УДК 65.011.56: 338.14

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

Ольга Владимировна КУЧИНА[1], к.э.н., доцент
Марина Ивановна БАРАБАНОВА[2], к.э.н., доцент
[1]Факультет экономики и финансов СЗИУ РАНХиГС при Президенте РФ
Санкт-Петербург, Российская Федерация
[2]Автономная некоммерческая организация высшего образования
«Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Россия
Адрес для корреспонденции: Барабанова М.И., 191023, Невский пр., 60. Санкт-Петербург

Аннотация

В условиях развития цифровой экономики существенно возрастают риски, связанные с организацией бизнес-процессов в организациях. Объектами риск-менеджмента при этом выступают производственные логистические системы, системы взаимодействия с клиентами, в том числе в сфере финансовых транзакций. В этой связи проблема информационной безопасности является значимой для всех хозяйствующих субъектов и выступает одним из направлений повышения уровня экономической безопасности. Сложная геополитическая обстановка также оказывает негативное воздействие на финансово-хозяйственную деятельность российских компаний, что повышает требования к обеспечению их экономической безопасности в целом, и информационной, в частности. В представленной статье выявляются тренды угроз информационной безопасности для компаний в нашей стране, исследуются конкретные ситуации, обусловившие возникновение экономического ущерба для компаний, проводится анализ причин технических сбоев, приведших к финансовому ущербу, вырабатываются направления по повышению уровня информационной безопасности хозяйствующих субъектов. Проведенный анализ, построенный на применении метода контекст-анализа, позволяет выявить зависимость между уровнем информационной безопасности и финансово-экономическим положением компаний. Полученные в результате исследования выводы позволяют выявить «слабые места» в процессе построения системы информационной безопасности компаний, а также определить место и роль риск-менеджмента для информационных систем в контексте достижения экономической безопасности хозяйствующих субъектов. Разработанные мероприятия, направленные на повышение уровня информационной безопасности, существенно расширяют управленческие практики риск-менеджмента российских компаний и формируют устойчивые предпосылки для совершенствования уровня экономической безопасности.

Ключевые слова

информационная безопасность, финансовая устойчивость, риск-менеджмент, экономический ущерб

UDC 65.011.56: 338.14

RISK MANAGEMENT OF THE INFORMATION COMPONENT OF ECONOMIC SECURITY OF BUSINESS ENTITIES

Olga Vladimirovna KUCHINA[1], Candidate of Economic Sciences, Associate Professor
Marina Ivanovna BARABANOVA[2], Candidate of Economic Sciences, Associate Professor

[1]Faculty of Economics and Finance of the Russian Presidential Academy of National Economy and Public Administration, St. Petersburg, Russian Federation

[2]Autonomous Nonprofit Organization of Higher Education «International Banking Institute named after A. Sobchak», St. Petersburg, Russia

Address for correspondence: M.I. Barabanova, 191023, Saint-Petersburg, Nevsky pr., 60

Abstract

In the context of the digital economy development, the risks associated with the organization of business processes in organizations increase significantly. The objects of risk management are production logistics systems, customer interaction systems, including in the field of financial transactions. In this regard, the problem of information security is significant for all economic entities and is one of the areas for increasing the level of economic security. The difficult geopolitical situation also has a negative impact on the financial and economic activities of Russian companies, which increases the requirements for ensuring their economic security in general, and information security in particular. The presented article identifies trends in information security threats for companies in our country, examines specific situations characterizing the economic damage of companies, formulates the causes of technical failures that led to financial damage, and develops directions for increasing the level of information security of business entities. The analysis, based on the use of the context analysis method, allows us to identify the relationship between the causes of information security threats and the financial and economic situation. The conclusions obtained as a result of the study make it possible to identify “weak points” in the process of building an information security system for companies, as well as to determine the place and role of risk management for information systems in the context of achieving the economic security of business entities. The developed directions aimed at increasing the level of information security significantly expand the risk management practices of Russian companies and form stable prerequisites for improving the parameters of economic security.

