УДК 004.056.53
DOI 10.33764/2618-981X-2022-6-3-8

Проблемы формализации процессов систем управления информационной безопасностью

В. Е. Антипов[1]*, *В. В. Селифанов*[1]

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

* e-mail: vvv-antipov@mail.ru

Аннотация. В данной статье поднимается проблема формализации процессов в системе управления информационной безопасностью. Рассматривается вопрос о необходимости и важности этапа формализации процессов, изучение и анализ национальных и международных стандартов. В процессе работы были проанализированы подходы к разработке системы управления информационной безопасностью, а также национальные стандарты ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27002-2012 и ГОСТ Р ИСО/МЭК 27005-2010, которые являются основными при создании системы управления информационной безопасностью (СУИБ) и подходов к оценке ее рисков. Учитывая положения национальных стандартов, а также изучив разные подходы к разработке СУИБ, в данной статье были сформированы практические рекомендации для формализации процессов СУИБ. Все рекомендации направлены на обеспечение безопасности сотрудников и организации, при реализации процессов формализации для соответствующей системы управления информационной безопасностью. Также на примере одной меры безопасности из стандарта ИСО/МЭК 27001 представлен одни из способов реализации политики, относительно формализации затрагивающих процессов представленной меры.

Ключевые слова: формализация, процессы, меры безопасности, политика безопасности.

Problems of formalization of ISMS processes

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

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

* e-mail: vvv-antipov@mail.ru

Abstract. This article raises the problem of formalization of processes in the information security management system. The question of the necessity and importance of the stage of formalization of processes, the study and analysis of national and international standards is considered. In the course of the work, approaches to the development of an information security management system were analyzed, as well as national standards ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27002-2012 and ГОСТ Р ИСО/МЭК 27005-2010, which are the main ones when creating an information security management system (ISMS) and approaches to assessing its risks. Taking into account the provisions of national standards, as well as having studied different approaches to the development of ISMS, practical recommendations for the formalization of ISMS processes have been formed in this article. All recommendations are aimed at ensuring the safety of employees and the organization, while implementing formalization processes for the appropriate information security management system. Also, using the example of one security measure from the ISO/IEC 27001 standard, one of the ways to implement the policy regarding the formalization of the processes affecting the presented measure is presented.

Keywords: formalization, processes, security measures, security policy

Введение

В современном мире любая из существующих организаций так или иначе использует IT-технологии. Данные, обрабатываемые в информационных системах, зачастую являются самой ценной и защищаемой информацией компании. Потеря или повреждение таких данных неотвратимо приведет к ущербу для компании или вовсе поставит под вопрос дальнейшее ее существование.

Подобные риски вынуждают выстраивать в организации эффективную систему защиты информации [1, 2, 3]. Комплексный подход, включающий в себя как технические, так и организационные меры, несомненно, является лучшим из подходов к обеспечению системы защиты информации [4]. Но построить эффективно работающую систему [3] – мало, ею нужно грамотно управлять.

Путей достижения грамотного управления всего два: либо опираться на свой личный опыт управления информационной безопасностью (ИБ) и самостоятельную разработку подхода к нему, либо использовать мировые практики, показавшие лучший результат в этой области. Отсюда напрашивается вопрос, почему нет единой универсальной модели построения СУИБ [5, 6] и почему формализация этого процесса вызывает столько сложностей [7]?

Целью данной статьи является анализ подходов к созданию СУИБ и разработка рекомендаций, направленных на сокращение проблем формализации процессов СУИБ.

