RUFIN Matvey Alexseevich – Student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow. E-mail: rufin.m@mail.ru

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ПРОИЗВОДСТВА (INDUSTRY 4.0): УГРОЗЫ, УЯЗВИМОСТИ И МЕТОДОЛОГИИ ОЦЕНКИ РИСКОВ

А.Г. Буторина

Аннотация. *Статья посвящена анализу проблем информационной безопасности промышленных автоматизированных систем управления в условиях цифровизации промышленности и реализации концепции Industry 4.0. Рассмотрены ключевые угрозы и уязвимости, возникающие в результате интеграции информационных и операционных технологий. Особое внимание уделено методологиям оценки рисков и стандарту IEC 62443 как базе построения защищенных архитектур автоматизации. Обоснована необходимость комплексного подхода к обеспечению кибербезопасности промышленных систем.*

Ключевые слова: *промышленные автоматизированные системы управления, информационная безопасность, Industry 4.0, кибербезопасность, IT/OT-конвергенция, оценка рисков, IEC 62443, промышленный интернет вещей.*

В условиях ускоряющейся цифровизации промышленного производства информационные технологии, программное обеспечение и системы автоматизации становятся ключевыми факторами повышения эффективности и устойчивости предприятий [1]. Концепция Industry 4.0 предполагает глубокую интеграцию вычислительных средств, сетевых технологий и автоматизированных систем управления технологическими процессами, что позволяет реализовать интеллектуальное управление производством, адаптивное планирование и обработку больших массивов данных в режиме реального времени [2]. Вместе с тем цифровая трансформация промышленности сопровождается значительным ростом рисков в области информационной безопасности, поскольку автоматизированные системы управления изначально разрабатывались с

приоритетом надежности и функциональной устойчивости, а не защиты от целенаправленных кибервоздействий [3].

Промышленные автоматизированные системы управления представляют собой совокупность аппаратных и программных компонентов, обеспечивающих мониторинг и автоматизацию технологических процессов в промышленности, энергетике и на объектах критической инфраструктуры [4]. К таким системам относятся SCADA-системы, распределенные системы управления, программируемые логические контроллеры, а также системы производственного уровня, интегрируемые с корпоративными информационными системами управления ресурсами предприятия. Исторически подобные системы функционировали в условиях физической или логической изоляции и использовали специализированные протоколы связи, что существенно ограничивало возможности внешнего воздействия. Однако из-за современной ИТ/ОТ-конвергенции данные ограничения постепенно утрачиваются, поскольку автоматизированные системы все чаще подключаются к корпоративным сетям и внешним цифровым сервисам для удаленного мониторинга, технического обслуживания и аналитической обработки данных [5].

Интеграция информационных и операционных технологий приводит к формированию единого цифрового пространства предприятия, в котором производственные системы становятся частью общей информационно-технологической инфраструктуры (ИТ-инфраструктуры). Это обстоятельство существенно расширяет поверхность атаки и делает промышленные объекты уязвимыми к угрозам, ранее характерным преимущественно для корпоративных информационных систем [6]. При этом последствия киберинцидентов в промышленной среде, как правило, носят более тяжелый характер, поскольку могут приводить не только к финансовым потерям и простою оборудования, но и к нарушению технологических процессов, физическому повреждению производственных объектов, экологическим авариям, угрожать жизни и здоровью персонала.

Результаты современных исследований, опубликованных в научных журналах, индексируемых в базе данных Scopus, свидетельствуют о стабильном росте количества кибератак, направленных на промышленные системы управления, а также об увеличении их сложности и точности [7]. Особую опасность представляют атаки на объекты критической инфраструктуры, использующие сочетание уязвимостей программного обеспечения, недостатков сетевой сегментации и ошибок в организационных мерах безопасности. В отличие от массовых вредоносных программ, такие атаки адаптируются под конкретную архитектуру промышленной системы и могут длительное время оставаться незамеченными, оказывая скрытое воздействие на параметры технологического процесса.

Существенной проблемой обеспечения информационной безопасности промышленных автоматизированных систем является ограниченная применимость традиционных средств киберзащиты. Многие стандартные механизмы, широко используемые в корпоративных ИТ-средах, не учитывают требования реального времени. Их некорректное внедрение может негативно сказаться на стабильности технологического процесса, что приводит к необходимости поиска компромисса между уровнем защищенности и надежностью функционирования системы. Данная особенность во многом объясняет низкий уровень внедрения современных средств информационной безопасности в существующих промышленных инфраструктурах [3].

Дополнительную сложность представляет длительный жизненный цикл автоматизированных систем управления. В отличие от корпоративных информационных систем, обновление которых происходит каждые несколько лет, промышленные системы могут эксплуатироваться в течение десятилетий. Это приводит к использованию устаревших операционных систем, протоколов и аппаратных платформ, для которых отсутствуют актуальные обновления защиты, что существенно повышает уровень уязвимости [6]. В таких условиях обеспечение кибербезопасности требует применения специализированных методологий оценки рисков и внедрения архитектурных решений, ориентированных на специфику промышленной среды.

