УДК 004.056.53
DOI 10.33764/2618-981X-2023-6-3-10

В. Е. Антипов[1], В. В. Селифанов[1]*

Разработка рекомендаций по улучшению систем управления информационной безопасностью для критической информационной инфраструктуры

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

Аннотация. В статье поднимается вопрос о методах внедрения систем управления информационной безопасностью (СУИБ) на значимых объектах критической информационной инфраструктуры (КИИ) с учетом специфики таких объектов. Рассматриваются способы таких реализации в соответствии с актуальной на сегодняшний день нормативной правовой документацией в области КИИ и СУИБ. В процессе анализа, предлагается переработанный подход к оценке рисков и разработка рекомендаций по улучшению действующей СУИБ с применением этого подхода. Также представлены результаты применения и реализации разработанных рекомендаций. Результаты состоят в том, что примененные рекомендации по улучшению СУИБ в организации, являющейся субъектом КИИ, позволили повысить качество и надежность СУИБ, снизить вероятность рисков и сократить время реагирования на инциденты информационной безопасности.

Ключевые слова: критическая информационная инфраструктура, система управления информационной безопасностью, управление рисками

V. E. Antipov[1], V. V. Selifanov[1]*

Development of Recommendations for Improving Information Security Management Systems for Critical Information Infrastructure

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

Abstract. The article raises the question of methods of implementing information security management systems (ISMS) on significant objects of critical information infrastructure (CII), taking into account the specifics of such objects. The methods of such implementation are considered in accordance with the current regulatory legal documentation in the field of CII and ISMS. In the process of analysis, a revised approach to risk assessment and the development of recommendations for improving the current ISMS using this approach are proposed. The results of the application and implementation of the developed recommendations are also presented. The results are that the applied recommendations for improving the ISMS in the organization that is the object of the CII allowed to improve the quality and reliability of the ISMS, reduce the likelihood of risks and reduce the response time to information security incidents.

Keywords: critical information infrastructure, information security management system, risk management

Введение

Каждая система, внедряемая в жизненный цикл организации, должна служить интересам организации и не препятствовать существующим бизнес-процессам, а создавать более благоприятную среду для их функционирования. Другими словами, любая система должна внедряться в существующие процессы компании с целью их оптимизации. В случае же, если нарушение процессов несет за собой возможный критический ущерб не только для самой организации, но и для каких-либо сфер государства, то это правило становится абсолютно бескомпромиссным. Значимые объекты критической информационной инфраструктуры Российской Федерации (далее – ЗО КИИ) как раз имеют в своем распоряжении подобные процессы, а значит и внедряемые в них системы должны преследовать конкретные цели. Система безопасности любого объекта состоит из комплекса принятых мер, позволяющих контролировать и противодействовать возможным возникающим рискам физической, экономической и информационной безопасности [1]. Чтобы управлять всем комплексом мероприятий, направленных на обеспечение безопасности в организации, создается специальное подразделение, назначаются ответственные, разрабатывается документация и т.д. Одним из важнейших аспектов обеспечения безопасности любой организации является внедрение системы управления информационной безопасностью (далее – СУИБ). СУИБ имеет в своем составе набор процедур и методов, используемых для обеспечения защиты информации от несанкционированного доступа. Учитывая специфику ЗО КИИ и требуемый к ним уровень обеспечения защиты информации, СУИБ для таких объектов должна базироваться на более специфичных подходах, нежели классических. А для более эффективного функционирования процесс внедрения СУИБ должен предполагать наличие четких и логичных требований. Целью данной статьи является разработка рекомендаций по улучшению СУИБ для ЗО КИИ и реализация разработанных рекомендаций на практике.

Методы и материалы

Для достижения поставленной цели были изучены и проанализированы национальные стандарты семейства СМИБ: ИСО/МЭК 27000 [2], ИСО/МЭК 27001 [3], ИСО/МЭК 27002 [4], ИСО/МЭК 27005 [5] и руководства по их применению, а также Постановление Правительства РФ № 127 [6] (далее – ПП № 127) и Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [7] (далее – Приказ № 239). Основой для разработок являлись не только нормативная правовая документация, но и публикации в разрезе тем, связанных с менеджментом информационной безопасности. Оценка и анализ функционирующей СУИБ проводились в действующей организации, являющейся субъектом КИИ.

