DOI:10.58168/AIARMTOES2025_62-68
УДК 004.9

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ
SECURITY ISSUES OF THE INDUSTRIAL INTERNET OF THINGS

Евдокимова С.А., к.т.н., доцент
ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»
г. Воронеж, Россия
evdsv@mail.ru
Evdokimova S.A., CSc (Engineering), Associate Professor
FSBEI HE «Voronezh State University of Forestry and Technologies named after G.F. Morozov»
Voronezh, Russian Federation

Аннотация: В соответствии с концепцией Индустрии 4.0 стремительно развивается промышленный интернет вещей, обеспечивающий интеграцию компьютерных сетей и автоматизацию производства для удаленного управления, контроля и сбора данных. Использование информационных и сетевых технологий, облачных систем обработки данных влечет за собой возможности кибератак. В работе рассматриваются основные угрозы безопасности промышленного интернета вещей.

Summary: In accordance with the concept of Industry 4.0, the industrial Internet of Things is rapidly developing, providing the integration of computer networks and automation of production for remote control, monitoring and data collection. The use of information and network technologies, cloud-based data processing systems entails the possibility of cyberattacks. The paper considers the main security threats of the industrial Internet of Things.

Ключевые слова: промышленный интернет вещей, информационная безопасность, угрозы безопасности, ISO 27001, IEC 62443.

Keywords: IIoT, information security, security threats, ISO 27001, IEC 62443.

Промышленный интернет вещей (IndustrialInternetofThings, IIoT) – это система объединенных компьютерных сетей и подключенных промышленных

(производственных) объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме [1]. IIoT позволяет автоматически управлять производственными процессами за счет объединения информационных и операционных технологий. Взаимосвязанное интеллектуальное оборудование, сенсорные устройства и компьютерные сети обеспечивают автоматизированный сбор и анализ данных, поддержку принятия решений для повышения производительности, эффективности распределения и управления всеми видами ресурсов и работы предприятия в целом.

Исходные данные поступают от различных датчиков, машин, оборудования и других устройств, подключенных к сети, и представляют собой цифровой отпечаток производственного процесса. Например, данные о состоянии оборудования, производственные показатели, параметры контроля качества продукции и другие; геоданные о местоположении транспортных средств, сотрудников, роботов и другого оборудования на территории предприятия; данные об энергопотреблении (расходы топлива на технологические процессы; объемы используемой воды в технологических операциях и т.д.), параметры окружающей среды (влажность, освещенность, уровень загрязнения воздуха), видеозаписи камер наблюдений и т.п.

Собранные данные передаются в централизованную облачную систему или базу данных и с помощью программного обеспечения используются для мониторинга работы машин, анализа показателей работы автоматизированной системы, выявления узких мест в производственных процессах.

Основными проблемами, которые возникают при внедрении IIoT, являются проблемы безопасности, конфиденциальности данных и обеспечения надежности функционирования всех устройств и системы в целом. IIoT предполагает совместное использование и передачу данных между несколькими устройствами, что требует защиту данных от внешних кибератак и угроз. В качестве каналов кибератак злоумышленники могут использовать удаленное подключение к отдельным устройствам, атаки на серверы и сегменты корпоративных промышленный сетей, уязвимости каналов технической поддержки и др. [2-5].

Для IIoT большое значение имеет непрерывность бизнес-процессов, поэтому особенно важно поддерживать бесперебойность работы устройств. Нарушения целостности данных может привести к неправильным решениям и потенциально опасным ситуациям, поэтому достоверность данных играет

большое значение для обеспечения безопасной и эффективной работы промышленных систем.

Описание основных видов угроз безопасности промышленного интернета вещей приведено в таблице 1.

