УДК 004.056
DOI 10.33764/2618-981X-2022-6-82-87

Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры

С. М. Кидяева[1], А. В. Шабурова[1], В. В. Селифанов[2]*
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] АО «ИнфоТеКС»
* e-mail: kidyaeva.s@yandex.ru

Аннотация. В условиях увеличения количества атак, связанных с информационной безопасностью, предприятиям необходимо пересмотреть принципы менеджмента рисков для поддержания актуальности и увеличения надежности системы менеджмента информационной безопасности. В статье рассмотрены актуальные вопросы менеджмента рисков значимых объектов критической информационной инфраструктуры. Проанализированы международные стандарты по информационной безопасности ГОСТ Р ИСО/МЭК27001-2021, ГОСТ Р ИСО/МЭК 27005-2010 и требования Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В частности, проанализированы правила категорирования объектов критической информационной инфраструктуры, утвержденные Постановлением Правительства от 8 февраля 2018 г. «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» относительно менеджмента рисков информационной безопасности. Представлена сравнительная таблица процесса менеджмента рисков организации, имеющей значимые объекты критической информационной инфраструктуры, и процесса категорирования объектов критической информационной инфраструктуры. Разработаны рекомендаций поддержания актуальности менеджмента рисков субъектов критической информационной инфраструктуры.

Ключевые слова: менеджмент рисков, критическая информационная инфраструктура, информационная безопасность

Issues of formation of risk management of significant objects of critical information infrastructure

S. M. Kidyaeva[1], A. V. Shaburova[1], V. V. Selifanov[2]*
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] JSC «InfoTeCS»
* e-mail: kidyaeva.s@yandex.ru

Abstract. With the increasing number of attacks related to information security, enterprises need to review the principles of risk management, to maintain the relevance and increase the reliability of information security management system. The article considers topical issues of risk management of significant objects of critical information infrastructure. International standards on information security ISO/IEC27001-2021, ISO/IEC 27005-2010 and requirements of the Federal Law of July 26, 2017. № 187-FL "On the security of critical information infrastructure of the Russian Federation". In particular, the rules of categorization of critical information infrastructure objects approved by the Government Decree of February 8, 2018. № 127 «On approving the rules of categorizing objects of

critical information infrastructure of the Russian Federation, as well as the list of indicators of criteria for the significance objects of critical information infrastructure of the Russian Federation and their values were analyzed» regarding information security risk management are analyzed. A comparative table of the risk management process for an organization that has significant critical information infrastructure facilities and the categorization process for critical information infrastructure facilities is presenting. Developed recommendations for maintaining the relevance of risk management of critical information infrastructure entities.

Keywords: risk management, critical information infrastructure, information security

Введение

В современных условиях ресурсы государства и бизнеса Российской Федерации активно подвергаются кибератакам, что может негативно отразиться на функционировании бизнеса, конкурентоспособности, имидже и финансовом состоянии организации [1]. По данным лаборатории Касперского в первом квартале 2022 г. эксперты расследовали в 4 раза больше инцидентов, связанных со сложными кибератаками на бизнес в России, чем за аналогичный период 2021 г. Также ситуацию осложняет приостановка деятельности ряда иностранных компаний в России, что выводит из строя существующие средства защиты информации [2].

Исходя из этого, информационная безопасность (далее – ИБ) организации должна обеспечивать такую защиту, при которой злоумышленник не сможет нанести неприемлемый ущерб. Для предотвращения такого ущерба и минимизации рисков для государства и населения страны усиливаются меры, определенные нормативно-правовыми актами Российской Федерации, регулирующими информационную безопасность [3].

Риск ИБ – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [4].

Учитывая направленность целевых компьютерных атак [5], основные типы организаций и сферы их деятельности, подверженные рискам, можно сопоставить с определением субъекта критической информационной инфраструктуры (далее – КИИ) [6].

Проанализировав научные статьи и материалы открытых источников, установлено, что вопрос рассмотрения менеджмента рисков информационной безопасности для значимых объектов КИИ изучен недостаточно. Поэтому цель настоящей статьи заключается в рассмотрении применимости принципов менеджмента рисков международного стандарта [4] относительно законодательства Российской Федерации, обеспечивающего безопасность значимых объектов КИИ, а также в выявлении основных возможных рисков информационной безопасности рисков субъектов КИИ и выработке рекомендаций поддержания актуальности рисков для таких субъектов.

