УДК 338: 65.011.46 JEL C83, D81, O21 DOI: https://doi.org/10.26425/2309-3633-2023-11-4-110-118
Получено: 18.09.2023 Статья доработана после рецензирования: 23.10.2023 Принято: 30.10.2023

Затраты и выгоды информационной безопасности бизнеса

Козырь Наталья Сергеевна
Канд. экон. наук, доц. каф. кибербезопасности и защиты информации
ORCID: 0000-0002-8323-0957, e-mail: n_k_@mail.ru

Кубанский государственный технологический университет, 350072, Московская ул., 2, г. Краснодар, Россия

Аннотация

В статье рассмотрен процесс обеспечения информационной безопасности с позиции оценки затрат и выгод, что позволяет понять экономические аспекты технико-экономического обоснования мероприятий в области защиты информации бизнеса. В практике российского бизнеса вопросы обеспечения информационной безопасности сфокусированы на соблюдении нормативных требований законодательства. Это приводит к тому, что хозяйствующие субъекты пренебрегают процедурой комплексной оценки эффективности мероприятий, которые должны учитывать затраты и выгоды реализации правового, организационного и технического обеспечения защиты информации. Вместе с этим для соответствия новым условиям технологического развития общества требуются пересмотр концепции защиты информации хозяйствующих субъектов и закрепление в политике информационной безопасности деятельности подходов к оценке риска на основе стоимости активов. Исследование содержит описание подхода «затраты/выгоды» по составным компонентам процесса обеспечения информационной безопасности бизнеса. Для понимания экономических аспектов обеспечения защиты информации представленное исследование фокусирует свое внимание на хозяйствующих субъектах рыночного типа хозяйствования (предприятие в своей деятельности получает прибыль). Определен состав компонентов процесса обеспечения информационной безопасности. На примере риск-менеджмента подробно рассмотрены затраты и выгоды информационной безопасности.

Ключевые слова: информационная безопасность, экономика защиты информации, экономика информационной безопасности, затраты ИБ, выгоды ИБ, экономическая безопасность, бюджет информационной безопасности, экономика кибербезопасности

Для цитирования: Козырь Н.С. Затраты и выгоды информационной безопасности бизнеса//Управление. 2023. Т. 11. № 4. С. 110–118. DOI: 10.26425/2309-3633-2023-11-4-110-118

Received: 18.09.2023 Revised: 23.10.2023 Accepted: 30.10.2023

Costs and benefits of business information security

Natalia S. Kozyr

Cand. Sci. (Econ.), Assoc. Prof. at the Cybersecurity and Information Protection Department

ORCID: 0000-0002-8323-0957, e-mail: n_k_@mail.ru

Kuban State Technological University, 2, Moskovskaya ul., Krasnodar 350072, Russia

Abstract

The article considers the process of information security from the position of cost-benefit assessment that allows to understand economic aspects of feasibility study of measures in the field of business information protection. In the practice of Russian business, the issues of information security are focused on compliance with regulatory requirements of the legislation. This leads to the fact that business entities neglect the procedure of comprehensive assessment of measures effectiveness that should consider the costs and benefits of legal, organizational, and technical information protection implementation. At the same time, in order to meet the new conditions of technological development of society, it is necessary to revise the concept of information protection of business entities and to fix in the policy of information security of activities the approaches to risk assessment based on assets value. The study contains a description of the cost/benefit approach to the constituent components of ensuring information security of business process. To understand the economic aspects of information security, the research focuses on business entities of the market type of economic activity (the enterprise makes profit in its activity). The composition of components of the ensuring information security process has been defined. On the example of risk management costs and benefits of information security have been considered in detail.

Keywords: information security, information security economics, information security economics, information security costs, information security benefits, economic security, information security budget, cybersecurity economics

For citation: Kozyr N.S. (2023) Costs and benefits of business information security. *Upravlenie / Management (Russia)*, 11 (4), pp. 110–118. DOI: 10.26425/2309-3633-2023-11-4-110-118

Введение / Introduction

Экономика информационной безопасности является важным аспектом в деятельности любой организации и сопровождается высокими расходами и затраты на защиту информации в структуре бюджета компаний каждый год увеличиваются[1]. Вместе с этим в средствах массовой информации не публикуется структура бюджета – организации называют лишь число кратного увеличения расходов в отношении бюджета информационной безопасности предыдущего года[2].