Keywords

information security, financial stability, risk-management, economic damage

Введение. В современных условиях трансформации мирового геополитического состояния особое значение для развития социально-экономической системы Российской Федерации играет обеспечение экономической безопасности страны. Основные нормативно-правовые положения данного понятия заложены в Стратегии экономической безопасности Российской Федерации. Согласно данному документу, «…экономическая безопасность – это состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации»[35]. Достижение данной цели предполагает создание условий для комплексного развития элементов народно-хозяйственной системы как в части развития инструментов поддержки предпринимательской активности, так и укрепления социально-политических институтов.

В научной литературе дефиниция «экономическая безопасность» предполагает различные подходы, ориентированные на отдельные ключевые цели и задачи. Так, Золаев Э.А. определяет «…экономическую безопасность как процесс поддержания и развития экономики, направленный на обеспечение экономического роста при укреплении суверенитета, а также сохранение устойчивости к внешним и внутренним угрозам при повышении условий и качества жизни населения» [1]. При этом в качестве ключевого инструмента достижения экономической безопасности выделяется управленческий аспект, предполагающий рассмотрение исследуемой дефиниции как процессного, а не статичного явления. Нярginен В.А. предполагает, что «…экономическая безопасность может быть рассмотрена как универсальная категория, проявляющая свое действие как на макро-, так и на микроуровнях…» [2]. Соответственно, цели и задачи достижения высоких параметров исследуемой категории предполагают единую концепцию. При этом инструментарий достижения экономической безопасности должен быть дифференцирован с учетом специфики объекта управления. Кроме этого, экономическую безопасность необходимо рассматривать в качестве комплекса мероприятий, реализуемых в интересах всех стейкхолдеров (клиентов, контрагентов, органов государственной власти, общества в целом).

[35] Указ Президента РФ от 13.05.2017 N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» https://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 14.07.2024).

На уровне хозяйствующих субъектов достижение экономической безопасности осуществляется в рамках построения эффективной системы управления бизнес-процессами компаний. С позиции данной точки исследования, Геиева Е.А. и Дадаева Д.М. определяют экономическую безопасность как «…наличие состояния финансово-экономической защищенности важнейших интересов, влияющих на реализацию бизнес-процессов предприятия, а также комплекс мер, направленных на отражение возникновения угроз и рисков внешнего и внутреннего характера, возникающие в ходе реализации ее операционной, финансовой и инвестиционной деятельности» [3]. Соответственно, основой для достижения экономической безопасности является разработка управленческих решений, направленных на мониторинг «слабых мест» при организации всех элементов производственного процесса в организации.

С позиции государственного управления решающую роль в повышении уровня экономической безопасности играет разработка механизмов, направленных на создание условий для достижения всеми элементами социально-экономической системы возможностей для постоянного развития и совершенствования. Достижение данной цели предполагает создание условий для эффективного контроля возможных рисков и создания инструментария для управления ими, что требует реализации комплекса организационно-правовых и экономических мероприятий.

В целом, управление рисками представляет собой «…систему управления организацией, ориентированную на предотвращение рисков либо снижение негативного воздействия от их наступления» [4]. Выбор метода оценки и способа по нивелированию угроз основывается, в первую очередь, на определении природы конкретного риска. Соответственно, первым шагом при организации риск-менеджмента является идентификация риска и его дифференциация с позиции классификационной группы. При этом каждый вид риска должен быть дифференцирован по вероятности возникновения, размеру ожидаемого ущерба и специфики компании [5].

Наиболее распространенной в настоящее время является классификация, согласно которой риск подразделяются по двум признакам:

1) по длительности воздействия: стратегические и операционные;

2) по природе ущерба: финансовые, технологические и юридические [6].

Соответственно, процесс управления рисками выступает составным элементом планирования в организации, построенного для различных временных и предметных параметров. Так, процесс построения эффективной

стратегии предполагает оценку внешних и внутренних факторов развития организации, а также мониторинг угроз и возможностей для каждой группы. Jose Marquez-Tejon разработал модель управления рисками, интегрированную в общую стратегию управления компанией [7]. Она предполагает использование разработанного автором программного решения, позволяющего обеспечивать организационную устойчивость компании. Данный подход позволяет на стадии операционного управления выработать управленческие решения для всех управляемых подсистем организации и, в целом, повысить уровень экономической безопасности. Отметим, что отсутствие достоверной и полной информации о наличии рисковых факторов негативно отражается на достижении стратегических целей организации и преломляется на уровне реализации отдельных операционных целей в принимаемые управленческие решения, дифференцированные по различным направлениям деятельности и бизнес-процессам. Так, в условиях цифровой экономики важнейшее значение приобретает необходимость защиты авторских прав на применяемые в компании технологические решения. Нарушения нормативно-правовых положений в этом направлении может привести к значительным финансовым потерям, а также замедлению темпов технологического развития компании.

