DOI: 10.37791/2687-0657-2025-19-2-108-120

Влияние информационной безопасности на устойчивое развитие бизнеса

Т.П. Горелова[1*]

[1]*Финансовый университет при Правительстве Российской Федерации, Москва, Россия*

[*]*tamara.gorelova2013@gmail.com*

Аннотация. Цифровая трансформация, переход компаний на дистанционную форму работы, формирование новых бизнес-моделей и развитие цифровизации в последние несколько лет установили сложную и быстроменяющуюся среду для функционирования бизнеса. Научной новизной статьи является модифицирующаяся роль информационной безопасности для бизнеса. Информационную безопасность для устойчивого развития бизнеса необходимо рассматривать как стратегическую бизнес-единицу с конкретной инновационной программой, отображенной в корпоративной стратегии развития компании. В исследовании отмечено, что на сегодняшний день бизнесу недостаточно иметь программное обеспечение для информационной безопасности, важно информационную безопасность рассматривать комплексно с проработкой процессов, решений, процедур и формированием локальных актов. Представлены выводы по каждому фактору, влияющему на эффективное развитие бизнеса. Выявлена необходимость совершенствования нормативно-правовой сферы в области информационной безопасности и представлено обоснование важности поддержки внедрения российских технологических решений наряду с возрастающей ролью информационной безопасности в деятельности компании. В условиях цифровизации информационная безопасность бизнеса является основой защиты коммерческих данных компании и сохранения конкурентоспособности на рынке. Обосновано, что российский рынок информационной безопасности и российский бизнес активно и динамично развиваются, а дальнейшее развитие бизнеса зависит от его устойчивости к кибератакам. Обоснованно доказывается, что информационная безопасность бизнеса в условиях цифровизации представляет собой основное условие успеха всей коммерческой деятельности. Теоретическая и практическая значимость исследования заключается во влиянии рассмотрения факторов информационной безопасности на устойчивое развитие бизнеса без привязки к сфере деятельности и показано, что учет обозначенных факторов необходим как для малого, так и крупного бизнеса. Показана динамика совершенствования нормативно-правовых документов в сфере информационной безопасности, выявлено влияние нормативно-терминологического аппарата информационной безопасности на выработку бизнес-решений в условиях цифровизации.

Ключевые слова: информационная безопасность бизнеса, решения по информационной безопасности, защита данных бизнеса, управление изменениями, информационно-аналитическое управление, формирование бизнес-решений в условиях цифровизации

Для цитирования: *Горелова Т.П.* Влияние информационной безопасности на устойчивое развитие бизнеса // Современная конкуренция. 2025. Т. 19. №2. С. 108–120. DOI: 10.37791/2687-0657-2025-19-2-108-120

The Impact of Information Security on Sustainable Business Development

T. Gorelova[1*]

[1]*Financial University under the Government Russian Federation, Moscow, Russia*

[*]*tamara.gorelova2013@gmail.com*

Abstract. Digital transformation, the transition of companies to a remote form of work, the formation of new business models and the development of digitalization over the past few years have established a complex and rapidly changing business environment. The scientific novelty of the article is the modifying role of information security for business. Information security for sustainable business development should be considered as a strategic business unit with a specific innovation program reflected in the corporate development strategy of the company. The study noted that today it is not enough for a business to have software for information security, it is important to consider information security comprehensively with the elaboration of processes, solutions, procedures and the creature of local acts. The conclusions on each factor influencing effective business development are presented. The necessity of improving the regulatory and legal sphere in the field of information security is identified and the rationale for the importance of supporting the implementation of Russian technological solutions along with the increasing role of information security in the company's activities is presented. In the context of digitalization, business information security is the basis for protecting the company's commercial data and maintaining competitiveness in the market. It is proved that the Russian information security market and Russian business are actively and dynamically developing, and the further development of the business depends on its resistance to cyberattacks. It is reasonably proved that business information security in the context of digitalization is the main condition for the success of all commercial activities. The theoretical and practical significance of the study lies in the influence of the consideration of information security factors on the sustainable development of business without reference to the field of activity and it is shown that taking into account these factors is necessary for both small and large businesses. The dynamics of improving regulatory and legal documents in the field of information security is shown, the influence of the normative and terminological apparatus of information security on the development of business solutions in the context of digitalization is revealed.

Keywords: business information security, information security solutions, business data protection, change management, information and analytical management, formation of business solutions in the context of digitalization

For citation: Gorelova T. The Impact of Information Security on Sustainable Business Development. *Sovremennaya konkurentsiya*=Journal of Modern Competition, 2025, vol.19, no.2, pp.108-120 (in Russian). DOI: 10.37791/2687-0657-2025-19-2-108-120

Введение

Достижение технологического лидерства России в условиях формирования глобального цифрового пространства и стратегическое участие государства в создании новой глобальной экономической экосистемы зависит от грамотно выстроенной системы защиты национальной безопасности в информационной среде. В процессе становления информационного общества и перехода к цифровой экономике возрастает спектр вопросов, требующих решений в области информационной безопасности (далее – ИБ).

