# АНАЛИЗ, МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ ЭКОСИСТЕМАХ

**УДК 004.89** **EDN XQSMTI**

## ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ (IIOT)

**Коды JEL:** C11, C63, C81, L86

***Грешонков А. М.,*** *доктор экономических наук, профессор кафедры корпоративных информационных систем и программирования, Воронежский государственный университет инженерных технологий, г. Воронеж, Россия*
*E-mail: aleksej-greshonkov@yandex.ru; SPIN-**код**: 2996-3213; ORCID: 0000-0001-8274-3323*

***Моисеев В. С.,*** *аспирант кафедры корпоративных информационных систем и программирования, Воронежский государственный университет инженерных технологий, г. Воронеж, Россия*
*E-mail: vadim.moiseev.2002@mail.ru; SPIN-код: отсутствует*

Поступила в редакцию 27.10.2025. Принята к публикации 21.11.2025

Аннотация
Актуальность темы. *Необходимость применения технологий искусственного интеллекта для обеспечения информационной безопасности в промышленном Интернете вещей (IIoT), приобретает в современных условиях большое значение.*
Цель. *Анализ основных угроз и уязвимости, возникающих в процессе интеграции промышленных сетей и систем управления в единую цифровую инфраструктуру. Обоснование методов машинного обучения и интеллектуального анализа данных, которые позволяют автоматизировать процесс выявления аномалий и атак в промышленных системах.*
Методология. *Методы логического и сравнительного анализа практик обеспечения информационной безопасности в промышленном Интернете вещей (IIoT).*
Результаты и выводы. *На основе анализа и оценки текущей ситуации в сфере обеспечения информационной безопасности в промышленном Интернете вещей (IIoT) определены направления развития интеллектуальных систем защиты, их структура и роль в предотвращении киберинцидентов на производственных объектах.*
Ключевые слова: *промышленный Интернет вещей, информационная безопасность, искусственный интеллект, машинное обучение, анализ данных, киберугрозы, автоматизация.*

**UDC 004.89** **EDN XQSMTI**

## INTELLIGENT INFORMATION SECURITY SYSTEMS IN THE INDUSTRIAL INTERNET OF THINGS (IIOT)

**JEL Codes:** C11, S63, S81, L86

***Greshonkov A. M.,*** *Doctor of Economics, Professor, Department of Corporate Information Systems and Programming, Voronezh State University of Engineering Technologies, Voronezh, Russia*
*E-mail: aleksej-greshonkov@yandex.ru; SPIN-code: 2996-3213; ORCID: 0000-0001-8274-3323*

***Moiseev V. S.,*** *graduate student of the Department of Corporate Information Systems and Programming, Voronezh State University of Engineering Technologies, Voronezh, Russia*
*E-mail: vadim.moiseev.2002@mail.ru; SPIN-code: missing*

Received by the editorial office 27.10.2025. Accepted for publication 21.11.2025

Abstract

Relevance of the topic. *The need to apply artificial intelligence technologies to ensure information security in the industrial Internet of Things (IIoT).*

Purpose. *Analysis of the main threats and vulnerabilities arising during the integration of industrial networks and control systems into a single digital infrastructure. Rationale for machine learning and data mining techniques that automate the process of detecting anomalies and attacks in industrial systems.*

Methodology. *Methods for logical and comparative analysis of information security practices in the industrial Internet of Things (IIoT).*

Results and conclusions. *Based on the analysis and assessment of the current situation in the field of information security in the industrial Internet of Things (IIoT), the directions for the development of intelligent security systems, their structure and role in preventing cyber incidents at production facilities are presented.*

Keywords: *industrial Internet of Things, information security, artificial intelligence, machine learning, data analysis, cyber threats, automation.*

**Введение**

Промышленный Интернет вещей (Industrial Internet of Things, IIoT) объединяет устройства, датчики, промышленные контроллеры и системы управления в единую экосистему для повышения эффективности производственных процессов. Сбор и анализ данных в реальном времени позволяют автоматизировать производство, однако с ростом числа подключенных устройств увеличивается и риск кибератак.

Проблема безопасности IIoT становится особенно актуальной в условиях цифровой трансформации промышленности и перехода к концепции «Индустрия 4.0». Угрозы для таких систем включают несанкционированный доступ, вмешательство в работу контроллеров, перехват управляющих команд, подмену данных датчиков, а также вредоносное воздействие на физические процессы.

Одной из ключевых задач является создание интеллектуальных систем, способных самостоятельно выявлять аномалии, анализировать сетевое поведение и предотвращать инциденты безопасности без участия человека. Для решения этих задач применяются методы искусственного интеллекта и машинного обучения.

***Использование методов машинного обучения для анализа данных IIoT***

Интеллектуальные алгоритмы позволяют анализировать потоковые данные, поступающие от устройств, и выделять нетипичные события, которые могут свидетельствовать о кибератаке или технической неисправности.