В практике российского бизнеса сформировался подход, основанный на соблюдении нормативных требований законодательства в сфере защиты информации без расчета экономической эффективности расходов на организационное и техническое обеспечение информационной безопасности хозяйствующего субъекта. В связи с этим наблюдается парадокс: с одной стороны, экономика и информационная безопасность неразрывно связаны (о чем свидетельствуют ежегодные сводки убытков бизнеса от хищения данных злоумышленниками), а с другой – отсутствует методическое обеспечение по расчету экономического обоснования и оценки эффективности мероприятий по защите информации. Такая ситуация обусловлена тем, что экономика защиты информации является междисциплинарной областью исследования, поэтому тема выпала из предмета исследования российских экономистов по причине необходимости глубокого понимания организационных и технических средств защиты информации.

Наряду с этим ученые в сфере технических наук изучают методы организационной и технической защиты информации, а специалисты информационной безопасности сосредоточены на обеспечении защиты данных на основе общего бюджета без углубления в вопросы эффективности процесса. Тема методического обеспечения экономики защиты информации охватывает большой масштаб вопросов, так как ежегодно на законодательном уровне увеличиваются требования к критически значимым субъектам бизнеса, для выполнения которых необходимы ресурсы, в том числе денежные. Таким образом, экономика информационной безопасности –актуальная тема для изучения как для экономистов, так и для специалистов информационной безопасности. В представленном исследовании рассмотрены аспекты защиты информации на основе затрат и выгод в разрезе ключевых компонентов информационной безопасности бизнеса.

Теория и методы исследования / Theory and research methods

В зарубежных публикациях экономика защиты информации рассматривается с различных аспектов на протяжении долгого периода времени:

1) изучается экономический анализ решений информационной безопасности в связи с необходимостью выполнения обязательных стандартов безопасности [Gao и др., 2022];

2) ведется поиск решений в вопросе инвестиций в экономическую безопасность с учетом бюджетных ограничений [Huang, Behara, 2013];

3) исследуется необходимость выделения бюджета на обучение сотрудников организации мерам информационной безопасности [Beautement, Sasse, 2009].

Российские научные статьи лишь в единичном случае содержат информацию о структуре затрат на информационную безопасность и вопросах проектного управления защиты информации [Петренко, 2006; Оганесян, Козырь, 2023]. Имеется определенный научный задел в сфере информационной безопасности бизнеса: рассмотрены вопросы обеспечения развития цифровой экономики, что опосредованно влияет на информационную безопасность бизнеса, сформирован состав факторов, представляющих собой угрозу информационной безопасности российской экономики [Барейко, Кожухина, 2019; Леднева, 2022]. В публикации С.М. Бычковой и Н.Н. Макаровой обоснована необходимость комплексного взгляда на экономическую безопасность бизнеса с учетом факторов информационной безопасности сетевого взаимодействия субъектов [Бычкова, Макарова, 2022]. На уровне микроэкономики затронуты аспекты угроз информационной безопасности с позиции обеспечения экономической безопасности бизнеса, описан механизм выявления угроз экономической безопасности цифрового предприятия [Барейко, Кожухина, 2019; Кулагина и др., 2020].

В исследованиях также присутствуют методы риск-менеджмента информационной безопасности бизнеса в реализации системы закупок предприятия, и рассмотрена цифровая трансформация как новый вызов в части обеспечения защиты информации хозяйствующего субъекта, где дается описание составных компонентов модели информационной

[1] Интерфакс. Опрос показал, что российский бизнес увеличит на 14 % расходы на кибербезопасность. Режим доступа: https://www.interfax.ru/russia/885667 (дата обращения: 10.09.2023).

[2] ТАСС. Вице-президент VK: бюджет на информационную безопасность в 2023 году увеличится в 2,5 раза. Режим доступа: https://tass.ru/interviews/16690609 (дата обращения: 10.09.2023).

безопасности бизнеса [Созаева, 2021; Королев, Гаврилов, 2019].

