Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

УДК 004.056 https://doi.org/10.33619/2414-2948/115/17

МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ОБЛАСТИ МЕТАЛЛУРГИЧЕСКОЙ ПРОМЫШЛЕННОСТИ

©Баранкова И. И., *ORCID: 0000-0001-9520-6797, SPIN-код: 8618-9276, д-р техн. наук, Магнитогорский технический университет им. Г. И. Носова, г. Магнитогорск, Россия, inna_barankova@mail.ru*
©Петрова Д. А., *ORCID: 0009-0009-8475-7476, Магнитогорский технический университет им. Г. И. Носова, г. Магнитогорск, Россия, dasha-petrova23@mail.ru*
©Андронков А. Д., *ORCID: 0009-0004-1035-4707, Магнитогорский технический университет им. Г. И. Носова, г. Магнитогорск, Россия, andronkov@mail.ru*

MODERNIZATION OF THE INFORMATION PROTECTION SYSTEM OF CRITICAL INFRASTRUCTURE FACILITIES IN THE METALLURGICAL INDUSTRY

©Barankova I., *ORCID: 0000-0001-9520-6797, SPIN-code: 8618-9276, Dr. habil., Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia, inna_barankova@mail.ru*
©Petrova D., *ORCID: 0009-0009-8475-7476, Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia, dasha-petrova23@mail.ru*
©Andronkov A., *ORCID: 0009-0004-1035-4707, Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia, andronkov@mail.ru*

Аннотация. Рассмотрен подход к модернизации системы защиты автоматизированной системы управления технологическими процессами (АСУ ТП) объекта критической информационной инфраструктуры (КИИ) металлургического предприятия. Цель исследования заключается в обосновании целесообразности модернизации даже при высоком уровне текущей защищённости в условиях внедрения новых регуляторных требований. В качестве исходных данных использованы материалы модели угроз, топология сети, архитектура объекта и его системы защиты, а также результаты оценки соответствия требованиям нормативных документов ФСТЭК России. В работе применена методология системного анализа, включая концепцию «зон и связей», методы экспертной оценки, инструментального анализа уязвимостей, а также сопоставление с реальными кейсами из смежных исследований, включая опыт промышленной модернизации на аналогичных объектах. Основные результаты включают идентификацию точечных уязвимостей, таких как: наличие устаревших операционных систем, отсутствие систем контроля и управления доступом, недостаточный мониторинг. Было сформировано несколько направлений модернизации: усиление контроля действий привилегированных пользователей, внедрение средств журналирования для привилегированных сессий и пользователей, а также сегментация уязвимых участков, которые не могут быть остановлены для дальнейшей модернизации в силу технологического процесса. Работа интегрирует теоретическую базу, аудит, практические ограничения и регуляторные установки, демонстрируя сквозной процесс обеспечения информационной безопасности: от диагностики до архитектурной трансформации. Полученные выводы могут быть применимы на аналогичных промышленных объектах с типовой инфраструктурой и отраслевыми особенностями. Представленные результаты подтверждают актуальность модернизации как стратегического процесса устойчивого управления безопасностью КИИ.

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

Abstract. The article examines an approach to modernizing the security system of an automated process control system (APCS) at a critical information infrastructure (CII) facility of a metallurgical enterprise. The study aims to justify the necessity of modernization even with a high level of existing protection, particularly in the context of implementing new regulatory requirements. The research utilizes input data including threat models, network topology, facility architecture and its protection systems, as well as results of compliance assessments with FSTEC Russia regulatory documents. The methodology employs system analysis, incorporating the "zones and conduits" concept, expert assessment methods, vulnerability scanning tools, and comparisons with real-world cases from related studies, including industrial modernization experience at similar facilities. Key findings include the identification of specific vulnerabilities such as outdated operating systems, lack of access control systems, and insufficient monitoring. Several modernization directions were developed: enhancing control over privileged user actions, implementing logging tools for privileged sessions and users, and segmenting vulnerable network segments that cannot be taken offline due to technological process requirements. The work integrates theoretical foundations, audit results, practical constraints and regulatory frameworks, demonstrating a comprehensive information security process from diagnostics to architectural transformation. The conclusions can be applied to similar industrial facilities with standard infrastructure and industry-specific characteristics. The presented results confirm the relevance of modernization as a strategic process for sustainable CII security management.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура (КИИ), субъект КИИ, объект КИИ, аудит, автоматизированная система управления технологическим процессом (АСУ ТП).

