УДК 004.056
DOI: http://dx.doi.org/10.21686/1818-4243-2018-2-61-70

Л.М. Ильченко[1], Е.К. Брагина[1], И.Э. Егоров[1], С.И. Зайцев[2]

[1] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия

[2] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Санкт-Петербург, Россия

Расчет рисков информационной безопасности телекоммуникационного предприятия

Целью данной работы является определение и оценка рисков информационной безопасности для типовой распределенной информационной системы телекоммуникационного предприятия, расположенной в пределах трех контролируемых зон. Основной акцент, при обеспечении информационной безопасности в рассматриваемой информационной системе, делается на минимизацию ущерба от угроз безопасности, направленных на целостность и доступность программно-аппаратного комплекса информационной системы, а не на конфиденциальность информационных ресурсов, обрабатываемых с их помощью.

В рамках исследования были рассмотрены международные и национальные стандарты в сфере защиты информации, регламентирующие вопросы менеджмента рисков информационной безопасности. В частности, были установлены основные требования к оценке и обработке рисков информационной безопасности, исходя из международного стандарта «ISO 27001:2013 Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности», а также проведено сравнение данного стандарта с его версией от 2005 года. В качестве ведущего метода оценки и обработки рисков был выбран качественный метод, как наиболее экономичный, в условиях отсутствия готовых данных о количестве реализованных атак в рассматриваемой информационной системе за отдельный промежуток времени.

В процессе были рассмотрены ценные активы организации, и, основываясь на бизнес-процессах телекоммуникационного предприятия были выделены основные и второстепенные активы, а также соответствующие им угрозы информационной безопасности, в соответствии с банком данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю.

Результатом проделанной работы стал расчет рисков информационной безопасности, основанный на выделении ценных активов организации, степени потенциального ущерба при реализации угроз на такие активы и вероятности реализации угроз для рассматриваемой информационной системы телекоммуникационного предприятия. Кроме этого, были выделены приемлемые риски, обработка которых не требуется в связи с тем, что фактическая стоимость их минимизации выше убытков от реализации соответствующих им угроз. В заключении были предложены возможные меры по минимизации рисков информационной безопасности, включающие в себя систему резервного копирования, систему защиты от несанкционированного доступа, систему антивирусной защиты, межсетевое экранирование, а также организационные меры и меры физической защиты.

Предложенный метод позволяет однозначно и обоснованно оценить риски информационной безопасности организации в условиях недостаточности исходных данных, а также отсутствии дополнительных программно-аппаратных средств для оценки рисков информационной безопасности, что позволяет применять его для типовых организаций, основываясь лишь на масштабировании рассматриваемой системы, при условии отсутствия в обрабатываемых сведениях информации, составляющей государственную тайну. Процедура обработки рисков помогает не только выявить и устранить существующие уязвимости и минимизировать вероятность реализации существующих угроз информационной безопасности, но и повысить уровень грамотности сотрудников предприятия, участвующих в процессе оценки и обработки рисков.

Ключевые слова: *информационная безопасность, менеджмент рисков информационной безопасности, телекоммуникационное предприятие.*

Lidiya M. Il'chenko[1], Elizaveta K. Bragina[1], Il'ya E. Egorov[1], Svyatoslav I. Zaysev[2]

[1] Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, Saint-Petersburg, Russia

[2] Admiral Makarov State University of Maritime and Inland Shipping», Saint-Petersburg, Russia

Calculation of risks of information security of telecommunication enterprise

The goal of this work is to identify and assess information security risks for a typical distributed information system within three controlled areas. The main emphasis, application of information security in the considered information system is done to minimize damage from security threats, aimed at the integrity and availability of the hardware and software complex of the information system, and not to the confidentiality of information resources processed with their help.

The study examined international and national standards in the field of information security, which regulate issues of information security risks management. In particular, the basic requirements for the assessment and processing of information security risks were established, based on the international standard "ISO 27001: 2013 Information technologies. Methods of protection. Information security management systems", as well as a comparison of this standard with its version from 2005 is made. As a leading method of risk assessment and processing, the most economical the qualitative method was chosen, in the absence of ready data on the number of attacks implemented in the considered information system for a certain period of time. In the process, valuable assets of the organization were considered, and based on the business process of the telecommunication company, major and minor assets were allocated, as well as the corresponding information security threats in accordance with the security threat data bank of the Federal Service for Technical and Export Control. The result of this work was the calculation of information security

risks, based on the allocation of valuable assets of the organization, the degree of potential damage in the implementation of threats to such assets and the probability of the implementation of threats to the information system of the telecommunication enterprise. In addition, acceptable risks were identified, the processing of which is not required due to the fact that the actual cost of minimizing them is greater than the losses from the implementation of threats over them. In conclusion, possible measures were proposed to minimize information security risks, including a backup system, a system for protecting against unauthorized access, an anti-virus protection system, firewalling, and organizational measures and physical protection measures. The proposed method makes it possible to reasonably assess information security risks of an organization in conditions of insufficient initial data, as well as the absence of additional hardware and software for assessing information security risks, which allows applying it to model organizations based only on scaling of the considered system, if there is no state information secret in the processed data. The risk management procedure helps not only to identify and eliminate the analysis of vulnerabilities and innovations in the field of risk assessment, but also to increase the literacy level of staff, involved in the assessment and risk management process.

