УДК 338.2:004

© Е. А. Селезнев[1], О. А. Горбунова[2], *2022*

[1,2] Самарский государственный технический университет (СамГТУ);

[2] Самарский университет государственного управления «Международный институт рынка» (Университет «МИР»), Россия

E-mail [1,2]: genuka76@mail.ru

СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ МЕСТО В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Информационные системы играют ключевую роль в обеспечении эффективной работы коммерческих и государственных предприятий, министерств, ведомств, некоммерческих организаций. В статье раскрывается сущность информационной безопасности. Делается акцент на том, что важнейшей составляющей информационной безопасности становится защита от информации, заключающаяся в предупреждении разрушающего воздействия информации на электронные средства, на системы и на людей. В ходе исследования определено место информационной безопасности в системе экономической безопасности предприятия, выявлены внутренние и внешние угрозы, влияющие на данную систему, рассмотрены наиболее популярные в настоящее время методики управления рисками информационной безопасности.

Ключевые слова: информационная безопасность, цифровизация, экономическая безопасность предприятия, антивирусы, защита данных.

Проблемы информационной безопасности в современном мире напрямую связаны с прогрессом в сфере информационных технологий [1]. Наиболее совершенные информационные технологии и технические средства информации связаны со сферой противостояния или же с подготовкой к нему. Информационная безопасность присутствует практически во всех сферах человеческой жизни. Она оказывает определенное влияние на состояние экономической, социальной, политической и других компонентов гражданской безопасности [6].

Цель данного исследования — выявить сущность информационной безопасности и определить ее место в обеспечении экономической безопасности предприятия.

Объектом исследования является экономическая безопасность предприятия, *предметом исследования* — информационная безопасность как основная составляющая экономической безопасности.

Общее понятие информационной безопасности (англ. information security, а также InfoSec) можно трактовать как практику предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации [8]. Таким образом, информационная безопасность — это в первую очередь защита и сохранение информации.

Так как на работу и деятельность предприятия могут влиять различные внешние и внутренние факторы, для стабильной работы, а также эффективного выполнения своего основное назначения — получения максимальной прибыли и удовлетворения запросов потребителей — должна быть обеспечена экономическая безопасность предприятия. Сущностью экономической безопасности предприятия является обеспечение состояния стабильности, устойчивости и защищенности экономической системы от негативного влияния внешних и внутренних факторов [5]. Экономическая безопасность предприятия — это комплексное понятие, под которым также понимается способность объекта противостоять внешним угрозам, воздействиям окружающей среды, а также внутренним опасностям, связанным со структурой организации. При правильном обеспечении экономической безопасности предприятие прогрессирует и обеспечено стабильной работой в настоящем и будущем [3].

Основной функцией экономической безопасности предприятия является обнаружение угроз различной природы [4], то есть факторов, которые прямо или опосредованно дестабилизируют эффективное функционирование организации. Экономическую безопасность можно также рассматривать как систему знаний о методах и приемах действий по обнаружению факторов-угроз, имеющих негативные последствия для работы [9].

В настоящее время с учетом глобальной цифровизации процессов, связанных с ведением бизнеса и применением во многих компаниях организации работы персонала в удаленном режиме, сохранение конфиденциальной информации предприятия стало занимать приоритетное место в области прогнозирования и предотвращения потенциальных угроз и рисков. Такая тенденция приводит к увеличенной нагрузке на службы информационной безопасности на предприятии, что, в свою очередь, вынуждает руководителей модифицировать мощности по мониторингу, контролю, хранению стратегически важной конфиденциальной информации путем приобретения

более нового программного обеспечения, поиска компетентных специалистов в области информационной безопасности, не заинтересованных в создании каналов утечек данных, что обеспечивается на уровне кадровой безопасности организации [10].

Информационная безопасность как один из неотъемлемых системных компонентов экономической безопасности предприятия включает в себя следующие мероприятия:

— составление руководством локальной документации в области информационной безопасности для обозначения границ секретности данных, подлежащих охране от злоумышленников;

— создание уровней доступа к информационной базе, сортировка видов защищаемой документации по данным уровням, определение круга лиц, входящих в тот или иной уровень доступа к базам данных;

— оснащение организации экономически обоснованной системой программного обеспечения, физическими мерами предотвращения создания каналов утечек данных;

— проведение работы с составом сотрудников по поводу вопросов обеспечения защиты конфиденциальных ресурсов;

— контроль документооборота при заключении договоров сотрудничества с контрагентами (поставщики, подрядчики, кредитные организации);

— изменение уровня секретности данных на более высокий или более низкий.

