УДК 004.056 Вестник УрФО № 3(45) / 2022, с. 76–82

Баранкова И.И., Семавина Е.А., Михайлова У.В. DOI: 10.14529/secur220309

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ, НАПРАВЛЕННЫЙ НА ОЦЕНКУ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ РОССИЙСКОГО И МЕЖДУНАРОДНОГО ЗАКОНОДАТЕЛЬСТВА

Статья посвящена аудиту информационной безопасности (ИБ) промышленных предприятий, направленному на оценку соответствия принятых мер защиты информации требованиям российского и международного законодательства. В материале поднят вопрос о необходимости проведения данного процесса и описаны его основные виды. Рассмотрены приказы ФСТЭК России, утверждающие требования к мерам защиты информации, и Национальный стандарт, содержащий указания по проведению аудита ИБ. Выделены основные вопросы и сложности проведения аудита автоматизированных систем управления технологическими процессами (АСУ ТП) и приведены рекомендации для упрощения процесса.

Ключевые слова: *информационная безопасность, аудит, критическая информационная инфраструктура (КИИ), автоматизированная система управления технологическим процессом (АСУ ТП), нормативно правовые акты (НПА).*

INFORMATION SECURITY AUDIT OF INDUSTRIAL ENTERPRISES, AIMED AT ASSESSING COMPLIANCE WITH RUSSIAN AND INTERNATIONAL LEGISLATION

The article is devoted to the audit of information security of industrial enterprises, aimed at assessing the compliance of the information protection measures taken with the requirements of Russian and international legislation. The material raises the question of the need for this process and describes its main types. The orders of the Federal Service for Technical and Export Control that approve the requirements for information security measures and the National Standard that contains instructions for information security auditing are considered. The main issues and complexities of auditing automated process control systems are highlighted and recommendations are given to simplify the process.

Keywords: *information security, audit, critical information infrastructure, automated process control system, regulatory documents.*

Информационная безопасность (ИБ) промышленных предприятий, а именно предприятий, относящихся к критическим информационным инфраструктурам (далее КИИ), является частью национальной безопасности Российской Федерации в информационной сфере. Кибератаки на информационные системы объектов КИИ могут стать причиной: аварии, экономического ущерба для предприятия и страны, угрозы жизни и здоровью сотрудников и граждан, проживающих в непосредственной близости от производства.

При обеспечении ИБ КИИ одинаково важно обеспечивать, как процессы разработки и реализации защитных мер, так и процессы проверок и контроля состояния ИБ [1]. Подобный контроль дает возможность провести проверку для установления валидности и актуальности используемых средств и систем защиты информации (СЗИ) [2].

На практике у большинства промышленных предприятий нет цельной, четко отлаженной СЗИ. Так, например, антивирусные программные средства установлены на многих АСУ ТП, чего не скажешь о системах обнаружения/предотвращения вторжений или правилах и регламентах реагирования на компьютерные инциденты. Вследствие чего возникает необходимость оценить положение дел и разобраться, какие меры по защите информации реализованы, а какие в обязательном порядке требуют немедленного внедрения.

Аудит информационной безопасности (далее аудит ИБ) способствует получению наиболее точных данных о текущем состоянии предприятия в сфере обеспечения безопасности информации [3]. Своевременное обнаружение всех возможных актуальных уязвимостей и угроз безопасности, которые могут возникнуть из-за недостатка принятых мер защищенности, позволит обеспечить построение адекватной и эффективной СЗИ, которая будет соответствовать специфике предприятия.

Аудит ИБ занимает особое положение среди процессов контроля и проверки, т.к. на данный момент для него не существует стро-

гого нормативного определения. Согласно ГОСТ Р ИСО 19011–2021 «аудит (audit): Систематический, независимый и документированный процесс установления объективного свидетельства и его объективного оценивания для получения степени соответствия критериям аудита» [4]. В области ИБ принято выделять четыре вида аудита такие как:

1. Экспертный направлен на выявление недостатков СЗИ с помощью опытных экспертов по обеспечению безопасности информации (ОБИ);

2. Оценка соответствия требованиям российского и международного законодательства. Цель настоящего аудита – выявление недостатков СЗИ посредством анализа полноты исполнения требований по ОБИ регламентов, нормативно правовых актов и законодательства;

3. Инструментальный анализ. Данный вид предполагает выявление уязвимостей программного и программно-аппаратного обеспечения исследуемой системы;

4. Комплексный аудит включает в себя все вышеперечисленные виды проведения проверки [5].

В данной статье будет рассматриваться второй, самый практичный вид аудита ИБ, в процессе которого устанавливается уровень выполнения требований регуляторов в области ИБ России (ФСТЭК России, ФСБ) и международных стандартов.

