УДК 004.738.5

# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В СИСТЕМАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Г.В. Нестерович, Е.И. Баяк
*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

**Аннотация.** Промышленный интернет вещей (IIoT) играет ключевую роль в современной промышленности, обеспечивая автоматизацию и повышение эффективности производственных процессов. Однако интеграция физических и цифровых систем создает серьезные риски для кибербезопасности, что может привести к катастрофическим последствиям, включая остановку производства и угрозу жизни сотрудников. В статье рассматриваются основные угрозы безопасности в системах IIoT, предлагаются методы обеспечения безопасности, также обсуждаются перспективные технологии. Подчеркивается важность комплексного подхода, включающего технические, организационные и регуляторные меры, для обеспечения устойчивости промышленных систем к кибератакам.
**Ключевые слова:** промышленный интернет вещей (IIoT), кибербезопасность, угрозы безопасности, методы защиты.

# ENSURING SECURITY IN INDUSTRIAL INTERNET OF THINGS SYSTEMS

G.V. Nesterovich, E.I. Bayak
*Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus*

**Abstract.** The Industrial Internet of Things (IIoT) plays a key role in modern industry, providing automation and increasing the efficiency of production processes. However, the integration of physical and digital systems creates serious risks for cybersecurity, which can lead to catastrophic consequences, including production shutdowns and threats to the lives of employees. The article examines the main security threats in IIoT systems, proposes security methods, and discusses promising technologies. The importance of an integrated approach, including technical, organizational and regulatory measures, is emphasized to ensure the resilience of industrial systems to cyberattacks.
**Keywords:** Industrial Internet of Things (IIoT), cybersecurity, security threats, protection methods.

## Введение

Промышленный интернет вещей (IIoT) стал неотъемлемой частью современной промышленности, открывая новые возможности для автоматизации, анализа данных и повышения эффективности производственных процессов. Однако интеграция физических и цифровых систем создает значительные риски, связанные с кибербезопасностью. Уязвимости в системах IIoT могут привести к серьезным последствиям: от остановки производства до угрозы жизни сотрудников. Например, в 2022 году кибератака на сталелитейный завод в Иране привела к разливу расплавленного металла, что наглядно демонстрирует, насколько критична защита промышленных систем.

Цель данной статьи – рассмотреть ключевые аспекты обеспечения безопасности в системах IIoT, включая основные угрозы, методы защиты и перспективные технологии, которые помогут минимизировать риски и обеспечить устойчивость промышленных объектов к кибератакам.

## Основные угрозы безопасности в IIoT

Промышленные системы, подключенные к интернету, сталкиваются с множеством угроз, которые могут быть как традиционными, так и специфическими для IIoT. Одной из главных проблем является уязвимость периферийных устройств. Промышленные контроллеры, датчики и шлюзы часто проектируются с упором на функциональность, а не на безопасность. Это делает их легкой мишенью для злоумышленников. Например, в 2024 году были обнаружены уязвимости в контроллерах Mitsubishi Electric, которые позволяли нарушать технологические процессы.

Еще одной серьезной угрозой является использование устаревшего программного обеспечения. Средний срок устаревания прошивки IoT-устройств составляет 6 лет, что делает их уязвимыми для эксплойтов. Это особенно актуально для промышленных систем, где обновление оборудования может быть дорогостоящим и сложным процессом.

Кроме того, незащищенные протоколы и сети представляют значительный риск. Многие промышленные системы до сих пор используют устаревшие протоколы, такие как Modbus, которые не предусматривают шифрование данных. Это позволяет злоумышленникам перехватывать информацию и вмешиваться в работу систем. В 2023 году исследования показали, что 70 % устройств передавали данные без шифрования, что делает их легкой добычей для хакеров.

Слабые механизмы аутентификации также остаются одной из ключевых проблем. Использование стандартных паролей и отсутствие многофакторной аутентификации упрощают подбор учетных данных. Ярким примером является ботнет Mirai, который в 2016 году атаковал устройства с паролями по умолчанию, вызвав глобальные сбои.

## Методы обеспечения безопасности

Для защиты систем IIoT необходимо применять комплексный подход, который включает как технические, так и организационные меры. Одним из наиболее эффективных методов является эшелонированная защита (Defense-in-depth). Этот подход предполагает создание многоуровневой архитектуры, где каждая система защищена несколькими уровнями безопасности. Например, использование межсетевых экранов, систем обнаружения вторжений (IDS) и сегментации сетей позволяет изолировать критические системы и минимизировать риски.