Методика

Применимость менеджмента рисков относительно значимых объектов КИИ характеризуется процессами присвоения категории значимости объекту КИИ. В связи с этим необходимо определить, что является рисками для таких объектов и сопоставить правила категорирования [7] с международным стандартом ГОСТ Р ИСО/МЭК 27005-2010 [4].

Каждый новый нормативно-правовой акт, касающийся деятельности организации, способствует увеличению рисков для нее. В связи с этим для определения актуальных рисков информационной безопасности, связанных с КИИ, предлагается рассматривать их путем анализа нормативно-правовых документов, учитывая их стремительное совершенствование. На основе анализа применимости документов и рассмотрения их в части менеджмента рисков информационной безопасности можно составить рекомендации по поддержанию актуальности рисков информационной безопасности субъекта КИИ.

Обсуждение

В рамках категорирования определяется потенциальный ущерб, который может быть нанесен из-за прекращения или частичного нарушения функционирования объекта КИИ [7] [8], влияющий на степень категории значимости. Ущерб является ключевым параметром для оценки рисков [9]. Сопоставим процесс категорирования объектов КИИ относительно менеджмента рисков информационной безопасности (табл. 1).

Таблица 1

Соотношение процессов менеджмента риска информационной безопасности и категорирования объектов КИИ

№	Процесс менеджмента риска ИБ	Процесс категорирования объектов КИИ
1	Установление контекста	Определение процессов, необходимых для функционирования организации
		Выявление из них критических процессов
		Выявление объектов, обрабатывающих информацию критических процессов
2	Оценка риска	Рассмотрение возможных действий нарушителей в отношении объектов КИИ
		Анализ угроз ИБ, которые могут привести к возникновению компьютерных инцидентов (банк данных угроз ФСТЭК России)
		Оценка возможных последствий в случае возникновения компьютерных инцидентов
3	Реализация плана обработки риска	Присвоение каждому из объектов КИИ одной из категорий значимости либо принятие решение об отсутствии необходимости присвоения им категорий значимости.
4	Проведение непрерывного мониторинга и переоценки рисков	Актуализация сведений в случае изменения сведений об объекте, сведений о субъекте, сведения о взаимодействии объекта КИИ и сетей электросвязи, сведения о лице, эксплуатирующем объект, сведения о программных и программно-аппаратных средствах, используемых на объекте, сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта
5	Поддержка и усовершенствование процесса менеджмента риска ИБ	Пересмотр не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости объектов КИИ или их значений

При рассмотрении менеджмента рисков относительно конкретного объекта [10] необходимо учитывать формирующиеся мировые тенденции, такие как новые формы работы, автоматизация всех процессов, научно-технический прогресс [11], внедрение искусственного интеллекта, использование облачных решений и биометрических технологий. Исходя из вышеперечисленного, совершенствование процесса менеджмента рисков, в соответствии с табл. 1, рассматривается крайне редко, что может привести к неактуальности рисков и нанесению ущерба организации. Отсутствие актуальных рисков приводит к неактуальности модели нарушителя [12], а также самой системы безопасности организации.

Правилами категорирования [13] не определены конкретизирующие сроки пересмотра влияющих факторов на систему менеджмента информационной безопасности. Для поддержания актуальности системы защиты вопросы обеспечения важна цикличность рассмотрения [14]. Учитывая постоянно растущие угрозы, предлагается ежеквартально пересматривать риски информационной безопасности.

Основной целью Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ № 187) является устойчивое функционирование КИИ, при проведении в отношении ее компьютерных атак [6]. Компьютерные атаки могут быть осуществлены через информационную инфраструктуру организации, состоящую из объектов КИИ. Правила категорирования объектов КИИ [7] определяют приемлемость рисков и их последствия. В случае возникновения инцидента субъект несет риски, не только связанные с репутационными, финансовыми и производственными мощностями, но и может повлечь за собой административную [15] или уголовную ответственность [16].

На основании анализа документов, регулирующих информационную безопасность субъектов КИИ, определены следующие риски информационной безопасности для значимых объектов КИИ:

– риск возникновения инцидента;

– прекращение функционирования объектов КИИ;

– риски, связанные с регуляторами, определенными ФЗ № 187 [6];

– риски импортозамещения [17];

– финансовые потери [18];

– снижение репутации;

– административной или уголовной ответственности [15] [16].