В дополнение к приведенной классификации отдельно отметим такой вид риска как репутационный, который может выступать в качестве подвида или составного элемента всех вышеперечисленных видов рисков. В результате возникновения рисковой ситуации в компании нарушается стабильность организации бизнес-процессов, снижается экономическая эффективность деятельности. При этом негативный эффект может носить пролонгированный характер и обуславливать возникновение кризиса в экономическом положении компании в стратегической перспективе, обусловленный снижением доверия контрагентов и клиентов компании.

Построение системы информационной безопасности в целях достижения экономической устойчивости компании основывается на проведении оценки рисков, выявлении наиболее значимых угроз и разработки инструментов по снижению вероятности наступления и размера ущерба. Важным направлением достижения поставленной цели выступает исследование возможностей для развития уровня технологической безопасности. Так, Воронкова О.В. и Семенова Ю.Е. рассматривают понятие «экономическая безопасность» с позиции оценки угроз и возможностей развития технологического суверенитета

и перехода на импортозамещение [8]. Докунина А.А. и Кутайцева О.Н. исследует взаимосвязь цифровой трансформации и повышения информационной и технологической безопасности компаний [9, 10], выделяя в качестве объекта исследования информационные системы хозяйствующих субъектов. В результате исследований данные авторы приходят к выводу о необходимости развития инструментария риск-менеджмента с целью сокращения размера финансовых потерь, а также интенсивного перехода на цифровизацию бизнес-процессов организации.

Важным элементом достижения целей экономической безопасности является соблюдение принципов информационной безопасности, предусматривающие реализацию доступности всех элементов, целостность и конфиденциальность используемых информационных технологий. Реализация первых двух принципов обеспечивается применением современных аппаратных и программных решений, а также привлечением квалифицированного персонала как в части информационно-технологического обеспечения, так и задействованных при реализации основных бизнес-процессов компании. Наиболее значимой в позиции риск-менеджмента является задача обеспечения конфиденциальности данных компании, что при расширении инфраструктуры цифровой экономики является предполагает использование комплексного подхода к построению всех информационных процессов. Несоблюдение принципов информационной безопасности приводит к возникновению репутационных рисков, обуславливающих финансовые потери компании.

Авторами J.Wenjin [11], L. Hadlington, S. Chivers [12] были проведены исследования, в котором авторы раскрывают сущность дефиниции «информационная безопасность», основываясь на существующей нормативной базе, практике применения в различных управленческих системах, а также выявляют стейкхолдеров обеспечения информационной безопасности на предприятии. I. Halima и I. Shareeful сконцентрировались в исследовании на способах оценки внешних рисков, оказывающих наиболее значимое влияние на бизнес-процессы компании. В результате была разработана методика оценки вероятности возникновения финансового риска, построенная на использовании технологии машинного обучения [13]. Согласно данному подходу, использование искусственного интеллекта позволит снизить количество кибератак на бизнес-процессы компании и повысит уровень информационной безопасности.

Таким образом, в современных условиях разработка стратегии информационной безопасности является неотъемлемым элементом построения

эффективной управленческой системы, способствующей достижения экономической безопасности компании.

Цель и задачи исследования. Цель исследования заключается в выявлении взаимосвязи использования инструментов нивелирования рисков информационной безопасности и обеспечения экономической безопасности хозяйствующих субъектов. Для достижения данной цели в исследовании будут выявлены основные тенденции в области информационной безопасности в компаниях Российской Федерации, проведен анализ кейсов, выявлены причины возникновения финансовых рисков в результате нарушения принципов информационной безопасности, определены дальнейшие направления совершенствования инструментов риск-менеджмента в целях обеспечения экономической безопасности.