К основным применяемым методам относятся:

• Методы обучения с учителем. Используются для классификации сетевых пакетов и событий как нормальных или подозрительных. Модель обучается на заранее размеченных данных, что позволяет эффективно выявлять известные типы атак (например, DDoS или SQL-инъекции).

• Методы обучения без учителя. Применяются для обнаружения ранее неизвестных угроз. Алгоритмы кластеризации (например, K-means, DBSCAN) группируют поведение устройств по схожим признакам, выявляя отклонения.

• Нейронные сети и глубокое обучение. Сверточные и рекуррентные нейросети способны анализировать временные ряды данных с датчиков, фиксируя малейшие отклонения от нормального состояния системы. Такие методы особенно эффективны для обнаружения сложных атак на уровне протоколов управления.

• Байесовские модели и деревья решений. Позволяют оценивать вероятность наступления инцидента, учитывать множество факторов риска и выстраивать предиктивные модели поведения устройств.

Использование этих методов обеспечивает формирование адаптивной системы защиты, которая со временем обучается на новых данных и повышает точность обнаружения угроз.

***Применение ИИ в системах мониторинга и реагирования***

Интеллектуальные системы безопасности IIoT включают несколько функциональных модулей:

1. Сбор данных. Поток телеметрии от сенсоров, контроллеров и шлюзов передается в систему мониторинга.

2. Предварительная обработка. Выполняется фильтрация и нормализация данных, удаляются шумы, исправляются ошибки измерений.

3. Интеллектуальный анализ. Применяются алгоритмы машинного обучения для выявления аномалий, а также прогнозирования потенциальных атак.

4. Принятие решений. На основе анализа формируются автоматические правила реагирования: блокировка узлов, уведомление оператора, изменение маршрутизации данных.

5. Отчётность и визуализация. Система отображает состояние устройств, угрозы, статисти-

ку атак и рекомендации по устранению уязвимостей.

Такой подход позволяет перейти от реактивной модели защиты (когда действия предпринимаются после инцидента) к превентивной — когда система самостоятельно предсказывает и предотвращает возможные инциденты.

***Архитектура интеллектуальной системы безопасности IIoT***

Архитектура системы включает следующие компоненты:

- Уровень устройств (Device Layer): промышленные контроллеры, сенсоры, исполнительные механизмы.
- Сетевой уровень (Network Layer): протоколы передачи данных (Modbus, MQTT, OPC-UA).
- Аналитический уровень (Analytics Layer): модули искусственного интеллекта, нейросетевые алгоритмы анализа.
- Уровень реагирования (Response Layer): автоматические действия, скрипты защиты, уведомления.
- Интерфейс оператора (Dashboard Layer): визуализация состояния сети, журнал событий, отчёты.

Для построения такой системы применяются современные технологии: Python, TensorFlow, Scikit-learn, а также платформы визуализации данных и базы знаний об уязвимостях (например, NVD).

Практическое значение и перспективы

Интеграция искусственного интеллекта в систему ИБ промышленного Интернета вещей имеет следующие преимущества:

- повышение точности обнаружения кибератак;
- автоматизация процессов реагирования;
- сокращение человеческого фактора;
- повышение надёжности работы промышленных комплексов;
- обеспечение соответствия стандартам безопасности (ГОСТ Р 57580, ISO/IEC 27001, NIST SP 800-82).

В перспективе развитие таких систем будет направлено на создание самообучающихся защитных платформ, способных адаптироваться к новым угрозам без необходимости ручной настройки. Использование федеративного обучения позволит обучать модели на распределённых данных без передачи конфиденциальной информации за пределы предприятия.

**Заключение**

Искусственный интеллект становится неотъемлемой частью современных систем информационной безопасности в промышленности. Применение машинного обучения и интеллектуального анализа данных позволяет обнаруживать угрозы в реальном времени, адаптироваться к новым видам атак и минимизировать риски человеческих ошибок.

Создание комплексных интеллектуальных систем защиты IIoT — ключевой шаг к устойчивому и безопасному развитию промышленности в условиях цифровой трансформации.

***Информация о конфликте интересов***

*Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи.*

**ЛИТЕРАТУРА**

1. ГОСТ Р 57580.1-2017. Защита информации. Безопасность финансовых (банковских) операций.

2. NIST SP 800-82 Rev.2. Guide to Industrial Control Systems (ICS) Security.

3. ISO/IEC 27001:2022 Information Security Management Systems — Requirements.

4. *Белов А. С.* Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. — 2022. — № 4. — С. 76—80.

5. *Герасимов С. А.* Искусственный интеллект в обеспечении кибербезопасности / С. А. Герасимов. — Санкт-Петербург : Питер, 2022.

6. *Гладких А. В.* Методы защиты от DDoS-атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.). — Екатеринбург, 2022. — С. 3—5.