Тема экономических исследований в обеспечении информационной безопасности бизнеса имеет большой потенциал на стыке междисциплинарных исследований с применением методов искусственного интеллекта [Седых, Фоканов, 2022; Частикова, Шелудько, 2022]. Вопросы обеспечения информационной безопасности должны рассматриваться комплексно на всех уровнях киберпространства с учетом особенностей региональных рынков Российской Федерации (далее – РФ, Россия) и соответствующим ресурсным обеспечением и эффективностью мероприятий [Путято, Макарян, 2020; Суслов и др., 2015; Третьякова, 2022; Кривошлыков и др., 2016].

В работе используются следующие общенаучные методы: формулирование исследовательского вопроса, обзор литературы, изучение предмета исследования, сбор данных, научный анализ, синтез и представление результата. Частные методы: использование принципов стоимостного анализа «затраты/выгоды».

Обеспечение информационной безопасности бизнеса: общее понимание процесса / Ensuring business information security: a common understanding of the process

Обеспечение информационной безопасности бизнеса в общем смысле сосредоточено на устранении рисков и уязвимостей, связанных с хранением, передачей и обработкой цифровых и физических информационных активов. Эти активы могут включать данные клиентов, финансовые отчеты, интеллектуальную собственность, персональные данные, конфиденциальную информацию, служебную или коммерческую тайну. Концептуально процесс обеспечения защиты информации состоит из семи блоков:

1) оценка, анализ, управление рисками;

2) стандарты, политики и процедуры безопасности;

3) контроль доступа и аутентификация;

4) защита данных и шифрование (криптография);

5) мониторинг информационной безопасности и реагирование на инциденты;

6) соблюдение требований законодательства;

7) осведомленность сотрудников и обучение.

Оценка рисков включает выявление и анализ потенциальных угроз информационным активам, таких как несанкционированный доступ к информации со стороны хакеров, утечка данных, инсайдерские угрозы, физическое хищение информационных источников или чрезвычайные обстоятельства, включая форс-мажоры и стихийные бедствия.

Разработка и внедрение политик, руководящих принципов и процедур относится к формированию локальных нормативных актов в области информационной безопасности организации. Уровень, количество и детализация локальных нормативных актов зависит от масштаба бизнеса, вместе с этим политика информационной безопасности является базовым документом для любой организации.

Контроль доступа и аутентификация включают внедрение механизмов, гарантирующих, что только авторизованные лица могут получить доступ к конфиденциальной информации. Это может включать такие технологии, как надежные пароли, многофакторная аутентификация, списки контроля доступа и его средства на основе ролей. В любом случае контроль доступа и аутентификация – неотъемлемая часть системы обеспечения информационной безопасности любого бизнеса.

Защита данных и шифрование (криптография) помогают предотвратить несанкционированный доступ или перехват информации, гарантируя, что даже в случае компрометации данных они останутся защищенными от злоумышленников. Независимо от масштаба бизнеса любая организация в своей деятельности имеет дело с персональными данными, которые должны быть надежно защищены.

Мониторинг информационной безопасности и реагирование на инциденты – постоянно осуществляемые действия в рамках комплексного обеспечения защиты информации хозяйствующего субъекта. Успешность реализации этого блока одновременно включает в себя использование технических средств защиты и обеспеченность организации квалифицированными кадрами.

Соблюдение требований законодательства – обязательные для исполнения нормативно-правовые требования, которые контролируются соответствующими регуляторами в сфере информационной безопасности. Объем организационных мероприятий коррелирует с блоком «стандарты, политики и процедуры безопасности» и зависит от масштаба бизнеса и отраслевой принадлежности.

Осведомленность сотрудников и обучение – неотъемлемый блок, решающий в том числе задачу соответствия нормам законодательства, которое за последние пять лет существенно повысило требования к информационной безопасности бизнеса. Повышение осведомленности и обучение сотрудников являются неотъемлемым и процессами для всех блоков обеспечения информационной безопасности.

В настоящем исследовании не делается акцент на детализации нормативно-правовой среды и структуре контролирующих органов, проверяющих соблюдение обязательных мероприятий по обеспечению информационной безопасности бизнеса. Описание составных блоков процесса защиты информации приведено с целью формирования общей модели организации, которая включает экономические аспекты обеспечения информационной безопасности бизнеса. Эта компонентная структура далее рассмотрена с точки зрения «затраты/выгоды» реализации мероприятий по обеспечению информационной безопасности бизнеса.