Keywords: information security, critical information infrastructure (CII), CII subject, CII object, audit, automated process control system.

В условиях повышения значимости информационной безопасности в промышленной сфере особое внимание уделяется защите объектов критической информационной инфраструктуры (КИИ).

Металлургическая отрасль использует сложные автоматизированные системы управления технологическими процессами (АСУ ТП), уязвимые к внешним и внутренним киберугрозам. В этой связи ключевым направлением обеспечения устойчивости и соответствия нормативным требованиям становится своевременная модернизация систем защиты.

Несмотря на приемлемый регуляторами уровень защищённости на ряде предприятий, динамично меняющаяся регуляторная база, эволюция методов атак и необходимость импортонезависимости требуют системного подхода к обновлению архитектуры информационной безопасности.

В 2024 г. регулятор в области информационной безопасности (ФСТЭК России) утвердила актуализированную методику оценки состояния технической защиты информации, которая подчёркивает важность не только формального наличия мер защиты, но и их фактической эффективности и актуальности. Таким образом, модернизация системы защиты АСУ ТП представляет собой не реакцию на инцидент, а стратегическую инициативу по адаптации к текущим и перспективным требованиям.

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

Цель настоящей работы — разработка и обоснование комплекса мер по модернизации системы защиты АСУ ТП объекта КИИ в металлургической отрасли на основе предварительно проведённого аудита информационной безопасности. Работа выстроена в логике сквозного подхода: от анализа текущего состояния — к выработке конкретных модернизационных решений, соответствующих современным стандартам и нормативным документам в области ИБ.

Методология, применённая в рамках данного исследования, базируется на принципах системного анализа, оценки соответствия требованиям регуляторов в области информационной безопасности, а также практических методах тестирования и анализа уязвимостей. Исследование проводилось в несколько этапов:

1. Анализ нормативной базы и требований;
2. Изучение внутренней документации объекта исследования;
3. Применение концепции «зон и связей». В рамках оценки структуры и защищённости АСУ ТП использована методология проектирования защищённых архитектур [1]. Система логически разделена на технологические зоны: зона управления, зона ПАЗ, зона кибербезопасности, демилитаризованная зона, зона энергообеспечения и др. Проведена инвентаризация активов и трассировка связей между зонами, с учетом требований концепции глубинной защиты;
4. Оценка текущего состояния системы защиты. Проведено сопоставление реализованных мер защиты с требованиями нормативных актов при помощи осмотра опросных листов на объект защиты, недостатков не выявлено. Проведена предварительная оценка по Методике ФСТЭК 2024 года, с формированием первичного показателя состояния технической защиты информации, который стремится к единице, что означает, что обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации, а уровень состояния защищенности характеризуется как минимальный базовый [2]. В частности, реализована сегментация сети, установлены межзоновые шлюзы, разграничение уровней АСУ ТП, базовая архитектура DMZ;
5. Экспертная оценка и классификация рисков. Выделены уязвимости, не влияющие на фундамент архитектуры, но требующие внимания, а именно: устаревшие операционные системы на ряде узлов, отсутствие СКУД-системы, недостаточный контроль действий привилегированных пользователей и их сессий, в том числе удаленных, а также временно ограниченные возможности мониторинга в связи с внедрением отечественных систем.

В рамках данной работы модернизация системы защиты рассматривается не как изолированный процесс, а как логическое продолжение системного аудита информационной безопасности, проведённого в соответствии с нормативными и методическими документами, в том числе Приказами ФСТЭК №31 и №239, а также Методикой оценки соответствия защищённости объектов КИИ.

Согласно статье И. И. Баранковой, Е. А. Семавиной, У. В. Михайловой [3], аудит ИБ промышленных объектов КИИ выявляет реальные несоответствия требованиям нормативно-правовых актов, а также недостаточную актуальность документации, устаревшие компоненты и слабости в технической реализации мер защиты. Аудит, выполненный по данной модели, включает в себя экспертный анализ, сопоставление с Приказами ФСТЭК, инвентаризацию СЗИ и сертификационных документов, а также фиксирует человеческий фактор и недостаточную компетентность персонала.

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

В статье М. В. Коновалова и И. Л. Иванова [4] рассматривается реальный кейс поэтапной модернизации системы защиты АСУ ТП на объекте металлургического производства, отнесённого к критической информационной инфраструктуре. Авторы подробно описывают переход от первичного обеспечения защищённости (изоляция, смена паролей, отключение ненужных служб) к более зрелым формам — внедрению централизованного управления, переходу на отечественное ПО, расширению зон мониторинга и учёту требований бизнеса. Отдельное внимание уделяется необходимости синхронизации технической модернизации с кадровыми мерами — повышением квалификации сотрудников и перераспределением функций между ИБ и эксплуатационным персоналом.

