный ресурс] // King's College London. URL: https://www.kcl.ac.uk/warstudies/assets/kcl-fasi-paper31-wings-still-clipped-web.pdf
13. Industrial Collapse: Crippled by Sanctions, Russia's Aviation Industry Produces Only One Commercial Aircraft in 2025 [Электронный ресурс] // URL: https://www.aviacionline.com/industrial-collapse-crippled-by-sanctions-russias-aviation-industry-produces-only-one-commercial-aircraft-in-2025.

References

1. Features and Prospects for the Development of Russian Civil Aircraft Industry in the Context of Sanctions Pressure from Western Countries [Electronic resource] // Lapushkin V.V. URL: https://cyberleninka.ru/article/n/osobennosti-i-perspektivy-razvitiya-rossiyskogo-grazhdanskogo-aviastroeniya-v-usloviyah-sanktsionnogo-davleniya-so-storony-stran

2. Promising Directions for the Development of Russian Civil Aircraft in the Context of Sanctions Pressure [Electronic resource] // Lapushkin B.I. URL: https://statecounsellor.wordpress.com/wpcontent/uploads/2025/08/pdf_240204.pdf
3. Forecasting the Impact of Economic Sanctions on the Development of the Russian Aircraft Industry [Electronic resource] // Springer Nature . URL: https://link.springer.com/article/10.1134/S107570071706003X
4. Russia in the global aircraft engine market: problems and prospects [Electronic resource] // RUDN / Pinchuk V.N. Zanchev D.A. URL: https://journals.rudn.ru/economics/article/view/36233
5. Industrial Collapse: Crippled by Sanctions, Russia's Aviation Industry Produces Only One Commercial Aircraft in 2025 [Electronic resource] // Aviacioline. URL: https://www.aviacionline.com/industrial-collapse-crippled-by-sanctions-russias-aviation-industry-produces-only-one-commercial-aircraft-in-2025
6. Western countries' sanctions policy against Russia and its impact on civil aviation [Electronic resource] // RIAC. URL: https://russiancouncil.ru/analytics-and-comments/columns/sanctions/politika-sanktsiy-zapadnykh-stran-protiv-rossii-i-ee-vliyanie-na-grazhdanskuyu-aviatsiyu
7. Farewell, Boeing and Airbus: Russian Aircraft Industry Goes Fully Domestic [Electronic resource] // Sputnik International. URL: https://www.themoscowtimes.com/2025/07/14/russian-aircraft-industry-struggles-to-replace-western-parts-amid-sanctions-a89814
8. Import Substitution in High-Tech Industries under External Sanctions [Electronic resource] // URL: https://managementscience.fa.ru/jour/article/download/384/322
9. https://www.wilsoncenter.org/blog-post/sanctions-are-spoiling-russias-plans-make-its-own-airplanes
10. 150 years of business intelligence: A brief history [Electronic resource] // URL: https://www.cio.com/article/221963/history-of-business-intelligence.html
11. Civil Aviation in the Era of Sanctions [Electronic resource] // VTsIOM News. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/grazhdanskaja-aviacija-v-ehpokhu-sankcii
12. Wings Still Clipped? Russia's Airpower after Three Years of Conflict and Embargo [Electronic resource] // King's College London. URL: https://www.kcl.ac.uk/warstudies/assets/kcl-fasi-paper31-wings-still-clipped-web.pdf
13. Industrial Collapse: Crippled by Sanctions, Russia's Aviation Industry Produces Only One Commercial Aircraft in 2025 [Electronic resource] // URL: https://www.aviacionline.com/industrial-collapse-crippled-by-sanctions-russias-aviation-industry-produces-only-one-commercial-aircraft-in-2025

Сеидов М.С-А., Ясевич Б.О. Мониторинг аномальной активности в операционной системе ЗОСРВ «Нейтрино» // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 177–185

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

МОНИТОРИНГ АНОМАЛЬНОЙ АКТИВНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ ЗОСРВ «НЕЙТРИНО»

Сеидов М.С-А., [1]Ясевич Б.О.
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: boris.yasevich2005@gmail.com

В рамках исследования выполнено экспериментальное развертывание системы мониторинга аномальной активности процессов, проведено обучение модели на данных штатного функционирования системы и выполнено моделирование различных типов аномального поведения. Оценивалась способность системы выявлять отклонения в поведении процессов, а также накладные расходы, связанные с её работой.
Результаты исследования показали, что предложенный подход позволяет обнаруживать аномальную активность в режиме, максимально приближенному к реальному времени, при умеренных затратах вычислительных ресурсов. Полученные данные подтверждают возможность применения поведенческого анализа для мониторинга процессов в операционной системе «Нейтрино»..

Ключевые слова: операционная система «Нейтрино», аномальная активность процессов, поведенческий анализ, мониторинг процессов, машинное обучение, производительность системы.

MONITORING ANOMALOUS ACTIVITY IN THE NEUTRINO RESEARCH SYSTEM

Seidov M.S.-A., [1]Yasevich B.O.
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: 1 boris.yasevich2005@gmail.com

As part of the study, an experimental deployment of an anomalous process activity monitoring system was carried out, a model was trained on data representing normal system operation, and various types of anomalous behavior were simulated. The system's ability to detect deviations in process behavior, as well as the overhead associated with its operation, was evaluated.
The experimental results showed that the proposed approach makes it possible to detect anomalous process activity in near real-time while incurring moderate computational costs. The obtained data confirm the feasibility of applying behavioral analysis for process monitoring in the Neutrino operating system.

Keywords: Neutrino operating system, anomalous process activity, behavioral analysis, process monitoring, machine learning, system performance.

Современные операционные системы повсеместно используются в специализированных и интегрированных вычислительных комплексах. В этих комплексах выдвигаются высокие требования к надежности, отказоустойчивости и предсказуемости работы. В этих системах отклонения от привычного поведения процессов приводят к снижению производительности, отказам и, следовательно, нарушению требований безопасности. В связи с этим задача

своевременного обнаружения аномальной активности процессов является актуальной и практически значимой. [1]

В жизни состояние операционной системы отслеживается с помощью с двух подходов: сигнатурного и правил-ориентированного. Эти подходы позволяют невероятно эффективно выявлять известные нарушения, однако обладают ограниченной гибкостью и плохо адаптируются к постоянно обновляющимся условиям эксплуатации. Кроме того, они не позволяют обнаруживать новые типы аномалий, не описанные ранее.

Одно из направлений, имеющих большой потенциал – поведенческий анализ, основанный на формировании модели нормального поведения системы. При таком виде анализа за аномалию принимается считается отклонение поведения в данный момент времени от ранее наблюдавшегося состояния, которое принимается как нормальное. Использование машинного обучения позволяет автоматизировать процесс построения эксклюзивной модели нормального поведения и снизить зависимость от ручной настройки параметров. [2]

В этой работе рассматривается экспериментальное обнаружение аномальной активности процессов в операционной системе «Нейтрино» с использованием поведенческого анализа. Работа ориентирована на практическую проверку применимости данного подхода в условиях реальной системы.

В этой работе мы изучаем операционную систему «Нейтрино» и то, как в ней работают программы. Главная задача – найти способы замечать, когда программы ведут себя странно, анализируя то, что они делают в системе. Мы хотим проверить, можно ли находить такие отклонения с помощью анализа поведения и машинного обучения.

Для этого мы настроили систему, которая следит за активностью программ. Сначала мы обучили модель на данных, которые получили, когда система работала нормально. Далее создали ситуацию аномальной активности, проверили обнаруживает ли ее система. Произвели оценку количества ресурсов, требуемых для работы системы мониторинга.

Обнаружение аномальной активности происходит с помощью сигнатурного и правил-ориентированного методов. Сигнатурный подход – сопоставление состояния с известным шаблоном. Его преимущество – высокая точность определения известных нарушений. Его недостаток – необходимость частого обновления шаблонов.

Правил-ориентированные методы используют пороговые значения параметров и заранее заданные условия. Недостатком данного подхода является сложность выбора универсальных порогов, а также высокая вероятность ложных срабатываний при изменении режима работы системы.

Поведенческий анализ представляет собой альтернативный подход, при котором система рассматривается с точки зрения характерных для неё паттернов активности. Отклонения от этих паттернов интерпретируются как потенциальные аномалии. Такой подход не требует явного описания всех возможных нарушений и может выявлять нетипичное поведение общего характера.

На практике поведенческий анализ часто реализуется с использованием методов машинного обучения, в том числе алгоритмов обучения без учителя. Для специализированных операционных систем важным требованием является низкая вычислительная сложность используемых моделей и возможность их работы в режиме реального времени. Поэтому при выборе конкретного решения необходимо учитывать не только точность обнаружения аномалий, но и накладные расходы, связанные с его использованием. [3]

Операционная система «Нейтрино» предназначена для применения в специализированных и встроенных вычислительных системах. Для данной ОС характерны модульная архитектура, чёткое разделение процессов и наличие стандартных средств получения информации о состоянии системы, что делает возможным проведение поведенческого анализа без существенного вмешательства в её работу. [4]

В качестве средства исследования используется программный комплекс мониторинга аномальной активности процессов. Комплекс включает сервис сбора и анализа данных, а также утилиту управления конфигурацией и режимами работы. Сбор информации о процессах осуществляется с использованием стандартных механизмов операционной системы, в частности данных, предоставляемых ядром и виртуальной файловой системой /proc. (Рисунок 1) [5]

В ходе эксперимента анализируются параметры, характеризующие поведение процессов: использование оперативной памяти, количество потоков, состав загруженных библиотек и параметры сетевой активности. Данные характеристики выбраны как наиболее информативные с точки зрения выявления отклонений от нормального функционирования и при этом доступные для мониторинга с минимальными накладными расходами.

Для анализа данных, собранных при использовании операционной системы, используется машинное обучение. С его помощью формируется образ нормального поведения процессов на основе наблюдений за работой системы в обычном, повседневном режиме. Полученная модель используется для выявления несоответствий нормальному поведению в режиме мониторинга без предварительного создания и указания конкретных сценариев нарушений.

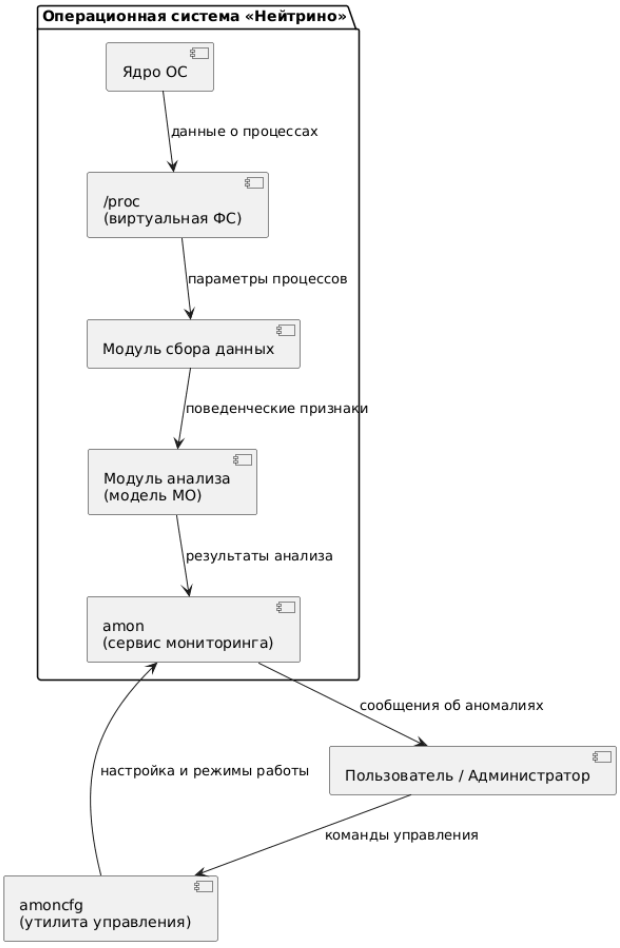

Рисунок 1 – Структурная схема программного комплекса мониторинга

Эксперимент проводился в специально созданном, изолированном программно-аппаратном окружении. На виртуальной машине была запущена операционная система «Нейтрино» и установлен программный комплекс мониторинга. Перед началом эксперимента была выполнена проверка успешности установки и работоспособности всех установленных компонентов.

Для запуска сервиса мониторинга использовалась стандартная команда запуска фонового процесса.

Запуск сервиса мониторинга amon:

```
#amon -v &

Config file loaded
Running kernl operator...
Loading analizer...
Using structure without learning data...
Modl name: amon neiral network
Modl desc: neiral net structure for amon
Modl ver: 1.1
Neuron count: 7

Kernel operator init done
```

Далее производилась настройка параметров мониторинга. В файле конфигурации задали список процессов, подлежащих анализу, набор контролируемых параметров и периодичность сбора данных. Конфигурация писалась таким образом, чтобы захватить процессы, привычные для штатного режима работы системы.

Фрагмент конфигурационного файла мониторинга:

```
{
 "name": "simple_user",
 "buffer_size": 1024,
 "providers": [
  {
   "name": "kernl_provider",
   "processes": [
    "io-usb",
    "io-hid",
    "netmgr"
   ],
   "data": [
    "memory",
    "threads",
    "libraries",
    "network"
   ],
```

"polling_time": 3000,
"structure": "structure/kernl/structure.json",
"anomaly_action": "scrips/anomaly.sh"
}
]
}

После загрузки конфигурации произошла очередная проверка правильности настроек с использованием специализированных команд. Отсутствие ошибок и предупреждений подтвердило готовность системы к переходу на следующий этап эксперимента. Следующий этап – обучение модели нормального поведения.

Для перехода в режим обучения использовалась базовая команда управления системой мониторинга. После её выполнения сервис начал сбор и аккумуляцию данных о поведении процессов без выполнения анализа на наличие непонятных аномалий в поведении системы.

Перевод системы в режим обучения:

amonctl -L

Обучение проводилось в условиях штатной работы системы, без подключения дополнительных устройств и без проведения нагрузочного тестирования. За отведённое время система записала, чем занимались процессы: сколько памяти использовали, сколько потоков создавали, какие библиотеки загружали и как работали в сети. Обучали систему достаточно долго, чтобы охватить все обычные варианты её работы.

Сколько времени займет обучение, зависит от того, как трудно повторить действие и насколько разные ситуации мы хотим считать надежными. Это может занять от пары секунд до гораздо большего времени.

После завершения обучения система мониторинга переводилась в режим анализа, в котором выполнялось сравнение текущего поведения процессов с ранее сформированной моделью нормального поведения. На данном этапе система начинала выявлять отклонения и фиксировать потенциальные аномалии.

Переход в режим мониторинга осуществлялся с помощью команды управления, после чего система начинала работать в режиме реального времени.

Перевод системы в режим анализа активности:

amonctl -R

Корректность завершения этапа обучения подтверждалась отсутствием ошибок в диагностическом выводе системы мониторинга.

Вывод состояния системы:

amonctl -S

Trust value: 99.9893%
Objects captured: 34
Alerts captured: 0
Time: 7 ms

Для проверки работы системы выполнялось моделирование аномальной активности. При обнаружении отклонений система мониторинга формировала диагностические сообщения, содержащие идентификатор процесса и параметр, по которому было зафиксировано несоответствие модели нормального поведения.

Для создания аномальной активности был выбран процесс запуска калькулятора (/phcalc), так как во время обучения системы мониторинга такого процесса не было, и система, вероятно, посчитает его аномальным и сообщит нам об этом. Просмотр аномалий проводился с помощью Amon GUI. [6]

Просмотр обнаруженных аномалий (рисунок 2)

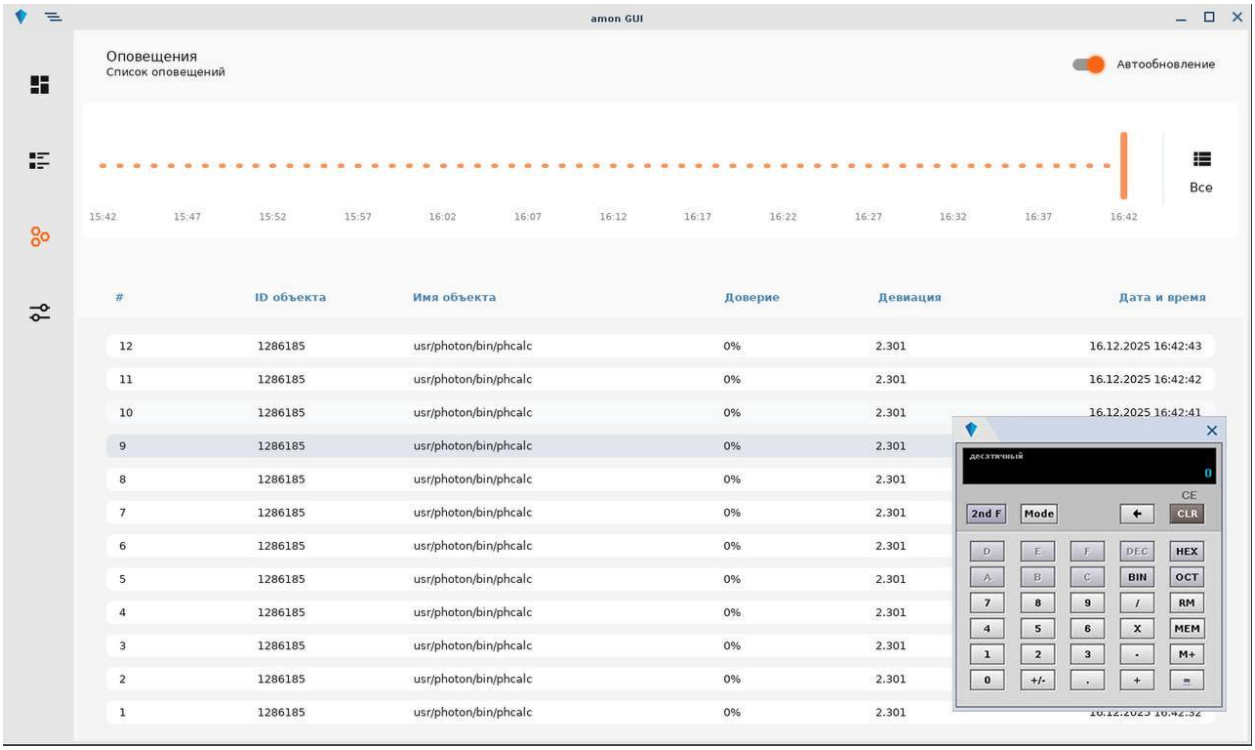

Рисунок 2 – Отслеживание аномальной активности через Amon GUI

На Рисунке 2 представлены имя объекта, вызвавшего аномальную активность, процент уверенности в его идентификации, а также точное время фиксации аномалии.

В рамках данного исследования рассматривалось влияние работы системы мониторинга на использование вычислительных ресурсов операционной системы «Нейтрино». Основное внимание уделялось загрузке процессора и потреблению оперативной памяти.

Измерения проводились в нескольких режимах работы системы: до начала мониторинга, в режиме обучения модели нормального поведения и после перехода в режим анализа. Для контроля состояния системы использовались стандартные средства операционной системы, а также графический интерфейс amon gui, обеспечивающий наглядную визуализацию работы сервиса мониторинга. [7]

Для анализа загрузки процессора использовался интерфейс amon gui, позволяющий отслеживать изменение нагрузки при переходе между режимами работы системы мониторинга. На начальном этапе, до запуска мониторинга, система находилась в стабильном состоянии без дополнительной вычислительной нагрузки. (Рисунок 3)

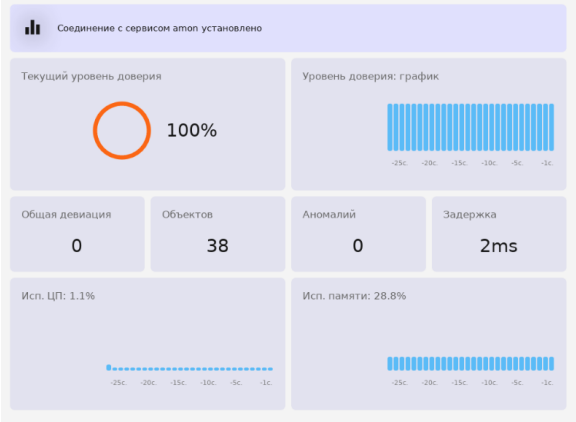

Рисунок 3 – Интерфейс amon gui до начала мониторинга

После запуска мониторинга и перехода системы в режим анализа наблюдалось умеренное увеличение загрузки процессора, связанное с выполнением операций сбора и обработки данных. При этом рост нагрузки не носил скачкообразного характера и оставался стабильным в течение всего времени наблюдения. (Рисунок 4)

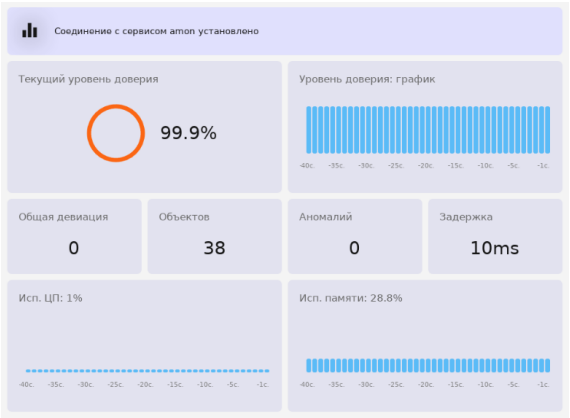

Рисунок 4 – Интерфейс amon gui после начала мониторинга

Анализ системы до и после запуска мониторинга показал, что этот процесс почти не влияет на производительность и может работать в фоновом режиме. Несмотря на то, что задержка выросла в 5 раз, она всё равно остаётся очень маленькой.

Мы посмотрели, сколько памяти требует мониторинг. В ход анализа мы смотрели за потребляемой памятью. Объем используемой памяти почти не менялся. Даже когда система находила новый процесс потребление памяти не увеличивалось.

Еще мы проверили влияние системы мониторинга на производительность компьютера. Увидели, что это не замедляет работу операционной системы.