Таблица 1 – Основные угрозы безопасности IIoT

Вид угрозы безопасности	Описание
Уязвимости устройств	Многие устройства IIoT имеют ограниченные вычислительные ресурсы и часто разрабатываются с минимальными затратами на безопасность. Это делает их уязвимыми для таких атак, как инъекции вредоносного кода, подбор паролей, отсутствие шифрования данных, передаваемых между устройствами и др.
Недостаточная сегментация сети	Если промышленные сети недостаточно сегментированы, то компрометация одного устройства, может привести к взлому всей системы управления.
Отсутствие обновлений ПО	Часто на предприятиях игнорируется необходимость установки обновлений ПО, или производители оборудования не предоставляют регулярные обновления ПО, что делает устройства IIoT уязвимыми
Проблемы с аутентификацией и авторизацией	На предприятиях часто используются стандартные пароли оборудования, отсутствует двухфакторная аутентификация, что упрощает подбор паролей и несанкционированный доступ к устройствам и данным
Слабая защита данных	Передача данных между устройствами и системами часто осуществляется без шифрования, что делает данные уязвимыми для перехвата и модификации.
Социальная инженерия	Работников предприятий могут обманом заставить установить вредоносное программное обеспечение или передать конфиденциальную информацию.
Ошибки конфигурации сетей и устройств	Вследствие ошибок конфигурации настроек оборудования появляются возможности для атак.
DDos-атаки	Могут привести к перегрузу сети и остановке производственных процессов

Продолжение таблицы 1

Вид угрозы безопасности	Описание
Вредоносное программное обеспечение	Подключение зараженного устройства сети может распространять вредоносные приложения по всей инфраструктуре IIoT
Аварии и сбои	Потеря связи между устройствами может привести к остановке производства или аварийным ситуациям

Для обеспечения безопасности промышленного интернета вещей существуют международные и отраслевые стандарты, которые описывают требования и методы обеспечения защиты данных, конфиденциальности и целостности информации, и позволяют минимизировать риски, связанные с кибератаками.

IIoT интегрируется в информационную среду, информационная безопасность которой опирается на стандарт ISO 27001 [6]. В основе операционных технологий лежит стандарт IEC 62443, который определяет требования и процессы внедрения и поддержания кибербезопасности систем промышленной автоматизации и управления [7]. Рекомендации по рискам, принципам и средствам контроля безопасности и конфиденциальности в Интернете вещей содержатся в стандарте ISO/IEC 27400 [8].

Авторы в [9] исследовали требования стандарта IEC 62443 для обеспечения безопасности IIoT и отметили, что среда IIoT имеет большое количество устройств, для которых характерны облачные вычисления, ограниченность внутренних ресурсов, интеграция с системой управления, что влечет за собой дополнительные уязвимости и угрозы безопасности.

В работе [10] авторы следовали трехэтапному подходу для контроля рисков безопасности, который включал идентификацию критически важных информационных систем; подробный анализ рисков для этих систем; определение мер безопасности, применимых к другим информационных системам. Оценка рисков выполнялась по двум параметрам – вероятность совершения атаки на систему и серьезность разрушений в случае атаки. Одним из самых больших выявленных рисков оказались ограниченные возможности аутентификации IoT-устройств.

Таким образом, в промышленном интернете вещей и АСУ ТП необходимо использовать программно-аппаратные средства защиты, позволяющие обеспечить межсетевое экранирование системы, разграничение прав доступа к объ-

ектам АСУ, анализ пакетов промышленных протоколов, предотвратить действия вредоносных и вирусных программ.

Для обнаружения угроз необходимо использовать систему обнаружения вторжения (СОВ), систему управления информацией и событиями безопасности (SIEM) и систему обнаружения и реагирования на конечные точки (EDR).

Список литературы

1. Верещагина, Е.А. Проблемы безопасности Интернета вещей : учебное пособие / Е.А. Верещагина, И.О. Капецкий, А.С. Ярмонов. – М. : Мир науки, 2021. – 105 с. – Сетевое издание. – URL: https://izd-mn.com/PDF/20MNNPU21.pdf.