Международный стандарт ISO 19011-2021 содержит общее представление о процессе аудита ИБ – термины, принципы, этапы и способ оценки компетентности аудитора. Руководствуясь данным документом, аудитор может грамотно и полно разработать программу аудита ИБ и все необходимые организационно-распорядительные документы (далее ОРД), список и содержание которых, от первого этапа «инициирования аудита» и до седьмого «завершение аудита», так же описаны в стандарте. Данные рекомендации применимы для аудита ИБ любых информационных систем, в том числе объектов КИИ.

Конкретно для объектов КИИ ФСТЭК России разработал Приказы №31 [6] и №239[7]. Данные документы необходимы для проведения выбранного вида аудита, т.к. содержат базовые наборы требований по «обеспечению защиты информации в автоматизированных системах управления производством и технологическим процессом» (АСУП и АСУ ТП). Далее важно заметить, что выполнение требований Приказа ФСТЭК России № 239 необходимо лишь для объектов КИИ, признанных значимыми на основании проведенной процедуры по правилам категорирования утвержденным Постановлением Правительства РФ № 127[8]. Незначимые же объекты КИИ должны выполнять требования Приказа ФСТЭК России №31, а также обязанности ч.2 ст. 9 Федерального закона №187[9] (требования данного ФЗ распространяются и на значимые объекты).

Рассматриваемые приказы во многом схожи. Они формируют требования и определяют составы мер по обеспечению безопасности на всех этапах жизненного цикла АСУ ТП (при разработке, внедрении, в ходе эксплуатации и при выводе из нее).

Наименование мер защиты информации идентичны, их различие состоит в том, что для незначимых объектов перечень мер определен для каждого из уровней значимости обрабатываемой в них информации, в то время как для значимых –по трем категориям значимости.

В ходе проведения аудита ИБ, когда все обязанности уже распределены между аудиторами и разработана требующаяся предварительная ОРД, для каждого объекта КИИ создается сводная таблица с данными о выполнении (не выполнении) требований соответствующего Приказа. В случае если мера защиты выполняется, не лишним будет указать, СрЗИ или нормативный документ, который ответственен за ее перекрытие. Для СрЗИ важно отметить номер и срок действия сертификата из реестра ФСТЭК, т.к. он может быть просрочен и используемое в работе СЗИ средство необходимо будет заменить.

Кратко можно выделить основные вопросы проведения аудита, которые безусловно потребуют ответов [10]:

1. Какие силы обеспечения ИБ организованы на предприятии?

2. Какие ОРД по ОБИ (и в каком объеме/составе) разработаны и внедрены на предприятии?

3. Какие внедрены программные/ программно-аппаратные СрЗИ и каков срок действия их сертификатов?

4. Какие осуществляются, как реализованы и чем регламентированы мероприятия для обеспечения безопасности информации?

Таким образом, основная часть аудита ИБ, направленного на оценку соответствия требований законодательства, сводится к анализу таблицы, в которой собрана инфор-

мация о том, какие меры приказа выполняются, а какие нет.

В проведении подобного рода аудита для промышленных предприятий существует множество тонкостей и сложностей [11], рассмотрим некоторые из них на примере цеха ЛПЦ-10 ПАО «ММК». Материалы для статьи были собраны при прохождении производственной преддипломной практики на предприятии ПАО «ММК» г. Магнитогорск.

Первое с чем столкнутся аудиторы на рассматриваемом объекте - это сбор информации о АСУ ТП. Компоненты системы, такие как: АРМ операторов/инженеров, сервера, ПЛК компоненты полевого уровня; локализированы и располагаются, строго соответствуя документам, а различного рода сетевое оборудование (коммутаторы, хабы и т.п.) рассредоточены по разным частям цеха без какой-либо документации, регламентирующей его физическое местонахождение. Отсутствие схем и правил размещения оборудования не дает возможности аудиторам видеть сетевую архитектуру целиком, что в свою очередь затрудняет выстраивание границ между технологической сетью с ее специфической конфигурацией и стандартной корпоративной [12]. Устранение данной сложности целиком зависит от владельца предприятия и руководителя цеха, поскольку именно им необходимо инициировать процесс разработки данной технической документации. Разработанные схемы расположения сетевого оборудования поспособствуют облегчению работы не только аудиторов, но и сетевых администраторов дочерних компаний, ответственных за обеспечение работы сетевой составляющей АСУ ТП, которые выполняют свои должностные обязанности из офиса и редко посещают цех.

Отсутствие действующего специалиста по ОБИ в цехе осложняет работу аудиторов, т.к. в данном случает инициируется работа с технологами (инженерами, операторами), которые знают, как устроены технологические процессы, однако совершенно не разбираются в области информационных технологий, в частности и в информационной безопасности. В следствие человеческого фактора и не полного понимания поставленной задачи, сотрудники на местах сами неосознанно начинают тормозить процесс аудита. Данная сложность устраняется путем расширения штата персонала. В цехе необходим администратор безопасности, контролирующий и поддерживающий СЗИ.