Методы и материалы

Под формализацией процессов понимается действия направленные на устранение хаотичности в деятельности как компании в целом, так и каждого сотрудника в отдельности [8]. В данной статье были проанализированы стандарты, связанные с СУИБ. Первым был проанализирован ГОСТ Р ИСО/МЭК 27001-2006 [5] – национальный стандарт РФ, гармонизированный с международным стандартом ИСО/МЭК 27001:2005 [5], устанавливающий требования к системе управления информационной безопасностью для организации защиты информационных ресурсов, целью которой является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и формирующих доверие заинтересованных сторон [1, 2, 10]. Данный стандарт является основным при рассмотрении СУИБ и служит ориентиром для анализа одного из подходов к созданию СУИБ. Вспомогательным стандартом служил ГОСТ Р ИСО/МЭК 27002-2012 [6] – национальный стандарт РФ, идентичный международному стандарту ИСО/МЭК 27002:2005 [6], предлагающий основные принципы и рекомендации по менеджменту информационной безопасности [6, 1, 2, 10]. Еще один немаловажный стандарт, который был использован для анализа, – это ГОСТ Р ИСО/МЭК 27005-2010 [7] – национальный стандарт РФ, идентичный международному стандарту ИСО/МЭК 27005:2008 [7] и являющийся руководством по менеджменту рисков информационной безопасности [7, 1, 2, 10]. Так как риски являются важнейшим элементом для любой системы безопасности, то руководствующие правила этого стандарта также попали в список анализируемой документации.

Обсуждение

Как было уже сказано, путей для построения грамотной СУИБ всего два [5, 6]. Рассматривая способ управления системой защиты информации на основе собственной разработки и личного опыта, необходимо привлечь к этому экспертов высокого уровня компетентности, ведь от их уровня будет зависеть эффективность этой системы в будущем. Каждый из этих сотрудников будет ориентироваться на свой личный опыт и в совокупности с другими такой подход даст достаточно качественную видимость системы управления, которую в дальнейшем останется лишь реализовать, учитывая все риски. Не смотря на, казалось бы, столь индивидуальный подход, эксперты группы по разработке СУИБ, несомненно, будут частично опираться в своих действиях на второй путь построения системы управления, т.е. использовать мировую практику.

Второй путь предполагает использование международного стандарта ИСО/МЭК 27001 [5], который в полной мере описывает управление ИБ. Стандарт описывает эффективные подходы к мониторингу, внедрению, анализу, разработке и прочим этапам создания системы управления ИБ [10]. Ключевой идеей СУИБ является построение системы на основе оценки рисков ИБ. Но без индивидуального видения специалиста такая система может получиться отнюдь не той, которая полностью удовлетворяет потребности организации и ее процессов, а также соответствует поставленным задачам. Отсюда можно сделать вывод, что первый путь построения системы управления ИБ отчасти поглощает второй.

Формализация процессов в компании проводится в рамках области деятельности СУИБ [7]. Этап формализации необходимо проводить для устранения хаотичности в деятельности всей компании и каждого сотрудника в отдельности. Грамотная реализация данного этапа может значительно упростить и ускорить работоспособность и функциональность организации, а также снизить вероятность возникновения рисков и угроз ИБ. При любом инциденте или при проверке одним из регулирующих органов всегда будет понятно, кто должен отвечать за конкретный набор задач, будь то сотрудник или целый отдел [9].

Этап формализации должен включать в себя проведение следующих работ [7]:

– подробное описание процессов организации, всевозможные перемещения информации и данных компании между подразделениями и между ответственными лицами;

– интервьюирование ответственных за те или иные процессы сотрудников с целью получения более полной информации о разных областях деятельности, их механизмов управления и контроля;

– формирование и выдача операционных инструкций в рамках описанных процессов области деятельности системы управления ИБ.

Описание процессов вполне может осуществляться параллельно с проведением анализа рисков и разработкой соответствующей документации. Отличным результатом всех этих работ будет являться готовый документ, имеющий полное описание карты процессов в рамках области деятельности СУИБ [5, 6] и который будет отвечать всем требованиям стандарта ИСО/МЭК 27001. Помимо вышеука-

занных работ необходимым будет выделить технические аспекты для дальнейшей первоочередной реализации. К таким аспектам можно отнести: сбор журналов аудита, инвентаризацию активов, защищенную настройку операционной системы (ОС), а также применение систем мониторинга событий ИБ SIEM, платформ IRP и SOAR.