Последние несколько лет для российского бизнеса условия неопределенности стали нормой для ведения деловой активности. Можно считать, что бизнес уже адаптировался к изменчивым обстоятельствам в логистике, финансовой политике, решении вопросов по импортозамещению, повышенному уровню риска инвестирования и переходу со стратегического планирования на краткосрочное.

В условиях пандемии COVID-19 в сочетании с масштабным процессом цифровизации бизнес, вне зависимости от своего масштаба, за несколько лет прошел цифровую трансформацию. Решение бизнес-задач с применением искусственного интеллекта, машинного обучения, предиктивной аналитики, Интернета вещей способствовали формированию ИТ-инфраструктуры. Вопросы защиты информации стали активно подниматься с 2020 г., и на сегодняшний день их важность только усиливается. В 2021 г. объем мирового рынка ИБ, согласно оценке компании MarketsandMarkets, составлял 217,9 млрд долл.[1], хотя компания Fortune Business Insights[2] дала более скромную оценку в 139,77 млрд долл. Объем российского рынка ИБ в это же время составил 125,1 млрд руб.[3], показав позитивный рост в 16%, что объясняется рядом факторов: пандемия, переход компаний на дистанционную форму работы, формирование новых бизнес-моделей и развитие цифровизации.

Информационная безопасность (распространенное сокращение – InfoSec) – это набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения. К области InfoSec относится безопасность физических объектов и сред, управление доступом и кибербезопасность[4].

Информационная безопасность бизнеса

За сравнительно короткий период времени активное внедрение информационных технологий во все сферы деятельности человека стало началом эпохи цифровой трансформации. Тренд цифровой трансформации выражается в полном изменении привычных информационных процессов, протекающих в организации [5, 9, 15]. Появились не просто новые способы связи и обмена информацией, а технологии, влияющие на решения в ИТ-сфере, а именно

[1] Эксперты: кибербезопасность является наиболее перспективной отраслью для инвестиций // ТАСС. 10.12.2021. URL: https://tass.ru/ekonomika/13173195 (дата обращения: 09.09.2023).

[2] Оценка потенциала российских решений в области кибербезопасности на международном рынке // ЦСР. Сентябрь 2022. URL: https://www.csr.ru/upload/iblock/a6d/h9lkrjgaawtho0hg7sy7ofgur7p9anx1.pdf (дата обращения: 13.11.2023).

[3] На российском рынке ИБ взрывной рост // CNews. 05.10.2022. URL: https://www.cnews.ru/news/top/2022-10-05_laboratoriya_kasperskogo (дата обращения: 25.10.2023).

[4] Что такое информационная безопасность (InfoSec)? // Майкрософт. URL: https://clck.ru/3LdP7m (дата обращения: 21.10.2023).

«сквозные» цифровые технологии и технологии индустрии 4.0, способствующие экономическому прорыву, конкурентоспособности организации и ее информационно-экономической безопасности. В таблице 1 приведены определения, показывающие,

Таблица 1. Трактовка понятия «информационная безопасность бизнеса»

Table 1. Interpretation of the concept of “business information security”

Организация – источник определения ***The organization is the source of the definition***	**Определение** ***Definition***	**Краткая характеристика определения** ***Brief description of the definition***
Облачные решения МТС для создания и развития цифровых продуктов	Информационная безопасность бизнеса	Комплекс организационных и технических мер, которые направлены на защиту и сохранение информации, систем и оборудования, использующихся для взаимодействия, хранения и передачи этой информации. Чем эффективнее обеспечивается информационная безопасность, тем лучше защищены данные компании от разнообразных воздействий. Они могут быть внутренними или внешними, случайными или преднамеренными[1]
Traffic Inspector Next Generation	Информационная безопасность предприятия	Комплекс мер организационного и технического характера, направленных на сохранение и защиту информации и ее ключевых элементов, а также оборудование и системы, которые используются для работы с информацией, ее хранения и передачи. Этот комплекс включает технологии, стандарты и методы управления информацией, которые обеспечивают ее эффективную защиту[2]
Дом.ru. Бизнес	Информационная безопасность предприятия	Информационная безопасность предприятия – это защита корпоративных файлов, систем, программ и хранилищ от посторонних[3]
Банк ВТБ (ПАО)	Информационная безопасность предприятия	Комплекс мер, которые направлены на сохранение и защиту ключевых элементов данных компании, а также оборудование и программное обеспечение, использующиеся для хранения и передачи информации[4]
Журнал National Businesss	Информационная безопасность бизнеса	Важнейшая составляющая успешного ведения бизнеса[5]
Андрианов В. В. «Обеспечение информационной безопасности бизнеса»	Информационная безопасность организации	Состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере [10]

[1] Информационная безопасность бизнеса: кто угрожает данным компании // МТС. 15.11.2021. URL: https://cloud.mts.ru/cloud-thinking/blog/informacionnaya-bezopasnost-biznesa/ (дата обращения: 15.10.2023).

[2] Информационная безопасность предприятия: ключевые угрозы и средства защиты // Traffic Inspector Next Generation. URL: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/ (дата обращения: 15.10.2023).

[3] Как организовать информационную безопасность в бизнесе // Дом.ru. Бизнес. 29.10.2023. URL: https://moscow.b2b.dom.ru/blog/kak-organizovat-informacionnuyu-bezopasnost (дата обращения: 01.11.2023).

