БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 3 (110). – 67–82

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-3-67-82

ВОПРОСЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

А.В. СИТСКАЯ[1], В.В. СЕЛИФАНОВ[2], П.А. ЗВЯГИНЦЕВА[3]

[1] *630108, РФ, 195112, г. Санкт-Петербург, БЦ «Золотая долина», площадь Карла Фаберже, 8, лит. Б, 3 эт., оф. 302, менеджер по продажам, департамент информационной безопасности. E-mail: Anastasiya.Sitskaya@softline.com*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент. E-mail: sfo1@mail.ru*
[3] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, доцент кафедры информационной безопасности. E-mail: polinasgugit@mail.ru*

Сегодня информационная безопасность властвует абсолютно во всех сферах деятельности человека. Нарушение безопасности всегда влечет за собой последствия, но в зависимости от структуры они могут быть незаметными или же, наоборот, могут остановить деятельность организации или даже страны. Вопрос обеспечения информационной безопасности объектов критической информационной инфраструктуры сегодня стал наиболее обсуждаем. Государственные регуляторы разработали множество нормативно правовых документов, которые содержат в себе требования к системе защиты объектов критической информационной инфраструктуры различных уровней значимости. Однако никто так и не создал ни одной методики, которая бы показала реальное состояние информационной безопасности объекта критической информационной инфраструктуры. Как следствие, как организация, так и регуляторы видят только общую картину состояния системы защиты, что, в свою очередь, создает множество уязвимых мест, которыми может воспользоваться злоумышленник для осуществления атаки. Вследствие атаки объекта критической информационной инфраструктуры вред может быть нанесен не только организации, но и людям, могут быть нарушены рабочие процессы всего государства. Именно поэтому вопрос создания такой методики становится не просто актуальным, но и необходимым как для внутреннего контроля самой организации, так и для автоматизации работы регуляторов при проведении очередных проверок. Методика покажет не только качественную оценку состояния системы защиты, но и возможные уязвимые места организации, которые необходимо устранить для повышения эффективности всей защиты.

* Статья получена 20 июля 2023 г.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, объект критической информационной инфраструктуры, аудит, аудит информационной безопасности, система защиты информации, разработка методики оценки, защита информационных систем

ВВЕДЕНИЕ

Объекты критической информационной инфраструктуры (далее – объект КИИ), определяемые согласно Федеральному закону от 26 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187) [1] как «информационные системы, автоматизированные системы управления субъектов критической информационной инфраструктуры», подлежат защите. Однако приведенное определение нельзя считать полным, так как оно требует дополнительного пояснения. Таким пояснением становится определение субъекта критической информационной инфраструктуры. Согласно Федеральному закону № 187 субъект КИИ – это «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей». В совокупности эти два определения дают достаточно полное понимание составляющих КИИ.

НОРМАТИВНО-ПРАВОВАЯ БАЗА

Исходя из определений видно, что данной области защиты информации (далее – ЗИ) должно быть уделено особое внимание. При нарушении требований ЗИ может быть нарушено функционирование одной из областей КИИ, а как следствие, полная остановка и угроза как сфере деятельности государства, так и жизни людей отдельных регионов страны. Именно серьезные по-

следствия при нарушении деятельности КИИ стали причиной для разработки ряда законодательных и нормативных правовых актов (далее – НПА), обязательных для соблюдения объектами КИИ.

Для чего же на самом деле нужна методика оценки? Она нужна, чтобы не просто в качественном или количественном виде увидеть состояние защиты системы, но и точно увидеть все уязвимости системы, которые может использовать злоумышленник для реализации эффективной атаки на информационные системы (далее – ИС) объекта КИИ. Понятно, что в зависимости от потенциала нарушителя последствия его атаки будут различными.

Если при нарушении деятельности объекта КИИ главные потери понесет сам объект (например, денежные потери), то внимание к такому объекту будет минимально и, собственно, защита своей инфраструктуры будет его проблемой. Однако если простой объекта КИИ в теории может вызвать серьезные последствия для государства, то защита такого предприятия приобретает высокую значимость. А за нарушения будут отвечать сотрудники предприятия согласно Уголовному и Административному кодексам Российской Федерации. Естественно, предприятие становится заинтересованным в реализации сильной и эффективной системы ЗИ.

