УДК 004.056 https://doi.org/10.33619/2414-2948/115/18

АУДИТ 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*
©Королев Б. С., *ORCID: 0009-0009-8046-4334, Магнитогорский технический университет им. Г. И. Носова, г. Магнитогорск, Россия, boris.korolev777@gmail.com*
©Пуршева С. С., *ORCID: 0009-0004-1865-3154, Магнитогорский технический университет им. Г. И. Носова, г. Магнитогорск, Россия, sofia.pursheva@gmail.com*

AUDIT OF SIGNIFICANT 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*
©Korolev B., *ORCID: 0009-0009-8046-4334, Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia, boris.korolev777@gmail.com*
©Pursheva S., *ORCID: 0009-0004-1865-3154, Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia, sofia.pursheva@gmail.com*

Аннотация. Рассматриваются ключевые аспекты проведения аудита информационной безопасности (ИБ) на промышленных предприятиях, с особым вниманием к металлургическому комплексу, где высокая степень автоматизации сочетается с использованием уязвимых промышленных технологий. Основное внимание уделено методологии оценки соответствия систем защиты информации актуальным нормативным требованиям, включая как национальные, так и международные стандарты безопасности. Представлена классификация основных видов аудита информационной безопасности. Особый акцент сделан на анализе регуляторных требований к обеспечению информационной безопасности промышленных объектов, включая положения профильных надзорных органов, таких как Федеральной службы по техническому и экспортному контролю (ФСТЭК) России. Рассмотрено значение результатов комплексного аудита информационной безопасности для повышения общего уровня защищенности предприятия, при этом учитываются не только формальные требования соответствия, но и практическая эффективность реализуемых мер защиты. Отмечены характерные трудности, связанные с применением традиционных методов аудита в условиях промышленных сетей, и предложены адаптированные решения. Предложен ряд практических советов, направленных на оптимизацию процедуры аудита и снижение потенциальных рисков. Результаты исследования представляют ценность для специалистов по информационной безопасности промышленных предприятий, аудиторов, а также представителей регулирующих органов.

Abstract. The article considers key aspects of conducting an information security (IS) audit at industrial enterprises, with special attention to the metallurgical complex, where a high degree of automation is combined with the use of vulnerable industrial technologies. The main attention is paid to the methodology for assessing the compliance of information security systems with current regulatory requirements, including both national and international security standards. A classification of the main types of information security audit is presented. Particular emphasis is

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

placed on the analysis of regulatory requirements for ensuring the information security of industrial facilities, including the provisions of specialized supervisory authorities, such as the Federal Service for Technical and Export Control (FSTEC) of Russia. The importance of the results of a comprehensive information security audit for increasing the overall level of enterprise security is considered, taking into account not only formal compliance requirements, but also the practical effectiveness of the implemented security measures. The characteristic difficulties associated with the use of traditional audit methods in industrial networks are noted, and adapted solutions are proposed. A number of practical tips are offered to optimize the audit procedure and reduce potential risks. The results of the study are valuable for information security specialists at industrial enterprises, auditors, and representatives of regulatory authorities.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, автоматизированная система управления.

Keywords: information security, critical information infrastructure, automated control system.

Защита информационных систем на промышленных объектах, особенно тех, что входят в перечень критической информационной инфраструктуры (КИИ), играет ключевую роль в обеспечении национальной безопасности России в цифровой сфере. Компьютерные атаки на такие объекты способны привести к серьезным последствиям, включая: техногенные катастрофы и аварийные ситуации; значительные финансовые потери как для компании, так и для государства; риски для жизни и здоровья персонала, а также населения, проживающего вблизи производственных зон. Таким образом, обеспечение устойчивости КИИ к киберугрозам становится не только корпоративной, но и общегосударственной задачей. Эффективное обеспечение информационной безопасности объектов КИИ требует комплексного подхода, сочетающего как внедрение защитных механизмов, так и регулярный мониторинг их эффективности [1]. Систематические проверки позволяют оценить корректность функционирования и своевременность актуализации применяемых средств защиты информации [2].

Анализ текущего состояния показывает, что многие промышленные предприятия сталкиваются с фрагментарностью в построении систем защиты. Хотя антивирусные решения получили широкое распространение в АСУ ТП, другие критически важные компоненты — такие как системы обнаружения вторжений (IDS/IPS) и регламенты реагирования на инциденты — часто отсутствуют. Эта диспропорция создает необходимость проведения детального аудита для выявления существующих уязвимостей и определения приоритетных направлений модернизации системы защиты. Проведение аудита информационной безопасности позволяет получить объективную оценку текущего уровня защищенности предприятия [3].