Keywords: *information security, information security risks' management, telecommunication enterprise.*

Введение

На сегодняшний день перед каждым предприятием, обеспокоенного вопросами безопасности своих информационных ресурсов, встает вопрос об организации системы защиты информации, которая бы позволила в полной мере обеспечить безопасность функционирования телекоммуникационного оборудования и циркулирующей информации в информационной системе предприятия. Эффективность защиты информации зависит от подхода к ее организации и правильного выбора методов расчета рисков информационной безопасности.

Существует множество методик оценки и обработки рисков, которые применимы к любой информационной системе, вне зависимости от уровня конфиденциальности обрабатываемой в ней информации, однако, как правило, для грамотного построения системы защиты информации с использованием таких методик требуется большой объем информации о реализованных атаках, а также о попытках их реализации, подлежащий программному анализу с целью выявления наиболее актуальных угроз информационной безопасности (далее – ИБ), то есть необходима своеобразная отправная точка, с которой и следует начинать создание системы защиты, об этом говорят стандарты BS 7799-3 и NIST 800-30, что не всегда возможно реализовать практически, ввиду ограниченности временных и финансовых ресурсов – это особенно актуально для телекоммуникационных организаций, так как объемы данных в таких предприятиях огромны, а анализ каждого пакета слишком дорогостоящая и трудоемкая процедура. В данной работе предлагается метод расчета рисков для системы, которую можно охарактеризовать большими объемами данных, и неопределенным числом пользователей. [1–3]

Необходимо отметить, что существует ряд методик оценки рисков информационной безопасности, позволяющих однозначно и с высокой степенью обоснованности выделить актуальные риски, международные и национальные стандарты предлагают достаточно исчерпывающий выбор методов по данному вопросу, однако их применение возможно только в условиях небольшого объема данных, и малого числа пользователей, а сами методики весьма обобщенные. Примерами конкретизированных методик, применение которых возможно на практике, являются работы [4–6], однако их использование целесообразно при наличии ограниченного числа конечных точек.

Отличительной чертой любого телекоммуникационного предприятия является чувствительность к безопасности и надежной работе всего аппаратно-программного комплекса для обеспечения непрерывности функционирования ключевых бизнес-процессов организации, что просто обязывает руководителей организации создать и поддерживать эффективную систему информационной безопасности. [7]

В рамках данной работы предложен качественный метод оценки рисков ИБ, основанный на разбиении информационной системы телекоммуникационного предприятия на типовые сегменты (включающие не более трех контролируемых зон), обладающие одинаковыми характеристиками с точки зрения информационной безопасности. А сама методика расчета рисков основывается на совокупности способов и методов определения и оценки рисков, предложенных рядом международных и российских стандартов в сфере информационной безопасности, применение которых возможно к рассматриваемой информационной системе.

1. Определение ценности активов

Одним из ключевых документов, описывающих требования к методу обработки и оценки рисков является международный стандарт «ISO 27001: Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности» (далее – стандарт ISO 27001). Процесс расчета рисков информационной безопасности актуален на всех этапах работы системы защиты информации и является интересным для владельца информации в первую очередь с точки зрения потерь в экономической сфере.

Несмотря на то, что в рамках требований ISO 27001:2013 не рассматриваются явные формулы для расчета рисков, исходя из данных документа можно выделить следующее:

– в процессе оценки рисков должны быть установлены критерии приемлемости риска и критерии для оценки рисков ИБ;

– должны быть даны гарантии того, что оценка рисков ИБ даст обоснованные и непротиворечивые массивы актуальных, для рассматриваемой системы, рисков ИБ;

– должна быть произведена идентификация рисков ИБ, направленных на такие свойства информационных ресурсов, как конфиденциальность, целостность и доступность;

– а также, должна производиться идентификация владельца риска, где под владельцем понимается физическое, юридическое лицо или подразделение, отвечающее за управление риском и обладающее необходимыми для этого полномочиями, в данном случае, речь может идти о руководителях, специалистах по информационной защите, отделах по ИБ и пр.; [8]

– в процессе анализа рисков ИБ должна быть произведена оценка потенциальных потерь в случае реализации риска;

– должна быть оценена вероятность реализации рисков и определена величина рисков;

– в процессе оценки рисков ИБ должно быть произведено сопоставление рисков с установленными критериями, а также определен вектор приоритетных направлений по их обработке. [9]

Стандарт ISO 27001:2013 существенно урезан, в отличие от стандарта ISO 27001:2005, где процесс оценки рисков был достаточно подробно рассмотрен, и включал в себя такие этапы, как идентификация уязвимостей и идентификация активов и их владельцев. [10–11]

Исходя из ГОСТ Р ИСО 31000-2010, существует множество методов по оценке рисков ИБ: «идентификация риска, анализ последствий реализации рисков ИБ, оценка эффективности существующих средств управления, количественная оценка уровня рисков ИБ, сравнительная оценка рисков ИБ, качественная, количественная или смешанная оценка вероятностных характеристик риска».