[4] Информационная безопасность: как защитить бизнес // Банк ВТБ (ПАО). URL: https://kdelu.vtb.ru/articles/informaczionnaya-bezopasnost-kak-zashhitit-biznes/ (дата обращения: 15.10.2023).

[5] Зачем вашему бизнесу информационная безопасность? // Nationaly Business. URL: https://nb159.ru/rubric/texnologii/zachem-vashemu-biznesu-informacionnaya-bezopasnost/ (дата обращения: 02.02.2024).

что информационная безопасность на сегодняшний день рассматривается бизнесом не как наличие необходимого программного обеспечения, а как комплекс мер и решений, необходимый для поддержания уровня защиты данных компании.

Наступившая эпоха цифровой трансформации повышает спрос на комплекс организационных и технических мер по защите информации с целью достижения состояния защищенности корпоративных данных организации. Разработки российских ИТ-компаний позволяют российскому бизнесу переключаться с привычных иностранных продуктов и технологий на отечественные, тем самым повышая интерес инвесторов к новым российским продуктам и технологиям и, соответственно, их продвижению и развитию сбыта.

ИБ-решения предприятия с каждым днем становятся всё актуальнее и приобретают более высокую важность. ИБ рассматривают как важную составляющую бюджета ИТ, которая в 2021 г. составляла от 4 до 13% на предприятиях обрабатывающей промышленности, образования и отрасли информационных технологий, предприятий государственного сектора.

Стоит отметить, что, к сожалению, большинство российский решений по информационной безопасности являются аналогами или локализованными версиями зарубежных решений. При этом представленные технологические решения, не имеющие зарубежных аналогов, разработаны для российского государственного сектора с ориентацией на специфику работы органов государственной власти и предприятий Российской Федерации [13, 15]. Следовательно, поднимается вопрос доступности отечественных уникальных технологических решений для малого и среднего бизнеса.

Стратегии развития информационной безопасности в компании вызывают повышенный интерес как ученых, практиков, так и государственных органов. При анализе научных трудов по развитию информационной безопасности бизнеса было выявлено, что развитие ИБ и развитие бизнеса рассматриваются отдельно. ИБ анализируется с позиции технических наук, а развитие бизнеса – с позиции экономики. Так, например, в разных работах авторы рассматривают различные аспекты, а именно проектирование, прогнозирование и разработку сценариев укрепления информационной безопасности организации [6, с. 45–46; 7, с. 3–10; 8, с. 21–25; 14, с. 45–54; 20]; важность формирования комплекса мероприятий по поддержке разработок российских ИТ-компаний с учетом конкурентных преимуществ (человеческий капитал) российских ИТ-компаний [2, с. 251–155; 12, с. 93–94; 13, с. 84–95]; необходимость международной правовой базы и формирование единого понятийного аппарата в сфере информационной безопасности [1, с. 100–102; 11, с. 53–56; 19, с. 267–270]; четкое определение требований к системе управления информационной безопасностью (СУИБ) с позиции международных стандартов в области информационной безопасности (ISO 27000, ISO 27001, ISO 27002) [16, с. 94–98; 17, с. 83–84]. В работе Лиене Крейкберга Лулео представлена интересная точка зрения: «Информационная безопасность – это защита информации и ее критических элементов» [18]. Автор исследования считает необходимым определить факторы ИБ, влияющие на бизнес независимо от его сферы деятельности и форм ведения бизнеса.

Заслуживает внимания работа [3], в которой в полном объеме рассмотрена сущность проблем и решений защиты информации. Отдельный раздел «Основные понятия и определения в области информационной безопасности» включает дополнительные подразделы, в которых понятийный аппарат информационной безопасности рассматривается как научная основа и предметная основа информационной безопасности. Выделен подраздел «Термины, определяющие

характер деятельности по обеспечению информационной безопасности», в котором отмечено, что развитие понятийного аппарата должно иметь правовую поддержку и это является специфической особенностью терминологической системы информационной безопасности. При этом стоит отметить, что при масштабном представлении терминов по трем разным подразделам понятия «информационная безопасность предприятия» или «информационная безопасность бизнеса» не представлены.

Вызывает интерес Практическая энциклопедия «Обеспечение информационной безопасности бизнеса» [10], подготовленная коллективом авторов Финансового университета при Правительстве РФ, Национального исследовательского университета «Высшая школа экономики», ООО «Центр безопасности информации» и Московским педагогическим государственным университетом, изданная в 2005 г. Этот научный труд свидетельствует о том, что данный вопрос не новый, поднимался рядом ученых и на сегодняшний день находится на этапе проработки, что свидетельствует об актуальности рассматриваемого вопроса данного исследования, а именно о возрастающей роли информационной безопасности бизнеса в условиях цифровизации. Объясняется это тем, что с формированием и последующим развитием информационного общества вопросы информационной безопасности поднимались с самого начала появления данного направления. Последние 20 лет наше общество динамично развивалось по спирали: от витка развития «информационное общество» в 2017 г. в соответствии с Национальной программой «Цифровая экономика РФ» мы перешли к цифровизации, а на сегодняшний день мы уже на этапе цифровой трансформации. Безусловно, все эти процессы не могли не сказаться на развитии информационной безопасности. И если раньше при становлении информационного общества вопросы информационной безопасности рассматривались в соответствии с уровнем информационного развития, то на сегодняшний день каждый бизнес и каждый потребитель [4] является частью цифрового общества с наличием конкретного цифрового опыта взаимодействия и с желаемым уровнем безопасности при осуществлении своей жизнедеятельности.