В настоящее время наиболее критичными и защищаемыми системами Российской Федерации являются значимые объекты критической информационной инфраструктуры, поэтому в первую очередь стоит упомянуть формализацию процессов СУИБ именно в них. Самое главное в системе значимого объекта критической информационной инфраструктуры (ЗО КИИ) – это вовремя обнаружить проблему и предотвратить ее, прежде чем она повлечет за собой какие-либо последствия, а также исключить вариант повторного ее появления. Избежать таких проблем и рисков возможно, используя внутренние политики в качестве формализации тех или иных процессов [7]. Если говорить о создании системы управления ИБ на основе ГОСТ Р ИСО/МЭК 27001 [5], то несомненно следует применять комплекс мер, предлагаемых стандартом [1, 2, 10]. Стоит упомянуть и такие стандарты как ГОСТ Р ИСО/МЭК 27002-2012 [6] и ГОСТ Р ИСО/МЭК 27005-2010 [7]. Первый позволит составить правильную базу для дальнейшей системы, выстроив основные принципы СУИБ [5], а второй поможет в работе с рисками ИБ, на основе которых будет выстраиваться весь дальнейший менеджмент ИБ. Данные стандарты в совокупности с ГОСТ Р ИСО/МЭК 27001 [5] позволят начать строить грамотную систему управления ИБ в организации и сформировать правильный базис в системе менеджмента ИБ [1, 2, 10].

Возвращаясь к мерам безопасности, в качестве примера рассмотрим политику контроля доступа, подразумевающую под собой правила предоставления, разграничения и контроля доступа сотрудников к системам и ресурсам организации. Реализацией такой меры занимаются специально выделенные сотрудники, имеющие соответствующий регламент и должностную инструкцию. Избежать риска несанкционированного доступа частично или полностью поможет внедрение соответствующей политики использования предоставления прав доступа сотрудникам [1, 2]. Подобная политика не должна накладывать ограничений, противоречащих культуре организации. Она должна защищать сотрудников, партнеров и саму организацию от намеренных или случайных незаконных действий индивидуумов. Системы Интернета, а также компьютеры, операционные системы, носители данных, программное обеспечение, учетные записи и прочее, являются собственностью организации [1, 2]. Эти системы при их обычном функционировании должны использоваться для целей бизнеса, а также служить интересам самой организации, ее клиентов и партнеров. Каждый обладатель того или иного доступа обязан знать эти руководящие принципы и вести себя в соответствии с ними. Целью такой политики является определение допустимого количества прав доступа в соответствии с занимаемой сотрудником должностью. Нарушение правил политики создает угрозы для организации в виде неправомерного получения информации и использования ее в корыстных целях, а также проблемы юридического характера. Область действия такой политики распространяется на всех сотрудников, внешних и временных работников, включая третьих лиц.

Еще одним актуальным на сегодняшний день примером будет служить политика удаленного доступа к интранету организации, целью которой будет являться определение норм и правил подключения к интранету организации. Политика также применима ко всем сотрудникам и компьютерам организации, имеющим подключение к интранету организации, а конкретно к удаленным соединениям. Гарантия локального соединения пользователя с организацией, будет значиться основным положением для сотрудников и контрагентов, получивших привилегию удаленного доступа. Удаленный доступ должен тщательно контролироваться посредством мер защиты, таких как идентификация и аутентификация, единая конфигурация программного обеспечения (ПО) со стороны компании и т. д.