Проанализировав процесс менеджмент рисков и процесс категорирования объектов КИИ, были выявлены недостатки процесса категорирования, а именно отсутствие периодичного пересмотра рисков ИБ, характерных для субъекта КИИ, позволяющих поддерживать менеджмент рисков в актуальном состоянии. В связи с этим даны следующие рекомендации поддержания актуальности рисков информационной безопасности:

– мониторинг влияния издаваемых нормативно-правовых документов;

– рассмотрение рисков, связанных с мировым прогрессом и обстановкой;

– пересмотр подхода рассмотрения рисков;

– ежеквартальный пересмотр рисков.

Использование представленных рекомендаций позволит обеспечить поддержание актуальности системы информационной безопасности в соответствии с изменениями внешних и внутренних факторов. Организациям, имеющим значимые объекты КИИ, в целях предотвращения ущерба внедрение менеджмента рисков позволит обеспечить стабильность и повысить безопасность системы информационной безопасности в критических условиях, тем самым, минимизировать расходы на информационную безопасность и финансовые потери.

Заключение

Рассмотрен менеджмент рисков информационной безопасности значимых объектов КИИ путем сопоставления процессов менеджмента рисков информационной безопасности относительно национального стандарта ГОСТ Р ИСО/МЭК 27005-2010 [4], и категорирования объектов КИИ [7]. При анализе выявлено, что периодичность пересмотра менеджмента рисков категорирования не соответствует поддержанию его в актуальности. Для определения актуальных рисков проанализированы мировые тенденции и направления развития информационной безопасности Российской Федерации. Исходя из этого выявлены основные направления рисков информационной безопасности субъектов КИИ и разработаны рекомендации поддержания актуальности менеджмента рисков субъекта КИИ, имеющего значимые объекты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ершов А. Ю. Актуальные вопросы системы менеджмента информационной безопасности // Современная наука: актуальные проблемы и пути их решения. – 2015. – № 8(21). – С. 63-66.

2. Количество сложных кибератак на бизнес в России увеличилось в 4 раза. – Текст: электронный // ixbt: [сайт]. – URL:https://www.ixbt.com/news/2022/03/25/kolichestvo-slozhnyh-kiberatak-na-biznes-v-rossii-uvelichilos-v-4-raza.amp.html.

3. Целевые кибератаки: что это, как работает и как с ними бороться. – Текст: электронный // securitylab: [сайт]. URL: https://www.securitylab.ru/blog/company/orange/349271.php.

4. ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

5. Таргетированные или целевые атаки. – Текст: электронный// tadviser: [сайт]. URL:https://www.tadviser.ru/index.php.

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

7. Постановление 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 Российской Федерации и их значений».

8. Постановление Правительства Российской Федерации от 24 декабря 2021 г. № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации».

9. Оценка рисков при построении защиты объектов критической информационной инфраструктуры. – Текст: электронный// safe-surf: [сайт]. – URL: https://safe-surf.ru/specialists/article/5287/666251/.

10. Дорофеев А. В. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. – 2014. – № 1(2).

11. Бердюгин А. А. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации) // Финансы: теория и практика. – 2020. – Т. 24. – № 6. – С. 51-60.

12. Куркин А. В. Оценка рисков информационной безопасности с применением нечеткого моделирования// Неделя науки Санкт-Петербургского государственного морского технического университета. – 2020. – Т. 2. – № 4. – С. 45.

13. Тимиргалеева Р. Р. Влияние системы менеджмента качества на моделирование бизнес-процессов обеспечения информационной безопасности и непрерывности бизнеса // Лучшая научная статья 2017 : сборник статей XII Международного научно-практического конкурса, Пенза, 30 октября 2017 года. –2017. – С. 65-68.

14. Макеев А. С. Менеджмент рисков информационной безопасности как непрерывный процесс// Молодой ученый. – 2016. – № 10(114). – С. 62-66.

15. Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

16. Федерального закона № 194-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

17. Указ Президента от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

18. Васильев С. Д. Разработка политики информационной безопасности// Инновации. Наука. Образование. – 2020. – № 24. – С. 1598-1604.