Выявление существующих уязвимостей и потенциальных угроз, обусловленных недостаточностью применяемых защитных мер, дает возможность сформировать эффективную систему защиты информации, учитывающую специфику конкретной организации. Аудит ИБ занимает особое место среди контрольных процедур, поскольку в нормативной базе отсутствует его четкое определение. В соответствии с ГОСТ Р ИСО 19011-2021 под аудитом понимается «систематический, независимый и документированный процесс получения объективных доказательств и их оценки для определения степени соответствия установленным критериям» (https://clck.ru/3MN2E7).

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

В практике информационной безопасности принято классифицировать аудит на четыре основных типа: экспертный анализ — осуществляется специалистами в области защиты информации с целью выявления недостатков существующей системы безопасности; проверка соответствия — направлена на оценку полноты выполнения требований национальных и международных нормативных документов в области ИБ; техническая диагностика – предусматривает обнаружение уязвимостей в программных и аппаратных компонентах информационной системы; комплексная оценка — сочетает все перечисленные методы аудита для всестороннего анализа системы защиты (https://clck.ru/3MN26t).

Рассматривается исследование, которе концентрируется на наиболее востребованном в практической деятельности виде аудита информационной безопасности — проверке соблюдения требований российских регуляторных органов (ФСТЭК России, ФСБ) и международных стандартов ИБ. Международный стандарт ISO 19011:2021, который служит руководством для разработки комплексной программы аудита, подготовки полного комплекта организационно-распорядительной документации, реализации всех этапов аудиторской проверки — от инициирования до завершения процедуры, предоставляет методологическую базу для проведения аудитов, включая: основополагающие термины и принципы; поэтапную структуру аудиторского процесса; критерии оценки квалификации аудиторов. Для организаций, относящихся к критической информационной инфраструктуре, ФСТЭК России утвердила два ключевых нормативных документа: Приказ №31 (https://clck.ru/3MN27Z), который устанавливает базовые требования по защите автоматизированных систем управления (АСУП и АСУ ТП) и Приказ №239 (https://clck.ru/3MN28F), который содержит дополнительные требования для объектов, признанных значимыми в соответствии с Постановлением Правительства РФ №127 (https://clck.ru/3MN28o).

Особенности применения нормативных актов: значимые объекты КИИ обязаны соблюдать требования Приказа №239; для незначимых объектов КИИ достаточно выполнения (требований Приказа №31; Положений ч. 2 ст. 9 ФЗ №187 (https://clck.ru/3MN29Z) (который также распространяется на значимые объекты). Оба приказа ФСТЭК имеют схожую структуру и регламентируют: комплекс мер информационной безопасности; требования на всех этапах жизненного цикла АСУ ТП: проектирование и разработка; внедрение и ввод в эксплуатацию; штатная эксплуатация; вывод из эксплуатации. Основные отличия заключаются в: объеме требований; глубине проработки защитных мер; критериях соответствия для разных категорий объектов. При анализе нормативных требований к защите информации важно отметить, что наименования защитных мер для различных категорий объектов КИИ остаются идентичными, однако принципы их классификации существенно различаются. Для незначимых объектов перечень мер защиты определяется в зависимости от уровня значимости обрабатываемой информации, тогда как для значимых объектов применяется более детализированный подход с разделением требований по трём категориям значимости.

На этапе непосредственного проведения аудита информационной безопасности, после распределения обязанностей между аудиторами и подготовки необходимой организационно-распорядительной документации, формируется сводная таблица соответствия. В ней фиксируется выполнение или невыполнение каждого требования соответствующего приказа ФСТЭК. Если мера защиты реализована, целесообразно указать конкретное средство защиты информации (СрЗИ) либо нормативный документ, обеспечивающий её выполнение. Особое внимание следует уделять сертифицированным СрЗИ: необходимо проверять не только их наличие, но и актуальность сертификатов ФСТЭК, поскольку использование средств с

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

истёкшим сроком сертификации может привести к несоответствию требованиям регуляторов и потребовать немедленной замены, так необходимо учитывать УП №250 (https://base.garant.ru/404561984/) о необходимости перехода на отечественные решения в сфере информационной безопасности. Такой подход к документированию результатов аудита позволяет не только систематизировать процесс проверки, но и выявить потенциальные уязвимости, связанные с устаревшими или некорректно применяемыми решениями. Кроме того, он обеспечивает прозрачность оценки и формирует основу для дальнейших рекомендаций по совершенствованию системы защиты информации на объекте КИИ.