Таким образом, любая внешняя угроза влияет на информационную безопасность организации, снижая ее устойчивость и возможность дальнейшего функционирования в цифровой среде. Однако отдельную группу угроз, сказывающихся на информационной безопасности предприятия, представляют внутренние вызовы, которые влияют на общую систему экономической безопасности организации (табл. 1).

В целом информационная безопасность организации формируется посредством обеспечения кадровой, финансовой, ресурсной и информационной составляющих.

Информационная угроза имеет место тогда, когда величина и вероятность возможного информационного ущерба больше определенного порогового значения, требующего принятия мер по его предотвращению, защите объекта безопасности. Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через риск обра-

зования канала несанкционированного получения (добывания) кем-то ценной информации и документов. Этот канал представляет собой совокупность незащищенных или слабо защищенных направлений возможной утраты информационных ресурсов ограниченного доступа, которые злоумышленник использует для получения необходимых сведений. Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

Таблица 1

Внутренние угрозы, влияющие на информационную безопасность предприятия

Описание угроз информационной безопасности	*Влияние на общую систему экономической безопасности*
Кадровая угроза, утечка информации в результате действий сотрудников	Снижение финансовых результатов, появление убытков, уход с рынка
Потеря информации в результате недобросовестной работы персонала по организации защиты информации	Доступность инновационных разработок конкурентам, потеря новых рынков сбыта
Снижение защитного потенциала программного обеспечения и серверов в организации	Увеличение расходов организации, нехватка ресурсов
Недостаточное финансирование информационной безопасности	Недостаток капитала, как следствие отсутствия средств для развития организации, угроза банкротства
Низкие темпы обновления защитных систем, несвоевременность пополнения банков данных новыми угрозами	Потеря ресурсов, утечка информации
Утечка данных клиентов	Потеря клиентов, расходы на восстановление защитных данных

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления). Исходя из вышеизложенного, в наиболее общем

виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой.

К объектам информационной безопасности в организации относят:

— информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;

— средства и системы информатизации — средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления в организациях, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

Выявление, анализ и оценка рисков информационной безопасности является ключевым этапом проектирования систем информационной безопасности предприятия. От того, насколько правильно будут оценены риски, зависит и эффективность системы информационной безопасности предприятия в целом.

Рассмотрим наиболее популярные в настоящее время методики управления рисками информационной безопасности [2].

Метод CRAMM (CCTA Risk Analysis and Managment Method) и реализующий его одноименный программный продукт от компании Insight Consulting Limited является мощным и универсальным инструментом проведения обследования информационных систем и анализа рисков информационной безопасности. Данный метод используется уже более 30 лет и за это время приобрел популярность во всем мире. Основным недостатком метода является то, что он не учитывает сопроводительной документации, и идентификация защищаемых ресурсов производится без привязки к бизнес-процессам предприятия.

Указанного недостатка не лишена и методика FRAP (Facilitated Risk Analysis Process), предлагаемая компанией Peltier and Associates. В данной методике определение защищаемых ресурсов производится с использованием опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей. Идентификация защищаемых ресурсов производится также без привязки к бизнес-процессам предприятия.

Метод CORAS представляет собой методику и программный инструмент моделирования риска. Программный продукт, реали-

зующий методологию CORAS, распространяется бесплатно. В методике CORAS не предусмотрена периодичность проведения оценки рисков и актуализация их значений. CORAS не позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности. Так же, как и в вышерассмотренных методиках, CORAS не дает возможности анализа бизнес-процессов предприятия с целью выявления защищаемых ресурсов.

Разработанная компанией RiskWatch одноименная методика ориентирована на количественные способы оценки рисков. Величина риска определяется как математическое ожидание потерь за год. Эффект от внедрения средств защиты количественно рассчитывается с помощью показателя ROI (Return on Investment – возврат инвестиций). Данный метод целесообразно использовать для проведения анализа рисков на программно-техническом уровне защиты без учета организационных и административных факторов.

Методика MSAT (Microsoft Security Assessment Tool), реализованная в соответствующем программном продукте от компании Microsoft, использует качественные оценки рисков информационной безопасности. Методика позволяет оценить эффективность инвестиций от внедрения средств защиты информационных активов, но не дает возможности принимать во внимание протекающие в компании бизнес-процессы с целью идентификации объектов защиты.

Все вышесказанное позволяет сделать вывод о том, что на сегодняшний день не существует общепринятой научно обоснованной методики выявления рисков информационной безопасности. Используемые при проектировании системы информационной безопасности предприятий и организаций частные методики в большинстве своем опираются на эмпирические подходы в оценке рисков информационной безопасности, основанные на накопленном компаниями-разработчиками опыте разработки систем управления рисками информационной безопасности [7].