Решение вышеперечисленных задач напрямую влияет на развитие и доступность всех мер по защите информации, поскольку только системный и комплексный подход, включающий организационные и технические процессы, может сформировать ИТ-ландшафт и ИТ-архитектуру для развития и поддержания устойчивой деловой активности бизнеса на российском рынке.

Так, в Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» отсутствует понятие ИБ, хотя в 2020 г. введены понятия «идентификация» и «аутентификация», но не уделено внимания понятию по предотвращению несанкционированного доступа и использования информации.

Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий», введенный в 2007 г., идентичен международному стандарту ИСО/МЭК 13335–1:2004 и в разделе «Термины и определения» в п. 2.14 содержит рассматриваемый термин, который трактуется как все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

В ГОСТ Р ИСО/МЭК 27001–2006, введенном в 2008 г., в разделе «Термины и определения» в п. 3.4 указано, что информационная безопасность – это свойство информации сохранять конфиденциальность, целостность и доступность. К термину дано примечание, что понятие может включать в себя также свойство сохранять аутентичность, подотчетность, неотказуемость и надежность.

Информационная безопасность в Доктрине информационной безопасности РФ рассматривается как информационная безопасность РФ и отдельно выделены понятия «средства обеспечения информационной безопасности» и «система обеспечения информационной безопасности»[1].

Мы считаем, что отсутствие единого нормативно-терминологического аппарата в области информационной безопасности оказывает достаточно сильное влияние на развитие и внедрение бизнес-решений в условиях цифровизации.

В Указе Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» ИБ разбирается как применение принципов и норм международного права и реализация равноправного партнерства в глобальном информационном пространстве с целью поддержание международного мира, безопасности и стабильности.

Изучение нормативно-правовых актов показало, что нормативная база развивается и совершенствуется, но нет единого понятийного аппарата, без которого сложно выстраивать структуру информационной безопасности бизнеса.

Национальные стандарты ФСТЭК России в теоретических разделах определили понятийный аппарат, который по содержанию частично идентичен зарубежному. Стоит отметить, что в нормативных документах Российской Федерации терминология расширяется, дополняется, подкрепляется совершенствованием новых подзаконных актов ФСТЭК, которые регламентируют взаимодействия участников на изменяющемся ландшафте рынка ИБ в России, и, следовательно, с развитием новых форм и технологий развития необходимо совершенствовать и понятийный аппарат с более четкой проработкой и детализацией, который будет соответствовать всем протекающим технологическим процессам.

Результаты

Основными факторами, влияющими на совершенствование информационной безопасности и, соответственно, динамику параметров данного показателя на развитие российского бизнеса, определены:

1. Стандарты и законодательство

За последние 20 лет в связи с глубоким внедрением информационных технологий, развитием науки и практики в области информационной безопасности стандарты по информационной безопасности прошли несколько этапов. На сегодняшний день можно смело говорить о наличии основополагающего, с широким охватом законодательства в области информационной безопасности, заключающегося в национальной стратегии в области ИБ и законах от защиты персональных данных до ведения информационной войны.

Российский рынок информационной безопасности находится в начале своего развития, и процессы или технологии, применяемые в России, только разрабатываются, развиваются и совершенствуются. Среди них стоит отметить подход Agile, решения класса User and Entities Behavior Analysis (анализ поведения пользователей и объектов), аутсорсинг ИБ, облачные сервисы

[1] Доктрина информационной безопасности РФ утверждена Указом Президента РФ от 05.12.2016 № 646.

типа Security as a Service (SECaaS – безопасность как услуга), сервисы Security & Threat Intelligence (интеллектуальные услуги по предотвращению угроз), SIEM-решения (Security Information and Event Management – управление информационной безопасностью и событиями ИБ).

В конце перового полугодия 2021 г. Международным союзом электросвязи (МСЭ) ООН был представлен обновленный Global Cybersecurity Index (GCI) за 2022 г., в котором Россия заняла 5-е место (табл. 2) и по результатам оценки набрала 98,06 балла.

Среди стран СНГ Россия удерживает лидерство. Места первой пятерки распределились следующим образом: 1-е место – Россия, 2-е место – Казахстан, 3-е место – Азербайджан, 4-е место – Узбекистан и 5-е место – Беларусь.

Влияние вышеназванного фактора на бизнес: развитие решений по информационной безопасности напрямую связано со стандартами и законодательством. Следовательно, устойчивое развития бизнеса в условиях цифровизации напрямую зависит от информационной безопасности, развитие которой необходимо осуществлять с учетом результативной зарубежной практики и формирования глобального взаимодействия в сфере борьбы с киберпреступлениями.

