УДК 528.71
DOI 10.33764/2618-981X-2023-6-224-231

А. В. Ситская[1], В. В. Селифанов[1]*

Вопросы управления информационной безопасностью на объектах критической информационной инфраструктуры

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: AnSits@yandex.ru

Аннотация. На сегодняшний день главной проблемой в области обеспечения информационной безопасности – это грамотное управление информационной безопасностью на объектах критической информационной инфраструктуры, подрыв деятельности которой может привести к нарушению функционирования целой отрасли как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Главный метод управления информационной безопасностью является аудит. Организация должна проводить как внешний, так и внутренний аудит. Главным результатом данной статьи становятся рекомендации правильного управления информационной безопасностью на объектах критической информационной инфраструктуры. Чтобы получить наглядные результаты необходимо правильно провести аудит, следуя определенным правилам. В статье рассматривается цикл У. Э. Деминга, повсеместно используемый во всех сферах как метод проведения аудита. Главный принцип цикла «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй» наглядно показывает правильную организацию эффективного управления информационной безопасностью.

Ключевые слова: информационная безопасность, объект критической информационной инфраструктуры, цикл Деминга, цикл PDCA

A. V. Sitskaya[1], V. V. Selivanov[1]*

Issues of Information Security Management at Critical Information Infrastructure Facilities

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: AnSits@yandex.ru

Abstract. To date, the main problem in the field of information security is the competent management of information security at critical information infrastructure facilities, the undermining of which can lead to disruption of the functioning of an entire industry such as healthcare, science, transport, communications, energy, banking, fuel and energy complex, in the field of nuclear energy, defense, missile andspace, mining, metallurgical and chemical industries. The main method of information security management is auditing. The organization must conduct both external and internal audits. The main result of this article are recommendations for proper information security management at critical information infrastructure facilities. To get visual results, it is necessary to conduct an audit correctly, following certain rules. The article discusses the W. E. Deming cycle, which is widely used in all spheres as a method of conducting an audit. The main principle of the "Plan-Do-Check-Act" or "plan-implement-check-act" cycle clearly shows the correct organization of effective information security management.

Keywords: information security, critical information infrastructure facility, deming cycle, PDCA cycle

Введение

В настоящее время одним из наиболее острых вопросов стал вопрос обеспечения информационной безопасности (ОИБ). На ОИБ объектов критической информационной инфраструктур (КИИ) нацелено наиболее пристальное внимание. В первую очередь ИБ объектов КИИ – это безопасность информационных систем (ИС) стратегически важных для государства областей. Нарушение безопасности ИС предприятия одной из стратегических областей может не просто остановить на некоторое время предприятие, но и снизить эффективность работы целой отрасли как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Для регулирования ИБ на объектах КИИ были выпущены как Федеральные законы (187-ФЗ от 26 июля 2017 г. [1]), Постановления правительства (ПП РФ №127 от 08.02.2018г.[2], ПП РФ №162 от 17.02.2018г. [3]), так и приказы таких регуляторов как ФСТЭК России (Приказ ФСТЭК России №227 от 06.12.2017г. [4], Приказ ФСТЭК России №235 от 21.12.2017г. [5], Приказ ФСТЭК России №239 от 25.12.2017г. [6]), так и ФСБ России (Приказ ФСБ России №366 от 24.07.2018г. [7], Приказ ФСБ России №368 от 24.07.2018г. [8], Приказ ФСБ России №196 от 06.05.2019г. [9], Приказ ФСБ России № 281 от 19.06.2019г. [10], Приказ ФСБ России № 282 от 19.06.2019г. [11]). Однако слепое следование законодательству не говорит об эффективности построенной системы защиты информации (СЗИ) на предприятии. Для обеспечения и поддержания эффективности СЗИ необходимо, чтобы на предприятии была эффективно построена система управления информационной безопасностью (СУИБ), адаптированная под конкретную ИС и учитывающая специфику организации.