Выбор метода оценки рисков ИБ должен основываться на следующих факторах:

– временные, финансовые, информационные ресурсы;

– степень неопределенности оценки рисков ИБ;

– наличие либо отсутствие возможности получение количественных оценок выходных денных, где выходными данными могут являться мнения, решения, перечни, а также рекомендации, в зависимости от метода и этапа оценки рисков ИБ. [12]

На практике, расчет рисков необходимо начинать с документа «Методология оценки и обработки рисков», который

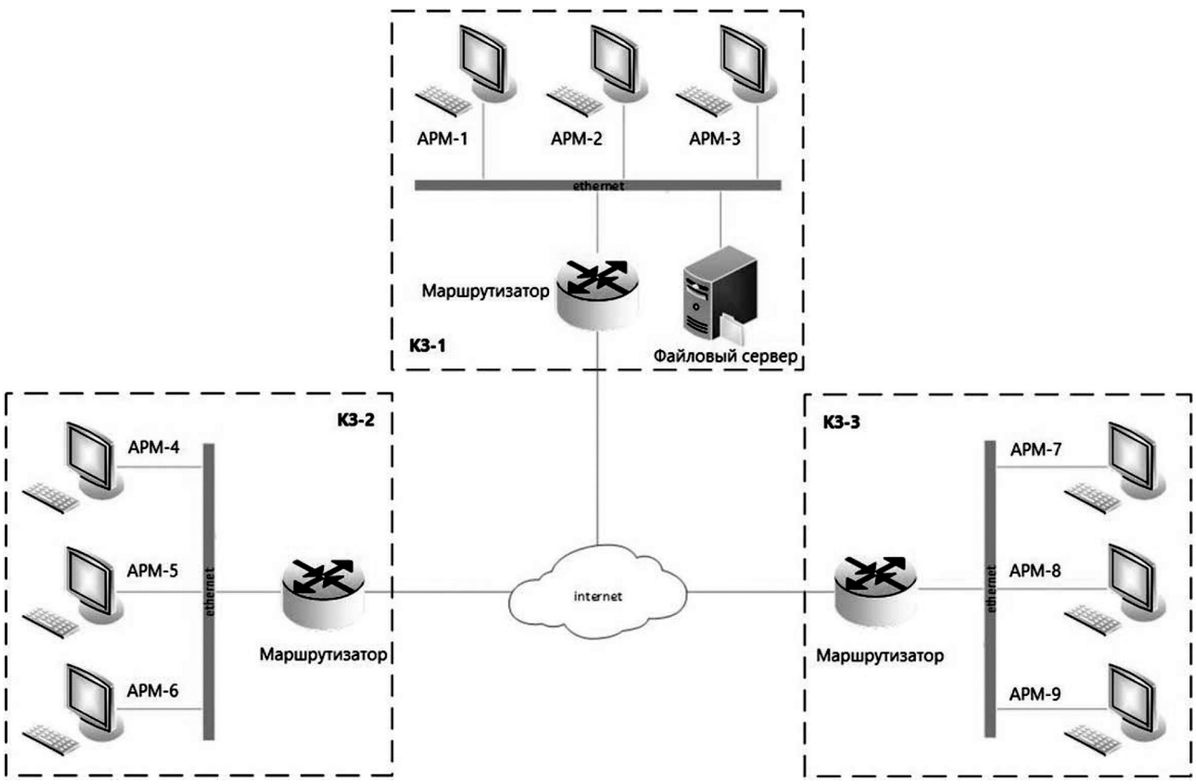

Рис. 1. Схематичное расположение распределенной информационная система

разрабатывается до анализа и обработки рисков.

Итогом мероприятий, проведенных в соответствии с методикой должен стать отчет с суммарными результатами всех мероприятий по оценке степени рисков и их обработке.

В данном случае рассматривается корпоративная распределенная многопользовательская информационная система (далее – ИС), имеющая подключение к сетям общего пользования, обрабатывающая информацию разного уровня конфиденциальности, не содержащую сведения, составляющие государственную тайну.

В соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ценные активы организации условно можно разделить на основные и вспомогательные.

Таблица 1

Шкала ценности активов

Идентификатор актива	Актив организации		Конфиденциальность	Целостность	Доступность	Ценность актива
A.	Основные активы Информация	Информация, необходимую для реализации назначения или бизнеса организации	2	4	4	**4**
B.		Информация личного характера, которая определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни	3	1	1	**3**
C.		Стратегическая информация, необходимая для достижения целей организации	2	2	1	**2**
D.		Информацию, обработка которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение	3	2	2	**3**
E.	Аппаратно-программный комплекс		–	3	4	**4**
F.	Носители информации		–	1	2	**2**
G.	Сеть		–	3	4	**4**
H.	Сотрудники		–	1	1	**1**
I.	Место функционирования организации		–	1	1	**1**

Основные активы:

1. Бизнес-процессы – совокупность различных видов деятельности, в результате которой создается продукт или услуга, представляющие интерес для потребителя.

2. Информация – сведения, являющиеся предметом собственности, подлежащие защите от нарушения конфиденциальности, целостности и доступности, в соответствии с требованиями правовых документов и требованиями владельца информации, вне зависимости от формы представления. Сведения, компрометация которых никаким образом не повлияет на деятельность организации, не рассматриваются как ценный актив.