2. Неготовность рынка к стандартизации услуг ИБ

Сфера стандартизации – это та область, которая всегда вызывает интерес, споры

Таблица 2. Данные Глобального индекса кибербезопасности на 2020 г.

Table 2. Data from the Global Cybersecurity Index for 2020

Страна ***Country***	***Score***	**Глобальный индекс кибербезопасности на 2020 г.** ***Global Cybersecurity Index for 2020***
ТОП-5		
Соединенные Штаты Америки	100	1
Соединенное Королевство Великобритании	99,54	2
Саудовская Аравия	99,54	2
Эстония	99,48	3
Корея	98,52	4
Сингапур	98,52	4
Испания	98,52	4
Российская Федерация	**98,06**	**5**
Объединенные Арабские Эмираты	98,06	5
Малайзия	98,06	5
Интересующие нас страны, не попавшие в ТОП-5		
Германия	97,41	13
Франция	97,6	9
Китай	92,53	33

Источник: Аналитический отчет «Цифровизация и кибербезопасность» // Экспертно-аналитический центр InfoWatch. 2021. URL: https://media.rbcdn.ru/media/reports/141101.pdf (дата обращения: 30.01.2024).

и требует тщательного продумывания каждого этапа данного процесса. В области информационной безопасности к стандартизации необходимо стремиться, но на сегодняшний день каждая компания самостоятельно определяет методы и технологии защиты, хотя и руководствуется стандартами информационной безопасности. Сложность данного процесса воспринимается как нормальное явление, поскольку бизнесу для решения этой задачи следует ответить на три вопроса: необходимость стандартизации ИБ; бюджет ИБ; окупаемость стандартизации ИБ-проекта.

Влияние данного фактора на бизнес: стандартизация информационной безопасности бизнеса на сегодняшний день невозможна по ряду причин: во-первых, условием реализации бизнеса является цифровизация, кардинальным образом меняющая и создающая новые инструменты, технологии, нивелировать которые можно, если их знать и быть к ним готовыми; во-вторых, опыт работы при низком уровне кибербезопасности заставляет собственников бизнеса самостоятельно искать новые способы информационной защиты для своего бизнеса и недоверчиво относиться к стандартным предложениям.

3. Фундамент информационной безопасности

Рынок информационной безопасности, как и другие рынки и сферы экономики, тесно связан с рынками ИТ-технологий, юридическими и консультационными услугами и находится под влиянием санкций, импортозамещения, меняющих ИТ-архитектуру. На сегодняшний день проблемы функционирования софта выражаются в сочетании наличия хороших софтверных решений и услуг и неразвитой элементной базы, слабой в создании высокопроизводительных аппаратных платформ.

Влияние вышеприведенного фактора на бизнес: информационная безопасность бизнеса, перестраивающаяся под влиянием санкций за период 2014–2023 гг., в сфере информационных технологий должна формироваться на основе концепции защиты и на подходах к информационной безопасности по нивелированию ограничений в сфере ИТ.

4. «Бумажная» безопасность или «фрэймворки»

При рассмотрении вопроса об информационной безопасности прежде всего подразумевается защита информации, киберпреступность, технологии и подходы к защите информационной безопасности. При этом такой важный вопрос, как действующие нормативные документы, регламентирующие данную сферу, не всегда затрагивается и выходит на первый план. Это объясняется тем, что в цифровом мире основная задача – определить эффективный способ и технологии защиты конфиденциальной информации. И когда в бизнесе служба информационной безопасности выстраивает защиту его конфиденциальной информации, то формируется система, которая должна функционировать и соответствовать нормативным правовым актам, организационно-распорядительным документам, нормативным и методическим документам по технической защите информации Федеральной службы по техническому и экспортному контролю России.

К сожалению, требования по защите критически важных объектов[1], закон Яровой, требования Банка России, обеспечение безопасности российского сегмента сети Интернет[2], защита персональных данных, импортозамещение – всё это остается на бумаге, и в реалии имеется недостаточная информационная защищенность компании.

Влияние вышеобозначенного фактора на бизнес: решения в сфере информационной безопасности разрабатываются,

[1] Информационная безопасность (рынок России) // TAdviser. 19.03.2025. URL: https://clck.ru/3LdXXH (дата обращения: 19.11.2023).

[2] Там же.

действуют и реализуются в цифровой среде по управлению цифровыми данными, то есть в форме электронного документа. Но в случае возникновения форс-мажорных обстоятельств, прокурорской проверки или другого надзорного органа бизнесу необходимо иметь действующие регламенты в бумажной форме, что вызывает дополнительные сложности и не может не сказываться на скорости развития данной сферы.

Выводы

Важность взаимосвязи информационной безопасности и бизнеса обусловлена тем, что бизнес, осуществляя цифровую трансформацию, реализовывает трансформацию и своих целей развития. Например, если главная задача компании – получение прибыли, повышение производительности при низких издержках, то поставленные цели с учетом развития цифровых технологий и устойчивости к кибератакам могут выражаться в освоении нового рынка, ниши и создании нового продукта. Следовательно, информационная безопасность позволит бизнесу не только удерживать свою конкурентоспособность на рынке, но и развивать ее, поскольку даст возможность предлагать информационно-защищенный товар или продукт. На сегодняшний день потребителю, осуществляющему выбор и покупку продукта в онлайн-формате, бизнес должен гарантировать безопасность сделки, что является основой успешного взаимодействия.