В практике бизнеса информационная безопасность не содержит в своем понимании экономического эффекта, несмотря на существующие формулы эффективности, где полученную выгоду следует разделить на понесенные затраты. Вместе с этим при обосновании бюджета информационной безопасности ведется калькуляция расходов и указывается сумма потенциальных выгод, которая носит условный характер. Обоснование экономической выгоды от мероприятий по обеспечению информационной безопасности является непростой задачей, так как информационная безопасность не приносит прибыли бизнесу, но обеспечивает непрерывность его существования. В связи с этим потенциальная выгода – это перспектива сохранения непрерывности деятельности хозяйствующего субъекта. В организациях рыночного принципа хозяйствования, деятельность которых сопровождается получением прибыли, расходы на обеспечение информационной безопасности не должны превышать потенциальные выгоды. Другими словами, бюджет на информационную безопасность лимитирован экономическими возможностями организации. Для понимания экономических аспектов обеспечения информационной безопасности бизнеса представленное исследование фокусирует свое внимание на хозяйствующих субъектах рыночного типа хозяйствования.

Затраты и выгоды риск-менеджмента информационной безопасности / Costs and benefits of information security risk management

Обзор прямых и косвенных затрат на обеспечение информационной безопасности сделан на примере первого компонента (блока) информационной безопасности – «оценка, анализ, управление рисками». С экономической точки зрения в процессе оценки, анализа и управления рисками возникают как прямые, так и косвенные затраты (табл. 1). Оценка выгод содержит прямые и потенциальные (косвенные) преимущества, которые может получить хозяйствующий субъект в результате реализации мероприятий по обеспечению информационной безопасности в сфере управления рисками.

Таблица 1

Затраты и выгоды процесса «оценка, анализ, управление рисками»

Table 1. Costs/benefits of the Information Security Risk Analysis process

	Перечень затрат	Перечень выгод
Прямые	• расходы на персонал; • инструменты и программное обеспечение; • сбор и анализ данных; • внешняя экспертиза; • обучение и сертификация	• идентификация рисков и определение приоритетов; • принятие обоснованных решений; • снижение финансовых потерь; • соблюдение нормативно-правовых требований; • диверсификация ресурсов
Косвенные	• время и усилия на осмысление задач; • простои и сбои в работе; • альтернативные издержки; • затраты на устранение; • риск деловой репутации	• улучшенная система безопасности; • доверие заинтересованных сторон; • непрерывность бизнеса; • защита репутации; • непрерывное совершенствование

Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

При рассмотрении последующих компонентов будет использован другой принцип, который лучше описывает «затраты/выгоды»: при анализе затрат и выгод будут учитываться только прямые издержки и выгоды. Такой подход обусловлен тем, что перечень косвенных расходов в большей степени совпадает для всех компонентов и может быть бесконечно расширен, а характер выгод несет в себе лишь потенциальные перспективы независимо от их категории и также имеет высокий уровень схожести.

Безусловные прямые затраты включают расходы на персонал, что является постоянной статьей расходов в процессе обеспечения информационной безопасности бизнеса. Сюда относятся заработная плата как сотрудников организации, в чьи должностные обязанности входит оценка рисков, так и привлеченных специалистов (если процесс передан на аутсорсинг). Для оценки рисков часто требуются специализированные программные продукты для сбора и анализа данных, оценки уязвимостей и составления отчетов. Расходы могут включать лицензионные сборы, подписку или расходы на техническое обслуживание.

Сбор соответствующих данных, проведение интервью или опросов, анализ информации для выявления потенциальных рисков – все это связано с прямыми расходами в виде оплаты труда специалистов. В состав затрат по сбору и анализу данных могут входить расходы, связанные с командировочными расходами для полевых исследований или

закупкой программного обеспечения для анализа данных. В некоторых случаях организациям может потребоваться привлечь внешних экспертов или консультантов, обладающих специализированными знаниями или сертификатами, для проведения оценки рисков.