Однако, казалось бы, система ЗИ построена и работает. Но как это может понять сторонний наблюдатель? Как наиболее наглядно показать, не углубляясь в техническую часть работы системы ЗИ, что она работает, и работает на необходимом уровне? Для решения данного вопроса нам необходимо в первую очередь правильно провести категорирование.

Категорирование объектов КИИ проводится согласно Постановлению Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений» (далее – Постановление Правительства) [2]. Согласно Постановлению Правительства категорирование объектов КИИ в обязательном порядке включает в себя следующие пункты [2]:

а) определение процессов, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономиче-

ским, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее – критические процессы);

в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее – перечень объектов);

д) оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

После того как объекты КИИ получили категории и их одобрил регулятор, актуальным становится вопрос: как защитить? Мы помним, что основную роль в формировании требований к технической защите организации КИИ взял на себя такой регулятор, как ФСТЭК России. Главным его НПА в части технической защиты стал приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – приказ ФСТЭК № 239) [3], содержащий в себе 17 групп мер, которые по своей сути обязательны к использованию, однако приказ предусматривает варианты, когда при наличии обоснования их можно исключить.

АУДИТ ОБЪЕКТА КИИ

Как же должен строиться аудит информационной безопасности (далее – ИБ), чтобы организация могла увидеть реальную картину состояний системы ЗИ? Проанализировав литературу [4–10], можно выделить три основных этапа аудита, исполнение которых отражает реальное состояние КИИ:

1) проверка полноты и достаточности существующей документации в организации по требованиям НПА в области защиты информации;

2) оценка качества документации в области ЗИ;

3) проверка реализации технической составляющей системы ЗИ согласно существующей НПА в области защиты информации.

Далее рассмотрим нюансы каждого этапа аудита.

Первый этап аудита заключается в проверке наличия всех существующих документов в области ИБ. На данном этапе должное внимание уделяется не качеству документа, а лишь факту его существования. То есть главная задача аудитора – составить актуальный перечень существующей документации организации. Для этого аудитор руководствуется документами [1–3, 11–15].

Так как у аудитора в наличии только НПА, которые регламентируют отдельные области ЗИ, при этом в большей степени не говорят конкретно, в каких документах и что должно содержаться, ему необходимо разработать перечень необходимых документов для стабильного функционирования организации. На базе такого перечня создается чек-лист для аудитора, который наглядно покажет наличие или отсутствие ряда документов.

На первом этапе формируется:

1) актуальный чек-лист необходимых документов организации;
2) количественная оценка наличия ряда документов в области ЗИ.

Поскольку чек-лист по своей сути создается индивидуально для каждого предприятия, то и количественная оценка должна напрямую зависеть от чек-листа, а точнее, от количества существующих в организации документов и от количества необходимых документов. Естественно, чек-лист имеет градацию оценок: 1 – документ в наличии, 0 – документ отсутствует. Из вышесказанного получаем следующую формулу:

$$E_{ch1} = \frac{\sum_{i=1}^{n} d_i}{n}, \qquad (1)$$

где E_{ch1} – оценка наличия необходимого перечня документов; i – номер документа чек-листа; n – количество документов в чек-листе; d_i – оценка наличия i-го документа.

На втором этапе аудитор уделяет внимание качеству документа. Для этого он должен не только знать НПА в области ЗИ, но углубиться в особенности построенной КИИ организации, чтобы оценить как актуальность документа, так и его достаточность. Пункты чек-листа второго этапа полностью идентичны чек-листу первого этапа, однако есть существенная разница. В данном чеклисте градация оценок состоит из трех уровней:

- 0 – если документ неактуален или отсутствует;
- 0,5 – если документ требует доработки;

- 1 – если актуален и полностью соответствует реальному функционированию системы ЗИ.

Такая градация необходима, чтобы как можно подробнее оценить состояние системы ЗИ.