Обсуждение

Система безопасности любого объекта состоит из комплекса принятых мер, позволяющих контролировать и противодействовать возможным возникающим рискам физической, экономической и информационной безопасности. Чтобы

управлять всем комплексом мероприятий, направленных на обеспечение безопасности в организации, обязательным решением следует принять внедрение СУИБ. Система управления имеет в своем составе набор процедур и методов, используемых для обеспечения защиты информации от несанкционированного доступа. В задачи СУИБ входит создание специального подразделения, назначение ответственных, разработка различного рода документации и пр. [8]. Говоря в разрезе организаций, являющихся субъектами КИИ, процесс внедрения СУИБ является обязательным шагом для обеспечения целостной безопасности объектов такой организации.

К сожалению, в настоящее время ни один нормативный правовой документ не объясняет в полной мере как реализовывать подобные системы на ЗО КИИ. Рассматривая ПП № 127 [6] в данном контексте, приходим к выводу о необходимость системного подхода к оценке рисков, который включает в себя анализ угроз и уязвимостей, оценку последствий возможных атак, а также определение рисков и мер по их снижению до приемлемого уровня. Иначе говоря, при категорировании ЗО КИИ по ПП № 127 [6] будет проведена работа с неприемлемыми рисками, а как оценивать остальные риски и выстраивать под них защиту не сказано. Данный подход недостаточен для ЗО КИИ, так как в случае таких объектов мало обеспечить безопасность только с технической стороны, необходимо действовать комплексно.

Открывая Приказ № 239 [7], наблюдается отсутствие в нем описания полной реализации СУИБ на объектах КИИ. Однако, данный приказ предписывает реализовать некоторые мероприятия по обеспечению безопасности в ходе эксплуатации значимого объекта субъектом КИИ. В состав этих мероприятий входят:

– планирование мероприятий по обеспечению безопасности ЗО КИИ;

– анализ угроз безопасности информации на ЗО КИИ и последствий от их реализации;

– управление (администрирование) подсистемой безопасности ЗО КИИ;

– управление конфигурацией ЗО КИИ и его подсистемой безопасности;

– реагирование на компьютерные инциденты в ходе эксплуатации ЗО КИИ;

– обеспечение действий в нештатных ситуациях в ходе эксплуатации ЗО КИИ;

– информирование и обучение персонала, работающего на ЗО КИИ;

– контроль за обеспечением безопасности ЗО КИИ.

На данном этапе, логичным будет обратиться к ГОСТ 27001 [3] и ГОСТ 27002 [4], так как первый определяет требования к разработке и внедрению мер для системы менеджмента информационной безопасности, а второй представляет перечень общепринятых мер обеспечения информационной безопасности и рекомендации по их внедрению. В совокупности эти два стандарта должны помочь реализовать требуемые мероприятия из Приказа №239 [7] и реализовать все необходимые меры для покрытия неприемлемых рисков, которые в свою очередь выявляются при категорировании ЗО КИИ [9] в соответствии с ПП № 127 [6]. Однако, говоря о КИИ мы приходим к выводу о том, что не можем

использовать в отношении оценки рисков стандарты ИСО/МЭК 27001 [2] и ИСО/МЭК 27002 [3] из-за разного подхода к рискам. Критические объекты информационной инфраструктуры с точки зрения безопасности имеют определенную специфику. Из определения значимого критического объекта вытекает отсутствие конструктивного механизма исчисления ущерба от инцидентов информационной безопасности, хотя категория ущерба в этом случае существенно шире множества субъектов управления безопасностью. Когда речь идет о значимом критическом объекте, нет оснований для определения уровня допустимого остаточного риска, так что это понятие становится несущественным. Ранее владельцы информационных активов принимали остаточный риск, но теперь его роль утрачивается. Традиционный метод управления, который использует уровень остаточного риска в качестве критерия для управления безопасностью, теперь уже неприменим.

Стоит упомянуть также и о не менее важном аспекте управления информационной безопасностью – моделировании угроз. Процесс моделирования угроз безопасности позволяет определить угрозы, их свойства и особенности, исходя из определенного набора агрессивных факторов. При моделировании учитываются облик, намерения и потенциал злоумышленника, векторы и сценарии возможных атак, а также информационные активы, которые могут быть наиболее уязвимыми. Моделирование угроз несомненно является неотъемлемой частью СУИБ и представляет собой процессно-циклическую деятельность. В различии подходов к моделированию угроз, нельзя однозначно сказать, что один подход «лучший» или «единственно правильный». Каждый из существующих подходов имеет слабые и сильные стороны, и для достижения максимальной эффективности необходимо комбинировать различные альтернативы. Методология совместной функциональной оценки угроз и концепция использования такой оценки базируется на известной модели Клементса-Хоффмана [10], которая строится, исходя из правила, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути воздействия злоумышленника на информационную систему. Для описания такой защиты информации рассматриваются три множества: множества угроз, множества объектов защиты и множество механизмов защиты. Элементы множеств угроз и защиты находятся в отношениях «угроза – объект». Угроза в данном случае соотносится с сущностью «объект». Каждая угроза может распространяться на любое число объектов, а объект в свою очередь может быть уязвим со стороны более чем одной угрозы. Цель такой методики состоит в том, чтобы множество механизмов защиты перекрывала множество объектов защиты от множества возможных угроз. Такая модель определяет основные векторы развития моделирования угроз несмотря на то, что добиться полного перекрытия всех смоделированных угроз практически невозможно.