Вспомогательные активы:

1. Аппаратно-программный комплекс – совокупность технических и программных средств, предназначенных для выполнения взаимосвязанных эксплуатационных функций по обработке информации ограниченного распространения, включающая в себя активную аппаратуру обработки данных, стационарную аппаратуру, периферийные обрабатывающие устройства, операционные системы и прикладное программное обеспечение.

2. Носители данных – носитель для хранения данных, включая электронный носитель и аналоговый.

3. Сеть – совокупность телекоммуникационных устройств, используемых для соединения нескольких физически удаленных сегментов информационной системы.

4. Персонал – в широком смысле, все субъекты, имеющие легитимный доступ в пределы контролируемой зоны и являющиеся потенциальными внутренними нарушителями.

5. Место функционирования организации – пределы контролируемой зоны, в которой функционирует информационная система.

ГОСТ Р ИСО/МЭК 27005-2010 условно разделяет информацию на: «информацию, необходимую для реализации назначения или бизнеса организации, информацию личного характера, которая определена особым образом, соответствующую национальным законам о неприкосновенности частной жизни, стратегическую информацию, необходимую для достижения целей организации, информацию, обработка которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение».

Первоначально необходимо определить ценность активов (далее – ЦН) организации, в данном случае будет рассмотрена четырехбалльная система оценки ценности активов:

1 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива не будет иметь последствий, как для организации в целом, так и бизнес-процессов, в частности.

2 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к незначительным потерям для организации, в условиях, когда восстановление прежнего со-

стояния системы возможно без остановки бизнес-процессов.

3 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к значительным финансовым потерям и/или окажет существенное негативное влияние на престиж организации, в условиях, когда восстановление прежнего состояния системы возможно, но требует больших временных и/или финансовых ресурсов.

4 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива может привести полной остановке бизнес-процессов, большим финансовым потерям и/или окажет значительное негативное влияние на престиж организации.

Так как бизнес-процессом является совокупность различных видов деятельности, в результате которой создается продукт или услуга, то в перечне актуальных угроз и существующих уязвимостей остальных ценных активов будут содержаться угрозы и уязвимости актуальные и для бизнес-процессов.

Особенностью рассматриваемой категории предприятий является то, что основной ущерб бизнес-процессам организации способны нанести угрозы доступности сетевого оборудования и программно-аппаратного комплекса, а не угрозы, направленные на нарушение конфиденциальности информационных ресурсов предприятия.

2. Оценка рисков информационной безопасности

Целесообразно обработку рисков ИБ рассматривать, как итеративный процесс, это позволит повысить уровень детализации оценки рисков при каждой последующей итерации.

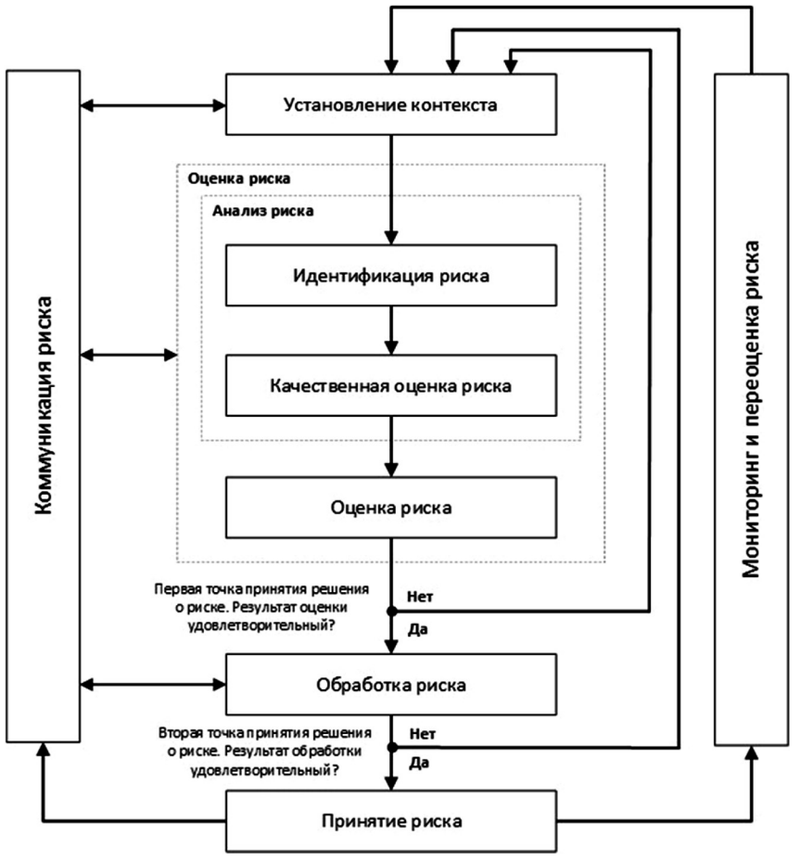

Рис. 2. Процесс оценки и обработки рисков ИБ

Пример итеративного процесса оценки и обработки рисков ИБ подробно описан в ГОСТ Р ИСО/МЭК 27005-2010 и показан на рис. 2, где под контекстом риска понимается установление критериев для обработки рисков ИБ, а также назначаются ответственные сотрудники или подразделение, занимающиеся вопросом менеджмента рисков ИБ. Под идентификацией риска понимается процесс нахождения и определения рисков ИБ, под оценкой риска понимается присвоение числовых значений последствиям реализации риска, а также вероятности его реализации. Приятие риска означает, что ущерб от реализации риска является приемлемым, а вероятность его реализации мала настолько, что позволяет не проводить процедур обработки риска ИБ. Коммуникация риска позволяет осуществлять обмен сведениями об актуальных рисках между причастными сторонами.