7. *Ефремов Н. А.* Процессы информатизации экономики и информационная безопасность / Н. А. Ефремов, Т. В. Мужжавлева // Экономика и предпринимательство. — 2023. — № 3. — С. 287—294.

8. *Малыгин В. В.* Информационная безопасность промышленных систем управления / В. В. Малыгин. — Москва : Бином, 2020.

9. Повышение уровня информационной безопасности опубликованных корпоративных ресурсов в Интернете = Information Security Hardening Published Corporate Resources on the Internet / А. В. Затонский, Б. С. Дмитриевский, Е. А. Митюков [и др.] // Защита информации. Инсайд. — 2022. — № 3. — С. 68—71.

10. *Федотова Г. В.* Угрозы кибербезопасности устойчивости цифровых платформ / Г. В. Федотова, Д. А. Куразова // BI-технологии и корпора-

тивные информационные системы в оптимизации бизнес-процессов цифровой экономики : материалы IX Междунар. науч.-практ. конф. (Екатеринбург, 2 дек. 2021 г.). — Екатеринбург, 2021. — С.118—122.

**LITERATURE**

1. GOST R 57580.1-2017. Information protection. Security of financial (banking) operations.

2. NIST SP 800-82 Rev.2. Guide to Industrial Control Systems (ICS) Security.

3. ISO/IEC 27001:2022 Information Security Management Systems — Requirements.

4. *Belov A. S.* Modernization of the Information Security System = Modernization of the Information Security System: The Approach to Determining the Frequency: an approach to determining the frequency / A. S. Belov, M. M. Dobryshin, D. E. Shugurov // Information Protection. Inside. — 2022. — № 4. — S. 76—80.

5. *Gerasimov S. A.* Artificial intelligence in ensuring cybersecurity / S. A. Gerasimov. — St. Petersburg : Peter, 2022.

6. *Gladkikh A. V.* Methods of protection against DDoS-attacks in intelligent networks / A. V. Gladkikh // Digital transformation of society and information security: materials All-Russia. scientific-practical. conf. (Yekaterinburg, May 18, 2022). — Yekaterinburg, 2022. — S. 3—5.

7. *Efremov N. A.* Processes of informatization of the economy and information security / N. A. Efremov, T. V. Muzhzhavleva // Economics and Entrepreneurship. — 2023. — № 3. — S. 287—294.

8. *Malygin V. V.* Information security of industrial control systems / V. V. Malygin. — Moscow : Binom, 2020.

9. Improving the level of information security of published corporate resources on the Internet = Information Security Hardening Published Corporate Resources on the Internet / A. V. Zatonsky, B. S. Dmitrievsky, E. A. Mityukov [et al.] // Information protection. Inside. — 2022. — № 3. — S. 68—71.

10. *Fedotova G. V.* Threats to cybersecurity stability of digital platforms / G. V. Fedotova, D. A. Kurazova // BI technologies and corporate information systems in optimizing the business processes of the digital economy: materials of the IX International. scientific.-pract. conf. (Yekaterinburg, 2 Dec 2021). — Yekaterinburg, 2021. — P. 118—122.

**УДК 330.322** **EDN XSDDWD**

# АНАЛИТИЧЕСКИЕ ПРОЦЕДУРЫ АНАЛИЗА ИНВЕСТИЦИОННЫХ ПРОЦЕССОВ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

**Коды JEL:** G30, G31, M10

***Дремов** А. Р., аспирант кафедры экономической безопасности, Воронежский государственный технический университет, г. Воронеж, Россия*
*E-mail: art_dremov@mail.ru; SPIN-код: 9619-4671*

***Букреев А.** М., доктор экономических наук, профессор, профессор кафедры экономической безопасности, Воронежский государственный технический университет, профессор кафедры экономики, финансов и менеджмента, Российская академия народного хозяйства и государственной службы при Президенте РФ (Воронежский филиал), г. Воронеж, Россия*
*E-mail: abukreev@zentrtorg.ru; SPIN-код: 1177-2602*

Поступила в редакцию 03.12.2025 Принята к публикации 13.12.2025

Аннотация

Актуальность темы. *Современным компаниям необходим качественный механизм управления инвестициями, адаптированный к условиям новой, цифровой реальности. Требуются комплексные теоретико-практические и методологические разработки по внедрению подобного механизма в условиях цифровой интерпретации управления инвестициями.*

Цель. *Предложить авторскую методику текущего анализа механизма управления инвестициями на предприятиях.*

Методология *исследования построена на аналитических процедурах оценки деятельности и инвестиционных процессов промышленных предприятий.*

Результаты и выводы. *Анализ особенностей инвестиционной деятельности и оценка текущей ситуации в сфере управления инвестициями позволяют сделать вывод о том, насколько реально действуют на предприятии механизм управления инвестициями, его отдельные элементы, или же требуются дополнительные разработки по формированию и внедрению данного механиз-*