Результаты второго этапа будут заключены в следующих пунктах:

1) заполненный чек-лист актуальности и полноты документов организации;

2) количественная оценка достаточности документов в области ЗИ.

После заполнения чек-листа второго этапа для получения объективной оценки состояния документации необходимо обратиться к формуле

$$E_{ch2} = \frac{\sum_{i=1}^{n} dp_i}{n}, \quad (2)$$

где E_{ch2} – оценка полноты содержания необходимого перечня документов; i – номер документа чек-листа; n – количество документов в чек-листе; dp_i – полнота i-го документа.

Третий этап аудита заключается в проведении технической проверки состояния системы ЗИ КИИ. На данном этапе аудитор должен достоверно убедиться в наличии и работоспособности технических средств ЗИ, которые используются организацией в построенной системе ЗИ.

Порядок проведения третьего пункта аудита подробно описан в статьях [16, 17], в которых представлен алгоритм построения графа, показанного на рис. 1. Граф подробно демонстрирует ход третьего этапа аудита и разбиение его на три параллели, построен на основе анализа и систематизации рейтинга SANS CIS Controls 8 и практического опыта ФСТЭК России. Каждая вершина графа сопоставлена с группами мер в соответствии с приказом ФСТЭК России № 239.

При оценивании каждой группы мер аудитор должен помнить, что не все меры равноценны между собой, а значит, использование мер разных уровней злоумышленником нанесет разный уровень последствий. Именно поэтому меры имеют разную градацию оценок.

Первая градация будет применима для критичных мер, которые составляют первые два уровня графа. Вторая градация будет включать в себя третий и четвертый уровни графа.

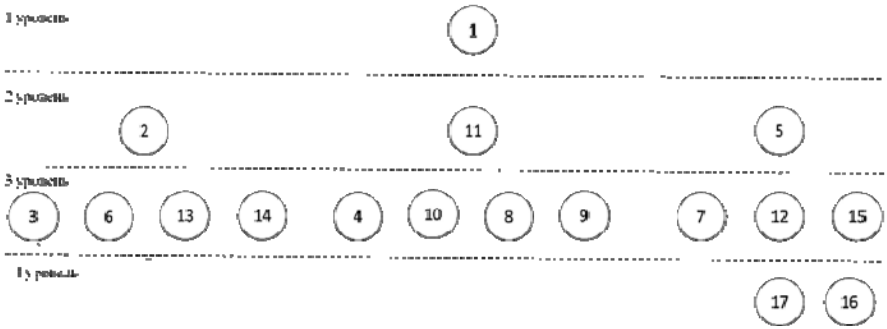

Рис. 1. Граф аудита ИБ

Fig. 1. Graph of IB audits

Менее критичные меры графа имеют следующую градацию:
– оценка 1 ставится, если мера реализована полностью;
– оценка 0 ставится, если мера не реализована или реализована частично.

Наиболее критичные меры графа имеют следующую градацию:
– оценка 1 ставится, если мера реализована полностью;
– оценка 0,5 ставится, если мера реализована не в полном объеме;
– оценка 0 ставится, если мера не реализована.

После получения результатов по достаточности реализации мер ЗИ необходимо получить конечные оценки, которые наглядно покажут состояние технической ЗИ. Для этого необходим эталон. Эталоном становится идеализированная система ЗИ, построенная в проверяемой организации. Согласно статье [16] применим следующий алгоритм вычисления оценки для третьего этапа аудита.

В первую очередь рассчитаем значения оценок для каждой из групп мер:

$$E_k = \frac{\sum_{i=1}^{n} M_i}{N}, \qquad (3)$$

где E_k – численное значение промежуточной оценки выбранных организацией групп мер; M_i – оценка *i*-й меры; N – число мер, необходимых в системе защиты; n – количество реализуемых мер.

Далее рассчитаем промежуточные оценки реализуемых групп мер. Для этого необходимо вычислить промежуточные значения по каждой ветви графа:

$$E_{bk} = \sum_{i=1}^{n} E_i \,, \tag{4}$$

где E_{bk} – числовое значение промежуточной оценки выбранной ветви мер; E_i – промежуточная оценка *i*-й группы меры, касающейся идентификации и аутентификации; *n* – число групп мер в ветви.