Материалы, методы и объекты исследования. Экономическая безопасность хозяйствующих субъектов является основой для формирования устойчивости экономической системы страны в целом. В условиях цифровизации социально-экономической системы неотъемлемым элементом экономической безопасности выступает информационная, предполагающая создание системы эффективного построения бизнес-процессов как внутри организации, так и в целях взаимодействия со всеми стейкхолдерами (органами государственной власти, контрагентами, клиентами). Объектом исследования будут выступать средние и крупные предприятия Российской Федерации, финансово-хозяйственная деятельность которых испытывала негативные воздействия, вызванные нарушением принципов информационной безопасности, в первую очередь, конфиденциальности. Методами исследования являются синтез и анализ, обобщение, контент-анализ. Материалами для исследования выступили статьи в периодических печатных и онлайн изданиях, тематические блоги, данные официальной статистики и органов государственной власти.

В качестве определения «информационная безопасность» будем рассматривать «…состояние информационной системы, при котором она наименее восприимчива к несанкционированному доступу и нанесению ущерба со стороны третьих лиц» [14]. Обеспечение данного состояния информационной системы предполагает постоянное проведение риск-менеджмента, объектом которого выступают как аппаратные, так и программные решения. Информационная безопасность бизнес-процессов позволяет создавать условия для устойчивого развития финансово-экономических параметров хозяйствующих субъектов. Соответственно, при осуществлении управления

рисками необходимо осуществлять мониторинг внешних факторов, и проводить анализ внутреннего потенциала компании, формирующего условия для обеспечения устойчивости информационной системы к негативным внешним воздействиям. В качестве объекта мониторинга должны рассматриваться информационные системы компаний, обеспечивающие реализацию технологического процесса. Необходимо постоянно проводить анализ используемых программных решений, оптимизирующих бизнес-процессы в организации, включая взаимодействие с клиентами и органами государственной власти, а также внутренние локальные системы.

В практике риск-менеджмента одним из методов оценки является метод построения «дерева отказов», предполагающий оценку возникновения различных видов рисков на каждом этапе осуществления производственного процесса. Соответственно, для каждого этапа проводится идентификация риска, оценка вероятности его возникновения и ожидаемый ущерб, и далее разрабатываются мероприятия по снижения как вероятности, так и размера ожидаемого риска. Применительно к процессу риск-менеджмента в целях обеспечения экономической безопасности алгоритм проведения оценки включает в себя следующие этапы:

1. Разработка перечня параметров экономической безопасности для предприятия.
2. Оценка «разрыва» фактических и плановых значений параметров экономической безопасности.
3. Выявление показателей информационной безопасности, влияющих на достижение параметров экономической безопасности.
4. Идентификация факторов внешней среды, оказывающих негативное воздействие на достижение плановых значений показателей информационной безопасности.
5. Оценка вероятности возникновения негативных факторов внешней среды и размера предполагаемого ущерба.
6. Идентификация факторов внутренней среды, негативно влияющих на достижение плановых значений информационной безопасности.
7. Оценка вероятности возникновения негативных факторов внутренней среды и размера предполагаемого ущерба
8. Разработка сценариев по повышению уровня информационной безопасности компании на основе результатов анализа внешних и внутренних угроз.
9. Разработка программ ресурсного обеспечения сценариев.

10. Оценка и выбор наиболее оптимального управленческого решения по повышению уровня информационной безопасности.
11. Реализация выбранного управленческого решения и оценка степени достижения плановых показателей информационной безопасности по итогам отчетного периода.
12. Оценка параметров экономической безопасности, основанных на достижении плановых значений параметров информационной безопасности, по итогам отчетного периода.
13. Внесение изменений в стратегические программы по развитию уровня информационной безопасности на предприятии с учетом результатов реализации программ на шаге 11 и 12.

Нарушение основных принципов информационной безопасности вызывает возникновение прямого финансового ущерба для компаний, а получение репутационного риска, действие которого также имеет отрицательный финансовый эффект. По итогам 2023 года в Российской Федерации ущерб от киберпреступлений составил 156 млрд руб., в то время как объем отечественного рынка информационной безопасности – 145 млрд руб. [15]. Киберпреступления и защита от них представляют собой постоянный итерационный процесс, нацеленный на разработку новых способов защиты информационной системы компаний. Соответственно, процедура риск-менеджмента в части обеспечения информационной безопасности должна быть нацелена на совершенствование программных и аппаратных средств защиты основных бизнес-процессов компании.