Считаем, что основным недостатком большинства работ, в которых изложены вышеописанные методики, является их ориентация на эмпирический подход, недостаточное внимание к возможностям, возникающим при использовании методов и средств проектирования информационных систем. К числу таких методов относится и методика структурно-функционального анализа, опирающаяся на применении CASE1-технологий.

В таблице 2 представлены средства защиты информационной безопасности.

Таблица 2

Классификация средств защиты информационной безопасности

Тип средств	*Характеристика*
Организационные	Законодательные и локальные нормативные акты, регламентирующие сферу информационной безопасности, а также действия по обслуживанию информационной инфраструктуры
Программные	Специализированное программное обеспечение для хранения, обработки и безопасной передачи информации
Аппаратные	Электронные, механические устройства, интегрированные в оборудование автоматизированной информационной системы, либо работающие в качестве автономной аппаратуры, защищающие от проникновения в информационную инфраструктуру
Аппаратно-программные	Совокупность специального оборудования и программного обеспечения, используемых для защиты данных

Отдельно стоит рассмотреть программные средства защиты информационной безопасности. В эту группу входят в первую очередь антивирусы, которые обезвреживают вирусы и восстанавливают зараженные файлы и программное оборудование. Также существуют облачные антивирусы. Решения DLP (Data Leak Prevention) позволяют предотвратить утечку информации, нарушения ее конфиденциальности. Криптография часто используется для шифрования данных, для предотвращения воровства и утечки информации. Прокси-серверы выступают посредником между пользователями или же системами. Безусловно, надежным и эффективным средством защиты является также VPN, что в переводе означает «виртуальная частная сеть», это средство позволяет использовать частную сеть для передачи или получения информации.

В заключение необходимо сказать о том, что информация является важнейшим ресурсом общественной жизни и становится ключевым элементом практически всех систем социальной жизни. В любой области, будь то политическая безопасность, экономическая безопасность, экологическая безопасность, общественная безопасность, существует связующий элемент, в роли которого выступает информационная безопасность. В своей финансово-хозяйственной деятельности предприятие непрерывно сталкивается с различными

видами поступающей информации — с открытой официальной, вероятной (неофициальной) и с тайной, полученной через неформальные контакты [6].

Для обеспечения защиты внутренней информации руководством предпринимаются различные меры:

— по пресечению возможности производственного шпионажа и утечке информации;

— по сбору информации о возможных инициаторах шпионажа;

— по технической защите документов, помещений, транспорта;

— по другой внешней информационной деятельности.

Именно поэтому для предприятия одним из приоритетных направлений экономической безопасности становится создание надежной системы, эффективно работающей с информацией и обеспечивающей нейтрализацию внутренних и внешних угроз.

Литература

1. Асанов Р. К. Формирование концепции «цифровой экономики» в современной науке // Социально-экономические науки и гуманитарные исследования. 2016. № 15. С. 143-148.

2. Бабаш А. В., Баранова Е. К. Актуальные вопросы защиты информации: монография. М.: РИОР, ИНФРА-М, 2017. 111 с.

3. Безуглая Н. С. Совершенствование системы обеспечения экономической безопасности предприятия на основе управления рисками (по материалам Краснодарского края): дис. ... канд. экон. наук / Н. С. Безуглая. 2012. 173 с.

4. Богомолов В. А. Экономическая безопасность: 2-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2018. 188 с.

5. Гомалеев А. О. Информационная безопасность как составляющая экономической безопасности организации // Аллея науки. 2018. Т. 1. № 10 (26). С. 993-998.

6. Мамаева Л. Н. Характерные проблемы информационной безопасности в современной экономике // Информационная безопасность регионов. 2016. № 1 (22). С. 21-24.

7. Панин Д. Н., Козлов З. С. Информационная безопасность в сфере корпоративных сетей // Дневник науки: электронный журнал. 2020. № 12 (48). С. 23. URL: http://dnevniknauki.ru/images/publications/2020/12/ technics/Panin_Kozlov.pdf

8. Преображенский Ю. П. Информационная безопасность – вызовы современного мира // Вестник Воронежского института высоких технологий. 2017. № 2 (21). С. 60-63.

9. Сергеев А. А. Экономическая безопасность предприятия. М.: Юрайт, 2019. 273 с.

10. Стародубцева Е. Б., Маркова О. М. Цифровая трансформация мировой экономики // Вестник АГТУ. Серия: Экономика. 2018. № 2. С. 7-15.

Статья поступила в редакцию 28.02.22г.
Рекомендуется к опубликованию членом Экспертного совета канд. экон. наук, д-ром полит. наук, доцентом В. А. Зиминым