Представленный опыт хорошо коррелирует с задачами, решаемыми в настоящей работе, и может служить примером практической реализации предложенных в исследовании мер.

Таким образом, результаты аудита ИБ являются входной точкой для процесса модернизации. На основе выявленных расхождений формируется техническое задание на доработку архитектуры защиты.

Модернизация позволяет: устранить унаследованные слабости (устаревшие операционные системы, отсутствие контроля привилегий); закрыть регуляторные несоответствия (например, в части физической охраны или логирования); привести систему к состоянию, пригодному для прохождения официальной проверки ФСТЭК по новой методике или подготовки к категорированию/оценке значимости. Такое сочетание подходов (аудит как диагностика и модернизация как лечение) обеспечивает непрерывный цикл совершенствования ИБ и соответствует рекомендациям ГОСТ Р ИСО МЭК 19011–2021 и современным принципам управления ИБ в промышленных системах [5].

Таким образом, результаты исследования позволили сформировать рекомендации по модернизации системы защиты, направленные на повышение уровня соответствия законодательству Российской Федерации и требованиям регуляторов, снижение рисков реализации наиболее вероятных и критичных угроз и в целом общее повышение устойчивости к внешнему и внутреннему вектору атак. На основании выявленных проблем была сформирована стратегия модернизации, включающая меры, описанные ниже.

1. Организационные: пересмотр локальной нормативной документации; внедрение политики управления доступом и контроля привилегий; регулярное повышение квалификации персонала; проведение учений по реагированию на инциденты;

2. Технические: сегментация сети с применением межсетевых экранов на границах уровней; обновление операционных систем и программного обеспечения; организация сегментации и изоляции узлов с устаревшими операционными системами; внедрение систем обнаружения и предотвращения вторжений (ids/ips); приоритетное внедрение отечественных решений и решений класса pam (журналирование сессий и команд администрирования); внедрение скуд в технические помещения и зоны размещения управляющего оборудования.

Следует отметить, что несмотря на приемлемый уровень организационной и технической зрелости системы защиты автоматизированной системы управления технологическими процессами, модернизация остаётся актуальной и необходимой в контексте следующих факторов, описанных ниже.

1. *Соответствие новым методическим указаниям ФСТЭК.* В мае 2024 г ФСТЭК России утвердила «Методику оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

Согласно данной методике, субъекты КИИ обязаны регулярно проводить самооценку состояния своей защиты с учётом полноты, актуальности и эффективности реализованных технических и организационных мер. Методика подчёркивает, что оценка должна быть не формальной, а аналитической, включающей в себя реальные показатели устойчивости системы. Это обуславливает необходимость совершенствования даже стабильной архитектуры.

2. *Принцип упреждающего реагирования.* Согласно ст. 10 Закона «О безопасности критической информационной инфраструктуры Российской Федерации» [6], субъект информационной инфраструктуры обязан обеспечивать постоянное совершенствование системы защиты.

Это включает адаптацию к эволюционирующим киберугрозам, применяемым средствам мониторинга, а также модернизацию унаследованных компонентов. В частности, наличие устаревших операционных систем требует внедрения компенсирующих мер, а не ожидания предписания регулятора.

3. *Подготовка к внешним проверкам*. Методика ФСТЭК 2024 г. планируется к применению в рамках государственного контроля. Проведение предварительной оценки и запуск точечных мер модернизации обеспечат соответствие проверочным листам, снижение административной нагрузки и готовность к инспекционным мероприятиям.

4. *Обеспечение устойчивости к будущим изменениям.* Модернизация способствует переходу от фрагментарных решений к системному обеспечению информационной безопасности. Это особенно актуально в условиях: расширения сетевой инфраструктуры; внедрения PAM, IDS/IPS и других инструментов для повышения обеспечения безопасности объекта, в частности, отечественных; необходимости масштабирования архитектуры без утраты защищённости.

Таким образом, модернизация системы защиты даже при высоком уровне исходной зрелости представляет собой регламентированный и стратегически обоснованный процесс, направленный на соответствие требованиям законодательства, снижение операционных и регуляторных рисков, а также повышение устойчивости объекта КИИ к развивающимся угрозам.

Результаты могут быть использованы как основа для практического внедрения предложенных мер, а также для последующего прохождения оценки соответствия требованиям безопасности информации.