Регулярные обновления и патчинг также играют ключевую роль в обеспечении безопасности. Автоматизация обновлений прошивки и ПО помогает устранять уязвимости до того, как они будут использованы злоумышленниками. Например, решения Kaspersky IoT Secure Gateway обеспечивают автоматическое обновление устройств через платформу Kaspersky Appicenter, что значительно снижает риски.

Строгая аутентификация и шифрование данных являются неотъемлемой частью защиты IIoT. Внедрение многофакторной аутентификации и использование современных протоколов шифрования, таких как TLS/SSL, позволяет защитить данные от перехвата и несанкционированного доступа. Например, использование WPA3 в Wi-Fi-сетях обеспечивает более высокий уровень безопасности по сравнению с предыдущими версиями.

Стандартизация и законодательное регулирование также играют важную роль в обеспечении безопасности. Принятие законов, обязывающих производителей обеспечивать безопасность на этапе проектирования, помогает устранить многие уязвимости. Например, британский законопроект 2020 года требует использования уникальных паролей и публикации сроков поддержки устройств, что способствует повышению уровня безопасности.

## Перспективные технологии защиты

С развитием технологий появляются новые методы защиты, которые могут значительно повысить безопасность систем IIoT. Одной из таких технологий являются кибериммунные системы. Архитектура Security by Design, как в KasperskyOS, предполагает встроенную защиту на уровне микроядра, что предотвращает 96 % эксплойтов, актуальных для Linux.

Искусственный интеллект и машинное обучение также находят применение в обеспечении безопасности. Эти технологии позволяют анализировать сетевой трафик в режиме реального времени и выявлять аномалии, которые могут свидетельствовать о кибератаке. Системы SIEM (Security Information and Event Management) уже активно используются для мониторинга и предотвращения угроз.

Блокчейн-технологии также начинают использоваться для защиты IIoT. Децентрализованное хранение данных и защита целостности транзакций помогают предотвратить подмену данных в системах smart-city и других промышленных приложениях.

Квантовое шифрование, хотя и находится на экспериментальной стадии, обещает стать революционным методом защиты данных. Использование квантовых ключей делает шифрование устойчивым ко взлому даже с использованием квантовых компьютеров.

## Заключение

Обеспечение безопасности в системах промышленного интернета вещей – это сложная и многогранная задача, которая требует комплексного подхода. Угрозы, с которыми сталкиваются промышленные системы, постоянно эволюционируют, что требует постоянной адаптации и внедрения новых технологий.

Ключевым аспектом защиты является не только использование современных технологий, но и обучение персонала, а также соблюдение стандартов и нормативных требований.

Инвестиции в безопасность на всех этапах жизненного цикла устройств – от проектирования до вывода из эксплуатации – являются необходимым условием для

обеспечения устойчивости промышленных систем к кибератакам. Только комплексный подход, сочетающий технические, организационные и регуляторные меры, позволит минимизировать риски и обеспечить безопасность в эпоху промышленного интернета вещей.

## Список использованных источников

1. Намиот Д.Е., Сухомлин В.А. (2023) О кибербезопасности систем интернета вещей. *Международный журнал открытых информационных технологий* (3), 85-94.
2. Маммадов И.Р. (2024) Уязвимости и риски устройств Интернета вещей. *Молодой ученый*, (545), 15–17.

## References

1. Butun I. (2020) *Industrial IoT: Challenges, Design Principles, Applications, and Security. Germany, Springer.*
2. Namiot D.E., Sukhomlin V.A. (2023) On the cybersecurity of Internet of Things systems. *International Journal of Open Information Technologies* (3), 85–94 (in Russian).
3. Mammadov I.R. (2024) Vulnerabilities and risks of Internet of Things devices. *Young scientist*. (545), 15–17 (in Russian).

### Сведения об авторах

**Нестерович Г.В.,** студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nesterovicgleb@gmail.com.
**БаякЕ.И,** инженер-программист, отдел интегрированных автоматизированных систем управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», e.baiak@bsuir.by.

### Information about the authors

**Nesterovich G.V.,** Student, Education Institution "Belarusian State University of Informatics and Radioelectronics", nesterovicgleb@gmail.com.
**Bayak E.I.,** Software Engineer, Department of integrated Automated Control Systems, Belarusian State University of Informatics and Radioelectronics, e.baiak@bsuir.by.