Тестирование системы, следящей за аномальной активности провели с помощью запуска приложения, которого не было при обучении.

Результаты эксперимента показали, что поведенческий подход позволяет выявлять аномалии в работе системы в режиме реального времени. Система не показала ложных срабатываний и не оказала сильного влияния на производительность машины.

В будущем можно анализировать больше параметров, автоматически подстраивать модель под меняющиеся условия и объединить систему мониторинга с другими инструментами для надёжности и безопасности..

Литература

1. QNX Software Systems. QNX Neutrino RTOS Architecture: официальная документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/ (дата обращения: 04.12.2025).
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. – 2009. – Vol. 41, No. 3, Art. 15. – 58 p. – DOI: 10.1145/1541880.1541882.
3. Уймин А. Г., Цифровые двойники сетевых инфраструктур: точность, методы и практические решения // Радиотехнические и телекоммуникационные системы. – 2023. – № 3 (51). – С. 44–52.
4. QNX Software Systems. Process Manager and Resource Managers in QNX Neutrino: техническая документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.sys_arch/topic/about.html (дата обращения: 04.12.2025).
5. QNX Software Systems. QNX OS (Neutrino) User’s Guide: руководство пользователя. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/8.0/com.qnx.doc.neutrino.user_guide/topic/about.html (дата обращения: 04.12.2025).
6. Мониторинг аномальной активности в операционной системе «Нейтрино»: форум Habr. [Электронный ресурс]. URL: https://habr.com/ru/companies/swd_es/articles/713690/ (дата обращения: 04.12.2025).
7. QNX Software Systems. System Analysis Toolkit (SAT) for QNX Neutrino: официальная документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.sat.userguide/topic/about.html (дата обращения: 04.12.2025).

References

1. QNX Software Systems. QNX Neutrino RTOS Architecture: Official Documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/ (accessed: 04.12.2025).
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. - 2009. - Vol. 41, No. 3, Art. 15. - 58 p. - DOI: 10.1145/1541880.1541882.
3. Uimin A. G., Digital twins of network infrastructures: Accuracy, methods, and practical solutions // Radiotechnical and telecommunication systems. - 2023. - No. 3 (51). - Pp. 44–52.
4. QNX Software Systems. Process Manager and Resource Managers in QNX Neutrino: technical documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.sys_arch/topic/about.html (accessed: 04.12.2025).
5. QNX Software Systems. QNX OS (Neutrino) User’s Guide: user’s guide. [Electronic resource]. URL: https://www.qnx.com/developers/docs/8.0/com.qnx.doc.neutrino.user_guide/topic/about.html (accessed: 04.12.2025).

6. Monitoring anomalous activity in the Neutrino operating system: Habr forum. [Electronic resource]. URL: https://habr.com/ru/companies/swd_es/articles/713690/ (accessed: 04.12.2025).
7. QNX Software Systems. System Analysis Toolkit (SAT) for QNX Neutrino: official documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.sat.userguide/topic/about.html (accessed: 04.12.2025).

Капитанчук В.В. Разработка модели процесса посадки самолета ТУ-134 / Капитанчук В.В., Забелин А.Н., Гамза С.А. // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 186–196

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.94

РАЗРАБОТКА МОДЕЛИ ПРОЦЕССА ПОСАДКИ САМОЛЕТА ТУ-134

[1]Капитанчук В.В., Забелин А.Н., Гамза С.А.
ФГКВОУ ВО "КРАСНОДАРСКОЕ ВЫСШЕЕ ВОЕННОЕ АВИАЦИОННОЕ УЧИЛИЩЕ ЛЕТЧИКОВ ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА А.К.СЕРОВА" МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, Краснодар, Росиия (350090, Краснодарский край, г. Краснодар-5, ул. Дзержинского, д. 135), e-mail: [1]kapvas@mail.ru

Настоящая статья посвящена моделированию процесса захода на посадку и посадки самолета Ту-134 на примере выполнения этого этапа полета в аэропорту города Тюмень. В результате моделирования раскрываются понятие и роль технологических процессов в авиационной деятельности.

Ключевые слова: технологические процессы, анализ инцидентов, RAMUS Education, ARIS Express.

DEVELOPMENT OF A LANDING PROCESS MODEL FOR THE TU 134 AIRCRAFT

[1]Kapitanchuk V. V., Zabelin A. N., Gamza S. A.
KRASNODAR HIGHER MILITARY AVIATION SCHOOL OF PILOTS NAMED AFTER HERO OF THE SOVIET UNION A.K. SEROV OF THE MINISTRY OF DEFENSE OF THE RUSSIAN FEDERATION, Krasnodar, Russia (350090, Krasnodar Krai, Krasnodar-5, Dzerzhinsky St, 135), e-mail: 1 kapvas@mail.ru

This article focuses on modelling the approach and landing process of the Tu 134 aircraft, using the example of executing this flight phase at Tyumen Airport. Through the modelling, the concept and role of technological processes in aviation activities are elucidated.

Keywords: technological processes, incident analysis, RAMUS Education, ARIS Express.

Введение

Современные организации функционируют в условиях высокой динамики внешней среды, что обусловливает необходимость системного анализа внутренних операций. В этих условиях моделирование технологических процессов выступает ключевым инструментом, позволяющим формализовать структуру деятельности, выявлять неэффективные участки и совершенствовать механизмы управления. Применение подобных моделей способствует повышению управляемости организации, обеспечению её устойчивого развития и поддержанию конкурентных преимуществ.

Объект исследования - процесс посадки самолёта Ту-134, включая аэродинамические, пилотажно-навигационные и эксплуатационные аспекты, влияющие на безопасность, точность и эффективность выполнения посадочной фазы полёта.

Предмет исследования - технологическая модель процесса посадки самолёта Ту-134, отражающая динамику движения воздушного судна на этапах захода на посадку, выравнивания и касания взлётно-посадочной полосы с учётом аэродинамических характеристик, режимов работы двигателей, параметров управления и внешних условий.

Цель работы - разработать модель процесса посадки воздушного судна Ту-134 с целью повышения качества и надёжности авиационных операций, а также создания основы для совершенствования методик анализа посадочных режимов, тренажёрной подготовки экипажей и внедрения современных технологий в области аэронавигации и управления полётами.

В авиационной практике термин «технологический процесс» — это строго структурированная последовательность согласованных действий, осуществляемых экипажем воздушного судна, службами управления воздушным движением и наземными подразделениями с целью достижения определённой задачи, в первую очередь — безопасного, эффективного и своевременного выполнения полёта. Ключевая функция данного процесса состоит в обеспечении предсказуемости, управляемости и строгого соответствия установленным нормативам и стандартам операционной деятельности в авиации. [8]

Применение методов моделирования в авиационной практике обеспечивает следующие преимущества:

1. Улучшение понимания процессов: визуализация процесса помогает всем заинтересованным сторонам (от сотрудников до руководства) лучше понимать, как именно процессы функционируют и взаимодействуют друг с другом;

2. Оптимизация и улучшение процессов: анализ существующих процессов позволяет выявить узкие места, избыточные или дублирующие действия и найти способы их оптимизации, что помогает повысить эффективность и уменьшить затраты;

3. Повышение качества: стандартизация процессов помогает установить чёткие критерии выполнения задач, что способствует поддержанию высокого уровня качества продукции или услуг;

4. Снижение рисков: документирование процессов и их анализа помогает выявить потенциальные риски и определить меры для их минимизации;

5. Управление изменениями: моделирование облегчает адаптацию процессов к изменениям в технологической среде, таким как внедрение новых технологий, изменение рыночных условий или законодательных требований;

6. Повышение качества взаимодействия, контроля и ответственности: чёткое описание процессов помогает распределить ответственность и улучшить контроль выполнения задач, а также способствует лучшей коммуникации и координации между различными отделами;

7. Сокращение времени на обучение: новым сотрудникам легче понять и влиться в работу, имея под рукой чёткие модели процессов, что сокращает время обучения и способствует повышению квалификации.

8. Поддержка систем автоматизации: моделирование является важным этапом для автоматизации процессов с помощью информационных систем и технологий, которые позволяют более точно формализовать процессы для их автоматизации.

Последовательность действий, формирующая процесс посадки воздушного судна, обладает характерными признаками технологических процессов. Каждый этап строго регламентирован, выполняется в определённой логической последовательности и направлен на достижение единой цели — обеспечение безопасного завершения полёта. Подобная структурированность позволяет рассматривать процесс посадки как комплексную операционную систему, функционирующую по принципам следующего алгоритма:

1. Снижение:

2. Заход на посадку (действия согласно типу захода на посадку);

3. Посадка:

4. Руление;

5. Заруливание на стоянку и останов двигателей;

6. Послеполётные процедуры:

Процесс посадки воздушного судна представляет собой деятельность, в которой своевременность и достоверность информационного обмена являются критически значимыми параметрами. Во взаимодействие включены члены экипажа, диспетчерские органы различных уровней, метеорологические и технические службы, а также автоматизированные системы управления воздушным движением. Передаваемая информация охватывает широкий спектр данных: от параметров полёта до характеристик взлётно-посадочной полосы и сведений о воздушной обстановке. Нарушения в информационных потоках способны привести к сбоям координации и снижению уровня безопасности. Таким образом, процесс посадки демонстрирует фундаментальный принцип эффективных технологических процессов: устойчивость результата обеспечивается наличием стандартизированных протоколов обмена и надёжных каналов коммуникации. [1-4]

Моделирование процесса посадки Ту-134 в RAMUS EDUCATIONAL

Ramus представляет собой программу для построения функциональных диаграмм, используемых для проектирования и моделирования различных технологических процессов. Применение методологии IDEF0 предполагает поэтапное формирование модели исследуемого процесса. На начальном этапе определяется цель моделирования и устанавливаются границы системы. Далее разрабатывается контекстная диаграмма, отражающая главную функцию (Рисунок 1). После этого проводится идентификация ключевых операций и установление связей между ними. Финальный этап предусматривает декомпозицию выявленных функций, уточнение структурных элементов и согласование модели с экспертным сообществом, что, обеспечивает её корректность и применимость.

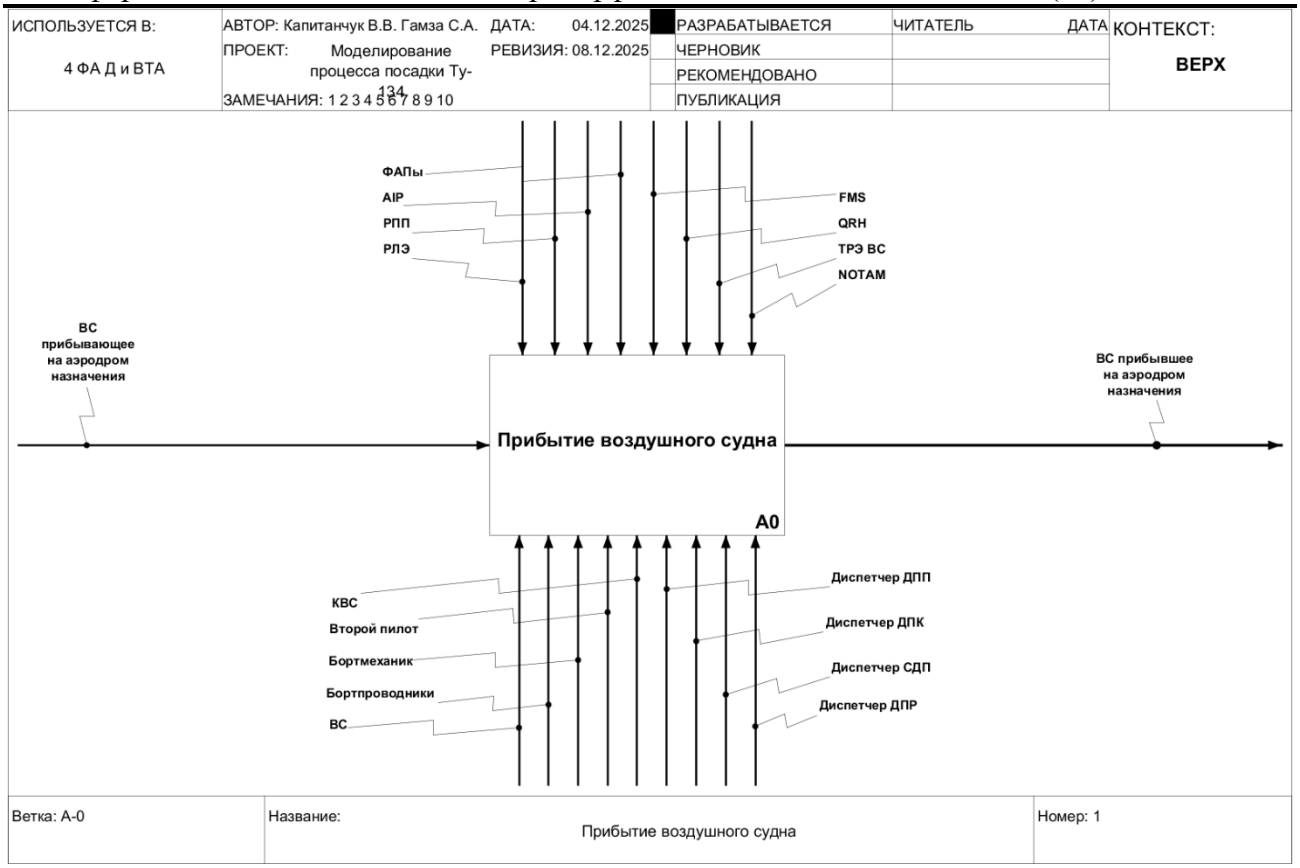

Рисунок 1 – Контекстная диаграмма EDEF0

Разработка модели процесса посадки ВС в RAMUS EDUCATIONAL выполнена на 22 листах. В структуре процесса посадки чётко регламентированы функции и зоны ответственности всех участников: экипажа, диспетчеров и наземных служб. Подобное распределение обязанностей соответствует процессному подходу к управлению, в рамках которого результат достигается посредством согласованной деятельности субъектов, выполняющих специализированные функции в общей системе. Диспетчерское обслуживание воздушных судов осуществляется на нескольких уровнях, каждый из которых выполняет специализированные функции. На маршруте управление полётом осуществляется районными центрами и локальными пунктами ОВД. На этапе подхода ответственность разделена между диспетчерским пунктом аэродрома и смежными структурами. Аэродромное обслуживание обеспечивается диспетчерской вышкой либо специализированными пунктами, на которые распределяются функции управления воздушным движением в пределах круга полётов, на старте, при рулении и посадке. Такое разграничение зон ответственности обеспечивает непрерывность и согласованность процесса управления полётом. Таким образом, с учётом всех данных, выполнена декомпозиция контекстной диаграммы процесса посадки ВС Ту-134. (Рисунок 2) [6-7, 17-18]

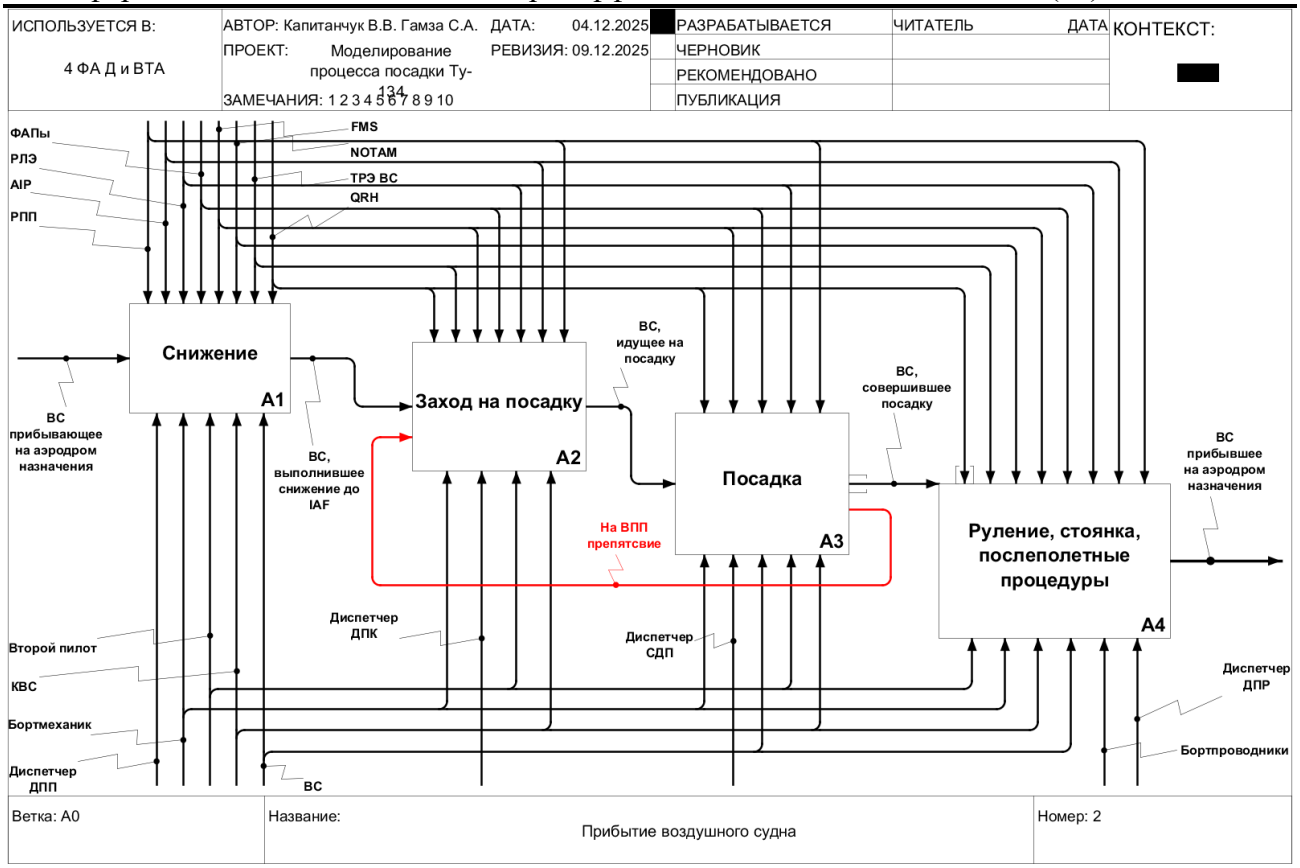

Рисунок 2 – Анализ инцидента по модели

Разработка модели процесса посадки ВС Ту-134 в ARIS EXPRESS.

Процесс посадки самолёта Ту-134 в аэропорту включает в себя несколько этапов:

1. Планирование (снижение);
2. Выравнивание;
3. Выдерживание;
4. Пробег.

Согласно РЛЭ и ТРЭ ВС Ту-134 после приземления в момент касания ВПП выпустить интерцепторы, опустить переднюю опору и включить реверс тяги. Торможение, как правило, начинать на скорости не более 250 км/ч. На скорости 110 км/ч выключить реверс. При необходимости разрешается использовать реверс тяги вплоть до полной остановки самолёта. К концу пробега убрать закрылки и интерцепторы. Непосредственно после приземления развернуть самолёт вдоль оси ВПП и выдерживать направление на пробеге педалями. На рисунке 3 изображён фрагмент модели процесса посадки Ту-134.

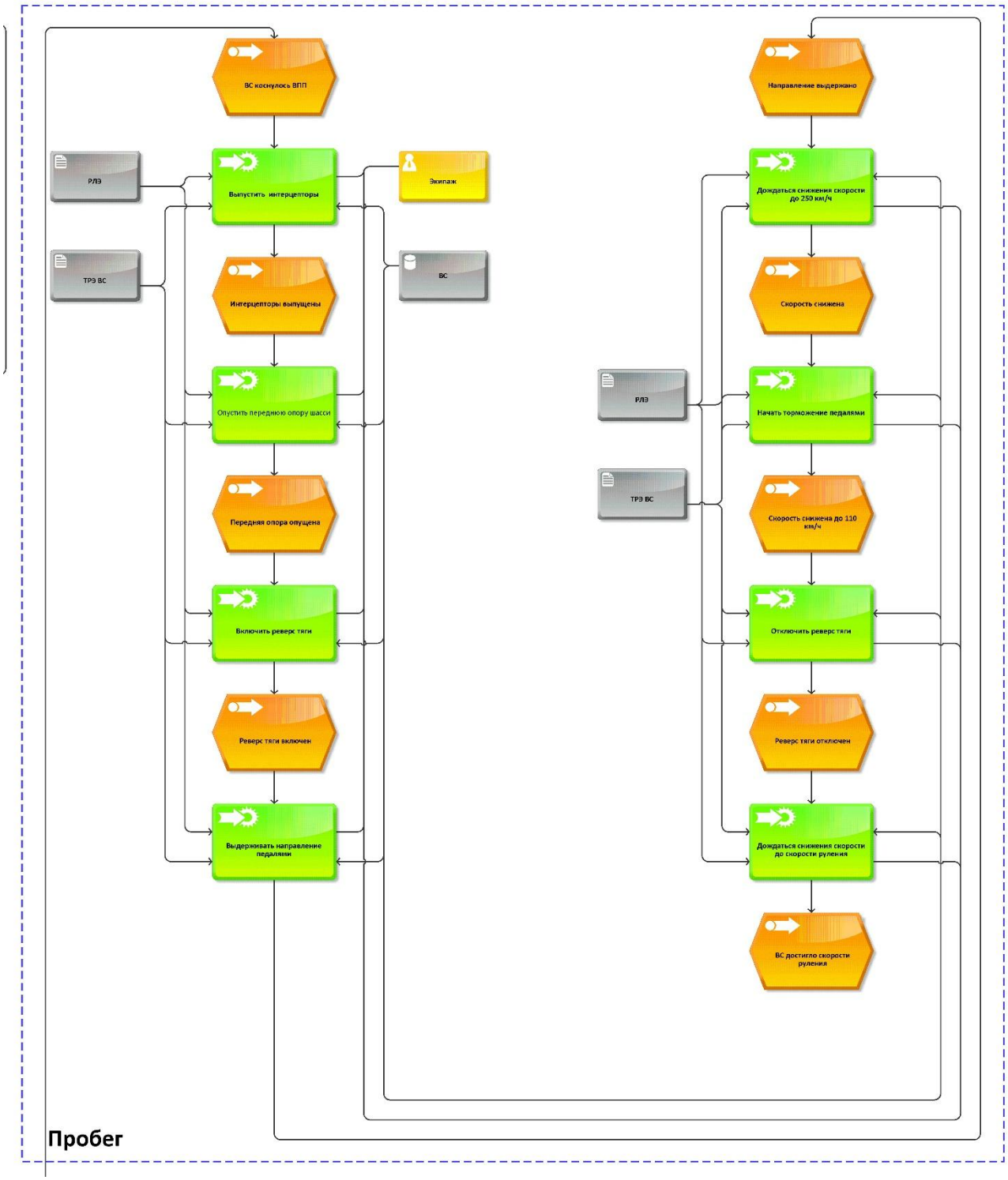

Рисунок 3 – Фрагмент модели процесса посадки Ту-134

Проведённое моделирование с использованием программы Ramus Educational и ARIS Express позволило исследовать процесс посадки воздушного судна на нескольких уровнях детализации. Ramus Educational продемонстрировал эффективность при построении укрупнённых схем, отражающих общую логику последовательности операций. В свою очередь, ARIS Express обеспечил визуальную возможность более глубокой аналитической проработки этапов процесса и выявления функциональных взаимосвязей между элементами системы. Проведенная апробация моделей, разработанных с использованием различных

программных средств — Ramus Educational и Aris Express, — базировалась на реальных данных о процессе посадки воздушного судна Ту-134 в аэропорту Тюмень. Этот выбор не случаен, поскольку процесс посадки является одной из наиболее критически важных, сложных и многофакторных операций в гражданской авиации, требующей высокой координации и точности.