Для того чтобы получить взвешенную оценку эффективности защиты ИС, используем весовые коэффициенты. В системе защиты четыре ветви, поэтому, чтобы оценка была объективной и цельной, необходимо просчитать среднеарифметическое всех полученных оценок. Исходя из вышесказанного получаем следующую формулу:

$$E_{ch3} = \frac{0,5E_{B1} + 0,2E_{B2} + 0,2E_{B3} + 0,1E_{B4}}{4} \,. \tag{5}$$

где E_{ch3} – взвешенная оценка выбранных организацией мер; E_{B1} – промежуточная оценка групп мер первой ветви; E_{B2} – промежуточная оценка групп мер второй ветви; E_{B3} – промежуточная оценка групп мер третьей ветви; E_{B4} – промежуточная оценка групп мер четвертой ветви.

Последним пунктом аудита становится расчет оценки, которая содержит результаты всех этапов аудита, полученных по приведенным ранее формулам. Конечная оценка состояния системы ЗИ объекта КИИ должна учитывать результаты работы всех трех этапов. Если все три этапа аудита равноценны, будет применяться формула

$$E = \frac{E_{ch1} + E_{ch2} + E_{ch3}}{3} \,,$$

где *E* – средневзвешенная оценка всех трех этапов аудита.

При получении итоговой оценки становится необходимым ее применение, т. е. сравнение с диапазоном допустимых значений в соответствии с уровнями объекта КИИ. Ни один из приказов не содержит в себе необходимых диапазонов, однако схожие диапазоны разработал Центральный банк Российской Федерации для обеспечения собственной безопасности. Такие

диапазоны прописаны в ГОСТ Р 57580.2–2018. Следует помнить, что финансовые организации также являются объектами КИИ, а значит, требования к системе защиты, разработанные ЦБ РФ и ФСТЭК, имеют схожую базу. Поэтому целесообразно использовать наиболее строгую систему оценивания, разработанную ЦБ РФ. Опираясь на вышеупомянутый ГОСТ, целесообразно использовать следующую градацию оценок:

– третий уровень ЗО КИИ соответствует диапазону $0{,}7 < E \leq 0{,}85$;
– второй уровень ЗО КИИ соответствует диапазону $0{,}85 < E \leq 0{,}9$;
– первый уровень ЗО КИИ соответствует диапазону $0{,}9 < E \leq 1$.

Здесь 1 – полное соответствие СЗИ эталонной СЗИ. Такие жесткие и высокие диапазоны оценок обоснованы тем, что нарушение функционирования ЗО КИИ в зависимости от его уровня может нанести непоправимый урон одной из пяти сфер согласно Постановлению Правительства [2].

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Для наглядного демонстрирования работы с разработанной методикой рассмотрим ее применение на практическом примере. Рассмотрим существующую систему ЗИ химическо-промышленной компании *N*. Система защиты информации имеет структуру, представленную на рис. 2.

Компания *N* провела категорирование ИС и определила, что ИС соответствует третьей категории. Согласно приказу ФСТЭК № 239 компания *N* обязана реализовать перечень мер, соответствующих третьей категории ЗО КИИ. Однако применение вслепую абсолютно всех мер нецелесообразно, так как если обратить внимание на структуру ИС, становится очевидно, что такие меры, как идентификация и аутентификация внешних пользователей, реализация защищенного удаленного доступа, управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных, защита информации при использовании мобильных устройств, являются излишними.

Для первого этапа аудита необходима реализация нулевых мер каждой из групп мер, а также разработка документов, которая необходима согласно перечисленным ранее НПА. Для второго же этапа аудита важно, чтобы документ не только был разработан, но и содержал в себе всю необходимую информацию. Так, например, если мы обратимся к 16-й группе мер, то в разработанном документе, регламентирующем правила и процедуры обеспечения действий в нештатных ситуациях, должны содержаться комментарии и перечень действий по каждой из групп мер ДНС. Таким образом, результатом двух этапов будут две оценки, отображающие полноту наличия документации и оценку ее качества.