2. Чернов, Д. В. Построение комплексной системы информационной безопасности АСУ ТП / Д.В. Чернов, В.В. Котов, С.Ю. Борзенкова // Машиностроение: сетевой электронный научный журнал. – 2023. – Vol. 10, № 2 – С. 27-32.

3. Винявский, А.А. Industrial Internet of Things: риски и защита в цифровую эпоху / А.А. Винявский // Автоматизация в промышленности. – 2024. - № 9. – С. 57-60.

4. Новикова, Т.П. Автоматизированное проектирование расположения базовых станций беспроводной сотовой связи / Т.П. Новикова, С.А. Евдокимова, Р.Ю. Медведев // Моделирование систем и процессов. – 2023. – Т. 16, № 4. – С. 61-70.

5. Козлов, С.Д. Метод анализа безопасности для промышленного интернета вещей / С.Д. Козлов, А.И. Ларин // Территория науки и образования. – 2024. –№ 1. – С. 71-74.

6. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Дата введ. 01.01.2022. – М. : СтандартИнформ, 2022. – 112 с.

7. ГОСТ Р МЭК 62443-2-1-2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. – М. : СтандартИнформ, 2015. – 141 с.

8. ISO/IEC 27400:2022. Кибербезопасность. Безопасность и конфиденциальность IoT. Руководящие положения. – Дата введ. 07.06.2022. – ISO, 2022. – 50 с.

9. Cindrić, I. Mapping of Industrial IoT to IEC 62443 Standards / I. Cindrić, M. Jurčević, T. Hadjina // Sensors. – 2025. – Vol. 25(3). – S. 728. – DOI: 10.3390/s25030728.

10. Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443 / H.L. Hassani [et al.] // Procedia Computer Science. – 2021. – Vol. 191. – Pp. 33-40.

References

1. Vereshchagina, E.A. Security problems of the Internet of Things : a textbook / E.A. Vereshchagina, I.O. Kopetsky, A.S. Yarmonov. – M. : Mir nauki, 2021. – 105 p. – Online edition. – URL: https://izd-mn.com/PDF/20MNNPU21.pdf.

2. Chernov, D. V. Building an integrated information security system for automated process control systems / D.V. Chernov, V.V. Kotov, S.Yu. Borzenkova // Mashino-stroenie: a network electronic scientific journal. – 2023. – Vol. 10, No. 2 – Pp. 27-32.

3. Vishnevsky, A.A. Industrial Internet of Things Risks and protection in the digital age / A.A. Vishnevsky // Automation in industry. - 2024. - No. 9. – pp. 57-60.

4. Novikova, T.P. Automated design of the location of base stations for wireless cellular communications / T.P. Novikova, S.A. Evdoki-mova, R.Yu. Medvedev // Modeling of systems and processes. – 2023. – T. 16, No. 4. – P. 61-70.

5. Kozlov, S.D. A method of security analysis for the industrial Internet of things / S.D. Kozlov, A.I. Larin // The territory of science and education. – 2024. – No. 1. – Pp. 71-74.

6. GOST R ISO/IEC 27001-2021. Information technology. Methods and means of ensuring security. Information security management systems. Requirements. – Date entered. 01.01.2022. Moscow : StandartInform, 2022. – 112 p.

7. GOST R IEC 62443-2-1-2015. Industrial communication networks. Security (cybersecurity) networks and systems. Part 2-1. Drawing up a program to ensure the security (cybersecurity) of the control system and industrial automation. – Moscow : StandartInform, 2015. – 141 p.

8. ISO/IEC 27400:2022. Cybersecurity. IoT security and Privacy. Guidelines. – Date entered. 06/07/2022. – ISO, 2022. – 50 p.

9. Cindrić, I. Mapping of Industrial IoT to IEC 62443 Standards / I. Cindrić, M. Jurčević, T. Hadjina // Sensors. – 2025. – Vol. 25(3). – S. 728. – DOI: 10.3390/s25030728.

10. Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443 / H.L. Hassani [et al.] // Procedia Computer Science. – 2021. – Vol. 191. – Pp. 33-40.