В период с 01.03.2024 по 15.07.2024 был проведен опрос среди специалистов по кибербезопасности средних и крупных компаний с целью выявления причин несанкционированного доступа к информационной системе и вероятности появления технических сбоев (рисунок 1).

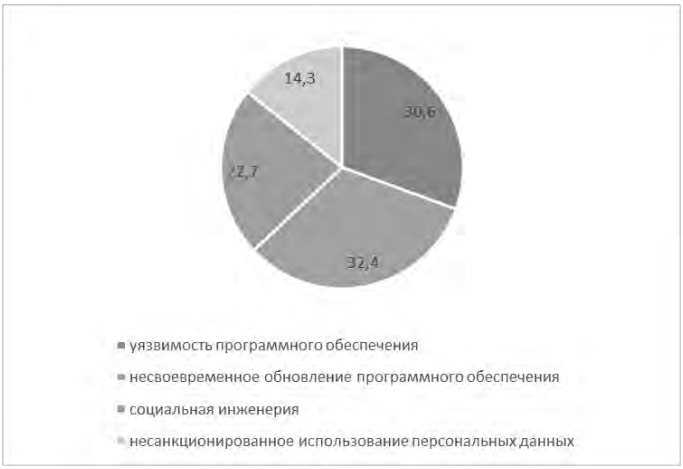

Рисунок 1 – Причины технических сбоев в хозяйственной деятельности
Источник: составлено авторами

Как следует из результатов опроса, практически равное значение имеют все представленные причины. При этом общим триггером для возникновения негативной ситуации в осуществлении бизнес-процессов является наличие некомпетентных и/или несоблюдающих этические нормы компании сотрудников. С точки зрения риск-менеджмента важное значение имеет постоянный мониторинг профессиональных и личных качеств работников, предполагающий весь комплекс управления трудовыми ресурсами, включая мотивацию, продвижение, повышение квалификации, онбординг и рекрутинг. Безусловно, данное направление эффективно только для одновременного обновления программных и аппаратных средств защиты информационной системы компаний

Результаты исследования. Рассмотрим наиболее значимые проблемы в обеспечении информационной безопасности, произошедшие за последние несколько лет в российских компаниях, результаты анализа представим в таблице 1.

30 января 2024 года в сегменте российских DNS-серверов наблюдался сбой, продолжавшийся в среднем 3 часа, затронувший практически всю страну. В наибольшей степени ареал технического сбоя наблюдался в Москве, Санкт-Петербурге, Московской и Ленинградской областях, республике Татарстан, Свердловской области. В первую очередь, объектами негативного воздействия выступили маркетплейсы, банки, поисковая система Яндекс. Основной причиной данной ситуации являлось неиспользование национальной системы

доменных имен, рекомендованной Министерством цифрового развития Российской Федерации. Совокупный ущерб хозяйствующих субъектов еще продолжает оцениваться, однако промежуточные результаты уже свидетельствуют о превышении ущербом порога в несколько десятков миллиардов рублей.

Яркий пример негативного внешнего воздействия в форме хакерской атаки демонстрирует кейс компании СДЭК – крупнейшего игрока на рынке коммерческих перевозок и почтовых отправлений. 26 мая 2024 года в результате несанкционированного доступа к базам данных компании, параметры логистической системы компании были изменены или удалены, что привело к невозможности осуществления предпринимательской деятельности. Период вынужденного простоя составил несколько дней, что привело к финансовому ущербу, превышающему полумиллиарда рублей. Между тем, одной из основных причин, не позволивших компании в короткие сроки противодействовать внешнему воздействию, являлось отсутствие своевременности в проведении backup – процедуры резервного копирования, позволяющего сохранять промежуточные результаты предпринимательской деятельности в части работы с клиентами.

Летом 2023 года компания Инфотел, предоставляющая услуги по организации взаимодействия между Центральным банком Российской Федерации и кредитно-финансовыми организациями, а также крупными юридическими лицами, была подвергнута хакерской атаке для уничтожения возможности осуществлять финансовые транзакции компаний-партнеров провайдера. Информация о размере ущерба ни компанией Инфотел, ни ее партнерами не раскрывается, однако с учетом количества участников рынка, подключенных к автоматизированной системе электронного взаимодействия (АСЭВ), обоснованно предполагать ущерб в несколько сот миллиардов рублей.