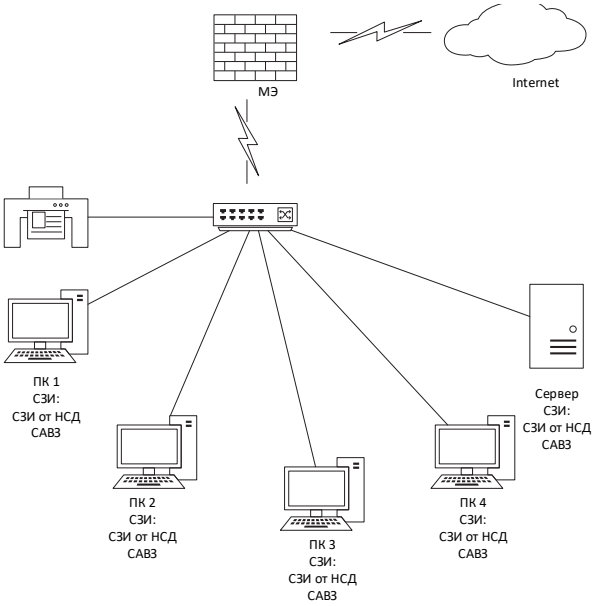

Рис. 2. Система защиты информации компании

Fig. 2. Company Information Security System

Конечными оценками СЗИ компании *N* стали:

- $E_{ch1} = 0,85$ – оценка достаточности разработанных документов;
- $E_{ch2} = 0,67$ – оценка полноты разработанных документов;
- $E_{ch3} = 0,71$ – оценка реализации мер приказа ФСТЭК № 239.

Получив оценки по каждому этапу, возможно рассчитать конечную оценку *E*:

$$E = \frac{E_{ch1} + E_{ch2} + E_{ch3}}{3} = 0,74 .$$

Из полученного значения оценки мы можем сделать вывод, что разработанная система соответствует нижней грани третьего уровня ЗО КИИ. При этом из приведенных результатов видно, что у компании есть проблемы не столько с наличием документов в области ЗИ, сколько с их актуальностью, что, в свою очередь, отражается как на реализации мер (оценка E_{ch3}), так и в целом на всей системе ЗИ.

ВЫВОД

Предложенная последовательность проведения аудита включает разбиение его на три этапа: аудит наличия документов, аудит качества документов, аудит реализации мер ЗИ в соответствии с законодательством. Такой подход покажет наиболее уязвимые места СЗИ в целом, а методика может точно показать места, которые необходимо закрыть организации, гибкая система оценивания покажет уровень защищенности всей СЗИ

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений».

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

4. ГОСТ Р ИСО 19011–2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента качества. – М.: Стандартинформ, 2021. – 35 с.

5. *Geldiyev H., Churiyev M., Mahmudov R.* Issues regarding cybersecurity in modern world // Digitalization and industry 4.0: Economic and societal development. – Wiesbaden: Springer Gabler, 2020. – P. 3–14. – DOI: 10.1007/978-3-658-27110-7_1.

6. *Ан В.Р., Табакаева В.А.* Разработка алгоритма проведения аудита кибербезопасности // МНСК-2021. Информационные технологии: материалы 59-й Международной научной студенческой конференции, Новосибирск, 12–23 апреля 2021 г. – Новосибирск, 2021. – С. 5. – EDN CAYHXE.

7. Разработка методики аудита кибербезопасности ГИС, относящихся к объектам критической информационной инфраструктуры Российской Федерации / В.Р. Ан, В.В. Селифанов, В.А. Табакаева, С.А. Буларга, А.С. Ворожцов // Сборник научных трудов НГТУ. – 2019. – № 3–4 (96). – С. 84–95. – DOI: 10.17212/2307-6879-2019-3-4-84-95. – EDN BOGOJY.

8. *Милославская Н.Г., Толстой А.И.* Проверка деятельности по управлению информационной безопасностью. – М.: Горячая линия – Телеком, 2022. – 172 с.

9. *Leksin V.N.* Effectiveness and efficiency of the activities of regional and municipal governments: Purpose and possibility of a correct assessment // Regional Research of Russia. – 2013. – Vol. 3. – P. 277–290. – DOI: 10.1134/S2079970513030076.