Под обработкой риска понимается процесс минимизации последствий от реализации риска и/или процесс минимизации вероятности реализации риска ИБ. [13]

Пример деятельности по обработке рисков ИБ представлен на рис. 3 в соответствии с ГОСТ Р ИСО/МЭК 27005-2010.

Следующим шагом является определение степени уязвимости каждого из ценных активов организации (далее – СУ).

В рамках данной работы будет рассмотрен выборочный ряд угроз ИБ, с ID в соответствии с банком данных угроз ФСТЭК:

– «угроза длительного удержания вычислительных ресурсов пользователями» (014);

– «угроза загрузки нештатной операционной системы» (018);

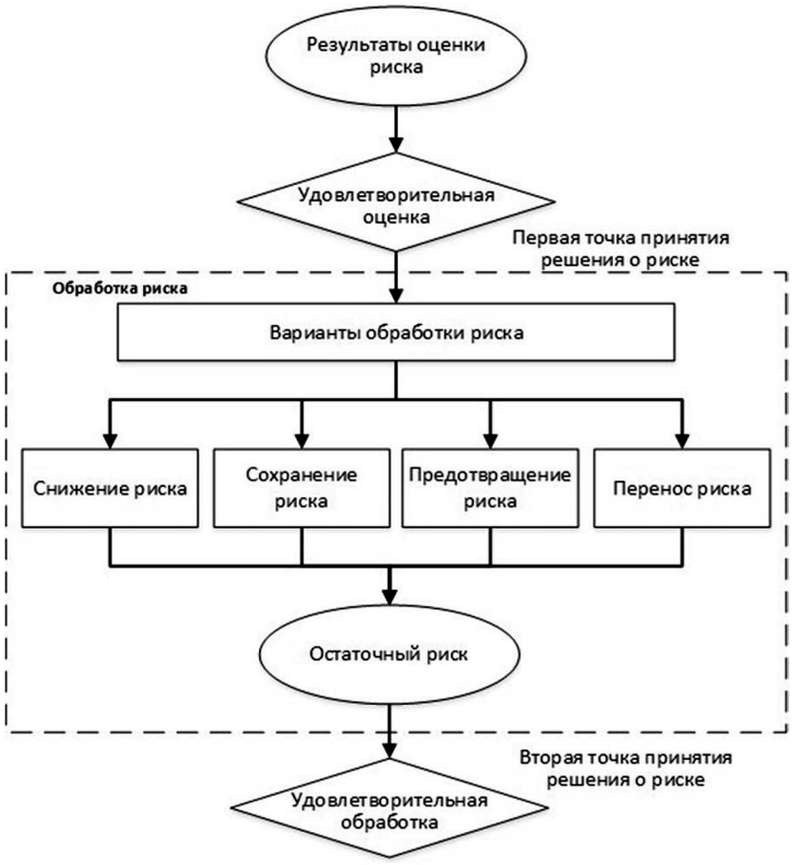

Рис. 3. Деятельность, направленная на обработку рисков ИБ

– «угроза избыточного выделения оперативной памяти» (022);

– «угроза изменения компонентов системы» (023);

– «угроза использования информации идентификации/аутентификации, заданной по умолчанию» (030);

– «угроза использования слабостей протоколов сетевого/локального обмена данными» (034);

– «угроза исследования механизмов работы программы» (036);

– «угроза несанкционированного удаления защищаемой информации» (091);

– «угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники» (113);

– «угроза повреждения системного реестра» (121);

– «угроза повышения привилегий» (122);

– «угроза преодоления физической защиты» (139);

– «угроза приведения системы в состояние «отказ в обслуживании» (140);

– «угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации» (143);

– «угроза утраты вычислительных ресурсов» (155);

– «угроза утраты носителей информации» (156);

– «угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации» (157);

– «угроза форматирования носителей информации» (158);

– «угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации» (160);

– «угроза неправомерного шифрования информации» (170);

– «угроза распространения «почтовых червей» (172);

– «угроза физического устаревания аппаратных компонентов» (182);

Таблица 2

Степень уязвимости актива

Угрозы ИБ	Ценные активы организации								
	A.	B.	C.	D.	E.	F.	G.	H.	I.
014	–	–	–	–	2	–	–	–	–
018	1	1	1	1	3	–	–	–	–
022	–	–	–	–	2	–	2	–	–
023	–	–	–	–	3	–	–	–	–
030	2	2	2	2	1	–	–	–	–
034	–	–	–	–	–	–	1	–	–
036	1	1	1	1	1	–	1	–	–
091	3	3	3	3	–	–	–	–	–
113	–	–	–	–	2	–	–	–	–
121	2	2	2	2	2	–	–	–	–
122	–	–	–	–	2	–	–	–	–
139	1	1	1	1	3	3	–	–	–
140	–	–	–	–	3	–	3	–	–
143	3	3	3	3	2	2	–	–	–
155	1	1	1	1	3	3	3	–	–
156	3	3	3	3	–	2	–	–	–
157	–	–	–	–	1	1	–	–	–
158	1	1	1	1	–	1	–	–	–
160	1	1	1	1	2	2	–	–	–
170	2	2	2	2	–	–	–	–	–
172	–	–	–	–	–	–	2	–	–
182	–	–	–	–	1	–	1	–	–
186	2	2	2	2	–	–	2	–	–
189	–	–	–	–	1	–	1	–	–