Обучение и сертификация – это неотъемлемая статья расходов, так как сотрудники службы информационной безопасности должны иметь соответствующий уровень образования и квалификации, а при необходимости должны быть отправлены на программы повышения квалификации или профессиональной переподготовки кадров. Затраты включают стоимость обучения, учебных материалов и сопутствующих платежей (регистрационные или экзаменационные сборы).

Косвенные затраты одинаково относятся ко всем блокам информационной безопасности. Так, время и усилия подразумевают временной лаг, который является важной частью процесса осмысления и подготовки к выполнению поставленных задач. Это включает планирование и подготовку, сбор данных, анализ и составление отчетов, что влечет за собой снижение производительности или потребность в дополнительных ресурсах для решения вопросов, которые связаны с отвлечением кадрового потенциала от основных обязанностей.

Следующий аспект затрат – возможные простои или сбои в производственном процессе. При проведении оценки рисков может возникнуть необходимость временно приостановить определенные бизнес-процессы или услуги для облегчения сбора или анализа данных.

Инвестирование ресурсов в мероприятия по оценке рисков означает отвлечение этих ресурсов от других потенциальных проектов или инициатив. Это может привести к альтернативным издержкам, когда организация отказывается от потенциальных выгод или приносящих доход видов деятельности, чтобы расставить приоритеты в усилиях по оценке рисков. Затраты на устранение возникают в случаях выявления недостатков в средствах контроля рисков системы. В этом случае появляются дополнительные расходы, связанные с внедрением необходимых мер по снижению рисков.

Риск деловой репутации возникает в случаях выявления значительных уязвимостей в системе информационной безопасности организации, которые могут привести к потере доверия клиентов и потенциальным юридическим последствиям (штрафы, возмещение убытков). Возникает уже совсем другой аспект информационной безопасности – этика ведения бизнеса, так как в мировой практике нередко возникают случаи сокрытия информации о выявленных рисках, а впоследствии случившиеся инциденты становятся достоянием средств массовой информации.

Следует отметить, что конкретные затраты, связанные с оценкой рисков, могут варьироваться в зависимости от таких факторов, как размер и сложность организации, отраслевая принадлежность, объем оценки, требуемый уровень контроля и нормативно-правовые требования регуляторов. Например, исполнение Федерального Закона «О защите персональных данных» одинаково распространяется на все хозяйствующие субъекты и требует обеспечения соответствующего уровня защиты, и в этом случае не может возникать вопрос «затраты/выгоды». При этом, выполняя требования Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК) в части обеспечения защиты информации, многие организации минимизируют оценку рисков до перечня угроз, определенных в соответствии с методикой органа. Однако это уже другие вопросы, которые не входят в состав задач представленного исследования.

В целом описание прямых и косвенных затрат позволяет сделать денежную оценку (например, по факту калькуляции издержек). Напротив, любая финансовая оценка потенциальных выгод является субъективной, так как денежная премия исключена в контексте обеспечения информационной безопасности бизнеса. Так, идентификация рисков и определение приоритетов позволяют аккумулировать ресурсы на решение целевых задач. Здесь и далее под выгодами понимается возможность экономии ресурсов без денежных поступлений от внедрения мероприятий по устранению риска. Оценка потенциальной выгоды должна производиться экспертным методом, который подразумевает наличие квалифицированных кадров в составе комиссии, оценочные критерии и протоколирование коэффициентов значимости.

В принятии обоснованных решений следует понимать, что риск-менеджмент является составным компонентом общей системы внутреннего контроля и не могут риски информационной безопасности рассматриваться самостоятельно. В принятии обоснованных решений речь идет о том, что следует учитывать влияние угроз информационной безопасности на бизнес, делать осознанный выбор и расставлять приоритеты в ресурсах на основе уровня риска информационной безопасности.

Выявляя и оценивая риски, организации могут внедрять меры по минимизации рисков, которые снижают вероятность и потенциальное воздействие неблагоприятных событий. Потенциальная выгода может измеряться в виде сохранения существующих

функций бизнес-процессов организации. Выявление и устранение потенциальных рисков помогает избежать штрафных санкций или последствий, возникающих в результате несоблюдения требований законодательства.

Диверсификация ресурсов – это потенциальная выгода от высвобождения расходов на информационную безопасность из тех сфер, в которых уровень обеспечения защиты информации уже высокий. Понимая риски и их потенциальное воздействие, организации могут расставлять приоритеты при распределении ресурсов в областях, требующих наибольшего внимания, гарантируя, что они используются там, где наиболее необходимы.