Обратимся к стандартам 27000 [2] и 27005 [5], и на их основе выведем переработанные и адаптированные под КИИ требования, и методы взаимодействия с рисками информационной безопасности в рамках СУИБ. ГОСТ 27000 [2] предлагает нам следующую схему работы с рисками: оценка рисков – выбор подхода

к обработке рисков – выбор и реализация мер по снижению рисков до приемлемого уровня. Предлагаемая схема будет изменена в части реализации мер, а именно планируется исключить понятие приемлемого уровня как такового. И как итог, особенностями предлагаемого переработанного метода будут являться:

– многоуровневый подход. В рамках данного подхода выделяются несколько уровней управления рисками: стратегический, тактический и оперативный. Каждый из этих уровней имеет свои задачи, функции и методы работы с рисками;

– интеграция с процессами управления. Работа с рисками должна быть тесно интегрирована с процессами управления информационной безопасностью в целом. Это позволяет более эффективно управлять рисками, так как предполагается рассматривать их не отдельно от других процессов, а в контексте общей стратегии управления безопасностью;

– анализ контекста. Особое внимание стоит уделить анализу контекста, в котором функционирует ЗО КИИ. Это позволит определить специфические риски и угрозы, свойственные данному контексту, и разработать наиболее эффективные меры по их управлению;

– ориентированность на результат. Основное внимание уделяется не процессам, а результатам работы с рисками. Это позволяет более эффективно выявлять и управлять рисками на ЗО КИИ.

Этапы по внедрению данного подхода в организацию будут следующими:

1) идентификация уязвимостей объекта критической информационной инфраструктуры;
2) оценка уровня риска, связанного с этими уязвимостями;
3) выбор мер по управлению рисками на основе анализа результатов оценки рисков;
4) реализация выбранных мер управления рисками;
5) оценка эффективности реализованных мер по управлению рисками и необходимости их корректировки.

Как уже было сказано ранее, такой подход базируется не на методе остаточного риска, используемого в качестве критерия для управления процессами безопасности, а на осознании бесконечной вероятности возникновения инцидента, что влечет за собой возможность постоянного снижения этой вероятности путем расширения перечня защитных мер.

В ходе собственного проведенного в рамках работы анализа функционирующей СУИБ в одной из организаций, являющейся субъектом КИИ, было выявлено, что анализируемая система не соответствуют требованиям ГОСТ 27001 [3] и ГОСТ 27002 [4]. Анализ показал разногласия между работой СУИБ в организации и требованиями указанных стандартов, а также отсутствие реализации некоторых позиций из этих требований. Несоответствия были связаны с отсутствием политик безопасности, недостаточной оценки рисков, отсутствием контроля над изменениями, недостаточным мониторингом и анализом событий. Результаты анализы достаточно предсказуемы, потому что, как уже говорилось,

настоящие нормативные правовые документы не позволяют проводить полноценную оценку рисков, а сложность структуры КИИ и малое количество методических материалов не позволяют внедрить и развернуть полноценную СУИБ. И как следствие допускаемое организациями пренебрежение полноценным обеспечением защиты ЗО КИИ, на наш взгляд, недопустимо.

На основе анализа и выявленных несоответствий были разработаны следующие рекомендации по улучшению СУИБ на ЗО КИИ с использованием, разработанного в рамках работы подхода к управлению рисками:

– разработать политику безопасности, которая будет описывать требования и правила по обеспечению безопасности информации в организации;

– проводить периодичную оценку рисков, по итогам которой разработать соответствующие меры по управлению рисками;

– усовершенствовать или внедрить процедуры управления доступом сотрудников к информационным ресурсам организации;

– разработать систему контроля над изменениями в информационных ресурсах;

– усовершенствовать мониторинг событий, а также анализ инцидентов информационной безопасности.