После внедрения ФЗ РФ №187 в 2018 году руководство предприятия озаботилось разработкой организационно распорядительной и технической документации, однако в рассматриваемом цехе технические паспорта на многие объекты информатизации устарели, а ОРД разработаны не в полном объеме, требуемом ФСТЭК России. В связи с чем аудитор будет вынужден анализировать полноту выполнения требований по реализации мер безопасности информации обходя каждый объект информатизации лично. Данная сложность, как и предыдущая легко устраняется наймом администратора безопасности в конкретный цех.

Особенности построения архитектуры АСУ ТП кардинально отличают ее от привычной всем корпоративной информационной системы (КИС): начиная от специфических протоколов передачи данных (Modbus, DP, FDL, FMS), используемого оборудования (датчики, программируемые логические контроллеры, OPC сервера и др.) и программного обеспечения (SCADA, MES системы), заканчивая средой, в которой они функционируют (цеха, производственные помещения). В КИС основной защищаемый ресурс – информация, а цель – обеспечение конфиденциальности [13]. В технологических системах первостепенной задачей является сохранение непрерывности производства, которую обеспечивают доступность и целостности данных [14]. АСУ ТП имеют жестко фиксированную конфигурацию, не допускающую существенных изменений (обновления ПО, использование наложенных СрЗИ, корректировка настроек «по умолчанию») [15]. Достаточно сложно создать СЗИ, использующую СрЗИ не влияющие на технологический процесс и учитывающие специфику его работы. В условиях роста геополитической напряженности вокруг России эта и без того нетривиальная задача стала еще сложнее. К сожалению, на рынке отечественных СрЗИ недостаточно программных и программно-аппаратных средств, которые бы в полной мере покрывали все требования регулятора в области защиты информации.

Множественные кибератаки, происходящие в начале 2022 года, показали, что существует острая необходимость в обеспечении безопасности информации на объектах КИИ. Вовремя проведенный аудит ИБ позволит промышленным предприятиям сформировать стратегию защиты информации и вы-

строить наиболее полную и оптимизированную СЗИ, которая в свою очередь не допустит возникновение угроз безопасности информации, или по крайней мере значительно сократит ущерб от их реализации.

Литература

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

2. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии // Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие». Материалы конференций ГНИИ «НАЦРАЗВИТИЕ». Выпускающий редактор Ю.Ф. Эльзессер, Ответственный за выпуск С.В. Викторенкова. 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. 2019. № 1(31). С. 53–56.

4. Национальный стандарт Российской Федерации. ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента» [Текст], Принят Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. – 2021. – 41 с.

5. Лекция 19: Аудит информационной безопасности. [Электронный ресурс] - Режим доступа: https://intuit.ru/studies/courses/600/456/lecture/10226 (Дата обращения: 20.03.2022).

6. Приказ ФСТЭК России №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (в ред. Приказов ФСТЭК России от 23.03.2017 № 49, от 09.08.2018 № 138, от 15.03.2021 № 46) [Текст], Утвержден ФСТЭК России от 14 марта 2014 г. – 2014. – 33 с.

7. Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35) [Текст], Утвержден ФСТЭК России от 25 декабря 2017 г. – 2017. – 37 с.

8. Постановление Правительства №127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изменениями от 24 декабря 2021 г.) [Текст], утверждено постановлением Правительства Российской Федерации от 8 февраля 2018 г. – 2018. – 20 с.

9. Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Текст], Принят Государственной думой 12 июля 2017г., Одобрен Советом Федерации 19 июля 2017 г. – 2017. – 20 с.

10. Особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры [Электронный ресурс] – Режим доступа: https://www.itsec.ru/articles/osobennosti-provedeniya-audita-informacionnoj-bezopasnosti-obektov-kriticheskoj-informacionnoj-infrastruktury (Дата обращения: 20.03.2022).

11. Barankova I.I., Mikhailova U.V., Kalugina O.B. Analysis of the problems of industrial enterprises information security audit // Lecture Notes in Electrical Engineering. 2020. Т. 641 LNEE. С. 976–985.

12. Специфика защиты АСУ ТП [Электронный ресурс] – Режим доступа: http://lib.itsec.ru/articles2/asu-tp/spetsifika-zaschity-asu-tp (Дата обращения: 20.03.2022).

13. Кибербезопасность АСУ ТП – что это и зачем [Электронный ресурс] – Режим доступа: https://www.dialognauka.ru/press-center/article/13226/ (Дата обращения: 20.03.2022).

14. Где кроются реальные проблемы защиты АСУ ТП [Электронный ресурс] – Режим доступа: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (Дата обращения: 20.03.2022).