Таблица 1 – Характеристика нарушений информационной безопасности

Наименование компании	Дата события	Внешний триггер технического сбоя	Приблизительный размер ущерба	Внутренняя уязвимость
Сбермаркет	30.01.202024	Нарушение работы DNS-серверов	1 – 1,5 млрд. руб.	Неготовность системных администраторов компаний своевременно перейти на использование НСДИ (национальная

				система доменных имен)
СДЭК	26-28 мая 2024	Хакерская атака на логистическую систему	300 млн-1 млрд руб.	Несоблюдение требований к созданию резервного копирования информации (бекапов).
АО Инфотел	Июнь 2023	Частичное разрушение информационной инфраструктуры в результате хакерской атаки	н/д	Отсутствие средств киберзащиты для предотвращения атак с помощью технологий социальной инженерии

Согласно данным компании InfoWatch, в 2023 г. наблюдалось увеличение количества персональных данных, подвергнутых несанкционированному доступу, на 60% по сравнению с 2022 годом. Отчасти это связано с развитием цифровой экономики и концентрацией личной информации клиентов в базах данных маркетплейсов, агрегаторов и иных участников рынка цифровых продуктов. Данное положение накладывает дополнительные обязательства на пользователей баз персональных данных по соблюдению их конфиденциальности, в том числе в рамках Федерального закона «О персональных данных» (ФЗ-152). По итогам 2023 года, согласно информации Роскомнадзора, общий размер штрафов за утечку персональных данных составил более 5,0 млн. рублей. Данный объем средств взыскан с компаний в результате рассмотрения дел об утечке персональных данных в судах, однако судебные решения выносятся менее чем в половине случаев нарушения ФЗ-152. Отметим, что максимальный размер штрафа за утечку персональных данных, произведенной без злого умысла, составляет 100 000 рублей, что значительно снижает мотивацию коммерческих компаний и государственных структур к развитию мер противодействия данному вида правонарушений. Несанкционированное использование персональных данных клиентов и/или сотрудников компании зачастую используется злоумышленниками совместно с технологией социальной инженерии. Соответственно, мероприятия по нивелированию данных угроз должны предполагать решения, позволяющие комплексно выявленные проблемы.

Выводы. Проведенный анализ наиболее значимых событий в экономической системе, обусловленных нарушением информационной

безопасности в российских компаниях за последние два года, свидетельствует о наличии четкой взаимосвязи между уровнем информационной безопасности компаний и состоянием их финансово-хозяйственной устойчивости. Отметим, что данная проблема актуальна для хозяйствующих субъектов во всех странах. Так, 19 июля 2024 года произошел технический сбой из-за некорректного обновления одного из компонентов корпоративного антивирусного модуля (системы EDR), который повлек за собой полную остановку критически важных систем и отказу в работе авиакомпаний, аэропортов и иных компаний, осуществляющих предпринимательскую деятельность на платформе Microsoft Windows, по всему миру. Одной из основных причин инцидента является некорректная работа продукта компании CrowdStrike, партнера Microsoft по предоставлению услуг по кибербезопасности. Сбой продолжался в течение 8 часов, и ущерб составляет более 1 млрд. долларов. Отметим, что компании, осуществляющие бизнес-процессы на операционных системах Linux и Mac, не затронула данная проблема, – соответственно, крупнейшие российские компании смогли избежать технического сбоя. Сама компания CrowdStrike после масштабного сбоя понесла существенные финансовые убытки: так, ее капитализация после 19.07.2024 снизилась с 100 до 75 млрд. долларов, а компания–партнер Microsoft потеряла 70 млрд. долларов по данному показателю оценки стоимости компании. Отметим, что ущерб основан на расчете прямых финансовых потерь, без оценки размера репутационного риска.

В целом, решение проблемы информационной безопасности предполагает создание условий, нацеленных на развитие инструментов, способных нивелировать негативное воздействие внешних вызовов, и повысить уровень информационной безопасности хозяйствующих субъектов. Магистральными направлениями являются:

- переход на отечественное программное обеспечение, снижающее степень вовлеченности в мировые информационные системы;
- использование концепции «открытого программного обеспечения», позволяющей расширить возможности для внедрения современных информационных технологий без необходимости постоянного взаимодействия с монополистами на рынке программного обеспечения, и возможности постоянного совершенствования продукта;
- создание условий для привлечения высококвалифицированных специалистов в сферу информационной безопасности Российской Федерации;

– расширение финансирования комплексных программных и аппаратных решений, нацеленных на интеграцию всех участников цифровой экономики, включая органы государственной власти и кредитно-финансовые институты.