Под апробацией в научной практике понимается процедура проверки результатов исследования с целью определения их практической значимости и надёжности. Она может включать представление материалов на научных конференциях, публикацию в рецензируемых изданиях, получение экспертных отзывов и анализ фактических данных. В рамках данного исследования апробация модели осуществлялась путём рассмотрения реального авиационного события, произошедшего с воздушным судном Ту-134 в аэропорту Тюмени 31 мая 1979 года, что позволило оценить применимость разработанных моделей в условиях реальной эксплуатационной ситуации.

Этот инцидент произошел во время выполнения рутинной, но ответственной учебной миссии. Заместитель командира авиаэскадрильи, опытный пилот, осуществлял полеты в простых метеорологических условиях (ПМУ), руководя программой ввода в строй двух молодых стажеров. Целью тренировок было закрепление навыков взлета и посадки. Однако в ходе выполнения ряда взлетов с последующей уборкой шасси и особо требовательных посадок на повышенной скорости с отклоненными на 10 и 20 градусов закрылками (что является нестандартной конфигурацией для приземления и может быть частью специфической тренировки или отработкой аварийных процедур), колеса самолета подверглись чрезмерным термическим и механическим нагрузкам (Рисунок 4). [10-11,15-16]

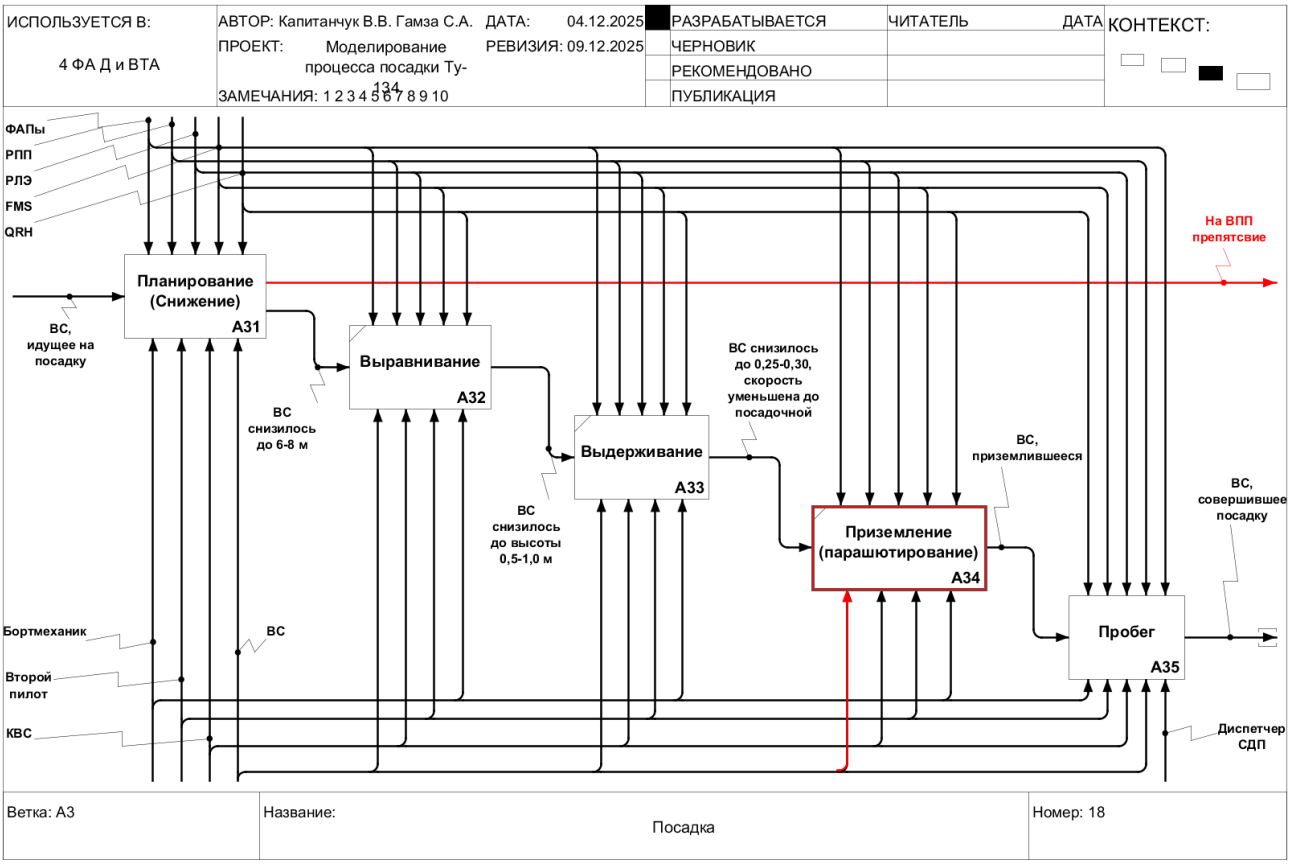

Рисунок 4 – Процесс посадки Ту-134

Постоянное интенсивное торможение на повышенных скоростях между последовательными касаниями взлетно-посадочной полосы привело к критическому перегреву шасси. Наиболее критический момент наступил после уборки шасси: поврежденная тележка, с горячими остатками разрушенного колеса и вытекающей гидрожидкостью, была втянута в тесное пространство левой гондолы двигателя. Контакт раскаленных фрагментов, либо искр, с вытекающей под давлением жидкостью мгновенно привел к возникновению пожара в левой гондоле. Дальнейшее развитие событий было усугублено неоперативностью и крайне слабой согласованностью действий служб, обеспечивающих полеты. Это указывает на системный сбой в аварийном реагировании: задержки в оповещении, нечеткие команды, возможно, недостаточная подготовка наземных расчетов или отсутствие четкого плана действий в подобной нештатной ситуации. В то время как пилоты боролись с пожаром в воздухе, наземные службы не смогли быстро и адекватно отреагировать, что позволило возгоранию развиться. В результате этой цепи событий — от специфического тренировочного режима до отказа техники и, что критично, неэффективного реагирования на земле — самолет получил катастрофические повреждения, которые сделали его непригодным для дальнейшей эксплуатации и привели к его окончательному списанию. Этот инцидент стал суровым уроком о взаимосвязи между технической исправностью, процедурами выполнения полетов и готовностью всех служб к нештатным ситуациям.

Заключение

В результате выполненных работ и проведённого анализа можно сделать следующие выводы:

Построение функциональных и причинно-следственных моделей в среде RAMUS обеспечило формализованное представление последовательности событий, распределения обязанностей и критических точек в системе управления полётом. Дополнительная визуализация процессов в ARIS позволила уточнить взаимодействие элементов системы, выявить структурные несоответствия и повысить наглядность представления данных.

Результаты анализа авиационного происшествия подтверждают, что сочетание человеческого фактора, организационных недостатков и отклонений от требований нормативных документов сыграло ключевую роль в развитии аварийной ситуации. Применение методик моделирования и визуализации продемонстрировало высокую эффективность в выявлении скрытых причин и системных ошибок.

Проведённый анализ авиационного происшествия с воздушным судном Ту-134 в Тамбове позволил комплексно оценить совокупность факторов, приведших к аварийной ситуации. Изучение нормативно-правовой базы выявило ключевые требования к организации полётов, взаимодействию служб и поддержанию уровня безопасности, а также дало возможность сопоставить фактические действия участников полёта с установленными стандартами.

Таким образом, комплексный подход — включающий изучение нормативной базы, построение моделей в RAMUS, визуализацию процессов в ARIS и детальный анализ АП — позволяет не только всесторонне исследовать обстоятельства происшествия, но и формировать рекомендации, направленные на повышение уровня безопасности полётов и предотвращение аналогичных событий в будущем.

Список литературы

1. В.П. Бехтир, Н.Е. Ковалев. Практическая аэродинамика самолёта Ту-134 / В.П. Бехтир, Н.Е. Ковалев – М. : Транспорт, 1984 г. – 260 с.
2. AVIC, Commercial Aircraft / AVIC – Режим доступа: https://www.avic.com/en/civilaviation/commercialaircraft/ – Загл. с экрана.
3. Самолёт Ту-134: руководство по лётной эксплуатации – Введ. 29.07.1996. – М. : МинТранс РФ – 496 с.
4. Лапшин В. С. Моделирование бизнес-процессов : учеб. пособие / В. С. Лапшин, Ю. В. Ямашкин. – Саранск : Изд-во Мордов. ун-та, 2018. – 124 с.
5. Рындин С. В. Методы и средства моделирования бизнес-процессов: методология ARIS : учеб.-метод. пособие / С. В. Рындина. – Пенза : Изд-во ПГУ, 2018. – 52 с.
6. Кара-Ушанов В. Ю. Функционально-структурное моделирование в системе RAMUS EDUCATIONAL / В. Ю. Кара-Ушанов – Екатеринбург, 2019. – 67 с.
7. Капитанчук В. В. Информационные технологии в управлении качеством и защита информации. Разработка функциональных моделей в среде Ramus Educational : практикум / В. В. Капитанчук. – Ульяновск : УВАУ ГА(И), 2024. – 60 с.
8. Об утверждении ФАП «Организация воздушного движения в РФ» : Приказ Минтранса РФ от 25.11.2011 г. №293.
9. Белякова А. Ю. Учебно-метод. пособие для самост. работы студентов по дисциплине «Управление информационными системами». Направление подготовки 09.03.03 Прикладная информатика. / А. Ю. Белякова. – Молодёжный: Изд-во Иркутский ГАУ, 2020. – 62 с.
10. Капитанчук В. В. Моделирование процессов в среде ARIS Express : метод. указания по выполнению практ. работ по дисциплине «Информационные технологии в управлении качеством и защита информации» / В. В. Капитанчук. – Ульяновск : УВАУ ГА(И), 2015. – 26 с.
11. Моделирование процесса устранения нарушений регулярности полетов в сбойных ситуациях Капитанчук В.В., Трофимов П.С. В сборнике: Международном журнале информационных технологий и энергоэффективности. УИ ГА Ульяновск, 2024. С. 23-32
12. Резник С.Д. Апробация и внедрение результатов диссертационного исследования: учеб.-метод. пособие для аспирантов / С.Д. Резник, О.А. Сазыкина. – Пенза: ПГУАС, 2014. – 28 с.
13. Постановление Правительства Российской Федерации (РФ) от 11.03.2010 г. №138 «Об утверждении Федеральных авиационных правил (ФАП) использования воздушного пространства РФ»;
14. Моделирование процесса действий пассажира для совершения рейса. Капитанчук В.В. В сборнике: Траектории взаимодействия в развитии цифровых навыков. Материалы всероссийской очной научно-практической конференции. УлГПУ Ульяновск, 2022. С. 36-39.
15. Разработка модели действий лица, вынашивающего преступные замыслы. Капитанчук В.В., Чамкаева К.С.В сборнике: Образование и информационная культура: теория и практика. материалы Всероссийской заочной научно-практической конференции. 2016. С. 39-42.

16. Моделирование процессов предполетного досмотра воздушного судна в аэропорту ульяновск. Капитанчук В.В., Калвайтис М.В. В сборнике: Информационные технологии в образовании. Материалы Международной заочной научно-практической конференции. Ульяновский государственный педагогический университет имени И.Н. Ульянова. 2015. С. 68-71
17. Моделирование процессов предполетного досмотра грузов в аэропорту ульяновск. Капитанчук В.В., Манзурина И.В. В сборнике: Информационные технологии в образовании. Материалы Международной заочной научно-практической конференции. Ульяновский государственный педагогический университет имени И.Н. Ульянова. 2015. С. 71-76.

References

1. V.P. Bekhtir, N.E. Kovalev. Practical Aerodynamics of the Tu-134 Aircraft / V.P. Bekhtir, N.E. Kovalev – Moscow: Transport, 1984. – 260 p.
2. AVIC, Commercial Aircraft / AVIC – Access mode: https://www.avic.com/en/civilaviation/commercialaircraft/ – Title from the screen.
3. Tu-134 aircraft: flight operation manual – Introduction. 29.07.1996. – Moscow: Ministry of Transport of the Russian Federation – 496 p.
4. Lapshin, V. S. Business Process Modeling: Textbook. / V. S. Lapshin, Yu. V. Yamashkin. – Saransk: Mordov. Univ. Press, 2018. – 124 p.
5. Ryndin, S. V. Methods and Tools for Business Process Modeling: ARIS Methodology: Textbook.-method. / S. V. Ryndina. – Penza : PSU Publishing House, 2018. – 52 p.
6. Kara-Ushanov V. Yu. Functional and structural modeling in the RAMUS EDUCATIONAL system / V. Yu. Kara-Ushanov – Yekaterinburg, 2019. – 67 p.
7. Kapitanchuk V. V. Information technologies in quality management and information protection. Development of functional models in the Ramus Educational environment : a workshop / V. V. Kapitanchuk. Ulyanovsk : UVAU GA(I), 2024. 60 p.
8. On the approval of the FAP "Organization of air traffic in the Russian Federation" : Order of the Ministry of Transport of the Russian Federation dated 25.11.2011 No. 293.
9. Belyakova A. Y. Educational method. self-help guide. students' work on the discipline "Information Systems Management". Field of study 09.03.03 Applied Informatics. / A. Yu. Belyakova. – Molodezhny: Irkutsk State Agrarian University Publishing House.
10. Kapitanchuk V. V. Process modeling in the ARIS Express environment : a method. instructions for the implementation of the practice. works on the discipline "Information technologies in quality management and information protection" / V. V. Kapitanchuk. Ulyanovsk : UVAU GA(I), 2015. 26 p.
11. Modeling of the process of eliminating violations of flight regularity in emergency situations Kapitanchuk V.V., Trofimov P.S. In the collection: International Journal of Information Technology and Energy Efficiency. UI GA Ulyanovsk, 2024. P. 23-32
12. Reznik S.D. Approbation and implementation of the results of the dissertation research: textbook.-method. manual for postgraduate students / S.D. Reznik, O.A. Sazykina. – Penza: PGUAS, 2014. – 28 p.

13. Resolution of the Government of the Russian Federation (RF) dated 11.03.2010 No. 138 "On Approval of the Federal Aviation Regulations (FAA) for the Use of the Airspace of the Russian Federation";
14. Simulation of the passenger's actions for making a flight. Kapitanchuk V.V. In the collection: Trajectories of interaction in the development of digital skills. Materials of the All-Russian intramural scientific and practical conference. UlGPU Ulyanovsk, 2022. pp. 36-39.
15. Development of a model of actions of a person harboring criminal intentions. Kapitanchuk V.V., Chamkaeva K.S. In the collection: Education and Information Culture: Theory and Practice. Materials of the All-Russian Correspondence Scientific and Practical Conference. 2016. Pp. 39-42.
16. Modeling the Processes of Pre-Flight Inspection of an Aircraft at the Ulyanovsk Airport. Kapitanchuk V.V., Kalvaitis M.V. In the collection: Information Technologies in Education. Materials of the International Correspondence Scientific and Practical Conference. I.N. Ulyanov Ulyanovsk State Pedagogical University. 2015. P. 68-71
17. Modeling of pre-flight cargo inspection processes at the Ulyanovsk airport. Kapitanchuk V.V., Manzurina I.V. In the collection: Information technology in education. Proceedings of the International correspondence scientific and practical conference. Ulyanovsk State Pedagogical University named after I.N. Ulyanov. 2015. Pp. 71-76.

Павлов К.К. Сравнительный анализ эффективности ZTNA и SASE для защиты распределённых удалённых рабочих мест // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 197–201

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ZTNA И SASE ДЛЯ ЗАЩИТЫ РАСПРЕДЕЛЁННЫХ УДАЛЁННЫХ РАБОЧИХ МЕСТ

Павлов К.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1),e-mail: kkpavlov2004@gmail.com

В работе проводится сравнительный анализ двух современных моделей кибербезопасности – Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE), используемых для защиты распределённых удалённых рабочих мест. Рассматриваются принципы функционирования, преимущества и ограничения каждой технологии, а также их применимость в условиях возросшей цифровой мобильности сотрудников. Автор подчёркивает ключевые различия между подходами «нулевого доверия» и конвергентной облачной безопасности, определяя оптимальные сценарии использования ZTNA и SASE для повышения уровня защиты организации.

Ключевые слова: ZTNA, SASE, удалённые рабочие места, безопасность сети, виртуализация, облачные сервисы, zero trust, корпоративная кибербезопасность.

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF ZTNA AND SASE FOR THE PROTECTION OF DISTRIBUTED REMOTE WORKPLACES

Pavlov K.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1),, e-mail: kkpavlov2004@gmail.com

This paper presents a comparative analysis of two modern cybersecurity models – Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) – used to protect distributed remote workplaces. The study examines the operational principles, advantages, and limitations of each approach, with particular attention to their relevance in the context of increasing employee mobility and decentralization of corporate infrastructures. Key distinctions between the zero-trust paradigm and converged cloud-based security are highlighted. The paper identifies optimal use cases for both ZTNA and SASE and outlines how these technologies enhance organizational security and resilience in remote-work environments.

Keywords: ZTNA, SASE, remote workplaces, network security, cloud security, zero trust, corporate cybersecurity.vulnerabilities, connection security.

Рост числа распределённых команд, массовый переход на удалённую работу и расширение использования облачных сервисов приводят к фундаментальным изменениям в организации корпоративной сетевой инфраструктуры. Такой переход невозможен без глубокого изменения подходов к нормативному регулированию облачной среды, поскольку, как отмечается в исследованиях, «для широкого и эффективного внедрения технологий нужны методические и нормативные документы, разъясняющие правовые рамки применения этих технологий, имеющиеся проблемы и риски и способы их минимизации» [7]. На

протяжении десятилетий основным способом удалённого безопасного подключения сотрудников оставались виртуальные частные сети (VPN). Однако VPN создают прямой доступ пользователя ко внутренней сети, что приводит к риску бокового перемещения злоумышленника в случае компрометации устройства или учётной записи. Кроме того, VPN не масштабируются под сотни и тысячи распределённых пользователей, требуют значительных аппаратных ресурсов и плохо адаптируются к облачной архитектуре [1]. В ответ на эти вызовы появились подходы, основанные на распределённой безопасности и принципе «ноль доверия»: Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE). Оба решения предназначены для замены или расширения функциональности VPN, но отличаются масштабом, архитектурой и задачами. Сегодня они становятся ключевыми технологиями при защите гибридных и удалённых рабочих мест. В этих условиях всё более широкое распространение получают архитектуры Zero Trust Network Access (ZTNA) и Secure Access Service Edge (SASE), которые предлагают альтернативу традиционным VPN, перераспределяя функции аутентификации, контроля доступа и анализа трафика между облаком и конечными устройствами [2].

ZTNA опирается на концепцию Zero Trust – модель, полностью отвергающую предположение о безопасном внутреннем периметре. Согласно Zero Trust, каждая попытка доступа должна быть проверена, независимо от источника соединения. Пользователь, устройство, сеть и контекст – всё должно пройти повторную аутентификацию и оценку риска [3].

Рассмотрим основные прицепы ZTNA:

1. Нулевое доверия по умолчанию: доступ не предоставляется автоматически, даже если пользователь уже находится внутри сети. Каждый запрос – отдельная проверка.

2. Минимизация прав доступа: пользователь получает доступ только к одному конкретному приложению, а не к целой сети. Это снижает вероятность lateral movement – бокового перемещения злоумышленников [4].

3. Непрерывная проверка контекста:

ZTNA анализирует:

- состояние устройства (patch level, антивирус, наличие шифрования),
- геолокацию,
- поведенческие факторы,
- сетевые аномалии [5].

4. Отсутствие прямых сетевых соединений: пользователь не подключается к корпоративной сети, а получает туннель только к конкретному приложению.

В преимущества данного подхода входит:

- высокая изоляция приложений;
- значительное снижение площади атаки;
- независимость от сетевой инфраструктуры;
- удобное масштабирование на небольшие команды;
- возможность быстрой интеграции с облаком.

Ограничения такого подхода:

- сложная миграция при наличии большого количества устаревших приложений;
- необходимость перестройки IAM и политики доступа;

- отсутствие единых инструментов сетевой безопасности.

ZTNA – является решение для организаций, которым требуется тонко настроенный, строго сегментированный доступ к критически важным ресурсам, особенно в средах с ограниченным числом удалённых пользователей.