Цикл Деминга как эффективная СУИБ

Главной проблемой, затрудняющей повышение качества управления параметрами ИБ, является непостоянность параметров объекта управления и постоянное изменение требований к качеству регулирования в процессе работы [12]. Функционирование наиболее эффективной СУИБ хорошо иллюстрирует цикл У.Э. Деминга (PDCA), где главная мысль: «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй». При соблюдении такого подхода СЗИ будет наиболее эффективна и работоспособна, т.к. большая часть уязвимостей будет выявлена и устранена вовремя. Однако реализация данного цикла также требует усилий.

Один из основополагающих стандартов, касающихся аудита, ГОСТ Р ИСО 19011-2021[13], который различает следующие типы аудита:

– внутренний аудит 1-й стороны проводится самой организацией или от ее имени для внутренних целей [14]. Основанием для проведения такого аудита служит внутренний контроль принятых нормативных документов по защите информации (ЗИ);

– внешний аудит 2-й стороны проводится сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени [14];

– внешний аудит 3-й стороны (независимая оценка) проводится внешними независимыми коммерческими организациями, имеющими лицензии на осуществление аудиторской деятельности в области ОИБ [14]. В области ЗИ объектов КИИ такой аудит является неотъемлемой частью функционирования предприятия, утвержденный законодательством РФ, и именно такой аудит зачастую приносит наибольший результат по контролю функционирования СЗИ.

Также ГОСТ Р ИСО 19011-2021[13] предлагает схему последовательности действий для управления программой аудита, которая очень ярко иллюстрирует цикл Деминга в области аудита ИБ.

Аудит на всех этапах жизненного цикла СЗИ

На этапе планирования как СЗИ, так и аудита происходит разработка технического задания (для СЗИ) и разработка программы проведения аудита. Первичный аудит объекта КИИ должен представлять из себя процесс категорирования. На данном этапе аудит может быть, как внутренним 1-й стороны, так и внешним 3-й стороны.

Во время этапа планирования аудита должны быть рассмотрены и реализованы следующие пункты, согласно [13]:

– установить объем программы в соответствии с поставленными целями и известными ограничениями;

– определить внешние и внутренние проблемы, риски и возможности, которые могут повлиять на программу;

– обеспечить выбор групп аудита, обладающих необходимой компетентностью для проведения аудита, определив их обязанности ответственность и полномочия;

– разработать все необходимые процессы, включая процессы для координации и планирования всех аудитов в рамках программы, разработка целей аудита, области и критериев, определения методов аудита, подбор аудиторской группы, разработка внешних и внутренних процессов коммуникаций;

– и т.п.

Далее, согласно циклу Деминга идет «реализация». При реализации стоит обратить внимание, что согласно законодательству, объекты КИИ разделяются на «значимые» и «не значимые». При этом «значимым» объектам необходимо присвоить категорию, в соответствии с которой далее и будет осуществляться построение/ модернизация предприятия. «Не значимые» объекты не участвуют в автоматизации критических процессов, а значит не подлежат категорированию.

Схема последовательности действий управления программой аудита представлена на рис. 1.