Несмотря на успех процесса цифровизации и то, что организации уже проходят цифровую трансформацию, не каждый бизнес понимает, что именно информационная безопасность играет ключевую роль в деятельности компании. Некоторые компании к формированию информационной безопасности относятся с повышенной серьезностью, обеспечивая данный вопрос финансовым средствами. К сожалению, только крупные компании могут позволить себе необходимое финансовое обеспечение по данному вопросу. В то же время мелкий и средний бизнес придерживаются классического подхода в создании конкурентоспособности – формирование уникального товарного предложения и не до конца оценивают значение финансовых вложений в формирование и укрепление своей информационной безопасности. Хотя этот факт легко объясняется тем, что крупный бизнес подвергается кибератакам в десятки, а то и сотни раз чаще по сравнению с мелким и средним бизнесом.

При изучении развития бизнеса, как правило, анализируется несколько последних лет – от трех до пяти. Интерес вызывают актуальные и свежие данные, последние достигнутые показатели, отображение уровня развития того или иного процесса, сервиса, доставки, развитие ассортимента, формирование новых моделей бизнеса, удержание цифровых потребителей, внедрение инструментов диджитал-маркетинга. Перечисленные показатели достигаются бизнесом в результате осуществления инвестиций. Поэтому развитие информационной безопасности бизнеса – это инвестиции, которые, во-первых, не каждый бизнес имеет, во-вторых, не каждый бизнес понимает важность этих инвестиций, и, наконец, в-третьих, не каждый бизнес владеет информацией, во что следует инвестировать, чтоб защитить себя от кибератак.

Мы считаем, что систематически должны проводиться исследования, которые отражали бы динамику развития уровня информационной защиты, инструментов, стратегий, возможных технологических решений, ПО и т. д. Следовательно, вопрос информационной безопасности бизнеса должен ставиться одновременно с появлением идеи открытия бизнеса.

Таким образом, для бизнеса решения в области информационной безопасности представляют собой технологии, способы, мето-

ды и инструменты защиты конфиденциальной информации, применение которых основывается на вопросах защиты от внутренних и внешних угроз, утечки данных, внедрение ПО для информационной безопасности и формирование системы обеспечения информационной безопасности организации.

Цифровая экономика оказала сильное влияние на развитие бизнеса, но множество внешних факторов, начиная с 2019 г., заставили бизнес не просто выживать, а развиваться и искать, формировать, внедрять и находить новые инструменты, решения и стратегии развития. Поставленный в данном исследовании вопрос имеет практическое значение, поскольку мы рассматриваем информационную безопасность бизнеса как стратегическую бизнес-единицу, влияющую на устойчивое развитие бизнеса и развитие которой зависит от наличия инвестиционной программы. Мы считаем, что ядром устойчивого развития бизнеса является защита бизнеса от кибератак, сохранение и укрепление корпоративных баз данных, необходимых для выработки управленческих решений, перевод решений по ИБ с уровня операционной деятельности на стратегический уровень и определение инвестиционной программы на этапе формирования корпоративной стратегии бизнеса. В условиях неопределенности и цифровой трансформации, в которых оказался бизнес, все решения и технологии на сегодняшний день оцифрованы, и именно от грамотного стратегического управления информационной безопасностью зависит устойчивое развитие бизнеса.

Список литературы

1. *Алиева М.Н.* Проблемы международно-правового сотрудничества в сфере информационной безопасности // Юридический вестник Дагестанского государственного университета. 2017. Т. 24. №4. С. 99–103. DOI: 10.21779/2224-0241-2017-24-4-99-103.
2. *Булачев Г.П.* Обоснование важности поддержки экспорта программного обеспечения в России на примере зарубежных стран // Экономика: вчера, сегодня, завтра. 2017. Т. 7. №4А. С. 249–257.
3. *Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В.* Теория информационной безопасности и методология защиты информации. – 2-е изд., испр. и доп. – СПб.: Университет ИТМО, 2018. – 100 с.
4. *Горелова Т.П., Серебровская Т.Б.* Поддержка бизнеса в условиях цифровой трансформации // Современная конкуренция. 2023. Т. 17. №2. С. 53–67. DOI: 10.37791/2687-0649-2023-17-2-53-67.
5. *Иванова А.И., Кравченко Н.А.* Влияние региональных условий на бизнес-демографию российских ИТ-компаний // Вопросы экономики. 2022. №5. С. 79–98. DOI: 10.32609/0042-8736-2022-5-79-98.
6. *Куркин А.В., Шевченко Я.С.* Оценка рисков информационной безопасности с применением нечеткого моделирования // Неделя науки Санкт-Петербургского государственного морского технического университета. 2020. Т. 2. №4. С. 45. DOI: 10.52899/9785883036063_613.
7. *Котенко И.В., Коломеец М.В., Жернова К.Н., Чечулин А.А.* Визуальная аналитика для информационной безопасности: области применения, задачи и модели визуализации // Вопросы кибербезопасности. 2021. №4 (44). С. 2–15. DOI: 10.21681/2311-3456-2021-4-2-15.
8. *Миняев А.А.* Методика оценки эффективности системы защиты территориально-распределенных информационных систем: автореф. дис. … канд. техн. наук. – СПб., 2021. – 22 с.
9. *Найденова Ю.Н., Теплых Г.В.* Оценка снижения эффективности российских компаний от ухода зарубежных вендоров ИТ-продуктов // Вопросы экономики. 2023. №8. С. 100–122. DOI: 10.32609/0042-8736-2023-8-100-122.
10. Обеспечение информационной безопасности бизнеса / под общ. ред. А.П. Курило; Центр исследований платежных систем и расчетов. – 2-е изд., перераб. и доп. – М.: Альпина Паблишерз, 2011. – 371 с.
11. *Смирнов В.М., Перебейнос К.А.* Правовые акты в сфере информационной безопасности как один из важнейших источников информационной безопасности РФ // Тенденции развития науки и образования. 2022. №85-1. С. 52–57. DOI: 10.18411/trnio-05-2022-14.