По итогам внедрения и реализации в вышеупомянутой организации, являющейся субъектом КИИ, разработанных рекомендаций, сотрудниками этой организации была проведена проверка эффективности СУИБ, спустя шесть месяцев после внедрения. Проверка, по итогам которой был составлен отчет показала, что следование разработанным рекомендациям действительно повысило качество и надежность СУИБ в организации. Итоговый отчет содержал в себе следующие результаты:

– разработка политики безопасности привела к увеличению осведомленности сотрудников об информационной безопасности и улучшению процедур по ее обеспечению;

– снижение рисков, связанных с обработкой и хранением конфиденциальной информации, благодаря внедрению соответствующих мер по управлению рисками и использования нового подхода;

– уменьшение вероятности несанкционированного доступа к информационным ресурсам организации после улучшения процедур управления доступом;

– уменьшение времени реакции на инциденты информационной безопасности на 10%, а также повышение качества их решения.

Заключение

В качестве заключения можно отметить, что СУИБ для критической информационной инфраструктуры является крайне важным элементом обеспечения безопасности и стабильности функционирования таких объектов. При этом реализация данной системы требует учета специфики работы критической информационной инфраструктуры. Правильная реализация СУИБ позволяет минимизировать возможность инцидентов, а в случае их возникновения – оперативно

реагировать и устранять их последствия. При внедрении СУИБ на ЗО КИИ, необходимо использовать подходы учитывающие особенности таких объектов, и отказаться от стандартных методов по управлению и оценке рисков, чтобы достичь максимально эффективного результата в обеспечении безопасности инфраструктуры. Также не следует забывать, что КИИ нуждается не только в информационной безопасности, но и в безопасности со всех других сторон многогранной структуры, которые могут быть подвержены атаке злоумышленников и нарушению своей целостности и доступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью / А. Г. Серова. – Текст : электронный // Социально-экономические и естественно-научные парадигмы современности : [материалы XIII Всероссийской научно-практической конференции]. – 2018. – С. 829–837 (дата обращения: 20.03.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

2. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология = Information technology. Security techniques. Information security management systems. Overview and vocabulary : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 813-ст : введен впервые : дата введения 2013-12-01 / подготовлен Федеральным бюджетным учреждением "Консультационно-внедренческая фирма в области международной стандартизации и сертификации. – Москва : Стандартинформ, 2019. – Текст : непосредственный.

3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования = Information technology. Security techniques. Information security management systems. Requirements : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст: взамен ГОСТ Р ИСО/МЭК 27001-2006 : дата введения 2022-01-01 / подготовлен Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Открытым акционерным обществом "Информационные технологии и коммуникационные системы" (ОАО "ИнфоТеКС") и Федеральным автономным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФАУ "ГНИИИ ПТЗИ ФСТЭК России"). – Москва : Стандартинформ, 2022. – Текст : непосредственный.

4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норма и правил менеджмента информационной безопасности = Information technology. Security techniques. Code of practice for information security management : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст: взамен ГОСТ Р ИСО/МЭК 17799-2005 : дата введения 2014-01-01 / подготовлен Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл") и Обществом с ограниченной ответственностью "Информационный аналитический вычислительный центр" (ООО "ИАВЦ"). – Москва : Стандартинформ, 2019. – Текст : непосредственный.

5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности = Information technol-

ogy. Security techniques. Information security risk management : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст: взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007 : дата введения 2011-12-01 / подготовлен Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл"), Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России"). – Москва : Стандартинформ, 2019. – Текст : непосредственный.

6. Российская Федерация: Постановления Правительства. 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 : Постановление Правительства № 127 : [утвержден Правительством Российской Федерации 8 февраля 2018 г.] – Москва : Стандартинформ, 2022. – Текст : непосредственный.

7. ФСТЭК России : Приказ ФСТЭК России от 25 декабря 2017 г. N 239. – Текст : электронный. – 2021. – URL: https://fstec.ru/ (дата обращения: 15.04.21) – Режим доступа: официальный сайт ФСТЭК России.

8. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799) / Н. В. Андреева. – Текст : электронный // Научно-технический вестник Санкт–Петербургского государственного университета информационных технологий, механики и оптики. – 2007. – С. 40–44 (дата обращения: 06.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

9. Внедрение международного стандарта ИСО/МЭК 27001 – основа управления информационной безопасностью предприятия / А. А. Кайсарова, А. К. Тулекбаева, А. А. Токтабек. – Текст : электронный // Вестник науки Южного Казахстана. – 2018. – № 4(4). – С. 103–106 (дата обращения: 10.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

10. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк. – Текст : электронный // Экономика и качество систем связи. – 2017. – С. 42–48 (дата обращения: 19.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.