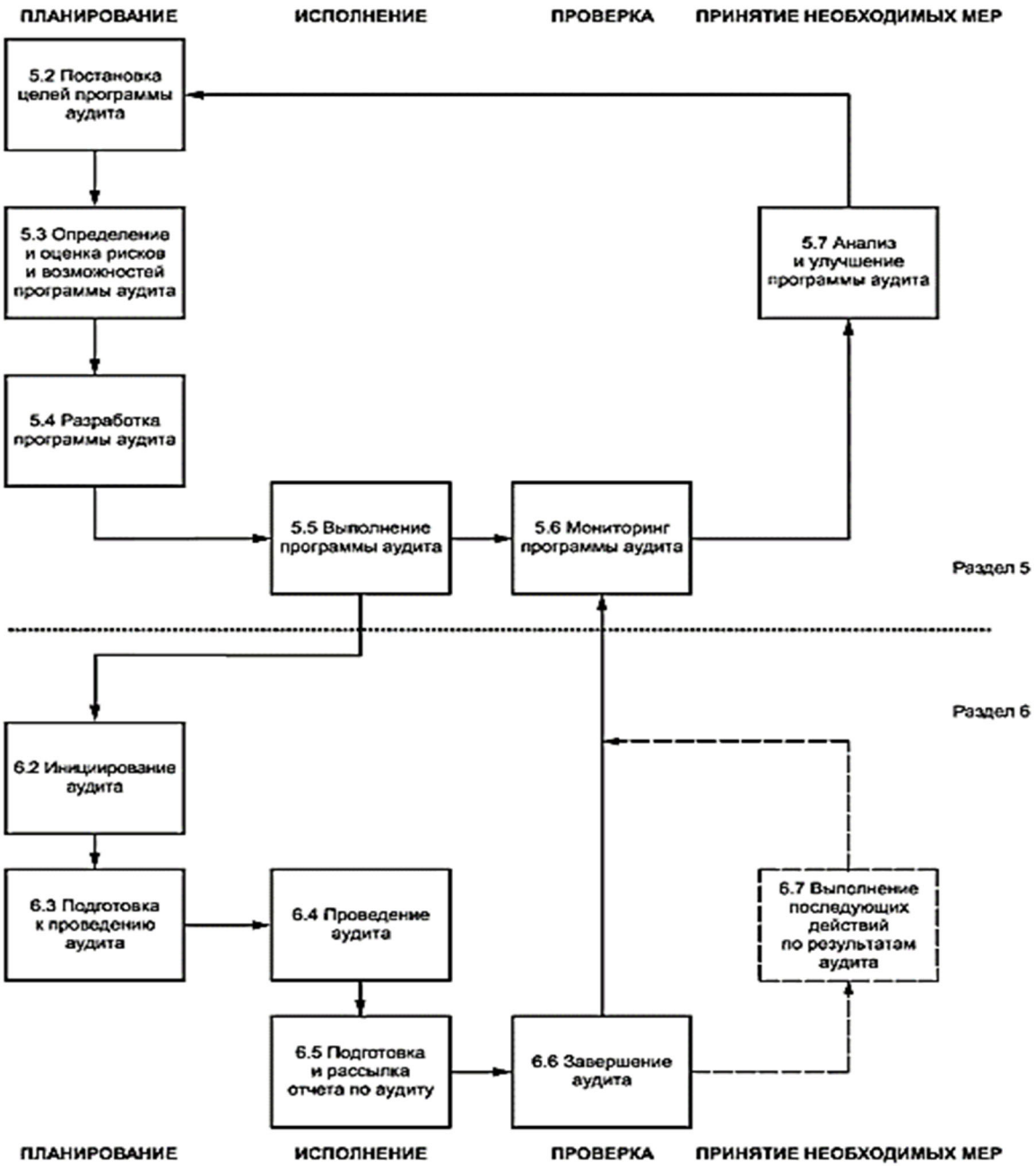

Рис. 1. Схема последовательности действий управления программой аудита [13]

Если при проведении аудита значимых объектов КИИ (ЗО КИИ) все достаточно понятно, аудитор в первую очередь обращает внимание на соблюдение законодательства, то при аудите не значимых объектов КИИ аудитор может не учитывать законодательство для ЗО КИИ, однако необходимо оценивать полноту выполнения субъектом КИИ обязанностей, возложенных на него частью 2 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». По решению субъекта КИИ, для обеспечения безопасности «не значимого» объекта КИИ может быть создана система безопасности, базирующаяся на требованиях для «зна-

чимых» объектов КИИ. В этом случае, в критерии аудита уже включаются все требования, характерные для безопасности «значимых» объектов КИИ [15].