В научных публикациях подчеркивается, что эффективная защита промышленных автоматизированных систем невозможна без комплексного подхода, учитывающего как технические, так и организационные аспекты безопасности. В последние годы особое значение приобретают международные документы, регламентирующие требования к кибербезопасности промышленных систем, среди которых ключевую роль играет стандарт IEC 62443. Он охватывает все этапы жизненного цикла автоматизированных систем и предлагает формализованный подход к управлению рисками информационной безопасности в промышленной среде [8].

Таким образом, исследование проблем информационной безопасности в условиях Industry 4.0 является актуальной научно-практической задачей, решение которой требует развития теоретических основ оценки киберрисков, адаптации существующих стандартов и разработки специализированных методов защиты, ориентированных на особенности промышленного производства [7].

В условиях возрастания сложности промышленных автоматизированных систем особое значение приобретает создание формализованных методологий оценки рисков информационной безопасности, адаптированных к специфике производственной среды [6]. В отличие от корпоративных информационных систем, где приоритет традиционно

отдается конфиденциальности информации, в промышленных системах ключевым требованием является обеспечение доступности и безопасного функционирования технологических процессов, поскольку даже кратковременные сбои могут приводить к существенным экономическим и технологическим потерям [3]. Это обстоятельство обуславливает необходимость пересмотра классических моделей угроз и внедрения специализированных подходов к анализу рисков, ориентированных на киберфизическую природу современных производственных систем [7].

Результаты научных исследований показывают, что использование универсальных методик оценки рисков, разработанных для ИТ-среды, не позволяет в полной мере учитывать взаимосвязь между цифровыми компонентами и физическими процессами, характерную для автоматизированных систем управления [6]. Из-за этого в последние годы все большее распространение получают подходы, основанные на сценарном анализе и моделировании последствий киберинцидентов для технологических процессов. Подобные методологии позволяют выявлять потенциальные цепочки развития инцидентов и оценивать их влияние на безопасность, надежность и устойчивость производственных систем [9].

Основой современных исследований проблем кибербезопасности промышленных систем является международный стандарт IEC 62443, который рассматривается как нормативная база для проектирования и эксплуатации защищенных автоматизированных систем управления [8]. Данный стандарт предлагает многоуровневую модель безопасности, разделяющую промышленную сеть на зоны и каналы связи, а также установление требований к защите на основе ожидаемого уровня угроз и возможностей потенциального нарушителя. Такой подход позволяет учитывать неоднородность промышленных сетей и адаптировать меры защиты в зависимости от критичности конкретных компонентов системы [4].

Важным аспектом практической реализации требований IEC 62443 является интеграция организационных и технических мер защиты, что предполагает тесное взаимодействие специалистов в области информационных технологий и автоматизации производства. Исследования показывают, что отсутствие согласованности между ИТ- и ОТ-подразделениями (операционно-технологическими) существенно снижает эффективность внедряемых мер безопасности, поскольку решения, разработанные без учета особенностей технологических процессов, могут негативно влиять на надежность и устойчивость функционирования системы [5]. В связи с этим в научной литературе подчеркивается необходимость формирования единой культуры кибербезопасности на уровне предприятия.

Значительное внимание уделяется вопросам сетевой архитектуры и сегментации промышленных сетей. Применение принципов зональной изоляции, использование демилитаризованных зон между корпоративным и производственным сегментами, а также внедрение специализированных межсетевых экранов рассматриваются как эффективные меры снижения риска распространения кибератак [4]. При этом подчеркивается, что сегментация должна сопровождаться постоянным мониторингом сетевого трафика с учетом специфики промышленных протоколов и требований реального времени [7].

Развитие технологий промышленного интернета вещей и рост объемов производственных данных создают предпосылки для применения методов интеллектуального анализа и машинного обучения в задачах обеспечения безопасности автоматизированных систем. В научных публикациях рассматриваются подходы, основанные на выявлении аномалий в поведении оборудования и сетевых взаимодействиях, что позволяет обнаруживать потенциальные инциденты на ранних стадиях их развития [10]. Вместе с тем отмечается, что эффективность таких методов во многом зависит от качества исходных данных и глубины понимания технологических процессов, что ограничивает их универсальность [7].

Отдельной проблемой остается обеспечение безопасности на этапе эксплуатации и технического обслуживания промышленных систем. Удаленный доступ к оборудованию, широко используемый для диагностики и обновления программного обеспечения, рассматривается как один из наиболее уязвимых элементов архитектуры автоматизированных систем управления [3]. В этой связи исследователи подчеркивают необходимость строгого контроля доступа, применения многофакторной аутентификации и ведения журналов действий пользователей, имеющих доступ к критическим компонентам системы [9].