Таблица 3

Вероятность реализации угроз

ID угрозы	014	018	022	023	030	034	036	091	113	121	122	139	140	143	155	156	157	158	160	170	172	182	186	189
Вероятность	2	1	2	3	1	2	2	4	2	2	2	3	2	2	2	4	3	3	3	2	2	3	3	2

– «угроза внедрения вредоносного кода через рекламу, сервисы и контент» (186);

– «угроза маскирования действий вредоносного кода» (189). [14]

В табл. 2 представлен результат оценки уязвимости актива для перечня угроз, где 1 – низкая уязвимость по отношению конфиденциальности, целостности и/или доступности ценного актива организации, 2 – средняя степень уязвимости, а 3 – высокая степень уязвимости.

Последним этапом перед расчетом рисков ИБ является оценка вероятности реализации угроз ИБ (далее – В), представленных в табл. 2. Оценка вероятности представлена в табл. 3, где 1 – угроза существует, но не встречалась в рассматриваемой сфере, 2 – угроза возникает в рассматриваемой сфере 2–3 раза в год, 3 – угроза была реализована в рассматриваемой системе, 4 – угроза возникает 2–3 раза в год в рассматриваемой системе.

3. Отчет об оценке рисков ИБ

Общий уровень риска ИБ для каждого из ценных активов организации рассчитывается по формуле 1, в табл. 4 представлен результат для активов A, E, G.

$$Р = ЦН \times СУ \times В \qquad (1)$$

Приемлемым риском считается риск, чье числовое значение находится в промежутке от 1 до 10, такой риск считается

Таблица 4

Оценка рисков ИБ

Ценный актив организации	Угрозы	ЦН	СУ	В	Р	Числовое значение оценки риска
Информация, необходимую для реализации назначения или бизнеса организации	018	4	1	1	4	Низкий
	030	4	2	1	8	Низкий
	036	4	1	2	8	Низкий
	091	4	3	4	48	Высокий
	121	4	2	2	16	Средний
	139	4	1	3	12	Средний
	143	4	3	2	24	Высокий
	155	4	1	2	8	Низкий
	156	4	3	4	48	Высокий
	158	4	1	3	12	Низкий
	160	4	1	3	12	Низкий
	170	4	2	2	16	Низкий
	186	4	2	3	24	Высокий
Аппаратно-программный комплекс	014	4	2	2	16	Средний
	018	4	3	1	12	Средний
	022	4	2	2	16	Средний
	023	4	3	3	36	Высокий
	030	4	1	1	4	Низкий
	036	4	1	2	8	Низкий
	113	4	2	2	16	Средний
	121	4	2	2	16	Средний
	122	4	2	2	16	Средний
	139	4	3	3	36	Высокий
	140	4	3	2	24	Высокий
	143	4	2	2	16	Средний
	155	4	3	2	24	Высокий
	157	4	1	3	12	Средний
	160	4	2	3	24	Высокий
	182	4	1	3	12	Средний
	189	4	1	2	8	Низкий
Сеть	022	4	2	2	16	Средний
	034	4	1	2	8	Низкий
	036	4	1	2	8	Низкий
	140	4	3	2	24	Высокий
	155	4	3	2	24	Высокий
	172	4	2	2	16	Средний
	182	4	1	3	12	Средний
	186	4	2	3	24	Высокий
	189	4	1	2	8	Низкий

Таблица 5

Рекомендованные контрмеры

Ценный актив организации	Угрозы	Риск	Приемлемый риск	Планируемые меры	Остаточный риск
Информация, необходимую для реализации назначения или бизнеса организации	091	48	От 1 до 19	Система резервного копирования, система защиты от НСД	12
	143	24		Система антивирусной защиты, межсетевое экранирование	12
	156	48		Учет носителей информации	12
	186	24		Система антивирусной защиты, межсетевое экранирование; Организационные меры	8
Аппаратно-программный комплекс	023	36		Межсетевое экранирование, система доверенной загрузки, система антивирусной защиты; Организационные меры	12
	139	36		Системы видеонаблюдения, адекватные средства физической защиты; Организационные меры.	12
	140	24		Система межсетевого экранирования	12
	155	24		Система межсетевого экранирования	12
	160	24		Системы видеонаблюдения, адекватные средства физической защиты; Организационные меры.	8
Сеть	140	24		Система межсетевого экранирования	12
	155	24		Система межсетевого экранирования	12
	186	24		Система антивирусной защиты, межсетевое экранирование; Организационные меры	8

незначительным, и обработка такого риска не требуется.