Данные мероприятия необходимо внедрять как на уровне государственного управления, так и в рамках стратегического развития хозяйствующих субъектов. При этом основополагающей управленческой задачей является интеграция мероприятий по проведению риск-менеджмента в стратегические планы компании. Разработка детализированных программ информационной безопасности позволит компаниям повысить уровень экономической устойчивости и сформировать предпосылки для повышения эффективности финансово-хозяйственной деятельности.

Список источников

1. **Золаев Э.А.** Экономическая безопасность государства: понятие и угрозы цифровизации // Экономическая безопасность. 2022. Том 5. № 2. С. 571-582.
2. **Няргинен В.А., Кучина А.А, Кучина Е.И.** Экономическая безопасность предприятий как фактор обеспечения экономической стабильности // вектор экономики. 2021. № 12 (66). С. 132-137.
3. **Геиева Л.А., Дадаева Д.М.** Экономическая безопасность предприятия как источник защиты от воздействия негативных факторов // Актуальные вопросы современной экономики. 2021. №11. С. 618-626.
4. **Солодимова Г.А., Мешалкина Н.Н.** Риск-менеджмент как инструмент повышения конкурентоспособности предприятия // Модели, системы, сети в экономике, технике, природе и обществе. 2017. №3. С. 90-96.
5. **Rausand M., Haugen S.** Risk Assessment: Theory, Methods, and Applications. L.: John Wiley & Sons, 2020. 762 p.
6. **Соколов Д.В.** Классификация рисков, как многозадачный инструмент риск-менеджмента организаций // Управление экономическими системами: электронный научный журнал. 2011. URL: https://cyberleninka.ru/article/n/klassifikatsiya-riskov-kak-mnogozadachnyy-instrument-risk-menedzhmenta-organizatsiy. (дата обращения: 11.06.2024).
7. **Marquez-Tejon J.** Integrated security management model: a proposal applied to organisational resilience // Security Journal. 2023. Vol. 37. P.375-398.
8. **Voronkova O.V., Semenova Y.E.** Economic security in the context of import substitution and the presence of foreign companies in the Russian market // Components of scientific and technological progress. 2021. № 8 (62). С. 20-24.
9. **Докунина А.А.** Экономическая безопасность предприятий в фокусе задач управления в условиях цифровой трансформации. М.: Российской экономический университет им. Г.В. Плеханова, 2024. 160 с.

10. **Кутайцева О.Н., Толмачева И.В., Толмачева А.А., Фишер В.И.** Цифровая экономика и экономическая безопасность // Экономика и бизнес: теория и практика. 2023. № 5-2 (99). С. 68-71.
11. **Wenjin J.** Security and privacy of digital economic risk assessment system based on cloud computing and blockchain // Neural Networks. 2024. Vol. 28. P.2753–2768.URL: https://www.researchgate.net/publication/377302942_Security_and_privacy_of_digital_economic_risk_assessment_system_based_on_cloud_computing_and_blockchain (дата обращения: 12.07.2024).
12. **Hadlington L., Chivers S.** Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors in Policing // Journal of Policy and Practice. 2020. Vol. 14. Issue 2. P.479–492. URL: https://doi.org/10.1093/police/pay027 (дата обращения: 10.07.2024).
13. **Halima I., Shareeful I.** An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing and Applications. 2022. Vol. 34. P. 15241-15271.
14. **Кравченко Г., Антышева Е.** Классификация рисков и угроз компании // SWorldJournal. 2018. № 5. URL: https://www.researchgate.net/publication/356196277_KLASSIFIKACIA_RISKOV_I_UGROZ_KOMPANII (дата обращения 01.07.2024).
15. **Королев П.А.** Ущерб от киберпреступлений в России превысил объем рынка информационной безопасности // Новости цифровой трансформации, телекоммуникаций, вещания и ИТ-Comnews. URL: https://www.comnews.ru/content/233687/2024-06-11/2024-w24/1008/uscherb-kiberprestupleniy-rossii-prevysil-obem-rynka-informacionnoy-bezopasnosti (дата обращения: 15.07.2024).