10. *Степашин С.В.* Государственный аудит в Российской Федерации // Государственный аудит. Право. Экономика. – 2009. – № 1. – С. 4–9. – EDN PCGDAD.

11. Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

12. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

13. Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

14. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

15. Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

16. *Sitskaya A., Selifanov V., Purgina M.* Development of weighting coefficients for assessing the quality of security measures implementation for significant objects of critical information infrastructure // Advances in Automation IV. RusAutoCon 2022. – Cham, Springer, 2023. – P. 411–420. – (Lecture Notes in Electrical Engineering; vol 986). – DOI: 10.1007/978-3-031-22311-2_39.

17. *Ситская А.В., Селифанов В.В.* Ранжирование мер обеспечения безопасности значимых объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 240–249. – DOI: 10.33764/2618-981X-2022-6-240-249. – EDN GFUGGU.

Ситская Анастасия Вадимовна, менеджер по продажам департамента информационной безопасности БЦ «Золотая долина». В настоящее время специализируется в области информационной безопасности. E-mail: Anastasiya.Sitskaya@softline.com

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. В настоящее время специализируется в области информационной безопасности. E-mail: sfo1@mail.ru

Звягинцева Полина Александровна, старший преподаватель кафедры информационной безопасности Сибирского государственного университета геосистем и технологи. Область научных интересов – защита информации. E-mail: polinasgugit@mail.ru

DOI: 10.17212/2782-2230-2023-3-67-82

Information security audit issues*

A.V. Sitskaya[1], V.V. Selifanov[2], P.A. Zvyagintseva[3]

[1] *Siberian State University of Geosystems and Technologies, 10 K. Plakhotnogo, Novosibirsk, 630108, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: Anastasiya.Sitskaya@softline.com*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

[3] *Siberian State University of Geosystems and Technologies, 10 K. Plakhotnogo, Novosibirsk, 630108, Russian Federation, associate professor of the Department of Information Security. E-mail: polinasgugit@mail.ru*

Today, information security reigns in absolutely all areas of human activity. Security breaches always have consequences, but depending on the structure, they can be invisible, or vice versa, stop the activities of an organization or even a country. The issue of ensuring information security of critical information infrastructure facilities has become the most discussed today. The state and its regulators to develop many regulatory legal documents that contain require-

* *Received 20 July 2023.*

ments for the system of protection of critical information infrastructure facilities of various levels of significance. However, no one has ever created a single technique that would show the real state of information security of a critical information infrastructure object. As a result, both the organization and regulators see only a general picture of the state of the defense system, which in turn creates many vulnerabilities that an attacker can use to carry out an attack. As a result of the attack on the object of critical information infrastructure, harm can be done not only to organizations, but also to people, the work processes of the entire state can be violated. That is why the issue of creating such a methodology becomes not only relevant, but also necessary both for the internal control of the organization itself and for automating the work of regulators during the next inspections. The methodology will show not only a high-quality assessment of the state of the protection system, but also show the possible vulnerabilities of the organization that need to be closed to improve the effectiveness of all protection.

Keywords: information security, critical information infrastructure, critical information infrastructure facility, audit, information security audit, information security system, development of evaluation methodology, protection of information systems

REFERENCES

1. Federal Law of July 26, 2017 No. 187-FZ "On the security of the critical information infrastructure of the Russian Federation". (In Russian).

2. Decree of the Government of the Russian Federation of February 8, 2018 No. 127 "On approval of the rules for categorizing critical information infrastructure facilities of the Russian Federation, as well as a list of indicators of criteria for the significance of critical information infrastructure facilities of the Russian Federation and their values". (In Russian).

3. Order of the FSTEC of Russia dated December 25, 2017 No. 239 "On approval of requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation". (In Russian).

4. State standard R ISO 19011–2021. *Conformity assessment. Guidelines for auditing management systems*. Moscow, Standartinform Publ., 2021. 35 p. (In Russian).