В целом анализ современных научных публикаций показывает, что обеспечение информационной безопасности промышленных автоматизированных систем в условиях Industry 4.0 представляет собой комплексную междисциплинарную задачу, требующую сочетания технических, организационных и управленческих решений [1]. Эффективная защита возможна лишь при условии системного подхода, основанного на оценке рисков, стандартизации процессов безопасности и учете специфики конкретного производства, что определяет основные направления дальнейших исследований в этой области [8].

Библиографический список

1. Kagermann H., Wahlster W., Helbig J. Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0. Final Report of the Industrie 4.0 Working Group. 2013. URL: https://en.acatech.de/publication /recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/ (дата обращения: 15.01.2026).

2. Industry 4.0 / H. Lasi [et al.] // Wirtschaftsinf. 2014. V. 56. P. 261–264. URL: https://link.springer.com/article/10.1007/s11576-014-0424-4 (дата обращения: 14.01.2026).

3. Cyber-Physical Systems Security – A Survey / A. Humayed [et al.] // IEEE Internet of Things Journal. 2017. Vol. 4. No. 6. P. 1802–1831. URL: https://ieeexplore.ieee.org/document/8016694 (дата обращения: 14.01.2026).

4. Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security // NIST Special Publication 800-82, Revision 2. 2015. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (дата обращения: 14.01.2026).

5. The industrial Internet of Things (IIoT): An Analysis Framework / H. Boyes [et al.] // Computers in Industry. 2018. No. 101 (8). P. 1–12. URL: https://www.sciencedirect.com/science/article/pii/S0166361517302327 (дата обращения: 15.01.2026).

6. A Review of Cyber Security Risk Assessment Methods for SCADA Systems / Y. Cherdantseva [et al.] // Computers & Security. 2016. No. 56. P. 1–27. URL: https://www.sciencedirect.com/science/article/pii/S016740481630097X (дата обращения: 15.01.2026).

7. Pedreira V., Barros D., Pinto P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 // Sensors. 2021. No. 21 (15). P. 5189. URL: https://www.mdpi.com/1424-8220/21/15/5189 (дата обращения: 15.01.2026).

8. International Electrotechnical Commission. IEC 62443: Industrial Communication Networks – Network and System Security. IEC. URL: https://webstore.iec.ch/publication/60259 (дата обращения: 15.01.2026).

9. Brancati F., Mazzocca N., Pugliese L. Cybersecurity Risk Assessment for Industrial Automation and Control Systems // International Journal of Information Security. 2023. No. 24. P. 76. URL: https://link.springer.com/article/10.1007 /s10207-023-01009-y (дата обращения: 15.01.2026).

10. Mitchell R., Chen I.-R. A Survey of Intrusion Detection Techniques for Cyber-physical Systems. ACM // Computing Surveys. 2014. Vol. 46. No. 4. P. 55. URL: https://dl.acm.org/doi/10.1145/2593512 (дата обращения: 15.01.2026).

CYBERSECURITY OF INDUSTRIAL AUTOMATED CONTROL SYSTEMS IN THE DIGITALIZATION OF PRODUCTION (INDUSTRY 4.0): THREATS, VULNERABILITIES, AND RISK ASSESSMENT METHODOLOGIES

A.G. Butorina

Abstract. *This article analyzes the information security issues of industrial automated control systems in the context of industrial digitalization and the implementation of the Industry 4.0 concept. Key threats and vulnerabilities arising from the integration of information and operational technologies are considered. Special attention is paid to risk assessment methodologies and the IEC 62443 standard as a basis for building secure automation architectures. The need for an integrated approach to ensuring cybersecurity of industrial systems is substantiated.*

Keywords: *industrial automation systems, information security, Industry 4.0, cybersecurity, IT/OT convergence, risk assessment, IEC 62443, industrial Internet of Things.*

Об авторе:
БУТОРИНА Анна Георгиевна – магистр, ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина», Екатеринбург. E-mail: Butorina.Anna@urfu.me

About the author:
BUTORINA Anna Georgievna – Master's Student, Ural Federal University named after the First President of Russia B.N. Yeltsin, Yekaterinburg. E-mail: Butorina.Anna@urfu.me

УДК 004

МИКРОКОНТРОЛЛЕРЫ В БЫТОВОЙ ТЕХНИКЕ

А.М. Минбаев

Аннотация. *В статье проведен комплексный анализ применения микроконтроллеров в бытовом сегменте. Рассмотрена эволюция архитектур микроконтроллеров от простейших 8-битных ядер до современных 32-битных систем на кристалле с интегрированными беспроводными интерфейсами. Детально систематизированы ключевые места их использования: крупная и мелкая бытовая техника (стиральные машины, холодильники, кухонные приборы), система домашней*