Средний риск, чье числовое значение находится в диапазоне от 11 до 21 рекомендован к обработке с целью его минимизации. [15–16]

Высокий риск, чье числовое значение находится в диапазоне от 22 до 64, данный риск считается существенным, и его обработка обязательна.

4. Возможные контрмеры

Допустим, что руководитель предприятия принимает решение, что риски с числовым значением выше 20 подлежат обработке с целью их минимизации. Возможные контрмеры представлены в табл. 5. [17–20]

После обработки рисков ИБ, остаточный риск стал приемлемым для каждой из актуальных угроз информационной безопасности.

Заключение

Предложенная методика позволила однозначно и обоснованно оценить риски информационной безопасности организации в условиях большого объема обрабатываемой информации и неограниченного числа пользователей и потребовала минимальных финансовых вливаний. Применение рассмотренного метода на практике способствовало выявлению основных угроз защиты безопасности, основываясь на банке данных угроз безопасности информации ФСТЭК России. Исходя из результатов оценки рисков информационной безопасности, в последствие, была создана модель угроз рассматриваемого телекоммуникационного предприятия.

Стоит отметить, что предложенная методика одинаково применима, как к автоматизированной информационной системе, так и к системам обработки информации без использования средств автоматизации. Однако, применение специализированных программных продуктов, позволяющих осуществлять оценку рисков ИБ, все же является приоритетным, так как может позволить функционировать системе управления рисками в режиме реального времени, при условии достаточности временных и финансовых ресурсов, в отличие от рассмотренного метода, практическая реализация которого возможно в качестве разового или периодически проводимого мероприятия.

Еще одной особенностью процедуры обработки рисков является то, что она помогает не только «закрыть» существующие уязвимости и минимизировать вероятность реализации существующих угроз ИБ, но и повысить компетентность сотрудников в вопросах защиты информации.

Литература

1. Некрылова Н.В. Предпосылки реализации элементов управления рисками бизнес-процессов в стандартах на системы менеджмента промышленного предприятия // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 204–215.

2. Андреева Н.В. Функциональная модель системы управления информационной безо-

References

1. Nekrylova N.V. Predposylki realizatsii elementov upravleniya riskami biznes-protsessov v standartakh na sistemy menedzhmenta promyshlennogo predpriyatiya. Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Obshchestvennye nauki. 2015. No. 2 (34). C. 204–215. (In Russ.)

2. Andreeva N.V. Funktsional'naya model' sistemy upravleniya informatsionnoy bezopasnost'yu

пасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799) // Научно-технический вестник информационных технологий, механики и оптики. 2007. № 39. С. 40–44.

3. Пугин В.В., Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // T-Comm – Телекоммуникации и Транспорт. 2012. № 6. С. 54–57.

4. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1–2 (25). С. 83–86.

5. Одинцова М.А. Методика управления рисками для малого и среднего бизнеса. // Экономический журнал. 2014. № 3 (35). URL: https://cyberleninka.ru/article/n/metodika-upravleniya-riskami-dlya-malogo-i-srednego-biznesa (дата обращения: 01.02.2018).

6. Глушенко С.А. Применение системы Matlab для оценки рисков информационной безопасности организации // Бизнес-информатика. 2013. № 4 (26). С. 35–42.

7. Губарева О.Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях. // Вестник Волжского университета им. В.Н. Татищева. 2013. № 2 (21). С. 76–81.

8. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3 (4). С. 69–73.

9. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23 p.

10. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4 (7). С. 69–74.

11. Ильченко Л.М. Анализ системы менеджмента информационной безопасности на базе стандарта ISO 27001:2013. // Материалы 5 научно-практической конференции студентов, аспирантов и курсантов «IT вчера, сегодня, завтра». 2017. С. 51–61.

12. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство.; Введен с 01.09.2011. Москва: Изд-во Стандартинформ, 2012.

13. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007; Введ. с 30.11.2010. Москва: Изд-во Стандартинформ, 2011.

14. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю URL: https://bdu.fstec.ru (дата обращения: 01.02.2018).

kak sredstvo vnedreniya standartov lineyki ISO/IEC 2700x (BS 7799). Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki. 2007. No. 39. P. 40–44. (In Russ.)

3. Pugin V.V., Gubareva O.Yu. Obzor metodik analiza riskov informatsionnoy bezopasnosti informatsionnoy sistemy predpriyatiya. T-Comm – Telekommunikatsii i Transport. 2012. No. 6. P. 54–57. (In Russ.)

4. Pletnev P.V., Belov V.M. Metodika otsenki riskov informatsionnoy bezopasnosti na predpriyatiyakh malogo i srednego biznesa. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2012. No. 1–2 (25). P. 83–86. (In Russ.)

5. Odintsova M.A. Metodika upravleniya riskami dlya malogo i srednego biznesa.. Ekonomicheskiy zhurnal. 2014. No. 3 (35). URL: https://cyberleninka.ru/article/n/metodika-upravleniya-riskami-dlya-malogo-i-srednego-biznesa (accessed: 01.02.2018). (In Russ.)

6. Glushenko S.A. Primenenie sistemy Matlab dlya otsenki riskov informatsionnoy bezopasnosti organizatsii. Biznes-informatika. 2013. No. 4 (26). P. 35–42. (In Russ.)