5. Geldiyev H., Churiyev M., Mahmudov R. Issues regarding cybersecurity in modern world. *Digitalization and industry 4.0: Economic and societal development*. Wiesbaden, Springer Gabler, 2020, pp. 3–14. DOI: 10.1007/978-3-658-27110-7_1.

6. An V.R., Tabakaeva V.A. [Development of an algorithm for conducting a cybersecurity audit]. *MNSK-2021. Informatsionnye tekhnologii* [MNSK-2021. Information technology]. Proceedings of the 59th International Students Scientific Conference, April 12−23, 2021. Novosibirsk, 2021, p. 5. (In Russian).

7. An V.R., Selifanov V.V., Tabakaeva V.A., Bularga S.A., Vorozhtsov A.S. Razrabotka metodiki audita kiberbezopasnosti GIS, otnosyashchikhsya k ob"ektam kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii [Development of a GIS cybersecurity audit methodology related to critical information infrastructure

facilities of the Russian Federation]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 3–4 (96), pp. 84–95. DOI: 10.17212/2307-6879-2019-3-4-84-95.

8. Miloslavskaya N.G., Tolstoi A.I. *Proverka deyatel'nosti po upravleniyu informatsionnoi bezopasnost'yu* [Verification of information security management activities]. Moscow, Goryachaya liniya – Telekom Publ., 2022. 172 p.

9. Leksin V.N. Effectiveness and efficiency of the activities of regional and municipal governments: Purpose and possibility of a correct assessment. *Regional Research of Russia*, 2013, vol. 3, pp. 277–290. DOI: 10.1134/S2079970513030076.

10. Stepashin S.V. Gosudarstvennyi audit v Rossiiskoi Federatsii [State audit in the Russian Federation]. *Gosudarstvennyi audit. Pravo. Ekonomika = State audit. Law. Economics*, 2009, no. 1, pp. 4–9.

11. Decree of the Government of the Russian Federation of February 17, 2018 No. 162 "On approval of the Rules for the implementation of state control in the field of ensuring the security of significant objects of the critical information infrastructure of the Russian Federation". (In Russian).

12. Order of the FSTEC of Russia dated December 21, 2017 No. 235 "On approval of Requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and ensuring their functioning". (In Russian).

13. Order of the FSB of Russia dated June 19, 2019 No. 282 "On approval of the Procedure for informing the FSB of Russia about computer incidents, responding to them, taking measures to eliminate the consequences of computer attacks carried out on significant objects of the critical information infrastructure of the Russian Federation". (In Russian).

14. Order of the FSTEC of Russia dated April 29, 2021 No. 77 "On approval of the Procedure for organizing and conducting work on the certification of informatization facilities for compliance with the requirements for the protection of limited access information that does not constitute a state secret". (In Russian).

15. Order of the FSB of Russia dated July 24, 2018 No. 367 "On approval of the List of information submitted to the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation and the Procedure for submitting information to the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation". (In Russian).

16. Sitskaya A., Selifanov V., Purgina M. Development of weighting coefficients for assessing the quality of security measures implementation for significant objects of critical information infrastructure. *Advances in Automation IV. RusAuto-*

Con 2022. Cham, Springer, 2023, pp. 411–420. DOI: 10.1007/978-3-031-22311-2_39.

17. Sitskaya A.V., Selifanov V.V. Ranzhirovanie mer obespecheniya bezopasnosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury [Ranking of security measures of significant objects of critical information infrastructure]. *Interekspo Geo-Sibir' = Interexpo GEO-Siberia*, 2022, vol. 6, pp. 240–249. DOI: 10.33764/2618-981X-2022-6-240-249.

Для цитирования:

Ситская А.В., Селифанов В.В., Звягинцева П.А. Вопросы аудита информационной безопасности // Безопасность цифровых технологий. – 2023. – № 3 (110). – С. 67–82. – DOI: 10.17212/2782-2230-2023-3-67-82.

For citation:

Sitskaya A.V., Selifanov V.V., Zvyagintseva P.A. Voprosy audita informatsionnoi bezopasnosti [Information security audit issues]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 3 (110), pp. 67–82. DOI: 10.17212/2782-2230-2023-3-67-82.