Косвенные выгоды от внедрения риск-менеджмента организации одинаковы для всех блоков обеспечения информационной безопасности бизнеса:

1) общее улучшение системы безопасности;
2) доверие заинтересованных сторон;
3) обеспечение непрерывности бизнеса;
4) защита репутации;
5) непрерывное совершенствование.

Финансовая оценка выгод от внедрения мероприятий по информационной безопасности всегда является актуальной темой для организаций. Реализация мероприятий по обеспечению информационной безопасности бизнеса включает оценку экономической целесообразности проекта. Вместе с этим расчет потенциальных выгод в денежном эквиваленте будет субъективным, и он будет зависеть от особенностей функционирования хозяйствующего субъекта.

Систематизация «затраты/выгоды» обеспечения информационной безопасности / Systematization of information security costs/ benefits

На примере риск-менеджмента описан принцип затрат и потенциальных выгод. Управление рисками является постоянным процессом системы менеджмента информационной безопасности и подразумевает наличие сотрудников, отвечающих за этот процесс. В табл. 2 представлен свод «затраты/выгоды» по всем блокам информационной безопасности бизнеса.

Таблица 2

Затраты/выгоды процесса обеспечения информационной безопасности

Table 2. Costs/benefits of the information security protection process

Блоки ИБ	Перечень затрат	Перечень выгод
Оценка, анализ, управление рисками	– расходы на инструменты и технологии оценки рисков; – выделение ресурсов для проведения регулярных оценок рисков; – время и усилия, необходимые для выявления и анализа потенциальных рисков	– улучшенное понимание структуры рисков организации; – выявление уязвимостей и областей, требующих улучшения; – обоснованное принятие решений по обеспечению информационной безопасности
Стандарты, политики и процедуры безопасности	– разработка и документирование политик и процедур безопасности; – ресурсы, необходимые для распространения информации и обеспечения соблюдения политик; – регулярное обновление политик в соответствии с нормативными требованиями	– четкие рекомендации для сотрудников по приемлемому использованию информационных ресурсов; – последовательные методы обеспечения безопасности во всей организации; – соблюдение отраслевых норм и требований законодательства
Контроль доступа и аутентификация	– внедрение и техническое обслуживание механизмов контроля доступа; – инвестиции в технологии аутентификации (например, биометрические данные, токены); – обучение сотрудников правильному использованию систем контроля доступа	– снижается риск несанкционированного доступа к конфиденциальной информации; – защита от инсайдерских угроз и несанкционированного доступа к данным; – подотчетность и отслеживаемость доступа к критически важным системам и данным
Защита данных и шифрование (криптография)	– внедрение технологий шифрования и управление ими; – ресурсы для управления ключами шифрования; – дополнительные ресурсы на аппаратное и программное обеспечение (процессы шифрования снижают производительность автоматизированных систем)	– защита конфиденциальных данных от несанкционированного доступа или перехвата; – соблюдение правил защиты данных и отраслевых стандартов; – повышение доверия со стороны клиентов и деловых партнеров
Соблюдение требований законодательства	– ресурсы, посвященные мониторингу нормативных актов; – внедрение средств контроля и мер по соблюдению требований комплаенса; – возможные штрафы за несоблюдение требований	– снижение юридических и финансовых рисков, связанных с несоблюдением требований; – повышение доверия и репутации среди клиентов и заинтересованных сторон; – улучшенные методы защиты данных и конфиденциальности

Окончание табл. 1

Блоки ИБ	Перечень затрат	Перечень выгод
Осведомленность сотрудников и обучение	– разработка и предоставление учебных материалов, курсов и семинаров; – выделение ресурсов для организации тренингов и программ повышения осведомленности; – время и усилия для постоянного обучения и укрепления сотрудников	– формирование корпоративной культуры информационной безопасности; – улучшенная способность выявлять угрозы безопасности и реагировать на них; – снижение вероятности инцидентов, связанных с социальной инженерией