SASE представляет собой более широкую архитектуру, чем ZTNA. Это не отдельный инструмент, а целостная экосистема безопасности, которая переносит сетевые и защитные функции в облако. SASE сочетает:

- SD-WAN,
- облачный межсетевой экран (FWaaS),
- защищённый веб-шлюз (SWG),
- брокер безопасности облачного доступа (CASB),
- встроенный механизм ZTNA,
- инспекцию и оптимизацию трафика [2].

Особенности CASE являются:

1. **Объединение сетевых и защитных функций в облаке**

Вся фильтрация и проверка трафика происходит в распределённых облачных точках присутствия, что снижает нагрузку на локальные ресурсы.

2. **Единая политика безопасности для всех пользователей**

Независимо от того, где находится сотрудник – в филиале, дома или в другом регионе.

3. **Широкий спектр интеграций**

SASE включает инструменты анализа угроз, DLP, защиту облачных сервисов, контроль теневых ИТ.

4. **Масштабируемость и производительность**

Поддержка тысяч пользователей по всему миру без необходимости увеличения мощности локальных дата-центров [5].

Преимущества и ограничения CASE

Преимущества:

- централизованное управление безопасностью;
- широкая функциональность «всё в одном»;
- улучшенная производительность благодаря глобальной оптимизации трафика;
- удобство для крупного бизнеса и распределённых филиальных сетей.

Ограничения:

- зависимость от качества интернет-соединения;
- необходимость готовности к активному использованию облачных сервисов;
- возможная сложность миграции при переходе от локальных решений.

SASE выступает идеальным вариантом для компаний, стремящихся к глобальной унификации управления безопасностью и снижению операционных затрат.

ZTNA и SASE часто воспринимают как альтернативы, но это некорректно. ZTNA – элементарная составляющая SASE, выполняющая узкую задачу контроля доступа. В то время как SASE расширяет её возможностями сетевой доставки и глубокой инспекции трафика (Таблица 1).

Таблица 1 – Сравнение подходов ZTNA и CASE

Критерий	**ZTNA**	**SASE**
Масштаб	Локальный, точечная защита приложений	Глобальный, защита всей сети
Подход	Zero Trust для доступа	Конвергентная безопасность и сеть
Основные функции	Контроль доступа, сегментация	FWaaS, SWG, CASB, SD-WAN, ZTNA
Инфраструктура	Чаще используется как дополнение	Полная облачная архитектура
Производительность	Зависит от конкретного сервиса	Оптимизируется через PoP
Применимость	Малый и средний бизнес	Средний и крупный бизнес

Рассмотрим практические сценарии применения подходов в рамках организация. Сценарий 1: Защита критически важных внутренних приложений. Компания может использовать ZTNA для обеспечения доступа только к внутренним ERP/CRM, огранивич боковое движение и минимизировав риски проникновения.

Сценарий 2: глобальная распределённая инфраструктура для корпораций с филиалами в разных странах оптимален SASE:

- единая политика;
- фильтрация трафика во всех точках присутствия;
- снижение нагрузки на корпоративные ЦОДы.

Сценарий 3: гибридная модель

Средний бизнес часто сочетает оба подхода:

- ZTNA — для внутренних приложений;
- SASE — для облачных ресурсов и интернета.

Такой подход позволяет адаптировать стратегию безопасности под разнообразные бизнес-процессы.

Текущий тренды внедрения ZTNA и CASE

Согласно аналитике ведущих компаний кибербезопасности:

- крупный бизнес чаще выбирает **SASE** благодаря масштабируемости и унификации процессов;
- средний бизнес комбинирует решения;
- малые компании предпочитают **ZTNA** как более доступное и быстрое в развёртывании [6].

ZTNA – является важным подходом Zero Trust, который становится обязательной частью корпоративной политики безопасности.

SASE превращается в облачную платформу, способную полностью заменить локальные средства безопасности и сетевую инфраструктуру.

Аналитические отчёты ведущих компаний в области кибербезопасности показывают, что крупные предприятия чаще выбирают SASE для глобальной масштабируемости и возможности централизованного управления распределёнными командами [6]. Средний бизнес стремится сочетать оба подхода, применяя ZTNA для защиты критичных внутренних ресурсов и SASE – для контроля внешних и облачных сервисов. Малые компании чаще внедряют ZTNA как более доступное и легко развёртываемое решение. Такое сочетание позволяет формировать гибкую модель безопасности, адаптированную к специфике организации.

ZTNA и SASE представляют собой эволюцию методов защиты распределённых рабочих мест. ZTNA обеспечивает строгую минимизацию доверия и эффективную сегментацию доступа, предотвращая распространение угроз в случае компрометации одного пользователя или устройства [4]. SASE предлагает более широкую архитектуру, в которой объединены сетевые и защитные функции, что создаёт единую облачную платформу для контроля трафика, предотвращения угроз и управления доступом [5]. В условиях возросшей цифровой мобильности именно совместное применение ZTNA и SASE обеспечивает наиболее высокий уровень безопасности и устойчивость корпоративной инфраструктуры к современным киберугрозам [6].

Список литературы

1. Бирих Э.В., Травкина Е.А. Сравнительный анализ подходов к безопасности технологий VPN и ZTNA // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом (Сборник материалов (тезисов) 53-й Международной конференции, Москва, 2024), 2024. – С. 72-74.
2. Gartner. The Future of Network Security Is in the Cloud. 2023.
3. John Kindervag. Zero Trust Architecture. Forrester Research, 2020.
4. NIST SP 800-207. Zero Trust Architecture. 2021.
5. Cisco. SASE and ZTNA Security Overview. 2023.
6. Palo Alto Networks. Global Remote Work Security Report, 2024.

References

1. Birikh E.V., Travkina E.A. Comparative Analysis of Approaches to VPN and ZTNA Security Technologies // Mobile Business: Prospects for the Development and Implementation of Radio Communication Systems in Russia and Abroad (Collection of Materials (Abstracts) of the 53rd International Conference, Moscow, 2024), 2024. – pp. 72-74.
2. Gartner. The Future of Network Security Is in the Cloud. 2023.
3. John Kindervag. Zero Trust Architecture. Forrester Research, 2020.
4. NIST SP 800-207. Zero Trust Architecture. 2021.
5. Cisco. SASE and ZTNA Security Overview. 2023.
6. Palo Alto Networks. Global Remote Work Security Report, 2024.

Исламова А.Р. Методы генерации API-автотестов на основе нейросетей: современное состояние, проблемы и перспективы// Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 202–205

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.4

МЕТОДЫ ГЕНЕРАЦИИ API-АВТОТЕСТОВ НА ОСНОВЕ НЕЙРОСЕТЕЙ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Исламова А.Р.
ФГБОУ ВО «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ», Уфа, Россия (450044, г. Уфа, ул. Космонавтов, 1.), e-mail: alsou.islamova@mail.ru

В статье представлен аналитический обзор современных подходов к автоматической генерации API-автотестов с применением технологий искусственного интеллекта, в частности больших языковых моделей (LLM). Рассмотрена эволюция методов от статического анализа формальных спецификаций до интеллектуальной обработки естественно-языковых требований. Проведена систематизация существующих решений, выделены три ключевых направления: генерация на основе OpenAPI-спецификаций, на основе текстовых требований и комбинированные подходы. Для каждого направления проанализированы принципы работы, преимущества и фундаментальные ограничения. Особое внимание уделено проблеме разрыва между синтаксической корректностью генерируемого кода и его семантической релевантностью бизнес-логике. В контексте цифровой трансформации критически важных отраслей, таких как нефтегазовая, обоснована необходимость разработки новых гибридных методологий. Определены перспективные векторы исследований, включая улучшение контекстного анализа, создание специализированных оценочных метрик и глубокую интеграцию в CI/CD-конвейеры.

Ключевые слова: обзор, автоматизация тестирования, генерация тестов, API, нейронные сети, большие языковые модели, LLM, OpenAPI, искусственный интеллект.

API AUTOTEST GENERATION METHODS BASED ON NEURAL NETWORKS: CURRENT STATUS, PROBLEMS AND PROSPECTS

Islamova A.R.
UFA STATE PETROLEUM TECHNOLOGICAL UNIVERSITY, Ufa, Russia (450044, Ufa, Kosmonavtov St., 1), e-mail: alsou.islamova@mail.ru

This article presents an analytical review of modern approaches to the automatic generation of API autotests using artificial intelligence technologies, in particular, large-scale language models (LLM). The evolution of these methods, from static analysis of formal specifications to intelligent processing of natural language requirements, is examined. A systematization of existing solutions is provided, highlighting three key areas: generation based on OpenAPI specifications, generation based on textual requirements, and combined approaches. The operating principles, advantages, and fundamental limitations of each approach are analyzed. Particular attention is paid to the gap between the syntactic correctness of generated code and its semantic relevance to business logic. In the context of the digital transformation of critical industries such as oil and gas, the need to develop new hybrid methodologies is substantiated. Promising research areas are identified, including improved contextual analysis, the creation of specialized evaluation metrics, and deep integration into CI/CD pipelines.

Keywords: review, test automation, test generation, API, neural networks, large language models, LLM, OpenAPI, artificial intelligence.

Введение

Динамичное развитие микросервисной архитектуры и практик непрерывной интеграции и поставки (CI/CD) превратило REST API в кровеносную систему современных цифровых экосистем. Обеспечение их надежности является критически важной задачей, от которой зависят ключевые бизнес-процессы, особенно в таких отраслях, как финансы, телекоммуникации и нефтегазовый сектор [1]. Традиционный процесс создания и поддержки сотен автотестов вручную стал узким местом, тормозящим скорость разработки и повышающим риски.

Прогресс в области искусственного интеллекта, особенно появление мощных больших языковых моделей (LLM), открыл новые горизонты для автоматизации этой рутины. Возникло отдельное научно-практическое направление, посвященное генерации исполняемого тестового кода на основе различных артефактов. Целью данного обзора является систематизация современных нейросетевых методов генерации API-автотестов, анализ их эволюции, сравнительная характеристика и выявление актуальных проблем и перспектив.

1. Классификация и анализ существующих методов

Современные подходы к генерации тестового кода с использованием ИИ можно классифицировать по типу и глубине используемого входного контекста.

1.1. Генерация на основе статического анализа OpenAPI-спецификации

Данный метод, являющийся исторически первым, основан на автоматизированном анализе структурированных описаний API, преимущественно в формате OpenAPI/Swagger. Инструменты и скрипты, включающие в себя LLM, специализированные на коде (Codex, CodeLlama), извлекают из спецификации эндпоинты, методы HTTP, параметры и схемы данных. На этой основе генерируются базовые позитивные тесты (проверка ответа 200 OK и соответствия JSON-схеме) и простейшие негативные (проверка на обязательные поля, невалидные типы данных) [2]. Основные преимущества: высокая скорость, полное синтаксическое покрытие API-контракта, гарантированная техническая корректность генерируемого кода, что позволяет легко встраивать процесс в CI/CD. Критический недостаток: полное игнорирование семантики, бизнес-правил и пользовательских сценариев. Тесты, созданные этим методом, не способны проверить корректность цепочки вызовов (например, «создать заявку → подтвердить её → отправить в работу») или логические условия («подтверждение заказа доступно только для пользователей с положительным балансом»).

1.2. Генерация на основе текстовых требований и User Stories

В этом подходе на вход модели (LLM общего назначения, такой как GPT-4 или Claude) подаются неструктурированные артефакты: пользовательские истории, функциональные требования, описания тест-кейсов на естественном языке [3, 4]. Модель, понимая контекст, генерирует тестовые сценарии, отражающие пользовательское восприятие системы. Преимущество: потенциально высокий уровень абстракции и привязка к реальным бизнес-потребностям, возможность выявления логических сценариев, неочевидных из формальной спецификации. Существенные недостатки: высокая вероятность «галлюцинаций» — модель может изобрести несуществующие эндпоинты, методы или параметры. Полученный код часто является концептуально верным, но технически некорректным, требуя глубокой и трудоемкой доработки инженером. Это снижает практическую применимость подхода в промышленной разработке.

1.3. Комбинированные (гибридные) методы

Данные методы представляют собой наиболее перспективное и практически ориентированное направление. Они пытаются преодолеть разрыв между синтаксисом и семантикой путем совместного использования разных типов входных данных [2, 3]. Как правило, OpenAPI-спецификация выступает в роли «источника истины» для обеспечения технической корректности генерируемого кода (правильные URL, методы, заголовки). Дополнительные текстовые контексты (поля description и summary внутри самой спецификации, связанные документы Confluence, пользовательские истории) используются для обогащения тестов: подбора осмысленных тестовых данных, добавления базовых проверок бизнес-логики и простых негативных сценариев [5]. Хотя такие подходы повышают практическую ценность результата, они все еще ограничены: сложные сквозные (E2E) рабочие процессы, зависящие от состояния системы, остаются за пределами их возможностей.

2. Ключевые проблемы и вызовы

Основной проблемой области является семантический разрыв — несоответствие между синтаксически правильным и семантически осмысленным тестом. Существующие инструменты хорошо справляются с генерацией формально корректного кода, но создание тестов, адекватно проверяющих бизнес-логику, остается сложной задачей. Дополнительными вызовами являются зависимость от качества входных данных, отсутствие стандартизированных метрик для оценки релевантности тестов и сложности интеграции в реальные процессы разработки.

3. Перспективные направления исследований

В качестве перспективных направлений исследований можно выделить несколько векторов. Наиболее важным представляется развитие гибридных архитектур с глубоким контекстным анализом, способных учитывать не только формальную спецификацию, но и весь корпус проектной документации для понимания предметной области. Также актуальна задача генерации тестов для современных архитектур — асинхронных API, событийно-ориентированных систем и сложных многошаговых рабочих процессов. Отдельным направлением должна стать разработка специализированных оценочных метрик, учитывающих не только качество кода, но и функциональную релевантность и адекватность проверок.

Заключение

Обзор показал, что область генерации API-автотестов с помощью нейросетей активно развивается, но находится на переходном этапе. Существующие подходы демонстрируют либо техническую корректность, либо семантическую осмысленность, но не сочетают оба качества одновременно. Наиболее перспективным путем представляется создание интеллектуальных гибридных методологий, способных осуществлять глубокий контекстный анализ разнородных артефактов разработки. Успех в этом направлении позволит создать качественно новый уровень обеспечения надежности программных систем, что особенно востребовано в условиях цифровой трансформации критически важных отраслей экономики.

Список литературы

1. Dmitrievsky A. N., Eremin N. A., Filippova D. S., Safarova E. A. Digital oil and gas complex of Russia // On a new paradigm for the development of oil and gas geology: Materials of the International Scientific and Practical Conference. – Kazan: Ikhlas, 2020. – P. 26-29.

2. Хабибулин Д.М. Использование искусственного интеллекта и машинного обучения в автоматизации тестирования // Международный научный журнал «Инновационная наука». – 2024. - № 8-1. – С. 34-43.
3. Волынец И.Г. Роль AI в оптимизации процессов тестирования программного обеспечения // Universum: технические науки. – 2025. - № 4 (133). – С. 46-51.
4. Фатыхов А.И., Салтанаева Е.А. Использование искусственного интеллекта для автоматизации процесса тестирования в информационных системах // Международный научный журнал «ВЕСТНИК НАУКИ». – 2024 г. – № 5 (74). Том. 4. – С. 1556-1561.
5. Тулфоров Д. М. Автоматизация тестирования веб-приложения, используя классификатор типов элементов машинного обучения // Международный журнал гуманитарных и естественных наук. 2020. №6-2. С.63-68.

References

1. Dmitrievsky A. N., Eremin N. A., Filippova D. S., Safarova E. A. Digital oil and gas complex of Russia // On a new paradigm for the development of oil and gas geology: Proceedings of the International Scientific and Practical Conference. – Kazan: Ikhlas, 2020. – Pp. 26-29.
2. Khabibulin D. M. Using artificial intelligence and machine learning in testing automation // International scientific journal "Innovation Science". – 2024. - No. 8-1. – Pp. 34-43.
3. Volynets I. G. The role of AI in optimizing software testing processes // Universum: technical sciences. – 2025. - No. 4 (133). – Pp. 46-51.
4. Fatykhov A. I., Saltanaeva E. A. Using Artificial Intelligence to Automate the Testing Process in Information Systems // International Scientific Journal "BULLETIN OF SCIENCE". - 2024. - No. 5 (74). Vol. 4. - P. 1556-1561.
5. Tulforov D. M. Automation of Web Application Testing Using a Machine Learning Element Type Classifier // International Journal of Humanities and Natural Sciences. 2020. No. 6-2. P. 63-68.

Коровин Н.А., Коровин М.А., Коровин Н.А. Апскейл фотоматериалов с применением нейронных сетей // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 206–214

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.932.4

АПСКЕЙЛ ФОТОМАТЕРИАЛОВ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

[1]Коровин Н.А., [2]Коровин М.А., [3]Коровин Н.А.
ФГАОУ ВО СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ, Ставрополь, Россия (355017, Ставропольский край, город Ставрополь, ул Пушкина, д. 1 а), e-mail: [1]nikki01946@gmail.com, [2]bigsky5068@gmail.com, [3]nikki01945@gmail.com

В статье рассматриваются этапы развития технологий апскейлинга: от первых попыток улучшения телевизионного сигнала в 1980-х годах до появления методов суперразрешения (super-resolution) на базе глубокого обучения. Особое внимание уделено истории применения нейронных сетей для улучшения фотоматериалов, включая ключевые прорывы (SRCNN, VDSR, EDSR, ESRGAN и др.) и разнообразие подходов – свёрточные сети, резидуальные сети, генеративно-состязательные сети и трансформеры. Описаны принципы работы этих методов. Представлены примеры визуальных результатов до и после апскейлинга, а также схемы работы нейросетевых моделей. Наконец, обсуждаются основные области применения технологий апскейлинга (восстановление старых фотографий и видео, медицине, видеоиграх и др.), а также делаются выводы о значении этих достижений для индустрии обработки изображений.

Ключевые слова: апскейлинг; суперразрешение; повышение разрешения; обработка изображений; нейронные сети; глубокое обучение; свёрточная сеть; масштабирование изображений.

UPSCALE OF PHOTOGRAPHIC MATERIALS USING NEURAL NETWORKS

[1]Korovin N.A., [2]Korovin M.A., [3]Korovin N.A.
NORTH CAUCASUS FEDERAL UNIVERSITY, Stavropol, Russia (355017, Stavropol Territory, Stavropol, Pushkin St., 1a), e-mail: [1] nikki01946@gmail.com, [2] bigsky5068@gmail.com, [3] nikki01945@gmail.com

This article excuses the stages of development of upscaling technologies: from the first attempts to improve television signals in the 1980s to the advent of super-resolution methods powered by deep learning. Special attention is paid to the history of using neural networks to enhance photographic materials, including key breakthroughs (SRCNN, VDSR, EDSR, ESRGAN, etc.) and the variety of approaches – convolutional networks, residual networks, generative adversarial networks, and transformers. The principles of operation of these methods are described. Examples of visual results before and after upscaling are presented, as well as diagrams illustrating the workings of neural network models. Finally, key application areas of upscaling technology are discussed (restoration of old photos and videos, medicine, video games, etc.), and conclusions are drawn about the significance of these advances for the image processing industry.

Keywords: upscaling; super-resolution; image resolution enhancement; image processing; neural networks; deep learning; convolutional network; image scaling.

Апскейлинг (англ. upscaling) – это процесс увеличения разрешения или масштаба цифрового изображения (фотографии, видеокадра и т.д.) с целью улучшения его четкости и детализации. Иными словами, апскейлинг позволяет преобразовать исходный низкокачественный визуальный материал в более качественный за счет добавления недостающей информации. Современные алгоритмы способны достраивать изображение – добавлять отсутствующие пиксели таким образом, чтобы итоговое изображение выглядело максимально натурально и четко. Данная технология сегодня находит широкое применение:

от улучшения старых фильмов и фотографий до масштабирования графики видеоигр и повышения качества видео с камер наблюдения. Развитие методов апскейлинга стало неотъемлемой частью цифровой эпохи, позволяя сохранять высокий уровень детализации даже при работе с изначально низким разрешением контента [1]. В следующих разделах рассмотрим, как возник и развивался апскейлинг, и какую роль в его прогрессе сыграли нейронные сети.

Ранние методы апскейла появились в 1980–2000-е гг. Концепция повышения разрешения изображений зародилась еще в 1980-х годах как теория обработки сигналов [5]. Первые практические реализации апскейлинга были связаны с телевидением: для улучшения качества аналогового ТВ-сигнала применяли простейшие алгоритмы масштабирования, например линейную интерполяцию, что давало лишь незначительное повышение четкости без серьёзных искажений. Также разрабатывались методы комбинирования нескольких кадров одной сцены (множественная съемка) для извлечения дополнительных деталей – так называемое мультифреймовое суперразрешение, требовавшее сложной оценки движения между кадрами. Эти классические подходы были вычислительно затратны и чувствительны к шуму и неточному выравниванию изображений.

С развитием цифровых технологий в 1990-е годы апскейлинг значительно продвинулся. Появились более сложные математические модели обработки: от алгоритмов фильтрации и реставрации изображения до методов на основе статистических предположений (регуляризация) и фрактального увеличения разрешения. Произошёл переход от аналоговых средств улучшения картинки к цифровым, что позволило внедрять апскейлинг в DVD-плееры и телесигналы высокого разрешения. Например, начали применяться бикубическая интерполяция и другие усовершенствованные алгоритмы ресемплинга, которые учитывали больше соседних точек при расчете новых пикселей по сравнению с простым линейным масштабированием. Тем не менее все эти методы оставались ограничены тем, что они основывались на фиксированных правилах обработки пиксельных данных и не могли придумать новые детали, отсутствующие в оригинале [1].