Подобные политики при реализации позволят уменьшить риски ИБ [1, 2], исходящие от сотрудников, использующих компьютеры и имеющих доступ к ресурсам и системам компании, а также повысят качество раскрытия инцидентов [9], так как четкая формализация процессов поможет в поиске источника угрозы. Исходя из всего вышесказанного, предлагаются следующие рекомендации для успешной формализации процессов СУИБ:

– методы формализации процессов следует начинать внедрять параллельно с разработкой самой СУИБ;

– формализация должна затрагивать все области, связанные с информационной безопасностью в организации, только тогда она будет иметь полноценный результат;

– разрабатываемые политики и правила должны максимально подробно описывать порядок процессов и виды ответственности для сотрудников;

– любая внедренная политика должна иметь цель обезопасить сотрудников и организацию от тех или иных рисков ИБ.

Заключение

После проведенного анализа подходов к созданию СУИБ и изучению соответствующих стандартов проблемой внедрения формализованных процессов на ЗО КИИ или же любом другом предприятии остается их количество и способ построения системы управления информационной безопасностью с его индивидуальным подходом. В свою очередь это означает невозможность предусмотрения всех необходимых мер по защите информационной безопасности и их внедрения путем формализации системы [7]. Решение инцидентов сильно затягивается в виду банального непонимания как их решать, или же вовсе откладывается с надеждой на то, что подобное больше не повторится. Но подобное отношение к рискам информационной безопасности может привести к критическим потерям организации [1, 2], а в случае значимых объектов КИИ это может привести к негативным или даже критичным последствиям для государственной структуры.

К сожалению, одной политики, подобной представленной в данной статье, мало для того, чтобы обеспечить полную безопасность процессов и бизнес-процессов организации по средствам формализации. Количество внедренных правил должны быть как минимум равны количеству выявленных рисков информационной безопасности при аудите, а их максимум ограничивается лишь соображениями руководителя. Еще одним не мало важным фактом после формализа-

ции всех процессов СУИБ является возможность беспроблемно возвращаться на любой из этапов построения системы для внесения корректировок или изменения структуры системы. Чем больше процессов будут подвержены подобной формализации, тем целостней и быстрей будет функционировать вся система управления информационной безопасностью [5, 6].

Анализ национальных и международных стандартов позволил понять основы построения СУИБ и послужил толчком к разработке рекомендаций по формализации процессов СУИБ. Разработанные рекомендации и приведенные примеры политик при их реализации и внедрении в организацию ускорят взаимодействие подразделений сотрудников, занимающихся тем или иным процессом, между собой, а решение инцидентов информационной безопасности [9] будут осуществляться за меньший промежуток времени и более точно, что в свою очередь является приоритетными свойствами для ЗО КИИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Серова А. Г. Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью / А. Г. Серова // Социально-экономические и естественно-научные парадигмы. 2018. – С. 829-837.

2. Серова А. Г. Теоретические основы и программные средства аудита системы управления информационной безопасностью государственного учреждения // Модернизация Российской экономики. Прогнозы и реальность. 2017. – С. 560-569.

3. Сиротюк В. О. Разработка эффективной системы управления безопасностью патентных организаций // Проблемы управления безопасностью сложных систем. 2019. – С. 88-93.

4. Безопасность пользователей в сети интернет : официальный сайт. – Москва. – Обновляется в течении суток. – URL: https://safe-surf.ru (дата обращения 19.04.2022). – Текст: электронный.

5. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Information technology. Security techniques. Information security management systems. Requirements. – Москва : Стандартинформ, 2019.

6. 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 – Москва : Стандартинформ, 2014.

7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management – Москва : Стандартинформ, 2011.

8. Comindware : официальный сайт. – Москва. – Обновляется в течении суток. – URL: https://www.comindware.com (дата обращения : 10.04.2022). – Текст : электронный.

9. Карасев С. В., Мацкевич А. Г., Рыболовлев А. А., Рыболовлев Д. А. Научно-практические предложения по разработке корпоративной системы управления инцидентами безопасности // Информационные системы и технологии. 2019. – № 6(116). – С. 109-116.

10. Коломыцев М. В., Носок С. А., Тоцкий Р. А. Сравнительный анализ моделей оценки зрелости информационной безопасности // Захист інформації. 2019. – Т. 21. – № 4. – С. 224-232.