Примечание: ИБ – информационная безопасность

Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

Следует отметить, что экономическая эффективность – неотъемлемая часть любого проекта и мероприятия по обеспечению информационной безопасности не являются исключением. В представленном исследовании показано, что оценка потенциальной выгоды от мероприятий по информационной безопасности является субъективной, так как включает ряд нематериальных компонентов (увеличение доверия клиентов, уменьшение риска потери данных, сокращение времени простоя системы). Вместе с этим составление детализированного перечня затрат и выгод является необходимой процедурой в планировании бюджета организации и подразумевает обоснование затрат, связанных с внедрением средств контроля информационной безопасности. Обоснование бюджета основывается на сравнении затрат по обеспечению защиты информации с потенциальными выгодами от мероприятий, что позволяет оценить эффективность системы информационной безопасности.

Заключение / Conclusion

Затраты на информационную безопасность могут включать расходы на приобретение и обновление программного обеспечения, обеспечение безопасных сетевых соединений, криптографические средства обеспечения безопасности, обучение персонала и аудит безопасности информационных систем. Оценка выгод информационной безопасности может включать защиту от потери конкурентных преимуществ, увеличение уровня доверия и уважения со стороны клиентов, улучшение репутации компании, снижение рисков в случае нарушения безопасности и снижение потерь при инцидентах информационной безопасности.

Следует отметить потенциал для дальнейших исследований в сфере экономики защиты информации, так как современная действительность бизнеса чаще обусловлена выполнением нормативных требований регуляторов рынка без учета потенциальных выгод от инвестиций в информационную безопасность. В связи с этим выгоды от обеспечения информационной безопасности бизнеса – это дальнейший ориентир для формирования культуры информационной безопасности и повышения уровня организационного развития.

Список литературы

Барейко С. Н., Кожухина К. А. Экономическая и информационная безопасность России в условиях цифровой экономики. Наука Красноярья. 2019;5(8):7–18. https://doi.org/10.12731/2070-7568-2019-5-7-18

Бычкова С.М., Макарова Н.Н. Анализ информационной безопасности в контексте системы экономической безопасности сетевого взаимодействия субъектов. ЭТАП: экономическая теория, анализ, практика. 2022;4:86–98. https://doi.org/10.24412/2071-6435-2022-4-86-98

Королев В.И., Гаврилов В.Е. Информационные системы цифровой экономики и подходы к обеспечению их информационной безопасности. Системы высокой доступности. 2019;1(15):38–46. DOI https://doi.org/10.18127/j20729472-201901-05

References

Bareiko S.N., Kozhukhina K.A. Economic and information security of Russia in the digital economy. Science of Krasnoyarsk. 2019;5(8):7–18. https://doi.org/10.12731/2070-7568-2019-5-7-18 (In Russian).

Beautement A., Sasse A. The economics of user effort in information security. Computer Fraud & Security. 2009;10:8–12.

Bychkova S.M., Makarova N.N. Analysis of information security in the context of the economic security system of network interaction of subjects. ETAP: Economic Theory, Analysis, Practice. 2022;4:86–98. https://doi.org/10.24412/2071-6435-2022-4-86-98 (In Russian).

Chastikova V.A., Sheludko M.A. Implementation of an expert system to identify current threats to the security of enterprise

Кривошлыков В.С., Жахов Н.В., Фомичева Л.М. Управление угрозами экономической безопасности: обзор теоретических концепций. Вестник Курской государственной сельскохозяйственной академии. 2016;9:69–74.

Кулагина Н.А., Чепикова Е.М., Мугутдинов Р.М. Механизм выявления угроз экономической безопасности цифрового предприятия в инновационных условиях ведения бизнеса. Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2022;1(12):115–126. https://doi.org/10.21869/2223-1552-2022-12-1-115-126

Леднева О.В. Развитие цифровой экономической трансформации в аспекте кибербезопасности и конфиденциальности пользователей России. Вопросы инновационной экономики. 2022;1(12):81–94. https://doi.org/10.18334/vinec.12.1.114255

Оганесян Л.Л., Козырь Н.С. Проектное управление в информационной безопасности. Вестник Академии знаний. 2023;4(57):207–209.

Петренко С.А. Оценка затрат на кибербезопасность. Труды Института системного анализа Российской академии наук. 2006;27:234–265.