Прорывом в области повышения качества изображений стали примерно-образные методы (example-based super-resolution). В 2003 году Уильям Фримен с коллегами предложили алгоритм, использующий обучающую выборку пар изображений низкого и высокого разрешения для улучшения качества. Их метод искал в базе фрагменты (патчи) изображений, сходные с участками увеличиваемого фото, и заменял их более детализированными фрагментами высокого разрешения. Этот подход на основе обученных примеров стал первым шагом к использованию обучаемых моделей в задаче апскейлинга вместо жестко запрограммированных правил. Появились алгоритмы, полагавшиеся на статистику больших наборов изображений, что позволило лучше восстанавливать текстуры и мелкие детали по сравнению с одной лишь интерполяцией. Тем не менее, вычислительно такие методы были сложны, а качество результата сильно зависело от репрезентативности базы образов.

Начало 2010-х ознаменовало новый этап: в обработке изображений получили развитие алгоритмы глубокого обучения, в частности свёрточные нейронные сети (Convolutional Neural Networks, CNN). Впечатляющий прогресс в смежных задачах компьютерного зрения натолкнул исследователей на мысль применить нейросети и для апскейлинга. Ключевая идея заключалась в том, чтобы обучить сеть восстанавливать изображение высокого разрешения по его низкоразрешенной версии, используя большие объемы данных. В 2014 году была

представлена первая модель глубокого обучения для суперразрешения – SRCNN (Super-Resolution CNN), предложенная Чао Дунгом и его коллегами. Несмотря на относительную простоту (всего три слоя), SRCNN смогла повысить качество увеличения изображений до уровня, значительно превосходящего традиционные методы интерполяции. Фактически, сеть научилась восстанавливать утраченные детали, опираясь на знание, приобретённое при обучении на большом наборе примеров. Успех SRCNN породил всплеск интереса к нейросетевому апскейлингу и стимулировал появление новых архитектур, ещё более совершенствующих результат [5].

Уже через пару лет глубина и сложность моделей выросли. В 2016 году была предложена очень глубокая свёрточная сеть VDSR (Very Deep Super Resolution) с 20 слоями, сумевшая достичь ещё большего прироста качества за счёт увеличения сети и введения резидуального обучения. В VDSR исходное изображение складывается с выходным сигналом сети, что позволяет ей учить только разницу (детали высокого частотного диапазона) между высоким и низким разрешением. Такой подход заметно упростил обучение глубоких сетей, устранив проблему затухающих градиентов, и улучшил точность восстановления мелких структур [6]. Далее последовали улучшенные архитектуры: в 2017 году – EDSR (Enhanced Deep SR), упростившая некоторые слои и убравшая ограничения нормализации для увеличения качества, а также модели с механизмами внимания. Параллельно были предприняты попытки сделать картинки визуально более реалистичными: вместо оптимизации только математических метрик ошибки исследователи начали применять генеративно-состязательные сети (GAN).

Одной из первых таких моделей стал SRGAN (2017 г.), в которой сеть-генератор училась создавать фотореалистичные детали, пытаясь обмануть сеть-дискриминатор, обученную отличать увеличенные изображения от настоящих высококачественных фотографий. Развивая эту идею, в 2018 году представлена модель ESRGAN (Enhanced SRGAN), которая еще лучше справлялась с восстановлением текстур – например, деталей кожи или травы – делая увеличенные изображения практически неотличимыми на глаз от оригинальных по резкости и нюансам. Одновременно продолжалось совершенствование прямых методов: увеличивалось количество слоев, вводились механизмы self-attention и другие улучшения архитектур.

В начале 2020-х годов в задаче суперразрешения стали применять и трансформерные нейросети – изначально разработанные для задач NLP модели внимания оказались эффективны и для обработки изображений. С их помощью удаётся учитывать дальние связи в изображении и еще лучше вписывать мелкие детали в общий контекст (примеры – модели типа IPT, SwinIR и др., применяемые в отдельных доменах, например для медицинских снимков) [5].

Получается, что за последнее десятилетие методы апскейлинга с помощью искусственного интеллекта прошли путь от первых экспериментальных сетей к целому семейству мощных алгоритмов, способных выдавать потрясающие результаты. Ниже рассмотрим более подробно, какие виды нейросетевых подходов к повышению разрешения существуют и как они работают.

Нейросетевой апскейлинг имеет различия по типам и принципам.

Single Image vs. Multi-Image – большинство современных нейросетевых методов ориентированы на повышение разрешения одного изображения – так называемое Single Image Super-Resolution (SISR). В этой задаче на вход подаётся одиночное фото низкого разрешения,

и сеть генерирует его высокоразрешенную версию. Однако есть и многокадровые варианты: видео-суперразрешение, где сеть обрабатывает последовательность кадров, учитывая информацию о движении, чтобы повысить чёткость видео без артефактов на стыках кадров. Например, такие алгоритмы используются при оцифровке и ремастеринге старых фильмов – каждый кадр улучшается, сохраняя плавность переходов между ними. Кроме того, существуют мультиспектральные и мультимодальные подходы, когда помимо обычного изображения нейросеть принимает дополнительную информацию (например, инфракрасный канал или карту глубины) для повышения качества – это позволяет добиваться лучшего результата за счёт комбинации разных данных, хотя такие методы применяются в узких областях (например, в спутниковой съемке).

Архитектуры на основе CNN – базой большинства решений для апскейлинга служат свёрточные нейронные сети. Простая архитектура типичной модели суперразрешения состоит из последовательности свёрточных слоёв, которые постепенно преобразуют размытое низкокачественное изображение в чёткое высококачественное. Рисунок 1 иллюстрирует принцип работы такой сети на примере оригинального алгоритма SRCNN.

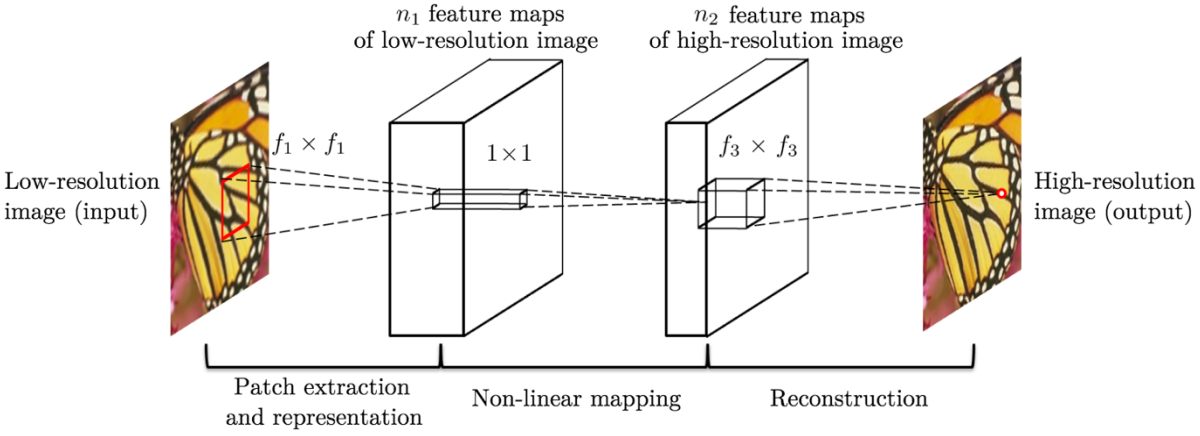

Рисунок 1 – Упрощенная схема работы сверточной нейросети SRCNN для повышения разрешения: входное низкого качества изображение пропускается через несколько слоёв (патч-экстракцию признаков, нелинейное преобразование и реконструкцию), в результате чего на выходе формируется изображение повышенного разрешения. Такая сеть обучается по большим наборам пар изображений (LR→HR) и способна восстанавливать утраченные детали.

Первый сверточный слой в подобных сетях выделяет из размытого изображения базовые черты (границы, текстуры) – фактически извлекает множество признаков низкого уровня. Последующие слои постепенно строят более сложные характеристики, сопоставляя полученные признаки с шаблонами, усвоенными из обучающей выборки. Наконец, финальный слой генерирует итоговое изображение более высокого разрешения, объединяя уточненные детали с общей структурой изображения. В примере SRCNN использовалось всего 3 слоя (9×9, 1×1 и 5×5 фильтры), однако даже такая небольшая сеть показала заметное улучшение по сравнению с интерполяцией. Более глубокие сети, например упомянутая VDSR из 20+ слоёв, идут дальше: они способны восстанавливать очень тонкие детали (например, текст или поры кожи на фото), но для их успешного обучения требовались дополнительные

приемы. Одно из ключевых усовершенствований – резидуальные (остаточные) связи. Добавление резидуальной связи означало, что сеть учит не всё изображение целиком, а лишь разницу между высоким и низким разрешением. На практике это позволило сосредоточить ресурсы на восстановлении мелких деталей, избегая повторного обучения тому, что уже присутствует во входном изображении (большие однородные области, низкочастотные компоненты и т.д.). Резидуальные архитектуры (ResNet) не только повысили качество, но и упростили обучение очень глубоких сетей, сделав возможным использование десятков и даже сотен слоёв без деградации градиента [6].

Генеративные модели и GAN. Одно из ограничений классических CNN-методов суперразрешения – стремление максимизировать показатели вроде PSNR (Peak Signal-to-Noise Ratio), что зачастую приводит к сглаживанию изображения. Сети, оптимизируемые по MSE (среднеквадратичной ошибке), восстанавливают «усреднённые» детали и могут давать слишком мягкую картинку. Чтобы получить более фотореалистичный результат, исследователи стали применять генеративные подходы. Наибольшую популярность получили генеративно-состязательные сети (GAN), состоящие из двух моделей: генератора, который пытается создать правдоподобное высококачественное изображение, и дискриминатора, задача которого – отличить сгенерированное изображение от настоящего высокого разрешения. В процессе совместного обучения генератор постепенно учится «обманывать» дискриминатор, добавляя всё более реалистичные высокочастотные детали. Применительно к апскейлингу такой подход впервые реализован в модели SRGAN (Ledig и др., 2017), а улучшен – в ESRGAN (Wang и др., 2018). Модель ESRGAN смогла генерировать текстуры (например, траву, волосы, кирпичную кладку) с высокой достоверностью, сильно приближая визуальное качество увеличенного изображения к оригиналу [5]. Однако GAN-методы имеют и недостатки: порой они могут «домысливать» детали слишком агрессивно, что приводит к появлению мелких артефактов или чересчур резких элементов, отсутствующих в оригинале. В практических приложениях часто комбинируют подходы – например, используют гибридные функции потерь: смесь перцептуальных критериев и традиционной MSE, чтобы добиться баланса между четкостью и достоверностью.

Ключевым фактором успеха глубинного апскейлинга стала доступность больших данных и возросшие вычислительные мощности. Нейросеть «учат» на паре изображений: исходном высококачественном и его искусственно уменьшенной копии (именно такую пару называют Teacher и Student изображениями). Огромные наборы таких пар (тысячи и миллионы изображений самых разных сцен) используются для тренировок – сеть постепенно подбирает параметры фильтров, минимизируя разницу между своим выходом и эталонным высоким разрешением. В процессе обучения нейронная сеть фактически запоминает паттерны реального мира: формы объектов, текстуры поверхностей, характерные шумы камеры и т.д. Например, видя тысячи портретов, сеть научается достраивать резкие глаза и ресницы даже на размытой фотографии, а анализируя пейзажи – узнаёт, как выглядит листва или трава при большом увеличении. В результате современный алгоритм апскейлинга – это не просто математическая интерполяция, а сложная модель, обладающая обобщёнными знаниями о разных типах изображений. Тем не менее, важно понимать ограничения: нейросеть не «угадывает» реальные отсутствующие детали, а генерирует правдоподобные детали по аналогии с тем, что видела на обучающих данных. Поэтому иногда возникают ситуации, когда пользователи ошибочно принимают сгенерированную детализацию за настоящую – например,

улучшенное ИИ фото может казаться раскрывающим черты лица, которых нет на исходном размытом снимке [3]. В критичных приложениях (например, обработка снимков в криминалистике) этот фактор обязательно учитывается.

Рисунок 2 – Фотография Трампа, усиленная искусственным интеллектом, которая стала вирусной на фоне слухов о плохом здоровье

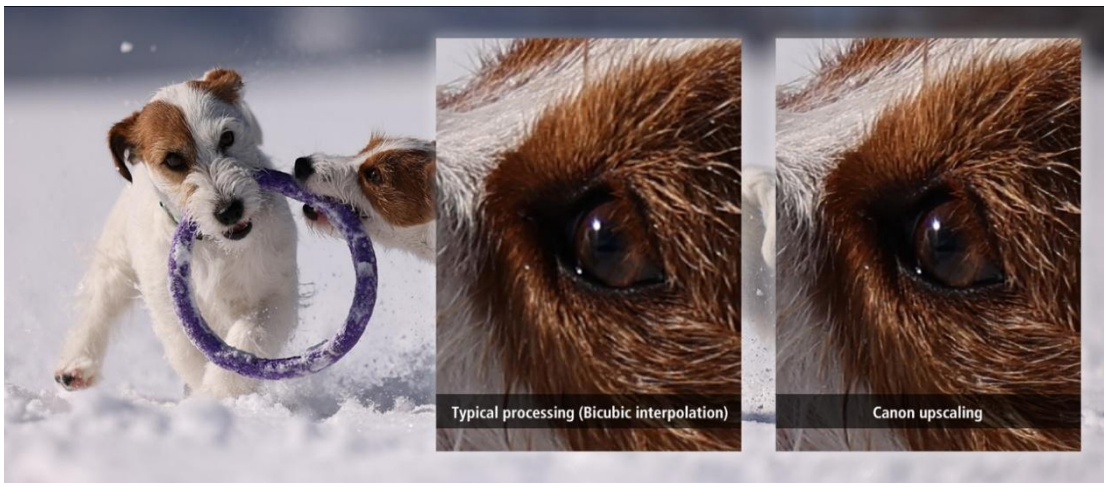

Рисунок 3 – Сравнение результатов традиционного бикубического увеличения (слева) и апскейлинга с помощью нейронной сети (справа) на фрагменте фотографии собаки. Видно, что нейросетевой метод сохраняет тонкую детализацию шерсти и границ лучше, тогда как при обычном масштабировании изображение размыто и теряет резкость.

Для конечного пользователя современные инструменты апскейлинга часто представляют собой «чёрный ящик», выполняющий сложные вычисления по нажатию кнопки. Благодаря оптимизациям и использованию аппаратного ускорения (GPU, TPU), нейросетевые модели способны работать практически в реальном времени. К примеру, в игровых приложениях технология DLSS (Deep Learning Super Sampling) от NVIDIA генерирует кадры

высокой чёткости из низкого разрешения прямо на лету, позволяя значительно повысить производительность без заметной потери качества картинки [4]. Аналогично, смартфоны при съемке могут автоматически улучшать детали фото с помощью встроенных моделей ИИ. Таким образом, нейросетевой апскейлинг перестал быть сугубо лабораторной разработкой – он внедряется в массовые продукты, зачастую незаметно для самого пользователя.

Сегодня методы увеличения разрешения с помощью ИИ широко применяются в самых разных областях. В медицине они помогают улучшать качество диагностических изображений (например, МРТ, КТ) для более точного анализа. В фотографии и кинематографе нейросети используются для реставрации и ремастеринга архивных материалов – старые фильмы, снятые в низком разрешении, обретают новую жизнь в формате HD и 4K, открывая зрителю ранее невидимые детали. Энтузиастами и профессионалами активно восстанавливаются старые фотоснимки: алгоритмы удаляют шум, повышают четкость лиц на исторических фотографиях, что было невозможно традиционными методами. В видеонаблюдении суперразрешение помогает разобрать номера автомобилей или лица в кадрах с камер низкого качества – это повышает эффективность систем безопасности. Отдельно стоит отметить сферу развлечений: помимо уже упомянутых видеоигр, апскейлинг используется в приложениях дополненной и виртуальной реальности для оптимизации рендеринга.

Важно подчеркнуть, что качество работы разных методов апскейлинга может различаться в зависимости от типа изображения. Например, для анимационной графики разработаны специализированные алгоритмы (такие как Waifu2x для аниме-артов [7]), учитывающие особенности рисунка и плоских областей цвета. Для лиц человека существуют модели, обученные на портретах, способные достоверно восстанавливать глаза, рот и прочие черты. В общем случае универсальные алгоритмы стараются быть максимально адаптивными. Современные тенденции в исследовании суперразрешения включают объединение подходов (например, каскадное применение нескольких моделей, где одна устраняет шум, другая увеличивает размер), а также изучение методов обучения без учителя для случаев, когда нет идеальных пар изображений для тренировки.

Прогресс в области нейронного апскейлинга не только улучшил метрики качества изображений, но и снизил порог входа для использования этих технологий. Если раньше для подобных задач требовалось специализированное оборудование и месяцы обучения модели, то теперь доступны готовые облачные сервисы, позволяющие вызвать суперразрешение через API или встроить в программный продук [5]. Это открыло дорогу множеству приложений: от улучшения пользовательских фотографий в социальных сетях до масштабных проектов оцифровки библиотек изображений и видеоархивов. Апскейлинг с помощью ИИ превратился из научного эксперимента в повседневный инструмент, значительно расширяющий возможности работы с визуальной информацией.

История развития технологий повышения разрешения наглядно демонстрирует, как искусственный интеллект открыл новую сферу обработки изображений. Нейросетевые алгоритмы апскейлинга за короткий срок преодолели ограничения классических подходов, научившись восстанавливать детали там, где раньше воображение упиралось в размытые пиксели. Сегодня суперразрешение служит связующим звеном между растущими запросами на качество визуального контента и ограничениями исходных данных – будь то старый фотоматериал или ресурсоограниченные устройства. Достижения в этой области не только дают эстетическое улучшение изображений, но и несут практическую ценность: делают

возможным анализ ранее непригодных материалов, улучшают точность медицинской диагностики, сохраняют культурное наследие в цифровом виде.

Список литературы

1. Умнова Александра. Апскейл – что такое. // Skyeng [Электронный ресурс] URL: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-apskeil/ (Дата обращения: 12.11.25 г.)
2. Технология масштабирования нейронных сетей // Canon Global Tech Article, 13.11.2023 [Электронный ресурс] URL: https://global.canon/en/technology/dl-upscaling-2023.html (Дата обращения: 12.11.25 г.)
3. Гроукут Мэтт. Фотография Трампа демонстрирует опасности, связанные с расширением возможностей искусственного интеллекта. // PetaPixel. [Электронный ресурс] URL: https://petapixel.com/2025/09/05/trump-photo-shows-the-perils-of-ai-upscaling-tools/ (Дата обращения: 12.11.25 г.)
4. NVIDIA DLSS: Ваши вопросы, ответы. // Официальный сайт Nvidia [Электронный ресурс] URL: https://www.nvidia.com/en-us/geforce/news/nvidia-dlss-your-questions-answered/ (Дата обращения: 12.11.25 г.)
5. Рост сверхразрешения: от классической обработки изображений до масштабируемых API искусственного интеллекта // IBM [Электронный ресурс] URL: https://community.ibm.com/community/user/blogs/paul-glenn2/2025/04/25/the-rise-of-super-resolution-from-classical-image#:~:text=The%20concept%20of%20super,sensitive%20to%20noise%20and%20misalignment (Дата обращения: 12.11.25 г.)
6. Сверхрезультативность // Bayern Collab [Электронный ресурс] URL: https://collab.dvb.bayern/spaces/TUMlfdv/pages/69119923/Super-Resolution (Дата обращения: 12.11.25 г.)
7. Еще более качественное масштабирование изображений с помощью Waifu2x. // Журнал Fedora Magazine. 2018-10-02. [Электронный ресурс] URL: https://fedoramagazine.org/better-image-upscaling-waifu2x/ (Дата обращения: 12.11.25 г.)

References

1. Umnova Alexandra. Upscale – what is it. // Skyeng [Electronic resource] URL: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-apskeil / (Date of request: 12.11.25)
2. Neural network scaling technology // Canon Global Tech Article, 11/13/2023 [Electronic resource] URL: https://global.canon/en/technology/dl-upscaling-2023.html (Date of request: 12.11.25)
3. Growcoot Matt. Trump Photo Shows The Perils of AI Upscaling Tools. // PetaPixel. [Электронный ресурс] URL: https://petapixel.com/2025/09/05/trump-photo-shows-the-perils-of-ai-upscaling-tools/ (Дата обращения: 12.11.25 г.)
4. NVIDIA DLSS: Your Questions, Answered. // Official Nvidia website [Электронный ресурс] URL: https://www.nvidia.com/en-us/geforce/news/nvidia-dlss-your-questions-answered/ (Дата обращения: 12.11.25 г.)
5. The Rise of Super-Resolution: From Classical Image Processing to Scalable AI APIs // IBM [Электронный ресурс] URL: https://community.ibm.com/community/user/blogs/paul-

glenn2/2025/04/25/the-rise-of-super-resolution-from-classical-image#:~:text=The%20concept%20of%20super,sensitive%20to%20noise%20and%20misalignment (Дата обращения: 12.11.25 г.)

6. Super Resolutuon // Bayern Collab [Электронный ресурс] URL: https://collab.dvb.bayern/spaces/TUMlfdv/pages/69119923/Super-Resolution (Дата обращения: 12.11.25 г.)
7. Even better image upscaling with Waifu2x. // Fedora Magazine. 2018-10-02. [Электронный ресурс] URL: https://fedoramagazine.org/better-image-upscaling-waifu2x/ (Дата обращения: 12.11.25 г.)