При первичном аудите аудитору необходимо оценить полноту и достаточность реализации СЗИ. А для ЗО КИИ соответствующей категории значимости согласно Приказу ФСТЭК России №239 [6] определить, какие меры выполняются, а какие нет, затем понять, как и насколько полно они выполняются.

Результатом первичного аудита будет являться понимание того, какая часть обязательных мер по обеспечению безопасности ЗО КИИ уже реализована, а какая требует реализации в процессе создания/модернизации СЗИ.

На следующем этапе цикла производится улучшение методов проведения аудита, корректировка сроков проведения аудита. Далее с учетом всех результатов предыдущих этапов проводится аудит, результаты которого в полной мере будут отражать текущее состояние СУИБ предприятия.

Однако проведение аудита не гарантирует эффективность работы СЗИ предприятия. В процессе внешнего аудита отдельное внимание уделяется именно СУИБ. И после получения отчета по аудиторской проверке руководству организации стоит обратить пристальное внимание именно к разделу, посвящённому СУИБ. Ведь дальнейшие результаты по устранению недостатков всей СЗИ возлагаются именное на СУИБ.

Анализ функционирования СУИБ основан на следующем:

– результаты мониторинга ИБ и контроля мер ОИБ, который иллюстрирует эффективность проводимых внутренних аудитов организации силами сотрудников самой организации;

– сведения об инцидентах ИБ. В сведениях содержится информация об существующих инцидентах, а также как они были проработаны, как была скорректирована СЗИ для предотвращения аналогичных инцидентов;

– результаты проведения аудитов и самоконтроля ИБ. В результатах будет раскрыт вопрос эффективности и объективности проводимых мероприятий сотрудниками подразделения ИБ;

– данные об угрозах ИБ, возможных нарушителях ИБ и уязвимостях. Сведения определяют дальнейшую работу СУИБ, которую руководство может отслеживать;

– данные об изменениях внутри организации. В сведениях содержится вся информация о деятельности СУИБ в процессе жизненного цикла ИБ организации.

Для проведения анализа функционирования СУИБ, согласно [14] необходимы следующие мероприятия:

– анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению законодательства РФ и стандартов, договорным обязательствам организации;

– анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению и управлению ИБ, требованиям политики ИБ организации;

– оценку адекватности модели угроз ИБ организации существующим угрозам ИБ;

– оценку рисков в области ОИБ организации, включая оценку уровней остаточного и допустимого риска ИБ;

– проверку адекватности используемых мер ОИБ требованиям внутренних документов организации и результатам оценки рисков ИБ;

– анализ отсутствия разрывов в технологических процессах ОИБ, а также несогласованности в использовании защитных мер ИБ.

Для контроля и анализа деятельности СУИБ в организации руководство утверждается план мероприятий, в том числе совещаний на уровне руководства, на которых проводится анализ проблем ОИБ.

В целом по результатам анализа СУИБ со стороны руководства необходимо реализовать тактические или стратегические улучшения СУИБ [15].

К тактическим улучшениям СУИБ относят корректирующие или превентивные действия, связанные с пересмотром отдельных процессов СУИБ. Примеры решений по тактическим улучшениям, согласно [16]:

– пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;

– пересмотр процедур эксплуатации отдельных видов защитных мер;

– пересмотр процедур обнаружения и обработки инцидентов;

– уточнение описи информационных активов;

– пересмотр программы обучения и повышения осведомленности персонала;

– пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;

– пересмотр планов обработки рисков;

– вынесение санкций в отношении персонала;

– пересмотр процедур мониторинга ИБ и контроля защитных мер;

– пересмотр программ аудитов;

– корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;

– ввод новых или замена используемых защитных мер.

К стратегическим улучшениям СУИБ относят корректирующие или превентивные действия, связанные с пересмотром политик ИБ организации. Примеры решений по стратегическим улучшениям, согласно [16]:

– уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ организации БС РФ;

– изменение в области действия СОИБ;

– пересмотр моделей угроз и нарушителей;

– изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

После пересмотра и корректировки СУИБ целесообразно заново провести внешний аудит, который покажет результаты работы организации над СУИБ. Тем самым организация снова войдет на этап планирования цикла Деминга.