При проведение аудита информационной безопасности предполагает обязательное рассмотрение нескольких принципиальных вопросов (https://clck.ru/3MN2An). В первую очередь необходимо определить организационную структуру, отвечающую за информационную безопасность на предприятии, включая анализ кадрового состава и распределения обязанностей. Не менее важным является изучение организационно-распорядительной документации по защите информации — ее полноты, актуальности и соответствия требованиям регуляторов. Особое внимание уделяется анализу внедренных средств защиты информации, включая проверку сроков действия их сертификатов соответствия. Кроме того, требуется оценить комплекс реализуемых защитных мероприятий, их нормативное обоснование и практическую эффективность. По сути, основная задача такого аудита сводится к детальному анализу таблицы соответствия, где фиксируется выполнение или невыполнение каждого требования нормативных документов.

На примере листопрокатного цеха можно выделить ряд характерных проблем. Первая существенная трудность связана с получением полной информации об архитектуре АСУ ТП. Если основные компоненты системы (рабочие места операторов, серверное оборудование, программируемые контроллеры) обычно хорошо задокументированы и размещены согласно регламентам, то сетевая инфраструктура (коммутаторы, концентраторы) часто не имеет соответствующей документации. Это значительно осложняет анализ сетевой топологии и определение границ между технологическими и корпоративными сетями. Решение данной проблемы требует от руководства предприятия инициировать процесс полного документирования сетевой инфраструктуры.

Еще одна серьезная проблема — отсутствие в цехе штатного специалиста по информационной безопасности. В результате аудиторам приходится взаимодействовать с технологическим персоналом, который, обладая глубокими знаниями производственных процессов, часто не имеет достаточной компетенции в вопросах ИТ-безопасности. Это приводит к неосознанному замедлению процесса аудита и требует либо расширения штата, либо введения должности администратора безопасности для цеха.

Несмотря на то, что после принятия ФЗ №187 в 2018 г. на предприятии была проведена работа по разработке необходимой документации, в рассматриваемом цехе многие технические паспорта устарели, а организационно-распорядительные документы не соответствуют в полной мере требованиям ФСТЭК. Это вынуждает аудиторов проводить физический осмотр каждого объекта информатизации, что значительно увеличивает временные затраты на проверку. Архитектурные решения автоматизированных систем управления технологическими процессами принципиально отличаются от традиционных корпоративных информационных систем по ряду ключевых параметров. Эти различия охватывают все уровни системы – от применяемых специализированных протоколов обмена данными (таких как Modbus, Profibus DP, Fieldbus Data Link и Manufacturing Message Specification) до уникального состава аппаратных компонентов, включающего датчики,

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

программируемые логические контроллеры и серверы OPC. Особого внимания заслуживает используемое программное обеспечение (SCADA-системы, MES-комплексы) и специфические условия эксплуатации в промышленных цехах и производственных зонах.

В отличие от корпоративных информационных систем, где основной акцент делается на защиту конфиденциальности данных (https://clck.ru/3MN2BH), для технологических систем первостепенное значение приобретает обеспечение бесперебойности производственных циклов (https://clck.ru/3MN2Bi). Это требует особого подхода к гарантированию доступности и сохранности целостности передаваемых данных. Характерной особенностью АСУ ТП является их жестко детерминированная конфигурация, которая исключает возможность произвольных модификаций (https://clck.ru/3MN2C7). Ограничения касаются: процедур обновления программного обеспечения; внедрения дополнительных средств защиты; изменения стандартных параметров настройки.