Петров А.О. Модель кластеризации малоэффективных источников теплоснабжения как инструмент модернизации коммунальной инфраструктуры «полупериферийных» территорий// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 215–218

Международный журнал информационных технологий и энергоэффективности

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

УДК 697.34:332.14:519.237.8

МОДЕЛЬ КЛАСТЕРИЗАЦИИ МАЛОЭФФЕКТИВНЫХ ИСТОЧНИКОВ ТЕПЛОСНАБЖЕНИЯ КАК ИНСТРУМЕНТ МОДЕРНИЗАЦИИ КОММУНАЛЬНОЙ ИНФРАСТРУКТУРЫ «ПОЛУПЕРИФЕРИЙНЫХ» ТЕРРИТОРИЙ

Петров А.О.
ФГАОУ ВО "СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ", Красноярск, Россия (660041, Красноярский край, г Красноярск, Свободный пр-кт, д. 79), e-mail: alek5eypetrov1989@yandex.ru

Статья посвящена решению актуальной проблемы модернизации неэффективных децентрализованных систем теплоснабжения («малого тепла») в малых городах и поселках России. В условиях критического износа инфраструктуры, дефицита финансирования и рассредоточенной застройки классические стратегии (полная централизация или децентрализация) зачастую неприменимы. Авторами предложен и обоснован адаптивный подход, основанный на принципе рациональной кластеризации – локальном объединении групп изношенных котельных в более управляемые узлы на базе наиболее перспективного действующего источника. На примере пгт. Мотыгино Красноярского края представлены результаты разработки и технико-экономического обоснования проекта реконструкции, предусматривающего объединение трех котельных. Доказана техническая реализуемость и экономическая эффективность проекта (NPV>0, DPP≈5,8 лет), основным источником экономии является снижение удельного расхода топлива на 24,7% за счет замещения малоэффективного оборудования современной автоматической блочно-модульной котельной. Успешная практическая реализация проекта в 2024 году подтвердила расчетные показатели, сделав предложенную модель тиражируемым решением для сотен аналогичных территорий.

Ключевые слова: Теплоснабжение, кластеризация, реконструкция, малоэффективные источники, энергоэффективность, технико-экономическое обоснование, «полупериферийные территории», автоматическая блочно-модульная котельная (АБМК).

A CLUSTERING MODEL FOR INEFFICIENT HEAT SUPPLY SOURCES AS A TOOL FOR MODERNIZING THE COMMUNAL INFRASTRUCTURE OF «SEMI-PERIPHERAL» TERRITORIES

Petrov A.O.
SIBERIAN FEDERAL UNIVERSITY, Krasnoyarsk, Russia (660041, Krasnoyarsk region, Krasnoyarsk, Svobodny prospekt, 79), e-mail: alek5eypetrov1989@yandex.ru

The article is devoted to solving the urgent problem of modernizing inefficient decentralized heat supply systems ("small heat") in small towns and villages in Russia. In the context of critical infrastructure wear, funding deficits, and dispersed development, classical strategies (full centralization or decentralization) are often inapplicable. The authors propose and justify an adaptive approach based on the principle of rational clustering - the local integration of groups of worn-out boiler houses into more manageable units based on the most promising existing source. Using the example of the urban-type settlement Motygino in the Krasnoyarsk Territory, the results of the development and feasibility study of a reconstruction project involving the integration of three boiler houses are presented. The technical feasibility and economic efficiency of the project (NPV > 0, DPP ≈ 5.8 years) are proven, with the main source of savings being a 24.7% reduction in specific fuel consumption due to the replacement of inefficient equipment with a modern automated block-modular boiler house (ABMK). The successful practical

implementation of the project in 2024 confirmed the calculated indicators, making the proposed model a replicable solution for hundreds of similar territories.

Keywords: Heat supply, clustering, reconstruction, inefficient sources, energy efficiency, feasibility study, "semi-peripheral territories", automated block-modular boiler house (ABMK).

Введение

Системный кризис в сфере коммунального теплоснабжения России, усугубляемый критическим физическим износом сетей (до 82% требуют замены) и низкой эффективностью децентрализованных источников, представляет угрозу энергетической безопасности, особенно для «полупериферийных» территорий – малых городов и поселков с рассредоточенной застройкой. [1] В сегменте «малого тепла» сосредоточено около 68 тыс. котельных, проблемы которых обусловлены децентрализацией, недогрузкой, дефицитом финансирования и кадров. Существующий арсенал стратегий модернизации (подключение к ТЭЦ, строительство крупных районных котельных, полная децентрализация) в чистом виде финансово и инфраструктурно нереализуем для таких условий. Это формирует научно-практический запрос на гибридные, адаптивные решения, не требующие полного отказа от существующей инфраструктуры.[2]

Цель исследования – разработка и обоснование модели реконструкции систем теплоснабжения «полупериферийных» территорий на принципе рациональной кластеризации малоэффективных источников.

Материалы и методы

Теоретической основой исследования выступили принципы системного анализа, теории жизненного цикла инженерной инфраструктуры и устойчивого развития. Практическая часть выполнена на примере системы теплоснабжения пгт. Мотыгино Красноярского края. Применены методы сравнительного и технико-экономического анализа, математического моделирования в программном комплексе ZuluThermo для гидравлических расчетов.[3]

Результаты и обсуждение

1. *Диагностика проблем системы.* Анализ существующего положения в пгт. Мотыгино выявил архаичную децентрализованную структуру из 9 изолированных котельных. Ключевые проблемы: критическая недогрузка (средний коэффициент загрузки ≈21%), значительный разброс удельного расхода условного топлива (УРУТ от 211,86 до 307,73 кг у.т./Гкал), высокий износ сетей, отсутствие резервирования. Наименее эффективной признана котельная №1 (УРУТ 307,73).

2. *Выбор стратегии.* Сравнительный анализ возможных стратегий модернизации (Таблица 1) показал, что кластеризация (локальное объединение) является сбалансированным вариантом, позволяющим повысить эффективность и надежность при умеренных капиталовложениях, не требуя долгосрочного генплана, в отличие от полной централизации или децентрализации.

Таблица 1 – Сравнительный анализ стратегий модернизации для пгт. Мотыгино (фрагмент)

Критерий	Сохранение статус-кво	Полная децентрализация	Строительство новой котельной	**Кластеризация**
Капитальные затраты	Минимальные	Очень высокие	Чрезвычайно высокие	**Умеренные**
Надежность системы	Низкая	Зависит от систем зданий	Высокая	**Повышение**
Реализуемость	Реализуема, но консервирует проблемы	Затруднена	Нереализуема	**Наиболее реализуема**

3. *Разработка проекта кластеризации***.** В качестве пилотного кластера выбраны территориально близкие котельные №1, №5, №11 с суммарной нагрузкой 1,723 Гкал/ч. Разработана принципиальная схема объединения с минимизацией длины новых теплотрасс (два участка суммарной длиной 780 м). Гидравлическое моделирование в ZuluThermo подтвердило техническую возможность объединения и позволило оптимизировать диаметры трубопроводов.[4]

4. *Технико-экономическое обоснование***.** Для замещения базовой котельной №1 обоснован выбор автоматической блочно-модульной котельной (АБМК) «Терморобот» мощностью 4,8 МВт в схеме 5+1 котлов, как наилучшей по критериям автоматизации, дистанционного управления и надежности. Расчеты показали, что реализация проекта приведет к:

- Снижению расхода сетевой воды на 10,6% и тепловых потерь на 14,9%.
- Снижению среднечасового расхода условного топлива на 24,7% за счет роста КПД.
- Годовой экономии эксплуатационных затрат в размере 17,37 млн руб., основными компонентами которой являются экономия топлива (10,67 млн руб.) и фонда оплаты труда (3,8 млн руб.).[5]
- Показателям экономической эффективности: NPV ≈ 42,5 млн руб., IRR ≈ 18,5%, дисконтированный срок окупаемости (DPP) – 5,8 лет при ставке дисконтирования 10%.[6]

Заключение

Разработана и всесторонне обоснована адаптированная модель реконструкции систем «малого тепла» для «полупериферийных» территорий, основанная на принципе рациональной кластеризации. Научная новизна подхода заключается в синтезе преимуществ системного анализа и практики энергосбережения, предлагающем промежуточное решение между полной централизацией и децентрализацией. Практическая значимость подтверждена успешной реализацией описанного проекта в пгт. Мотыгино в 2024 году, в результате которого достигнуто повышение надежности, снижение эксплуатационных затрат и оптимизация

кадровых ресурсов. Предложенная модель является тиражируемой и может быть применена для сотен аналогичных населенных пунктов Российской Федерации. Для широкого внедрения подхода рекомендуется использование механизмов государственно-частного партнерства и разработка типовых проектных решений.

Список литературы

1. Федеральный закон от 30.12.2009 № 384-ФЗ «Технический регламент о безопасности зданий и сооружений».
2. СП 124.13330.2012 «Тепловые сети». Актуализированная редакция СНиП 41-02-2003.
3. Национальный проект «Экология»: официальный сайт. URL: https://www.mnr.gov.ru/activity/np_ecology/ (дата обращения: 20.03.2025).
4. Программный комплекс для моделирования систем теплоснабжения «ZuluThermo»: официальный сайт. URL: https://www.politerm.com/products/geo/zulugis/ (дата обращения: 20.03.2025).
5. Официальный сайт компании «Терморобот» (г. Новосибирск). URL: https://termorobot.ru/ (дата обращения: 20.03.2025).
6. Схема теплоснабжения пгт. Мотыгино. URL: https://motygino-r04.gosweb.gosuslugi.ru/netcat_files/64/1759/ETS_26.PP21_550.P.00.00_UCh_ST.pdf (дата обращения: 20.03.2025).

References

1. Federal Law of 30.12.2009 No. 384-FZ "Technical Regulations on the Safety of Buildings and Structures."
2. SP 124.13330.2012 "Heating Networks." Updated version of SNiP 41-02-2003.
3. National Project "Ecology": official website. URL: https://www.mnr.gov.ru/activity/np_ecology/ (accessed: 20.03.2025).
4. Software package for modeling heat supply systems "ZuluThermo": official website. URL: https://www.politerm.com/products/geo/zulugis/ (accessed: 20.03.2025).
5. Official website of the company "Termorobot" (Novosibirsk). URL: https://termorobot.ru/ (accessed: March 20, 2025).
6. Heat supply scheme for the urban-type settlement of Motygino. URL: https://motygino-r04.gosweb.gosuslugi.ru/netcat_files/64/1759/ETS_26.PP21_550.P.00.00_UCh_ST.pdf (accessed: March 20, 2025).

Жильцов Д.А. Проектирование корпуса ракеты носителя среднего класса из модифицированного композита // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 219–223

Международный журнал информационных технологий и энергоэффективности

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

УДК 006.022

ПРОЕКТИРОВАНИЕ КОРПУСА РАКЕТЫ НОСИТЕЛЯ СРЕДНЕГО КЛАССА ИЗ МОДИФИЦИРОВАННОГО КОМПОЗИТА

Жильцов Д.А.
ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)" (ФИЛИАЛ "ВОСХОД" В Г.БАЙКОНУРЕ , Байконур, Россия (468325, город Байконур, ул Гагарина, д. 5), e-mail: hegai5012@gmail.com

Рассмотрим перспективу использование модифицированного композита на основе углерод-углерода для изготовления из него обшивки корпуса ракеты носителя среднего класса. Проведем сравнительный анализ прочностных и массовых характеристик проектируемого корпуса из нового материала с традиционными алюминиевыми сплавами. Методология работы состоит из расчета массы конструкции, анализа статистической прочности при действии внутреннего давления и осевых перегрузок, а также оценку надежности на основе вероятностных методов. Данная работа покажет весь потенциал использования новых материалов в ракетостроении ведь основная задача это надежность и низкая масса ракеты для эффективной эксплуатации изделия.

Ключевые слова: Корпус, фуллерен, углерод-углеродный композит, прочность, надежность, масса конструкции.

DESIGN OF A MIDDLE-CLASS CARRIER MISSILE BODY MADE OF A MODIFIED COMPOSITE

Zhiltsov D.A.
"MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY)" (BRANCH "VOSKHOD" IN BAIKONUR, Baikonur, Russia (468325, Baikonur, Gagarina str., 5), e-mail: hegai5012@gmail.com

Consider the prospect of using a modified carbon-carbon composite to make the skin of a medium-class launch vehicle. We will conduct a comparative analysis of the strength and mass characteristics of the projected hull made of a new material with traditional aluminum alloys. The methodology of the work consists of calculating the mass of the structure, analyzing the statistical strength under internal pressure and axial overloads, as well as assessing reliability based on probabilistic methods. This work will demonstrate the full potential of using new materials in rocket engineering, as the main goal is to ensure the reliability and low mass of the rocket for efficient operation.

Keywords: Housing, fullerene, carbon-carbon composite, strength, reliability, and structural weight.

Современная тенденция развития ракетостроения направлена на снижения массовых характеристик конструкции для повышения эффективности работы и увеличения массы полезного груза. Для ракет носителей среднего класса выводящие на орбиты земли около 5-15 тон, корпус, включая баки горючего и окислителя, составляют значительную часть стартовой массы. Традиционными материалами являются алюминиево-литиевые сплавы и полимерные композиционные материалы. Однако эти материалы сталкиваются с ограничением: АЛ сплавы имеют невысокую удельную прочность, стандартные композитные материалы имеют ограниченную стойкость к воздействию криогенных температур и агрессивных компонентов топлива, а также к тепловым потокам.[1]

Углерод- углеродный композитный материал состоит из углеродного волокна и углеродной матрицы, обладает уникальным сочетанием свойств: высокой термостойкостью до 3000°C в инертном состоянии, низкой плотностью и массой, стойкой к агрессивным внешним воздействиям.

Теоретически обоснуем применение углерод – углеродного композита с внедренным фуллереном для корпуса ракеты носителя среднего класса путем проведения прочностного расчета и сравнительного анализа с традиционными материалами по критериям массы, прочности и надежности.[2]

За основу принимаем цилиндрическую часть корпуса ракеты: диаметр корпуса D=3.5 м, длинна цилиндрической части L=10 м, рабочее давление в баке P=0.35 МПа, коэффициент осевой перегрузки n_x=4, запас прочности f=1.5.

Сравниваем материалы:

1) Алюминиевый сплав (АЛ-ч): Плотность p=2700 кг/м^3, предел прочности $\sigma_в = 450$ МПа.

2) Углепластик: Плотность p=1550 кг/м^3, предел прочности $\sigma_в = 1800$ МПа.

3) УУ-С60: Плотность p=1650 кг/м^3, предел прочности $\sigma_в = 1200$ МПа.

Повышенная плотность по сравнению с углепластиком обусловлена более плотной углеродной структурой матрицы, однако ключевое преимущество – высокая рабочая температура и стойкость к термоударам.[3]

Рассчитаем прочность и массу конструкции, представим, что конструкция корпуса рассчитывается как тонкостенная оболочка. Основные нагрузки: внутреннее давление и осевая сила.

Используя формулы 1 и 2, определим осевое усилие и продольное напряжение от отделения и осевой силы.

$$N = \frac{(\pi \cdot D^2 \cdot p)}{4} \quad (1)$$

$$\sigma = \frac{(p \cdot D)}{(4 \cdot \delta)} + \frac{(N \cdot n_x)}{(\pi \cdot D \cdot \delta)} = \frac{(p \cdot D(1 + n_x))}{(4 \cdot \delta)} \quad (2)$$

Условие прочности: $\sigma \leq [\sigma] = \sigma_в$

Требуемая толщина стенки определяется из условия прочности:

$\delta_{треб} = \frac{(p \cdot D(1+n_x))}{(4 \cdot \delta)}$

Масса цилиндрической части корпуса определяется по формуле 3.

$$m = \pi \cdot D \cdot L \cdot \delta \cdot \rho \quad (3)$$

Все результаты расчетов сведены в таблице 1.

Таблица 1 – результаты расчетов

Материал	$\sigma_{в}$, МПа	$\delta_{треб}$,мм	m,кг
Алюминий (АЛ-ч)	450	10,2	3020
Углепластик	1800	2,55	435
УУ-С60 композит	1200	3,83	655

Конструкция из УУ-С60 композита тяжелее углепластика на 60%, но легче алюминия на 77%. Однако прочностной расчет не учитывает термонагружение на материал.

Проведем термомеханический анализ в зоне стыковки бака с двигательным отсеком корпуса, где температура воздействия на материал достигает до 800-1000°С от работающего двигателя. Для алюминия и стандартного углепластика это критично.

Эквивалентное напряжение с учетом температурной нагрузки для зоны стыка найдем, используя формулу 4.

$$\sigma_{экв} = \sqrt{\sigma_{мех}^2 + \sigma_{тепл}^2}\text{, где } \sigma_{тепл} = \mathrm{E} \cdot \alpha \cdot \Delta\mathrm{T} \quad (4)$$

Для УУ-С60 композита примем Е=150 ГПа, коэффициент теплового расширения $\alpha = 2 \cdot 10^{-6}\,{}^{1}/_{\circ\mathrm{C}}$, $\Delta\mathrm{T} = 1000^{\circ}\mathrm{C}$ и $\sigma_{мех} = 800$ МПа.<

Таким образом условия прочности выполняется (754<800), но для алюминия и углепластика в таких условия прочность обеспечить невозможно.

Оценим надежность как вероятность безотказной работы корпуса под нагрузкой. Используя вероятностный подход, где прочность материала R и нагрузка S являются случайными величинами.

Вероятность отказа: $P_f = P(R - S < 0)$ индекс надежности β связанная с P_f через стандартное нормальное распределение.[4]

Допусти, что прочность материала подчиняется нормальному распределению.

Коэффициент вариации прочности:

1) Для алюминия $V_R = 0.05$ высокая однородность.
2) Для углепластика $V_R = 0.08$ разброс из-за технологических дефектов.
3) Для УУ-С60 $V_R = 0.12$ высокий разброс из-за сложности технологии внедрения фуллерена.

Коэффициент вариации надежность учтем, как $V_S = 0.15$.

Рассчитаем индекс надежности β по формуле Корнелла:

$$\beta = \frac{\left(\frac{\mu_R}{\mu_S - 1}\right)}{\sqrt{V_R^2 \cdot \left(\frac{\mu_R}{\mu_S - 1}\right)^2 + V_S^2}}\text{, где } \left(\frac{\mu_R}{\mu_S}\right) = f \text{ запас прочности.} \quad (5)$$

Результаты расчетов представлены в таблице 2.

Таблица 2 – результаты расчетов

Материал	Запас прочности	V_R	V_S	Индекс надежности	Вероятность отказа P_f оценночное
Алюминий (АЛ-ч)	1.5	0.05	0.15	2.9	0.002
Углепластик	1.5	0.08	0.15	2.72	0.003
УУ-С60	1.5	0.12	0.15	2.5	0.006

Конструкция из УУ-С60 композита имеет несколько низкую расчетную надёжность так как это обусловлено тем, что характеристики материала являются полностью расчетными на ранних стадиях освоения новой технологии производства.

Сравним все результаты измерений и ведем их в таблицу 3.

Таблица 3 – Сводка результатов сравнительного анализа

Критерий	Алюминий (АЛ-ч)	Углепластик	УУ-С60
Требуемая толщина стенки, мм	10.2	2.55	3.82
Расчетная масса корпуса, кг	3020	435	695
Снижение массы относительно алюминия	0%	85%	77%
Максимальная рабочая температура, °С	150	400	1600
Стойкость к термоудару	Низкая	Средняя	Очень высокая
Индекс надежности	2.9	2.72	2.5
Технологическая готовность	9	8-9	7
Основные преимущества	Отработанная технология производства	Минимальная масса	Сочетание легкости, прочности и термостойкости

Проведенные исследования демонстрирует высокий потенциал УУ-С60 композита, модифицированного фуллеренами, для применения в конструкциях корпуса РН. Применение данного материала является перспективной и революционной задачей, решение которой позволит создать РН нового поколения с улучшенными массовыми и тепловыми характеристиками.

Список литературы

1. Фирсанов В. В. «Методы расчёта установок ЛА на прочность». Учебное пособие, изданное в 1994 году издательством МАИ.
2. Савельев, Л. М. Прочность летательных аппаратов [Электронный ресурс] : интерактив. мультимед. пособие в системе дистанц. обучения "Moodle" / Л. М. Савельев, И. С. Ахмедьянов ; Минобрнауки России, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т). - Самара, 2012. - on-line
3. «Моделирование и конструирование элементов летательных аппаратов»: учебное пособие, авторы — А. Д. Припадчев, А. А. Горбунов, А. Г. Магдин, И. С. Калинина, 2025 год.
4. «Конструкция и проектирование летательных аппаратов»: книга, авторы — И. С. Голубев (под ред.), А. Самарин, В. Новосельцев, 1995 г.

References

1. V. V. Firsanov, "Methods for Calculating the Strength of Aircraft Installations." A textbook published in 1994 by MAI Publishing House.
2. L. M. Saveliev, "Aircraft Strength" [Electronic resource]: interactive multimedia manual in the Moodle distance learning system / L. M. Saveliev, I. S. Akhmedyanov; Ministry of Education and Science of the Russian Federation, Samara State Aerospace University named after S. P. Korolev (National Research University). - Samara, 2012. - online
3. "Modeling and Design of Aircraft Elements": a textbook by A. D. Pripadchev, A. A. Gorbunov, A. G. Magdin, I. S. Kalinina, 2025.
4. “Design and engineering of aircraft”: book, authors - I. S. Golubev (ed.), A. Samarin, V. Novoseltsev, 1995.

Павлов И.С. Особенности конструкции и расчёта анкерных участков контактной сети переменного тока на железнодорожных линиях / Павлов И.С., Елохов А.В., Жуйков И.О. // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 224–229

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.332.3

ОСОБЕННОСТИ КОНСТРУКЦИИ И РАСЧЁТА АНКЕРНЫХ УЧАСТКОВ КОНТАКТНОЙ СЕТИ ПЕРЕМЕННОГО ТОКА НА ЖЕЛЕЗНОДОРОЖНЫХ ЛИНИЯХ

[1]Павлов И.С., Елохов А.В., Жуйков И.О.
ФГБОУ ВО «КРАСНОЯРСКИЙ ИНСТИТУТ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА», Красноярск, Россия (660028, г.Красноярск, ул. Новая Заря, 2И, корп. 1), e-mail: [1]admka1536@gmail.com

В статье рассматриваются особенности конструкции и расчёта анкерных участков контактной сети переменного тока, применяемых на железнодорожных линиях. Проанализированы основные элементы анкерных участков, их функции и технические параметры, обеспечивающие стабильное натяжение проводов при изменении температуры и механических нагрузок. Приведены принципы расчёта усилий в контактных проводах, а также рассмотрены типовые схемы анкеровки. Особое внимание уделено требованиям к изоляторам, компенсаторам и поддерживающим устройствам. В работе отмечается важность точности расчётов при проектировании анкерных участков для обеспечения надёжности и безопасности электрифицированного железнодорожного транспорта.