Заключение

Наиболее эффективной СУИБ станет при следовании циклу У.Э. Деминга (PDCA), который заключается в следующем: «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй». Следуя циклу Деминга, на всех этапах жизненного цикла СЗИ целесообразно проводить различные аудиты, которые в свою очередь покажут большую часть уязвимостей, которые организация сможет устранить. Безопасность как ЗО КИИ, так и объектов КИИ напрямую зависит от правильного построение СУИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Закон Российской Федерации "«О безопасности критической информационной инфраструктуры Российской Федерации». Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак." от 26.07.2017 N 187-ФЗ.

2. Постановление Правительства РФ "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения" от 08.02.2017 № 127.

3. Постановление Правительства РФ "Об утверждении Правил поставки газа в Российской Федерации" от 05.02.1998 N 162.

4. Приказ ФСТЭК России «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» от 06.12.2017 N 227.

5. Приказ ФСТЭК России "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" от 21.12.2017 N 235.

6. Приказ ФСТЭК России "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" от 25.12.2017 N 239.

7. Приказ ФСБ России "О Национальном координационном центре по компьютерным инцидентам" от 24.07.2018 N 366.

8. Приказ ФСБ России "Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения" от 24.07.2018 N 368.

9. Приказ ФСБ России "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты" от 06.05.2019 N 196.

10. Приказ ФСБ России "Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации" от 19.06.2019 N 281.

11. Приказ ФСБ России "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" от 19.06.2019 N 282.

12. Табакаева В. А., Карманов И. Н., Ан В. Р. Особенности интеллектуальных систем управления информационной безопасностью объектов критической информационной инфраструктуры [электронный ресурс] / Интерэкспо Гео-Сибирь. 2020. №2. URL: https://cyberleninka.ru/article/n/osobennosti-intellektualnyh-sistem-upravleniya-informatsionnoy-bezopasnostyu-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 11.04.2023).

13. ГОСТ Р ИСО 19011-2021 "Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента" от 11.05.2021.

14. Милославская Н.Г., Толстой А.И. Проверка деятельности по управлению информационной безопасностью: учеб. пособие для вузов, 220966 изд. Горячая линия - Телеком, 2022.

15. Кузнецов Д. Защита КИИ: от слов к делу [Электронный ресурс] // «Information Security/ Информационная безопасность: электрон. журн. 2019. N 3. URL: http://cs.groteck.ru/IB_3_2019/4/index.html (дата обращения: 31.03.2023).

16. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения" (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. N Р-399).

17. Кидяева С. М., Шабурова А. В., Селифанов В. В. Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры [Электронный ресурс]// Интерэкспо Гео-Сибирь. 2022. №. URL: https://cyberleninka.ru/article/n/voprosy-organizatsii-menedzhmenta-riskov-znachimyh-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 15.04.2023).

18. Ан В. Р. Табакаева В. А., Селифанов В. В. разработка критериев оценки соответствия требованиям безопасности на объекте информатизации // Интерэкспо Гео-Сибирь. 2021. №. URL: https://cyberleninka.ru/article/n/razrabotka-kriteriev-otsenki-sootvetstviya-trebovaniyam-bezopasnosti-na-obekte-informatizatsii (дата обращения: 21.04.2023).

19. Ан В.Р., Табакаева В.А., Селифанов В.В. разработка методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам критической информационной инфраструктуры, функционирующих на базе центров обработки данных // Интерэкспо Гео-Сибирь. 2020. №1. URL: https://cyberleninka.ru/article/n/razrabotka-metodiki-audita-kiberbezopasnosti-gosudarstvennyh-informatsionnyh-sistem-otnosyaschihsya-k-znachimym-obektam (дата обращения: 11.04.2023).