12. *Соловьева А.А., Ромазан Д.В.* Перспективы освоения «Новых рынков» для России в экспорте ИТ-услуг в регионе Большого Средиземноморья // Тенденции развития Интернет и цифровой экономики: Труды V Всероссийской с международным участием научно-практической конференции (Симферополь – Алушта, 2–4 июня 2022 г.). – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 92–95.
13. *Ступин Р.С.* Перспективные меры поддержки зарубежного патентования и экспорта ИКТ-продукции // Вестник цифровой экономики. 2020. № 1. С. 81–102.
14. *Трошин Д.В.* Формализованная модель подготовки решений по нейтрализации угроз экономической безопасности на федеральном уровне // Государственное управление. Электронный вестник. 2019. № 74. С. 44–61.
15. *Якимова В.А., Хмура С.В.* Измерение цифровых экономических разрывов в бизнес-секторе региональной экономики // Журнал Новой экономической ассоциации. 2023. № 4 (61). С. 70–92. DOI: 10.31737/22212264_2023_4_70-92.
16. *Disterer G.* ISO/IEC 27000, 27001 and 27002 for Information Security Management // Journal of Information Security. 2013. Vol. 4. No. 2. P. 92–100. DOI: 10.4236/jis.2013.42011.
17. *Jinhui L., Nasonova N.V.* Information security requirements for a small business company // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. науч.-техн. семинара (Минск, ноябрь-декабрь 2020 г.) / редкол.: М.Н. Бобов [и др.]. – Минск: БГУИР, 2020. С. 82–85.
18. *Kreicberga L.* Internal threat to information security: countermeasures and human factor within SME. – University of Technology, 2010. – 69 p.
19. *Pernebekova A.P., Ahbergenovich B.A.* Information Security and the Theory of Unfaithful Information // Journal of Information Security. 2015. No. 6. P. 265–272. DOI: 10.4236/jis.2015.64026.
20. *Ye C., Shi W., Zhang R.* Research on gray correlation analysis and situation prediction of network information security // EURASIP Journal on Information Security. 2021. Article 3. DOI: 10.1186/s13635-021-00118-1.

Сведения об авторе

Горелова Тамара Петровна, ORCID 0000-0003-3546-9426, канд. экон. наук, доцент, кафедра операционного и отраслевого менеджмента, Финансовый университет при Правительстве Российской Федерации, Москва, Россия, tamara.gorelova2013@gmail.com

Статья поступила 11.12.2024, рассмотрена 25.12.2024, принята 03.02.2025

References

1. Aliyeva M.N. The problems of international and legal cooperation in the field of information security. *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta*=Law Herald of Dagestan State University, 2017, vol.24, no.4, pp.99-103 (in Russian). DOI: 10.21779/2224-0241-2017-24-4-99-103.
2. Bulachev G.P. Substantiation of the importance of supporting software export in Russia on the example of foreign countries. *Ekonomika: vchera, segodnya, zavtra*=Economics: Yesterday, Today and Tomorrow, 2017, vol.7, no.4A, pp.249-257 (in Russian).
3. Gatchin Yu. A., Sukhostat V.V., Kurakin A.S., Donetskaya Yu. V. *Teoriya informatsionnoi bezopasnosti i metodologiya zashchity informatsii* [Theory of information security and methodology of information protection]. 2nd edition, corr. and add. St. Petersburg, ITMO University, 2018, 100 p.
4. Gorelova T., Serebrovskaya T. Business Support in the Context of Digital Transformation. *Sovremennaya konkurentsiya*=Journal of Modern Competition, 2023, vol.17, no.2, pp.53-67 (in Russian). DOI: 10.37791/2687-0649-2023-17-2-53-67.
5. Ivanova A.I., Kravchenko N.A. The impact of regional conditions on the business demography of Russian IT companies. *Voprosy Ekonomik*i, 2022, no.5, pp.79-98 (in Russian). DOI: 10.32609/0042-8736-2022-5-79-98.
6. Kurkin A.V., Shevchenko Ya.S. Risk assessment of information security with fuzzy modeling. *Nedelya nauki Sankt-Peterburgskogo gosudarstvennogo morskogo tekhnicheskogo universiteta*, 2020, vol.2, no.4, p.45 (in Russian). DOI: 10.52899/9785883036063_613.