7. Gubareva O.Yu. Otsenka riskov informatsionnoy bezopasnosti v telekommunikatsionnykh setyakh. Vestnik Volzhskogo universiteta im. V.N. Tatishcheva. 2013. No. 2 (21). P. 76–81. (In Russ.)

8. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013. Voprosy kiberbezopasnosti. 2014. No. 3 (4). P. 69–73. (In Russ.)

9. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23 p.

10. Dorofeev A.V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost'. Voprosy kiberbezopasnosti. 2014. No. 4 (7). P. 69–74. (In Russ.)

11. Il'chenko L.M. Analiz sistemy menedzhmenta informatsionnoy bezopasnosti na baze standarta ISO 27001:2013.. Materialy 5 nauchno-prakticheskoy konferentsii studentov, aspirantov i kursantov «IT vchera, segodnya, zavtra». 2017. P. 51–61. (In Russ.)

12. GOST R ISO 31000-2010. Menedzhment riska. Printsipy i rukovodstvo.; Vveden s 01.09.2011. Moscow: Izd-vo Standartinform, 2012. (In Russ.)

13. GOST R ISO/MEK 27005-2010. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti. Vzamen GOST R ISO/MEK TO 13335-3-2007 i GOST R ISO/MEK TO 13335-4-2007; Ved. s 30.11.2010. Moskva: Izd-vo Standartinform, 2011. (In Russ.)

14. Bank dannykh ugroz bezopasnosti informatsii. Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu URL: https://bdu.fstec.ru (accessed: 01.02.2018). (In Russ.)

15. Шаго Ф.Н., Зикратов И.А. Методика оптимизации планирования аудита системы менеджмента информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 111–117.

16. Выборнова О.Н., Давидюк Н.В., Кравченко К.Л. Оценка информационных рисков на основе экспертной информации (на примере ГБУЗ АО «Центр медицинской профилактики») // Инженерный вестник Дона. 2016. № 4 (43). С. 86.

17. Пащенко И.Н., Васильев В.И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 117–126.

18. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска; Введ. с 01.12.2012. Москва: Изд-во Стандартинформ; 2012.

19. Эмануэль А.В., Иванов Г.А., Гейне М.Д. Применение менеджмента рисков на основе стандарта ИСО 14971: методические подходы // Вестник Росздравнадзора. 2013. № 3. С. 45–60.

20. Лютова И.И. Моделирование уровня приемлемого риска информационной безопасности // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2014. № 2 (141). С. 175–180.

15. Shago F.N., Zikratov I.A. Metodika optimizatsii planirovaniya audita sistemy menedzhmenta informatsionnoy bezopasnosti. Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki. 2014. No. 2 (90). P. 111–117. (In Russ.)

16. Vybornova O.N., Davidyuk N.V., Kravchenko K.L. Otsenka informatsionnykh riskov na osnove ekspertnoy informatsii (na primere GBUZ AO «Tsentr meditsinskoy profilaktiki»). Inzhenernyy vestnik Dona. 2016. No. 4 (43). P. 86. (In Russ.)

17. Pashchenko I.N., Vasil'ev V.I. Razrabotka trebovaniy k sisteme zashchity informatsii v intellektual'noy seti Smart Grid na osnove standartov ISO/IEC 27001 i 27005. Izvestiya YuFU. Tekhnicheskie nauki. 2013. No. 12 (149). P. 117–126. (In Russ.)

18. GOST R ISO/MEK 31010-2011. Menedzhment riska. Metody otsenki riska; Vved. s 01.12.2012. Moskva: Izd-vo Standartinform; 2012. (In Russ.)

19. Emanuel' A.V., Ivanov G.A., Geyne M.D. Primenenie menedzhmenta riskov na osnove standarta ISO 14971: metodicheskie podkhody. Vestnik Roszdravnadzora. 2013. No. 3. P. 45–60. (In Russ.)

20. Lyutova I.I. Modelirovanie urovnya priemlemogo riska informatsionnoy bezopasnosti. Vestnik Adygeyskogo gosudarstvennogo universiteta. Series 5: Ekonomika. 2014. No. 2 (141). P. 175–180 (In Russ.)

Сведения об авторах

Лидия Михайловна Ильченко
Магистрант
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург, Россия
Эл. почта: Lidiya9510@yandex.ru

Елизавета Константиновна Брагина
Магистрант
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург, Россия
Эл. почта: AlisBrain@mail.ru

Илья Эдуардович Егоров
Магистрант
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Санкт-Петербург, Россия
Эл. почта: mynameisiliaegorov@gmail.com

Святослав Игоревич Зайцев
Магистрант
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Санкт-Петербург, Россия
Эл. почта: sunilink@yandex.ru

Information about the authors

Lidiya M. Il'chenko
Master student
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
E-mail: Lidiya9510@yandex.ru

Elizaveta K. Bragina
Master student
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
E-mail: AlisBrain@mail.ru

Il'ya E. Egorov
Master student
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
E-mail: mynameisiliaegorov@gmail.com

Svyatoslav I. Zaytsev
Master student
Admiral Makarov State University of Maritime and Inland Shipping
Saint-Petersburg, Russia
E-mail: sunilink@yandex.ru