Разработка эффективных механизмов защиты, которые одновременно не нарушают технологические процессы, учитывают специфику работы оборудования и соответствуют всем нормативным требованиям представляет собой значительную техническую сложность. В условиях современных геополитических реалий эта задача существенно усложнилась. Анализ рынка показывает недостаточное количество российских разработок в области средств защиты информации, которые могли бы полностью удовлетворять всем требованиям регулирующих органов в части защиты промышленных автоматизированных систем. События начала 2025 г., связанные с участившимися случаями кибернетических атак, наглядно продемонстрировали критическую важность защиты информационных систем объектов критической информационной инфраструктуры. Регулярное проведение комплексных проверок состояния информационной безопасности позволяет промышленным организациям: Разработать эффективную стратегию противодействия цифровым угрозам. Создать многоуровневую систему защиты информации. Оптимизировать существующие механизмы безопасности. Результатом грамотно организованного аудита становится формирование такой системы защиты информации, которая либо полностью предотвращает реализацию потенциальных угроз, либо минимизирует их возможные последствия для производственных процессов. Особое значение приобретает способность такой системы оперативно адаптироваться к изменяющимся условиям киберсреды и новым методам атак. Проведенный анализ подтверждает выводы, где акцентируется необходимость баланса между нормативными требованиями, бизнес-процессами и технической реализацией модернизации [4].

Такой подход обеспечивает не только соответствие стандартам ФСТЭК, но и устойчивость промышленных объектов к современным киберугрозам. Ярким примером эффективности аудита и последующей модернизации является опыт смежного объекта КИИ — металлургического комбината, где внедрение поэтапных мер (включая замену сетевого оборудования на отечественные аналоги, обновление протоколов связи и усиление контроля доступа) позволило сократить количество инцидентов информационной безопасности на 40% за первый год эксплуатации обновленной системы [4].

Это подтверждает, что систематический аудит и адаптация защитных механизмов к специфике производства являются ключевыми факторами успеха. Современные вызовы в области кибербезопасности требуют от предприятий не только своевременного выявления уязвимостей, но и разработки превентивных мер защиты, учитывающих как текущее состояние технологий, так и прогнозируемые векторы развития киберугроз. В этом контексте аудит информационной безопасности становится не просто проверкой, а важнейшим инструментом стратегического управления рисками в цифровой среде.

Список литературы:

1. Санарбаев Р. Ж., Михайлова У. В. Типовые проблемы аудита информационной безопасности на примере транспортной компании ООО «АН-СЕР» // Образование России и актуальные вопросы современной науки: Материалы II Всероссийсской научно-практической конференции. 2019. С. 147–151.

2. Михайлова У. В., Быкова Т. В. Аудит информационной безопасности на предприятии // Материалы научно-практической конференции. 2019. С. 341-345.

3. Баранкова И. И., Михайлова У. В., Быкова Т. В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии // Вестник УрФО. Безопасность в информационной сфере. 2019. №1 (31). С. 53-56.

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.

References:

1. Sanarbaev, R. Zh., & Mikhailova, U. V. (2019). Tipovye problemy audita informatsionnoi bezopasnosti na primere transportnoi kompanii OOO “AN-SER”. In *Obrazovanie Rossii i aktual'nye voprosy sovremennoi nauki: Materialy II Vserossiisskoi nauchno-prakticheskoi konferentsii,* 147–151. (in Russian).

2. Mikhailova, U. V., & Bykova, T. V. (2019). Audit informatsionnoi bezopasnosti na predpriyatii. In *Materialy nauchno-prakticheskoi konferentsii,* 341-345. (in Russian).

3. Barankova, I. I., Mikhailova, U. V., & Bykova, T. V. (2019). Slozhnosti, voznikayushchie pri provedenii audita informatsionnoi bezopasnosti na predpriyatii. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere,* (1 (31)), 53-56. (in Russian).

4. Konovalov, M. V., Ivanov, I. L. (2022). Modernizatsiya sistemy zashchity informatsii, ob"ekta KII, trudnosti modernizatsii na deistvuyushchem ASU TP "Nagrevatel'nye pechi", tsekha prokata metalla. *Aktual'nye problemy sovremennoi nauki, tekhniki i obrazovaniya,* (1), 39–42. (in Russian).

Работа поступила
в редакцию 15.04.2025 г.

Принята к публикации
23.04.2025 г.

Ссылка для цитирования:

Баранкова И. И., Королев Б. С., Пуршева С. С. Аудит значимых объектов критической инфраструктуры в области металлургической промышленности // Бюллетень науки и практики. 2025. Т. 11. №6. С. 129-134. https://doi.org/10.33619/2414-2948/115/18

Cite as (APA):

Barankova, I., Korolev, B., & Pursheva, S. (2025). Audit of Significant Critical Infrastructure Facilities in the Metallurgical Industry. *Bulletin of Science and Practice, 11*(6), 129-134. (in Russian). https://doi.org/10.33619/2414-2948/115/18