15. Безопасность АСУ ТП [Электронный ресурс] – Режим доступа: http://www.asku.ru/services/sec_services/sec_industry/ (Дата обращения: 20.03.2022).

References

1. Sanarbaev R.ZH., Mihajlova U.V. Tipovye problemy audita in-formacionnoj bezopasnosti na primere transportnoj kompanii OOO "AN-SER" // Obrazovanie Rossii i aktual'nye voprosy sovremennoj nauki. sbornik statej II Vserossijskoj nauchno-prakticheskoj konferencii. 2019. P. 147–151.

2. Mihajlova U.V., Bykova T.V. Audit informacionnoj bezopasno-sti na predpriyatii // Sbornik izbrannyh statej po materialam nauchnyh konferencij GNII «Nacrazvitie». Materialy konferencij GNII «NACRAZVITIE». Vypuskayushchij redaktor YU.F. El'zesser, Otvetstven-nyj za vypusk S.V. Viktorenkova. 2019. P. 341–345

3. Barankova I. I., Mihajlova U. V., Bykova T. V. Slozhnosti, voznikayushchie pri provedenii audita informacionnoj bezopas-nosti na predpriyatii [Difficulties arising during the audit of information security at the enterprise]. Vestnik UrFO, 2019, no. 1(31), P. 53–56.

4. Nacional'nyj standart rossijskoj federacii. GOST R ISO 19011-2021 «Ocenka sootvetstviya. Rukovodyashchie ukazaniya po provedeniyu audita sistem menedzhmenta» [Text], Adopted by the Order of the Federal Agency for Technical Regulation and Metrology of April 21 2021 r. – 2021. – 41 P.

5. Lekciya 19: Audit informacionnoj bezopasnosti. Available a: https://intuit.ru/studies/courses/600/456/lecture/10226 (Accessed: 20.03.2022).

6. Prikaz FSTEK Rossii №31 «Ob utverzhdenii trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh siste-mah upravleniya proizvodstvennymi i tekhnologicheskimi proces-sami na kriticheski vazhnyh ob"ektah, potencial'no opasnyh ob"ektah, a takzhe ob"ektah, predstavlyayushchih povyshennuyu opas-nost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy» [Tekst], Utverzhden FSTEK Rossii ot 14 marta 2014 g. – 2014. – 33 P.

7. Prikaz FSTEK Rossii №239 «Ob utverzhdenii trebovanij po obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj in-formacionnoj infrastruktury rRossijskoj Federacii» [Tekst], Utverzhden FSTEK Rossii ot 25 dekabrya 2017 g. – 2017. – 37 P.

8. Postanovlenie Pravitel'stva №127 «Ob utverzhdenii pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infra-struktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij» [Tekst], Utverzhdeno Pravitel'stvom Rossijskoj Federacii 8 fevralya 2018 g. – 2018. – 20 P.

9. Federal'nyj zakon №187 «O bezopasnosti kriticheskoj informacionnoj infra-struktury rossijskoj federacii» [Tekst], Prinyat Gosudarstvennoj dumoj 12 iyulya 2017g., Odobren Sovetom Federacii 19 iyulya 2017 g. – 2017. – 20 P.

10. Osobennosti provedeniya audita informacionnoj bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury. Available a: https://www.itsec.ru/articles/osobennosti-provedeniya-audita-informacionnoj-bezopasnosti-obektov-kriticheskoj-informacionnoj-infrastruktury (Accessed: 20.03.2022).

11. Barankova I.I., Mikhailova U.V., Kalugina O.B. Analysis of the problems of industrial enterprises information security audit // Lecture Notes in Electrical Engineering. 2020. T. 641 LNEE. P. 976–985.

12. Specifika zashchity ASU TP. Available a: http://lib.itsec.ru/articles2/asu-tp/spetsifika-zaschity-asu-tp (Accessed: 20.03.2022).

13. Kiberbezopasnost' asu tp – chto eto i zachem? Available a: https://www.dialognauka.ru/press-center/article/13226/ (Accessed: 20.03.2022).

14. Gde kroyutsya real'nye problemy zashchity ASU TP Available a: https://lib.itsec.ru/articles2/import/gde-kroyutsya-realnye-problemy-zaschity-asu-tp (Accessed: 20.03.2022).

15. Bezopasnost' ASU TP Available a: http://www.asku.ru/services/sec_services/sec_industry/ (Accessed: 20.03.2022).

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой Информатики и информационной безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

СЕМАВИНА Екатерина Александровна, студент кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им Г.И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38, E-mail: katuxa.karlina@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им Г.И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38, E-mail: ylianapost@gmail.com

BARANKOVA Inna Ilyinichna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc., Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru

SEMAVINA Ekaterina Alexandrovna, student, Department, Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: katuxa.karlina@mail.ru

MIKHAILOVA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Magnitogorsk State Technical University named after G. I. Nosova. Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com