Отдельного внимания заслуживает факт, что в настоящее время в Государственной Думе Российской Федерации рассматривается законопроект № 581689-8 о внесении изменений в Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». После прохождения всех этапов законотворческого процесса и вступления документа в силу, представленные в данной работе подходы к модернизации могут быть адаптированы и расширены с учётом новых требований.

Список литературы:

1. Сухих Я. А., Правиков Д. И., Кузичкин А. А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами // Безопасность информационных технологий. 2020. Т. 27. №2. С. 97-117.

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

2. Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утв. ФСТЭК России 02.05.2024.

3. Баранкова И. И., Семавина Е. А., Михайлова У. В. Особенности проведения аудита безопасности объектов КИИ в промышленности // Вестник УрФО. Безопасность в информационной сфере. 2022. № 3(45). С. 76–82.

4. Коновалов М. В., Иванов И. Л. Модернизация системы защиты информации, объекта КИИ, трудности модернизации на действующем АСУ ТП "Нагревательные печи", цеха проката металла // Актуальные проблемы современной науки, техники и образования. 2022. №1. С. 39–42.

5. ГОСТ Р ИСО 19011-2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента. Введ. 2021-07-01. М.: Стандартинформ, 2021.

6. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. 2017. №31 (ч. I). Ст. 4825.

7. Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

8. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах».

References:

1. Sukhikh, Ya. A., Pravikov, D. I., & Kuzichkin, A. A. (2020). Razrabotka zashchishchennykh arkhitektur avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami. *Bezopasnost' informatsionnykh tekhnologii, 27*(2), 97-117. (in Russian).

2. Metodika otsenki pokazatelya sostoyaniya tekhnicheskoi zashchity informatsii i obespecheniya bezopasnosti znachimykh obektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii. Approved by FSTEC of Russia, 02.05.2024. (in Russian).

3. Barankova, I. I., Semavina, E. A., & Mikhailova, U. V. (2022). Osobennosti provedeniya audita bezopasnosti obektov KII v promyshlennosti. *Vestnik UrFO. Bezopasnost v informatsionnoi sfere, 3*(45), 76–82. (in Russian).

4. Konovalov M. V., & Ivanov I. L. (2022). Modernizatsiya sistemy zashchity informatsii, obekta KII, trudnosti modernizatsii na deistvuyushchem ASUTP "Nagrevatelnye pechi", tsekha prokata metalla. In *Aktualnye problemy sovremennoi nauki, tekhniki i obrazovaniya,* (1), 39–42. (in Russian).

5 GOST R ISO 19011-2021 (2021). Otsenka sootvetstviya. Rukovodyashchie ukazaniya po provedeniyu audita sistem menedzhmenta. Introduced 2021-07-01. Moscow. (in Russian).

6. Federalnyi zakon ot 26 iyulya 2017 g. №187-FZ “O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii” (2017). *Sobranie zakonodatelstva Rossiiskoi Federatsii, 31* (Part I), Art. 4825. (in Russian).

7. Ob utverzhdenii Trebovanii po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii: Prikaz FSTEK Rossii ot 25.12.2017 №239 (red. ot 29.12.2020) (2017). *Ofitsial'nyi internet-portal pravovoi informatsii, 159*. (in Russian).

8. Ob utverzhdenii Poryadka sozdaniya gosudarstvennoi sistemy obnaruzheniya, preduprezhdeniya i likvidatsii posledstvii komp'yuternykh atak: Prikaz FSTEK Rossii ot 14.03.2014 № 31 (red. ot 25.12.2020). (2014). *Byulleten' normativnykh aktov federal'nykh organov ispolnitel'noi vlasti, 52*, st. 7137. (in Russian).

Работа поступила
в редакцию 14.04.2025 г.

Принята к публикации
22.03.2025 г.

Ссылка для цитирования:

Баранкова И. И., Петрова Д. А., Андронков А. Д. Модернизация системы защиты информации значимых объектов критической инфраструктуры в области металлургической промышленности // Бюллетень науки и практики. 2025. Т. 11. №6. С. 122-128. https://doi.org/10.33619/2414-2948/115/17

Cite as (APA):

Barankova, I., Petrova, D., & Andronkov, A. (2025). Modernization of the Information Protection System of Critical Infrastructure Facilities in the Metallurgical Industry. *Bulletin of Science and Practice, 11*(6), 122-128. (in Russian). https://doi.org/10.33619/2414-2948/115/17