Путято М.М., Макарян А.С. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства. Прикаспийский журнал: управление и высокие технологии. 2020;3(51):94–102. https://doi.org/10.21672/2074-1707.2020.51.1.094-102

Седых Н.В., Фоканов И.П. Проблемы и перспективы развития технологии искусственного интеллекта. Естественно-гуманитарные исследования. 2022;44(6):266–267.

Созаева Д.А. Внедрение риск ориентированного управления регулируемыми закупками. Проблемы теории и практики управления. 2021;9:33–47. https://doi.org/DOI 10.46486/0234-4505-2021-9-33-47

Суслов С.А. Роль информационных технологий в повышении конкурентоспособности региональных рынков. Дискуссия. 2015;8(60):45–49.

Третьякова С.Н. ESG-повестка устойчивого развития в условиях новых российских реалий. Экономика: теория и практика. 2022;2(66):36–41. https://doi.org/10.31429/22240 42X_2022_66_36

Частикова В. А., Шелудько М. А. Реализация экспертной системы для определения актуальных угроз безопасности информации предприятий. Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022;3:80–89.

Gao X., Gong S., Wang, Y., Wang X., Qiu M. An economic analysis of information security decisions with mandatory security standards in resource sharing environments. Expert Systems with Applications. 2022;206:117894.

Beautement A., Sasse A. The economics of user effort in information security. Computer Fraud & Security. 2009;10:8–12.

Huang C.D., Behara R.S. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics. 2012;1(141):255–268.

information. Scientific works of KubSTU. 2022;3:80–89. (In Russian).

Gao X., Gong S., Wang, Y., Wang X., Qiu M. An economic analysis of information security decisions with mandatory security standards in resource sharing environments. Expert Systems with Applications. 2022;206:117894.

Huang C.D., Behara R.S. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics. 2012;1(141):255–268.

Korolev V.I., Gavrilov V.E. Information systems of the digital economy and approaches to ensuring their information security. High Availability Systems. 2019;1(15):38–46. DOI https://doi.org/10.18127/j20729472-201901-05

Krivoshlykov V.S., Zhakhov N.V., Fomicheva L.M. Managing threats to economic security: a review of theoretical concepts. Bulletin of the Kursk State Agricultural Academy. 2016;9:69–74. (In Russian).

Kulagina N.A., Chepikova E.M., Mugutdinov R.M. Mechanism for identifying threats to the economic security of a digital enterprise in an innovative business environment. Proceedings of the Southwestern State University. Series: Economics. Sociology. Management, 2022;1(12):115–126. https://doi.org/10.21869/2223-1552-2022-12-1-115-126 (In Russian).

Ledneva O.V. Development of digital economic transformation in the aspect of cybersecurity and privacy of Russian users. Issues of innovative economy. 2022;1(12):81–94. https://doi.org/10.18334/vinec.12.1.114255 (In Russian).

Oganesyan L.L., Kozyr N.S. Project management in information security. Bulletin of the Academy of Knowledge. 2023;4(57):207–209. (In Russian).

Petrenko S.A. Assessment of cybersecurity costs. Proceedings of the Institute of System Analysis of the Russian Academy of Sciences. 2006;27:234–265. (In Russian).

Putyato M.M., Makaryan A.S. Cybersecurity as an integral attribute of multilevel protected cyberspace. Caspian Journal: Management and High Technologies. 2020;3(51):94–102. https://doi.org/10.21672/2074-1707.2020.51.1.094-102 (In Russian).

Sedykh N.V., Focanov I.P. Problems and prospects of artificial intelligence technology development. Natural sciences and humanities research. 2022;44(6):266–267. (In Russian).

Sozaeva D.A. Introduction of risk-oriented management of regulated purchases. Problems of theory and practice of management. 2021;9:33–47. https://doi.org/DOI 10.46486/0234-4505-2021-9-33-47 (In Russian).

Suslov S.A. The role of information technologies in increasing the competitiveness of regional markets. Discussion. 2015;8(60):45–49. (In Russian).

Tretyakova S.N. ESG-agenda of sustainable development in the conditions of new Russian realities. Economics: Theory and Practice. 2022;2(66):36–41. https://doi.org/10.31429/22240 42X_2022_66_36 (In Russian).