Ключевые слова: контактная сеть, анкерный участок, переменный ток, натяжение проводов, компенсаторы, изоляторы, электрификация железных дорог.

DESIGN AND CALCULATION FEATURES OF ANCHOR SECTIONS OF AC CONTACT NETWORKS ON RAILWAY LINES

[1]Pavlov I.S., Elokhov A.V., Zhuykov I.O.
KRASNOYARSK INSTITUTE OF RAILWAY TRANSPORT, Krasnoyarsk, Russia (660028, Krasnoyarsk, Novaya Zarya St., 2I, Bldg. 1), e-mail: 1 admka1536@gmail.com

The article examines the design and calculation features of anchor sections of alternating-current overhead contact systems used on railway lines. The main elements of anchor sections, their functions, and technical parameters that ensure stable wire tension under temperature and mechanical load variations are analyzed. The principles of calculating forces in contact wires and typical anchoring schemes are described. Special attention is paid to insulators, tensioning devices, and supporting components. The study emphasizes the importance of calculation accuracy in the design of anchor sections to ensure the reliability and safety of electrified railway transport.

Keywords: overhead contact system, anchor section, alternating current, wire tension, compensators, insulators, railway electrification.

Введение

Современная железнодорожная инфраструктура требует высокой надёжности и стабильности работы систем электроснабжения. Одним из ключевых элементов контактной сети переменного тока являются анкерные участки, предназначенные для разделения пролётов, компенсации температурных изменений и обеспечения постоянного натяжения контактных проводов.

Анкерный участок выполняет функцию механического разделения контактной подвески на отдельные пролёты и одновременно служит для компенсации температурных удлинений проводов с помощью грузовых или пружинных компенсаторов. Конструкция анкерного участка должна обеспечивать минимальные колебания натяжения и надёжную работу токосъёмного устройства при движении подвижного состава [1].

При проектировании анкерных участков необходимо учитывать ряд факторов: климатические условия эксплуатации, тип контактной подвески, механические свойства проводов, усилия натяжения, расстояния между опорами и влияние внешних нагрузок. Ошибки в расчётах или выборе конструктивных решений могут привести к отклонению проводов от проектного положения, что снижает безопасность и эффективность движения поездов.

Целью настоящего исследования является анализ особенностей конструкции и расчёта анкерных участков контактной сети переменного тока, определение ключевых факторов, влияющих на их надёжность, и разработка рекомендаций по оптимизации проектных решений.

Анкерные участки контактной сети переменного тока на железнодорожных линиях — это механически независимые отрезки контактной подвески, ограниченные анкерными опорами. Их конструкция и расчёт направлены на обеспечение надёжности, безопасности и эффективности токосъёма при переменном токе. Основные аспекты включают длину участков, типы анкеровки, сопряжения, а также нормативные требования [2].

Принципы построения

Секционирование — разделение контактной сети на отдельные участки (секции) для удобства обслуживания и ремонта. Это достигается с помощью изолирующих сопряжений, нейтральных вставок, секционных и врезных изоляторов.

Анкеровка проводов

Крепление проводов контактной подвески к анкерной опоре с передачей на неё их натяжения. Виды анкеровки:

- **Жёсткая** — провода закреплены неподвижно (применяется на коротких участках).
- **Компенсированная** — с компенсаторами для автоматического регулирования натяжения.
- **Полукомпенсированная** — компенсаторы только для контактного провода.

Средняя анкеровка

Узел в середине анкерного участка, предотвращающий смещение проводов.

Зигзагообразное расположение контактных проводов

На прямых участках пути для равномерного износа накладок токоприёмников.

Защита от перенапряжений

Устройства для защиты от атмосферных и коммутационных перенапряжений.

1. Назначение и конструкция анкерного участка

Анкерный участок контактной сети — это механически независимый отрезок контактной подвески, ограниченный анкерными опорами. Его назначение — обеспечение надёжного токосъёма, ограничение зон повреждения при обрыве проводов, упрощение монтажа, обслуживания и ремонта контактной сети [3].

Конструкция анкерного участка включает Анкерные опоры, промежуточные опоры, компенсаторы, среднюю анкеровку и сопряжения.

2.1. Основные элементы анкерного участка

Классическая схема анкерного участка включает следующие элементы:

- **контактный провод (МФ-100, МФ-85)** — обеспечивает передачу тока;
- **несущий трос (БрНЖ-70, БрНЖ-95)** — удерживает контактный провод через струны;
- **струны** — соединяют контактный провод с несущим тросом, обеспечивая заданный зигзаг и высоту подвески;
- **анкеры (анкерные опоры)** — закрепляют концы контактной подвески;
- **компенсаторы** — обеспечивают постоянное натяжение при изменении длины проводов от температуры;
- **изоляторы и разъединители** — обеспечивают электрическую изоляцию и возможность отключения участка при необходимости.

Анкерные участки, как правило, имеют длину **от 1,2 до 1,8 км** в зависимости от климатического района, рельефа местности и типа подвески. В северных регионах длина анкерного участка уменьшается, чтобы снизить влияние температурных деформаций.

2.2. Типы анкеровки

В практике электрификации железных дорог применяют несколько схем анкеровки контактной сети:

1. **Односторонняя анкеровка** — оба конца анкерного участка закреплены на одной опоре. Применяется для коротких участков.

2. **Двусторонняя анкеровка** — каждый конец участка закреплён на разных опорах. Используется чаще всего на магистралях.

3. **Сдвоенная анкеровка** — используется при соединении двух независимых участков, что позволяет повысить надёжность и компенсировать температурные различия.

Анкерные узлы выполняются из оцинкованной стали и снабжены изоляторами, обеспечивающими надёжную изоляцию от опоры [4].

3. Надёжность и эксплуатационные особенности анкерного участка контактной сети

Анкерный участок – **это критически** важный элемент контактной сети, обеспечивающий стабильность токосъёма и локализацию повреждений. Его надёжность определяется совокупностью конструктивных решений, качеством монтажа и систематичностью технического обслуживания.

Надёжность анкерного участка формируется под воздействием климатических условий (ветер, гололёд, перепады температур от −40 до +50 °C),
динамических нагрузок от взаимодействия токоприёмника с контактным проводом,

электромагнитных воздействий (перенапряжения, токовые нагрузки), коррозионных процессов (влияние влаги, солей, промышленных выбросов), механического износа контактных элементов.

Эти факторы обусловливают необходимость применения материалов и конструкций с повышенными прочностными и эксплуатационными характеристиками.

4. Современные методы проектирования и диагностики анкерных участков

Современные методы проектирования и диагностики анкерных участков контактной сети направлены на повышение надёжности, снижение затрат и обеспечение бесперебойной работы железнодорожного транспорта. Они включают применение компьютерных технологий, неразрушающих методов контроля и комплексных диагностических систем.

Проектирование анкерных участков

При проектировании учитывают множество факторов: климатические условия, механические нагрузки, электромагнитные воздействия и требования к токосъёму. Основные подходы:

1. **Компьютерное моделирование и расчёт параметров**. Используются специализированные программы для индивидуального расчёта консолей, определения длин пролётов и эквивалентных пролётов. Это позволяет учитывать уникальные условия каждого участка и минимизировать ошибки [5].
2. **Унификация параметров**. Применяются стандартизированные значения длины пролётов, анкерных участков и других параметров, что упрощает производство и обслуживание.
3. **Выбор материалов и конструкций**. Предпочтение отдаётся экономичным профилям проката, высокопрочным и атмосферостойким сталям, а также композитным материалам. Например, алюминиевые консоли отличаются коррозионной устойчивостью, лёгкостью и низкой стоимостью обслуживания.
4. **Секционирование и компенсация**. Для повышения надёжности применяют изолирующие и неизолирующие сопряжения анкерных участков, среднюю анкеровку, а также компенсированные системы анкеровки с использованием компенсаторов, регулирующих натяжение проводов при температурных изменениях. studfile.net +1
5. **Учёт кривых и искусственных сооружений**. Длина анкерного участка уменьшается в кривых в зависимости от радиуса, а при прохождении через мосты и тоннели учитываются специфические требования к трассировке и креплению проводов. biblioserver.usurt.ru +1

Диагностика анкерных участков

Для контроля состояния анкерных участков применяются различные методы, включая неразрушающий контроль и комплексные системы мониторинга:

1. **Ультразвуковая дефектоскопия**. Используется для оценки прочности бетона опор и состояния анкерных болтов. Например, прибор УК-1401М позволяет проводить диагностику надземной части опор, а А-1220 — проверять анкерные болты фундаментов металлических опор без откопки [6]. Эхометод ультразвуковой дефектоскопии позволяет выявлять внутренние дефекты и определять глубину их залегания. lk.dvgups.ru +2

2. **Вагон-лаборатория ВИКС-ЦЭ**. Это современное средство комплексной диагностики, которое позволяет автоматизировать измерения параметров контактной сети, включая геометрические параметры подвески, взаимодействие с токоприёмником, износ контактного провода и перегрев элементов. Система использует лазерные и стереотелевизионные технологии, что обеспечивает высокую точность и скорость контроля.

3. **Измерение механических параметров**. Контролируются высота подвески контактного провода, его смещение относительно оси пути, величина контактного нажатия токоприёмника. Для этого применяются оптические датчики, регистрирующие кратковременные отрывы и нарушения в работе цепи «контактный провод — токоприёмник — контактный рельс».

4. **Диагностика заземлений и изоляторов**. На участках переменного тока измеряют сопротивление индивидуально заземлённых опор и входные сопротивления групповых заземлений. Состояние изоляторов проверяют на наличие трещин, сколов и загрязнений, которые могут привести к пробою.

5. **Визуальный осмотр и инструментальная проверка**. Включает оценку состояния бетона опор (трещины, выветривание), измерение ширины трещин и глубины повреждений с помощью микроскопа МПБ-2 или щупа, а также проверку наклона опор и габаритов установки.

Современные подходы к проектированию и диагностике анкерных участков позволяют минимизировать риски отказов, продлить срок службы конструкций и обеспечить бесперебойную работу железнодорожного транспорта. Ключевыми тенденциями являются цифровизация процессов, использование композитных материалов и развитие методов неразрушающего контроля.

Таким образом, конструкция и расчёт анкерных участков контактной сети переменного тока требуют учёта множества факторов: климатических условий, скорости движения поездов, типа подвески, нормативных требований и особенностей работы при переменном токе. Это обеспечивает надёжность и безопасность эксплуатации железнодорожной инфраструктуры.

Список литературы

1. Бондаренко В. С. Контактная сеть электрифицированных железных дорог. — М.: Транспорт, 2015. — 312 с.
2. Миронов А. Н., Поляков В. И. Электрификация железных дорог: учебник для вузов. — М.: Академия, 2018. — 420 с.
3. Правила устройства и технической эксплуатации контактной сети железных дорог РФ (ПУТЭКС). — М.: Минтранс России, 2020. — 256 с.
4. ГОСТ 32144–2013. Электрическая энергия. Совместимость технических средств. Нормы качества электрической энергии в системах электроснабжения общего назначения. — М.: Стандартинформ, 2013.
5. Панов А. А. Механические расчёты контактной подвески переменного тока. // Вестник транспорта. — 2021. — №4. — С. 45–53.

6. Бондаренко В. С. Принципы построения контактных сетей переменного тока железных дорог // Транспорт и связь. — 2022. — Т. 8, № 3. — С. 112–119.

References

1. Bondarenko V. S. Contact Network of Electrified Railways. Moscow: Transport, 2015. 312 p.
2. Mironov A. N., Polyakov V. I. Railway Electrification: A Textbook for Universities. Moscow: Academy, 2018. 420 p.
3. Rules for the Installation and Technical Operation of the Contact Network of Railways of the Russian Federation (PUTEKS). Moscow: Ministry of Transport of Russia, 2020. 256 p.
4. GOST 32144–2013. Electrical Energy. Compatibility of Technical Equipment. Electrical Energy Quality Standards in General-Purpose Power Supply Systems. Moscow: Standartinform, 2013.
5. Panov A. A. Mechanical Calculations of AC Catenary Suspension. Transport Bulletin. 2021, No. 4. — P. 45–53.
6. Bondarenko V. S. Design principles of AC railway contact systems // Transport and Communications Journal. — 2022. — Vol. 8, No. 3. - P. 112–119.

Черных П.А. Совершенствование режимов работы тепловых сетей для северных территорий// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 1(63) с. 230–234

Международный журнал информационных технологий и энергоэффективности

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

УДК 697.34:332.14:519.237.8

СОВЕРШЕНСТВОВАНИЕ РЕЖИМОВ РАБОТЫ ТЕПЛОВЫХ СЕТЕЙ ДЛЯ СЕВЕРНЫХ ТЕРРИТОРИЙ

Черных П.А.
ФГАОУ ВО "СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ", Красноярск, Россия (660041, Красноярский край, г Красноярск, Свободный пр-кт, д. 79), e-mail: chernih84@gmail.com

Организация надёжного теплоснабжения объектов капитального строительства, функционирующих в условиях крайнего Севера и территорий с резко континентальным климатом, предполагает безусловное соблюдение требований по бесперебойной подаче теплоносителя в объёмах, соответствующих проектным нормативам, и с параметрами, удовлетворяющими технологическим и санитарно-гигиеническим нормам. Основополагающим фактором, определяющим возможность выполнения этих условий, выступает гидравлическая устойчивость тепловой сети — её способность сохранять заданные гидравлические характеристики при колебаниях внешних и внутренних нагрузок. В настоящей работе представлены результаты исследований, направленных на повышение уровня гидравлической устойчивости и стабилизацию гидравлических режимов в системах централизованного теплоснабжения, функционирующих в северных районах.

Ключевые слова: Северные территории, гидравлическая устойчивость, методы расчета потокораспределения, теплоснабжение, режимы работы, тепловая сеть.

IMPROVING THE OPERATING MODES OF HEATING NETWORKS FOR NORTHERN TERRITORIES

Chernykh P.A.
SIBERIAN FEDERAL UNIVERSITY, Krasnoyarsk, Russia (660041, Krasnoyarsk region, Krasnoyarsk, Svobodny prospekt, 79), e-mail: chernih84@gmail.com

Providing reliable heating for buildings and infrastructure located in extreme northern and sharply continental climatic zones necessitates uninterrupted delivery of heat carrier in volumes consistent with design specifications and with parameters meeting technological and sanitary-hygienic requirements. A decisive factor enabling compliance with these conditions is the hydraulic stability of the heating network — its ability to maintain preset hydraulic characteristics despite fluctuations in external and internal loads. This paper presents research outcomes aimed at improving hydraulic stability and stabilizing hydraulic modes in district heating systems operating in northern areas.

Keywords: Northern territories, hydraulic stability, methods of calculating flow distribution, heat supply, operating modes, heating network.

Обеспечение устойчивой и эффективной работы систем централизованного теплоснабжения в условиях сурового климата — задача высокой научной и практической значимости. Особенно актуальна она для регионов Восточной Сибири, где перебои в подаче тепла могут привести не только к нарушению комфортных условий проживания, но и к аварийным ситуациям, угрожающим сохранности зданий и сооружений. Под гидравлической устойчивостью понимается способность тепловой сети сохранять заданные значения давлений и расходов теплоносителя в узлах подключения потребителей при изменениях как во внешних

(температура наружного воздуха, интенсивность ветра), так и во внутренних (изменение тепловой нагрузки, включение/отключение участков сети) условиях. Чем выше степень гидравлической устойчивости, тем меньше воздействие колебаний параметров сети на работу отопительных систем отдельных зданий — фактор, имеющий первостепенное значение для северных районов, где отклонения от расчётных режимов могут вызвать необратимые последствия, включая замерзание трубопроводов.

В работах [1–2] рассматриваются вопросы пространственного моделирования и визуализации гидравлических режимов, реализуемых на основе геоинформационных платформ и интегрированных в цифровую картографическую основу конкретного населённого пункта. Этот подход позволяет существенно повысить наглядность анализа и способствует принятию обоснованных управленческих решений при эксплуатации и реконструкции систем теплоснабжения. Предложенная в [1] методика предварительного анализа гидравлических характеристик городских тепловых сетей, базирующаяся на использовании открытой геоинформационной системы, учитывает не только геометрическое расположение источников теплоснабжения и протяжённость трубопроводных магистралей, но также в полной мере принимает во внимание особенности рельефа — что крайне важно при проектировании и диагностике сетей в труднодоступных и пересечённых районах Красноярского края, включая зоны вечной мерзлоты.

В публикации [3] приведены результаты мониторинга энергопотребления свыше 250 реально эксплуатируемых зданий, осуществлённого при помощи разработанной авторами автоматизированной системы сбора и анализа данных с тепловых пунктов. Такой подход позволяет с высокой достоверностью оценивать как тепловые, так и гидравлические параметры работы системы в реальном времени, выявлять отклонения от проектных показателей, а также оптимизировать настройки регулирующей арматуры. Данный метод особенно эффективен при анализе работы сетей в условиях северных территорий, где значительные сезонные перепады температур создают дополнительные сложности при балансировке системы.

В работах [4–6] подробно исследуется распределение тепловой энергии по инженерным системам зданий с различной степенью автоматизации — от полностью ручного управления до интеллектуальных систем с адаптивным регулированием. Приведены результаты численного моделирования реальных тепловых сетей централизованного теплоснабжения, включая сравнение расчётных и экспериментально измеренных параметров. Анализ показывает, что корректное управление гидравлическими режимами возможно только при комплексном подходе: сочетании математического моделирования, натурных замеров и последующей корректировки настроек регулирующих устройств. Отмечается, что стабильность расхода теплоносителя на стороне потребителя напрямую зависит от корректной работы регулирующих клапанов, установленных в индивидуальных тепловых пунктах (ИТП), и от их взаимодействия с системами автоматики зданий.

В работах [7, 8] исследуются специфические аспекты гидравлической устойчивости применительно к открытым системам теплоснабжения с непосредственным водоразбором, широко распространённым в ряде районов Сибири. Предложены инженерные решения, направленные на повышение устойчивости гидравлических режимов в таких системах, в том числе за счёт перехода на закрытые схемы или модернизации существующей арматуры и схем подключения.

Количественно гидравлическая устойчивость систем теплопотребления характеризуется коэффициентом Y, определяемым как отношение расчётного (проектного) расхода теплоносителя Vp через систему конкретного потребителя к максимально возможному расходу Vmax, который может возникнуть при работе всей сети в нештатных режимах (например, при отключении части потребителей или резком изменении наружной температуры).

Для зданий с отлаженными автоматизированными тепловыми пунктами Y равен:

$$Y = \frac{V_p}{V_{\text{макс}}} = \sqrt{\frac{\Delta H_{\text{аб}}}{H_{\text{сг}}}} = \sqrt{\frac{\Delta H_{\text{аб}}}{\Delta H_{\text{аб}} + \Delta H_{\text{сет}}}} = \sqrt{\frac{1}{1 + \frac{\Delta H_{\text{сет}}}{\Delta H_{\text{аб}}}}}.$$

Гидравлическая устойчивость систем теплопотребления зданий тем больше, чем меньше потеря напора в тепловой сети $\triangle H_{\text{сет}}$ и чем больше потеря напора на вводе тепловой сети в здание $\triangle H_{\text{аб}}$. Поэтому для повышения гидравлической устойчивости системы следует все избытки напора, имеющиеся в сети, поглощать при помощи сопротивлений (балансировочных клапанов) и регулирующих клапанов на тепловых пунктах зданий.

Для зданий, оборудованных современными автоматизированными тепловыми пунктами с дросселирующими и регулирующими устройствами, значение Y стремится к единице, что свидетельствует о высокой степени независимости системы отопления от колебаний параметров в магистральной сети. Согласно аналитическим соотношениям, гидравлическая устойчивость напрямую возрастает при снижении потерь напора в основной тепловой сети и увеличении потерь напора на вводе в здание (например, за счёт установки балансировочных клапанов). Следовательно, для повышения устойчивости целесообразно искусственно «поглощать» избыточный напор не в магистралях, а непосредственно на ИТП — с помощью правильно подобранных дроссельных и регулирующих органов.

В процессе эксплуатации тепловых сетей изменение расходов (например, из-за сезонного переключения на летний режим, ремонтных работ или подключения новых абонентов) неизбежно приводит к нарушению гидравлической устойчивости. В связи с этим особое внимание уделяется мероприятиям по уравниванию тепловых нагрузок и выравниванию давлений в различных узлах сети. Для обеспечения безопасной и надёжной эксплуатации требуется строгое ограничение диапазона допустимых давлений как в подающем, так и в обратном трубопроводах — как в статических (при остановленных насосах), так и в динамических (при работающем насосном оборудовании) режимах.

Так, максимальное давление в подающей магистрали, как правило, ограничено прочностными характеристиками оборудования и не должно превышать 160 м вод. ст. Минимальное же давление в подающем трубопроводе определяется из условия предотвращения вскипания теплоносителя — особенно критично при высоких температурах (например, 150 °C), поскольку даже кратковременное вскипание может вызвать гидравлические удары и отказы оборудования.

В обратной магистрали максимальное давление обычно лимитируется прочностью наиболее уязвимых компонентов, например, чугунных радиаторов отопления, подключённых по зависимой схеме, и не превышает 60 м вод. ст. Минимальное давление в обратке регламентируется необходимостью исключения завоздушивания систем — воздух в трубопроводах снижает теплоотдачу, вызывает кавитацию насосов и коррозионные процессы.

Сравнительный анализ пьезометрических графиков, построенных для

гидростатического и гидродинамического режимов, с предельно допустимыми значениями давлений позволяет своевременно выявлять угрозы: вскипания теплоносителя при пониженном давлении в подающей линии, завоздушивания систем при недостаточном давлении в обратном трубопроводе, механического разрушения оборудования при превышении верхних пределов давления.

Кроме того, такой анализ даёт возможность оценить общую работоспособность системы при аварийных, пиковых или переходных режимах, отличных от проектных.