7. Kotenko I. V., Kolomeets M. V., Zhernova K. N., Chechulin A. A. Visual analytics for information security: Areas of application, tasks and visualization models. *Voprosy kiberbezopasnosti*, 2021, no.4(44), pp.2-15 (in Russian). DOI: 10.21681/2311-3456-2021-4-2-15.
8. Minyaev A. A. *Metodika otsenki effektivnosti sistemy zashchity territorial'no-raspredelennykh informatsionnykh system. Avtoref. dis. kand. tekhn. nauk* [Methodology for evaluating the effectiveness of the system of protection of geographically distributed information systems. Cand. eng. sci. abstr. dis.]. St. Petersburg, 2021, 22 p.
9. Naidenova Yu. N., Teplykh G. V. Evaluation of losses in the efficiency for Russian companies due to the foreign it vendors withdrawal from the market. *Voprosy Ekonomiki*, 2023, no.8, pp.100-122 (in Russian). DOI: 10.32609/0042-8736-2023-8-100-122.
10. *Obespechenie informatsionnoi bezopasnosti biznesa* [Ensuring business information security]. Ed. by A. P. Kurilo; Center for Research on Payment Systems and Settlements. 2nd edition, reprint. and add. Moscow, *Al'pina Publisherz* Publ., 2011, 371 p.
11. Smirnov V. M., Perebeynos K. A. *Pravovye akty v sfere informatsionnoi bezopasnosti kak odin iz vazhneishikh istochnikov informatsionnoi bezopasnosti* RF [Legal acts in the field of information security as one of the most important sources of information security of the Russian Federation]. *Tendentsii razvitiya nauki i obrazovaniya*, 2022, no.85, pp.52-57. DOI: 10.18411/trnio-05-2022-14.
12. Solovyova A. A., Romazan D. V. *Perspektivy osvoeniya «Novykh rynkov» dlya Rossii v eksporte IT-uslug v regione Bol'shogo Sredizemnomor'ya* [Prospects for the development of "New markets" for Russia in the export of IT services in the Greater Mediterranean region]. *Tendentsii razvitiya Internet i tsifrovoi ekonomiki: Trudy V Vserossiiskoi c mezhdunarodnym uchastiem nauchno-prakticheskoi konferentsii (Simferopol' – Alushta, 2–4 iyunya 2022 g.)* [Trends in the development of the Internet and digital economy: Proceedings of the V All-Russian Scientific and Practical Conference with International Participation (Simferopol – Alushta, June 2–4, 2022)]. Simferopol, V. I. Vernadsky Crimean Federal University, 2022, pp.92-95.
13. Stupin R. S. Emerging measures to support foreign patenting and export of ICT products. *Vestnik tsifrovoi ekonomiki*, 2020, no.1, pp.81-102 (in Russian).
14. Troshin D. V. Formalized model of preparing solutions to neutralize threats to economic security at the federal level. *Gosudarstvennoe upravlenie. Elektronnyi vestnik*=Public Administration. E-journal, 2019, no.74, pp.44-61 (in Russian).
15. Yakimova V. A., Khmura S. V. Measuring digital economic gaps in the business sector of the regional economy. *Zhurnal Novoi ekonomicheskoi assotsiatsii*=Journal of the New Economic Association, 2023, no.4, pp.70-92 (in Russian). DOI: 10.31737/22212264_2023_4_70-92.
16. Disterer G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 2013, vol.4, no.2, pp.92-100. DOI: 10.4236/jis.2013.42011.
17. Jinhui L. Nasonova N. V. Information security requirements for a small business company. *Telekommunikatsii: seti i tekhnologii, algebraicheskoe kodirovanie i bezopasnost' dannykh: materialy mezhdunar. nauch.-tekhn. seminara (Minsk, noyabr'-dekabr' 2020 g.)* [Telecommunications: Networks and Technologies, Algebraic Coding and Data Security: Proceedings of the International Scientific and Technical Seminar (Minsk, November-December 2020)]. Ed. board: M. N. Bobov [et al.]. Minsk, BSUIR, 2020, pp.82-85.
18. Kreicberga L. Internal threat to information security: countermeasures and human factor within SME. University of Technology, 2010, 69 p.
19. Pernebekova A. P., Ahbergenovich B. A. Information Security and the Theory of Unfaithful Information. Journal of Information Security, 2015, no.6, pp.265-272. DOI: 10.4236/jis.2015.64026.
20. Ye C., Shi W., Zhang R. Research on gray correlation analysis and situation prediction of network information security. EURASIP Journal on Information Security, 2021, article 3. DOI: 10.1186/s13635-021-00118-1.

About the author

Tamara P. Gorelova, ORCID 0000-0003-3546-9426, Cand. Sci. (Econ.), Associate Professor, Operational and Industry Management Department, Financial University under the Government of the Russian Federation, Moscow, Russia, tamara.gorelova2013@gmail.com

Received 11.12.2024, reviewed 25.12.2024, accepted 03.02.2025