References

1. **Zolayev E.A.** Ekonomicheskaya bezopasnost' gosudarstva: ponyatiye i ugrozy tsifrovizatsii // Ekonomicheskaya bezopasnost'. 2022. Tom 5. № 2. S. 571-582.
2. **Nyarginen V.A., Kuchina A.A, Kuchina Ye.I.** Ekonomicheskaya bezopasnost' predpriyatiy kak faktor obespecheniya ekonomicheskoy stabil'nosti // vektor ekonomiki. 2021. № 12 (66). S. 132-137.
3. **Geiyeva L.A., Dadayeva D.M.** Ekonomicheskaya bezopasnost' predpriyatiya kak istochnik zashchity ot vozdeystviya negativnykh faktorov // Aktual'nyye voprosy sovremennoy ekonomiki. 2021. №11. S. 618-626.
4. **Solodimova G.A., Meshalkina N.N.** Risk-menedzhment kak instrument povysheniya konkurentosposobnosti predpriyatiya // Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve. 2017. №3. S. 90-96.
5. **Rausand M., Haugen S.** Risk Assessment: Theory, Methods, and Applications. L.: John Wiley & Sons, 2020. 762 p.
6. **Sokolov D.V.** Klassifikatsiya riskov, kak mnogozadachnyy instrument risk-menedzhmenta organizatsiy // Upravleniye ekonomicheskimi sistemami:

elektronnyy nauchnyy zhurnal. 2011. URL: https://cyberleninka.ru/article/n/klassifikatsiya-riskov-kak-mnogozadachnyy-instrument-risk-menedzhmenta-organizatsiy. (data obrashcheniya: 11.06.2024).
7. **Marquez-Tejon J.** Integrated security management model: a proposal applied to organisational resilience // Security Journal. 2023. Vol. 37. P.375-398.
8. **Voronkova O.V., Semenova Y.E.** Economic security in the context of import substitution and the presence of foreign companies in the Russian market // Components of scientific and technological progress. 2021. № 8 (62). S. 20-24.
9. **Dokunina A.A.** Ekonomicheskaya bezopasnost' predpriyatiy v fokuse zadach upravleniya v usloviyakh tsifrovoy transformatsii. M.: Rossiyskoy ekonomicheskiy universitet im. G.V. Plekhanova, 2024. 160 s.
10. **Kutaytseva O.N., Tolmacheva I.V., Tolmacheva A.A., Fisher V.I.** Tsifrovaya ekonomika i ekonomicheskaya bezopasnost' // Ekonomika i biznes: teoriya i praktika. 2023. № 5-2 (99). S. 68-71.
11. **Wenjin J.** Security and privacy of digital economic risk assessment system based on cloud computing and blockchain // Neural Networks. 2024. Vol. 28. P.2753–2768.URL: https://www.researchgate.net/publication/377302942_Security_and_privacy_of_digital_economic_risk_assessment_system_based_on_cloud_computing_and_blockchain (data obrashcheniya: 12.07.2024).
12. **Hadlington L., Chivers S.** Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors in Policing // Journal of Policy and Practice. 2020. Vol. 14. Issue 2. P.479–492. URL: https://doi.org/10.1093/police/pay027 (data obrashcheniya: 10.07.2024).
13. **Halima I., Shareeful I.** An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing and Applications. 2022. Vol. 34. P. 15241-15271.
14. **Kravchenko G., Antysheva Ye.** Klassifikatsiya riskov i ugroz kompanii // SWorldJournal. 2018. № 5. URL: https://www.researchgate.net/publication/356196277_KLASSIFIKACIA_RISKOV_I_UGROZ_KOMPANII (data obrashcheniya 01.07.2024).
15. **Korolev P.A.** Ushcherb ot kiberprestupleniy v Rossii prevysil ob"yem rynka informatsionnoy bezopasnosti // Novosti tsifrovoy transformatsii, telekommunikatsiy, veshchaniya i IT-Comnews. URL: https://www.comnews.ru/content/233687/2024-06-11/2024-w24/1008/uscherb-kiberprestupleniy-rossii-prevysil-obem-rynka-informacionnoy-bezopasnosti (data obrashcheniya: 15.07.2024).