Наиболее эффективным инженерным решением для поддержания давлений в допустимых пределах является организация регулируемой зоны давления — так называемой нейтральной точки. Эта точка располагается, как правило, на байпасной линии, соединяющей нагнетательный и всасывающий коллекторы сетевых насосов. В нейтральной точке поддерживается постоянное заданное давление, которое служит управляющим сигналом для автоматики: при падении давления ниже нормы включается подпиточный насос, а при его превышении — активируется дренажный клапан, сбрасывающий избыточную воду в контур подготовки подпиточной воды. При этом обеспечивается непрерывная циркуляция теплоносителя через байпас, что позволяет сохранять стабильный напор в системе даже при частичной загрузке насосного оборудования. Регулирование давления в нейтральной точке осуществляется посредством управления степенью открытия запорно-регулирующей арматуры. При полной остановке насосов в системе сохраняется гидростатический напор, равный проектному значению, определяемому высотой расположения расширительного бака или параметрами подпиточной установки.

Вывод.

Для разработки эффективных мероприятий, направленных на повышение гидравлической устойчивости и стабилизацию гидравлических режимов в тепловых сетях, функционирующих в условиях северных территорий, необходимо осуществлять комплексное компьютерное моделирование как расчётных, так и возможных нештатных (аварийных, ремонтных, пиковых) режимов работы систем теплоснабжения с учётом перспективного подключения дополнительных потребителей, поскольку только такой системный подход, сочетающий в себе прогнозирование динамики нагрузок, анализ пространственного распределения параметров сети и учёт особенностей местного рельефа и климата, позволяет обеспечить надёжную, устойчивую и энергоэффективную эксплуатацию тепловых сетей в экстремальных климатических условиях и, как следствие, гарантировать бесперебойное теплоснабжение населения и объектов инфраструктуры в северных регионах страны.

Список литературы

1. Липовка Ю.Л., Липовка А.Ю., Венин А.С. Компьютерная визуализация гидравлических режимов городских тепловых сетей на базе гис-технологий // Известия высших учебных заведений. Строительство. 2025. № 8 (800). С. 98-106.
2. Липовка Ю.Л., Венин А.С., Липовка А.Ю., Колосов М.В. Использование геоинформационных систем в решении задач проектирования тепловых сетей // Известия высших учебных заведений. Строительство. 2023. № 11 (779). С. 60-72.

3. Колосов М.В., Липовка Ю.Л. Анализ режимов работы горячего водоснабжения с использованием разработанной системы мониторинга // Региональная архитектура и строительство. 2024. № 3 (60). С. 163-174.
4. Липовка Ю.Л., Панфилов В.И., Липовка А.Ю., Тучин А.В. Математическое моделирование потокораспределения на тепловых пунктах // Энергосбережение и водоподготовка. 2008. № 3 (53). С. 65-67.
5. Липовка Ю.Л., Панфилов В.И. Экспериментальное изучение потокораспределения на автоматизированных тепловых пунктах // Энергосбережение и водоподготовка. 2008. № 2 (52). С. 52-54.
6. Калабин, Д.А., Липовка, А.Ю., Липовка, Ю.Л. Компьютерное моделирование и натурные замеры потокораспределения действующей тепловой сети // Вестник Иркутского государственного технического университета. 2021. Т. 25. № 1 (156). С. 44-56.
7. Липовка Ю.Л. Влияние непосредственного водоразбора на режимы работы последовательно включенных теплообменников // Известия высших учебных заведений. Строительство и архитектура. 1979. № 6. С. 95-100.
8. Липовка Ю.Л., Венин А.С., Михайлова А.С. Гидравлический режим тепловой сети при переходе с открытой на закрытую систему теплоснабжения // Энергосбережение и водоподготовка. 2019. № 6 (122). С. 53-56.

References

1. Lipovka Yu.L., Lipovka A.Yu., Venin A.S. Computer visualization of hydraulic modes of urban heating networks based on GIS technologies // News of higher educational institutions. Construction. 2025. No. 8 (800). pp. 98-106.
2. Lipovka Yu.L., Venin A.S., Lipovka A.Yu., Kolosov M.V. Using geographic information systems in solving problems of heating network design // News of higher educational institutions. Construction. 2023. No. 11 (779). pp. 60-72.
3. Kolosov M.V., Lipovka Yu.L. Analysis of hot water supply operating modes using the developed monitoring system // Regional architecture and construction. 2024. No. 3 (60). pp. 163-174.
4. Lipovka Yu.L., Panfilov V.I., Lipovka A.Yu., Tuchin A.V. Mathematical Modeling of Water Flow Distribution at Heating Substations // Energy Saving and Water Treatment. 2008. No. 3 (53). pp. 65-67.
5. Lipovka Yu.L., Panfilov V.I. Experimental Study of Water Flow Distribution at Automated Heating Substations // Energy Saving and Water Treatment. 2008. No. 2 (52). Pp. 52-54.
6. Kalabin, D.A., Lipovka, A.Yu., Lipovka, Yu.L. Computer Modeling and In-kind Measurements of Water Flow Distribution in an Operating Heating Network // Bulletin of the Irkutsk State Technical University. 2021. Vol. 25. No. 1 (156). pp. 44-56.
7. Lipovka Yu.L. The Influence of Direct Water Draw-off on the Operating Modes of Series-Connected Heat Exchangers // News of Higher Educational Institutions. Construction and Architecture. 1979. No. 6. pp. 95-100.
8. Lipovka Yu.L., Venin A.S., Mikhailova A.S. Hydraulic Regime of a Heating Network During the Transition from an Open to a Closed Heat Supply System // Energy Saving and Water Treatment. 2019. No. 6 (122). pp. 53-56.

Назаров Н.В. Исследование характера работы защитных сооружений стенок котлована в стеснённых городских условиях // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 235–240

Международный журнал информационных технологий и энергоэффективности

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

УДК 624.13:624.04:69.05:711.4

ИССЛЕДОВАНИЕ ХАРАКТЕРА РАБОТЫ ЗАЩИТНЫХ СООРУЖЕНИЙ СТЕНОК КОТЛОВАНА В СТЕСНЁННЫХ ГОРОДСКИХ УСЛОВИЯХ

Назаров Н.В.
ФГБОУ ВО «КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМ. И.Т. ТРУБИЛИНА», Краснодар, Россия (350044, Краснодарский край, город Краснодар, ул. им. Калинина, д.13), e-mail: kolyanazarov577077@gmail.com

Статья посвящена актуальной проблеме обеспечения устойчивости и минимального воздействия на окружающую застройку при устройстве глубоких котлованов в условиях плотной городской инфраструктуры. В работе проведён комплексный анализ характера работы различных типов защитных сооружений с учётом специфических факторов стеснённых условий: наличие исторической и современной застройки, ограниченность площадки, сети подземных коммуникаций, необходимость минимизации вибраций и дополнительных осадок фундаментов существующих зданий. На основе анализа полевых данных мониторинга и теоретических исследований выявлены закономерности деформирования грунтового массива и конструкций ограждения в зависимости от выбранной технологии, последовательности производства работ и применяемых методов усиления. Особое внимание уделено вопросам пространственной жёсткости сооружения и его взаимодействию с углами котлована. Разработаны практические рекомендации по оптимизации проектных решений и организации мониторинга на всех этапах строительства для снижения рисков аварийных ситуаций и ущерба третьим лицам. Результаты исследования могут быть использованы проектировщиками и строителями для повышения технико-экономической эффективности и безопасности подземного строительства в городах.

Ключевые слова**:** Защитные сооружения котлована, стеснённые городские условия, шпунтовое ограждение, стена в грунте, буросекущие сваи, мониторинг деформаций, осадки окружающей застройки, пространственная жёсткость, анкерное крепление, распорная система.

INVESTIGATION OF THE NATURE OF THE PROTECTIVE STRUCTURES OF THE EXCAVATION WALLS IN CRAMPED URBAN CONDITIONS

Nazarov N.V.
"KUBAN STATE AGRARIAN UNIVERSITY". I.T. TRUBILINA", Krasnodar, Russia (350044, Krasnodar City, Kalinina Street, 13), e-mail: kolyanazarov577077@gmail.com

The article is devoted to the urgent problem of ensuring sustainability and minimal impact on the surrounding buildings when installing deep excavation pits in conditions of dense urban infrastructure. The paper provides a comprehensive analysis of the nature of the work of various types of protective structures, taking into account the specific factors of cramped conditions: the presence of historical and modern buildings, limited site, underground communications network, the need to minimize vibrations and additional precipitation of the foundations of existing buildings. Based on the analysis of field monitoring data and theoretical studies, patterns of deformation of the soil mass and fencing structures have been identified, depending on the chosen technology, the sequence of work and the reinforcement methods used. Special attention is paid to the issues of spatial rigidity of the structure and its interaction with the corners of the excavation. Practical recommendations have been developed to optimize design solutions and organize monitoring at all stages of construction to reduce the risks of accidents and damage to third parties. The results of the study can be used by designers and builders to improve the technical and economic efficiency and safety of underground construction in cities.

Keywords: Excavation defenses, cramped urban conditions, tongue-and-groove fencing, wall in the ground, borehole piles, deformation monitoring, precipitation of surrounding buildings, spatial rigidity, anchoring, spacer system.

Введение

Активное освоение подземного пространства в крупных городах для возведения транспортных узлов, паркингов и многофункциональных комплексов неизбежно связано с устройством глубоких котлованов в непосредственной близости от существующих зданий. [1] Эта задача перестаёт быть чисто строительной и приобретает ярко выраженный геотехнический и градостроительный характер. Основная сложность заключается в необходимости обеспечить не только локальную устойчивость выемки, но и гарантировать сохранность окружающей исторической и современной застройки, чувствительной к любым дополнительным деформациям оснований. Традиционные подходы к проектированию ограждений котлованов, основанные преимущественно на обеспечении несущей способности, в стеснённых условиях оказываются недостаточными. На первый план выходит критерий деформационной пригодности конструкции, то есть её способности ограничивать перемещения грунтового массива и, как следствие, осадки фундаментов соседних сооружений. Таким образом, характер работы защитных сооружений в таких условиях качественно меняется: из пассивного элемента, удерживающего откос, оно превращается в активный барьер, взаимодействующий с комплексной системой «грунтовый массив – подземные коммуникации – фундаменты зданий». Исследование этого взаимодействия, выявление закономерностей деформирования и разработка на этой основе практических рекомендаций являются актуальной научно-практической задачей.[2]

Характер работы защитного сооружения в городской среде определяется совокупностью жёстких ограничений. Близость объектов, часто имеющих историческую ценность и не рассчитанных на современные динамические воздействия, диктует предельно допустимые значения осадок и кренов, зафиксированные в нормативных документах. Разветвлённая сеть подземных коммуникаций – коллекторов, трубопроводов, кабельных линий – накладывает прямые ограничения на применение таких эффективных методов, как анкерное крепление, так как зона их заделки может пересекаться с этими инженерными системами. [3] Ограниченные размеры строительной площадки исключают возможность устройства пологих откосов или размещения тяжёлой техники с внешней стороны контура котлована, вынуждая проектировщиков использовать внутренние распорные системы, которые, в свою очередь, стесняют рабочее пространство для основной строительной техники. Высокий уровень грунтовых вод, характерный для многих мегаполисов, требует от ограждения совмещения функций подпорной и противофильтрационной конструкции. Наконец, социальный фактор – необходимость минимизации шума, вибраций и пыли – напрямую влияет на выбор технологии устройства ограждения, зачастую исключая высокопроизводительные, но динамичные методы. Все перечисленные условия формируют уникальную среду, в которой деформационные свойства системы становятся главным объектом управления.

В практике городского строительства наибольшее распространение получили три основных типа ограждений: шпунтовое из стального профиля, из буросекущих свай и «стена в грунте». Каждое из них обладает специфическим характером работы. Шпунтовое ограждение, являясь наиболее гибким, работает по схеме балки на упругом основании, опёртой на ярусы креплений. Его основной недостаток в стеснённых условиях – значительные горизонтальные перемещения верхней части, особенно на опаснейшей начальной стадии разработки до установки первого яруса распор или анкеров. Эти перемещения неизбежно

вызывают осадки поверхности за контуром котлована по механизму развития зоны сдвига в грунте. Однако скорость монтажа и возможность многократного использования делают шпунт целесообразным для котлованов средней глубины при условии безупречной оперативности работ по раскреплению.[4]

Буросекущая свая представляет собой более жёсткую систему. Работая как сплошная подпорная стенка, она обеспечивает существенно меньшие перемещения. Её ключевая особенность – секущий принцип, при котором соседние сваи взаимно перекрываются, создавая не только конструктивную, но и гидроизоляционную преграду. Качество этого перекрытия напрямую определяет эффективность всего ограждения. «Стена в грунте», выполняемая методом подземного бетонирования в предварительно выкопанной траншее, является самой жёсткой и, соответственно, самой дорогой конструкцией. Её характер работы приближен к работе монолитной железобетонной стенки, заделанной в грунт. [5] Она обеспечивает минимальные деформации и часто становится частью постоянных конструкций возводимого подземного сооружения. Обобщение данных натурных наблюдений за различными объектами показывает, что при одинаковой глубине и геологических условиях разница в максимальных горизонтальных перемещениях между шпунтом и «стеной в грунте» может достигать двух-трёх раз, что является критически важным аргументом при выборе вблизи ответственных сооружений.

Характер работы самого ограждения неразрывно связан с работой системы, его удерживающей. Распорная система, создающая внутренний силовой каркас, обеспечивает жёсткое и предсказуемое закрепление. [6] Её эффективность в огромной степени зависит от соблюдения технологической дисциплины: распоры должны устанавливаться незамедлительно по мере выемки грунта, с обязательным предварительным натяжением, которое сразу включает их в работу и снижает начальные деформации. Основной недостаток – занятость внутреннего пространства, осложняющая ведение основных строительных работ. Анкерная система, передающая усилие на массив грунта за пределами котлована, освобождает это пространство, но её применение в городских условиях сопряжено с рядом принципиальных трудностей. Помимо конфликта с подземными коммуникациями, зона анкерного поля может выходить за пределы земельного участка застройщика, что требует сложных юридических и технических согласований. Кроме того, неконтролируемое растяжение анкерового массива также может провоцировать нежелательные осадки.[7]

Важнейшим аспектом, часто недооцениваемым при проектировании, является пространственная работа ограждения котлована. Котлован представляет собой объёмную конструкцию, и его углы обладают естественным упрочнением за счёт эффекта пространственного защемления грунта. Натурные замеры неизменно фиксируют, что горизонтальные перемещения в середине длинной стороны ограждения значительно превышают перемещения в угловой зоне. [8] Это явление, известное как «угловая арка» или эффект пространственной жёсткости, позволяет более рационально подходить к проектированию, дифференцируя жёсткость и крепление ограждения по его периметру, а также правильно расставляя точки геотехнического мониторинга, концентрируя их на наиболее опасных участках – серединах длинных пролётов.

На основе анализа характера работы ограждающих конструкций можно сформулировать ряд принципиальных рекомендаций для практики. На стадии проектирования выбор типа ограждения должен быть обусловлен не столько экономией, сколько прогнозируемым

уровнем деформаций и уязвимостью соседней застройки. Для объектов вблизи памятников архитектуры или ветхих зданий предпочтение следует отдавать максимально жёстким системам. [9] Проект производства работ должен детально регламентировать технологическую последовательность, уделяя особое внимание критическим операциям: скорости разработки и моментам установки каждого яруса крепления. Необходимо тщательно прорабатывать вопросы водоотлива и противофильтрационных мероприятий, так как изменение гидрогеологического режима является одной из частых причин неучтённых осадок.

На стадии строительства непрерывный геотехнический мониторинг становится не формальностью, а главным инструментом управления безопасностью. [10] Программа наблюдений должна включать систематический геодезический контроль горизонтальных и вертикальных перемещений ограждения, маркшейдерские наблюдения за осадками и кренами окружающих зданий, а также, по возможности, измерение усилий в элементах крепления. Полученные данные должны оперативно анализироваться и сравниваться с прогнозными расчётами. [11] Приближение значений к предельно допустимым или неблагоприятная динамика должны служить незамедлительным сигналом для применения заранее разработанных мероприятий по усилению: устройства дополнительного яруса крепления, выполнения инъекционного упрочнения грунта с внешней стороны котлована или подведения подкосов. Такой системный, основанный на обратной связи подход позволяет перейти от пассивного констатирования деформаций к активному управлению поведением системы «котлован – ограждение – застройка».[12]

Таким образом, исследование подтверждает, что характер работы защитных сооружений котлованов в стеснённых городских условиях коренным образом отличается от такового на свободных площадках. Ключевым становится деформационный критерий, а ограждение выполняет функцию активного барьера, минимизирующего зону влияния строительных работ. Наибольшее воздействие на окружающую среду оказывают гибкие системы при нарушении технологии их раскрепления, в то время как жёсткие конструкции, несмотря на высокую стоимость, могут оказаться экономически оправданными за счёт снижения рисков и предотвращения ущерба. Учёт пространственной работы, тщательная проработка последовательности операций и организация непрерывного мониторинга с оперативной обратной связью являются обязательными элементами успешной и безопасной реализации проекта. Дальнейшие исследования в этой области целесообразно направлять на более детальную типизацию поведения различных систем в зависимости от конкретных городских и геологических контекстов, а также на формализацию критериев для обоснованного выбора технологии на ранних стадиях проектирования.

Список литературы

1. СП 22.13330.2016 «Основания зданий и сооружений». Актуализированная редакция СНиП 2.02.01-83*.
2. СП 116.13330.2012 «Инженерная защита территорий, зданий и сооружений от опасных геологических процессов. Основные положения». Актуализированная редакция СНиП 22-02-2003.
3. Мангушев Р.А., Никифорова Н.С., Усманов Р.А. Геотехническое сопровождение строительства в стесненных условиях мегаполисов. – СПб.: Изд-во Политехн. ун-та, 2018. – 280 с.

4. Теличенко В.И., Тер-Мартиросян З.Г. Технологии устройства ограждений котлованов в городском строительстве. – М.: Изд-во АСВ, 2015. – 320 с.
5. Ухов С.Б., Семёнов В.В., Знаменский В.В. и др. Механика грунтов, основания и фундаменты. – М.: Изд-во АСВ, 2019. – 592 с.
6. Петрухин В.В., Лебедев С.Н. Анализ причин деформаций ограждения котлована в стеснённых городских условиях // Основания, фундаменты и механика грунтов. – 2021. – № 4. – С. 17-23.
7. Фадеев А.Б., Семёнов Е.В. Сравнительная эффективность буросекущих свай и шпунта при строительстве в стеснённых условиях // Жилищное строительство. – 2020. – № 1-2. – С. 38-42.
8. Глотов Н.М., Чистяков А.Д. Пространственная работа ограждений глубоких котлованов // Вестник гражданских инженеров. – 2019. – № 3(74). – С. 52-58.
9. Решение стратегических задач развития территорий: современные подходы / Е. М. Вольская, О. В. Веретенникова, Е. В. Балабенко [и др.]. – Харьков : Издательство «НТМТ», 2016. – 261 с.
10. Решение стратегических задач развития территорий: современные подходы / Е. М. Вольская, О. В. Веретенникова, Е. В. Балабенко [и др.]. – Харьков : Издательство «НТМТ», 2016. – 261 с.
11. Балабенко, Е. В. Концептуальные принципы развития жилищного строительства путем использования форм государственно-частного партнерства / Е. В. Балабенко, О. А. Стукалова // Экономика строительства и городского хозяйства. – 2016. – Т. 12, № 3. – С. 107-114
12. Балабенко, Е. В. Методика оценки строительного комплекса: корпоративный уровень / Е. В. Балабенко, А. В. Бородацкая, Н. В. Брайла // π-Economy. – 2024. – Т. 17, № 1. – С. 113-125

References

1. SP 22.13330.2016 "Foundations of Buildings and Structures." Updated version of SNiP 2.02.01-83*.
2. SP 116.13330.2012 "Engineering Protection of Territories, Buildings, and Structures from Hazardous Geological Processes. Basic Provisions." Updated version of SNiP 22-02-2003.
3. Mangushev R.A., Nikiforova N.S., Usmanov R.A. Geotechnical Support for Construction in Confined Conditions of Megacities. St. Petersburg: Polytechnic University Press, 2018. 280 p.
4. Telichenko V.I., Ter-Martirosyan Z.G. Technologies for the construction of excavation pit fencing in urban construction. Moscow: ASV Publishing House, 2015, p. 320
5. Ukhov SB, Semenov VV, Znamensky VV, et al. Soil Mechanics, Foundations, and Foundations. Moscow: ASV Publishing House, 2019, p.592
6. Petruhin VV, Lebedev SN. Analysis of the causes of excavation pit fencing deformations in confined urban conditions // Foundations, Foundations, and Soil Mechanics. 2021, No. 4, pp. 17-23.
7. Fadeev AB, Semenov EV. Comparative efficiency of secant piles and sheet piles in construction in confined conditions // Housing construction. – 2020. – No. 1-2. – pp. 38-42.
8. Glotov N.M., Chistyakov A.D. Spatial work of deep excavation fences // Bulletin of civil engineers. – 2019. – No. 3(74). – pp. 52-58.

9. Solving strategic problems of territorial development: modern approaches / E. M. Volskaya, O. V. Veretennikova, E. V. Balabenko [et al.]. – Kharkov: NTMT Publishing House, 2016. – p. 261
10. Solving strategic problems of territorial development: modern approaches / E. M. Volskaya, O. V. Veretennikova, E. V. Balabenko [et al.]. – Kharkov: NTMT Publishing House, 2016. – p.261
11. Balabenko, E. V. Conceptual principles of housing construction development through the use of public-private partnership forms / E. V. Balabenko, O. A. Stukalova // Economics of construction and urban economy. - 2016. - Vol. 12, No. 3. - pp. 107-114
12. Balabenko, E. V. Methodology for assessing the construction complex: corporate level / E. V. Balabenko, A. V. Borodatskaya, N. V. Braila // π-Economy. - 2024. - Vol. 17, No. 1. - pp. 113-125