Специальность ВАК: 5.2.3
УДК: 338.246.87: 004.056
EDN: RNARFS

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРУКТУРЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ПРЕДПРИЯТИЙ

Марина Ивановна БАРАБАНОВА, к.э.н., доцент
Проректор по учебной работе, Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака» (Санкт-Петербург, Россия).
Адрес: 191023, Невский пр., 60, Санкт-Петербург, Россия, e-mail: barabanova@ibispb.ru
Борис Геннадьевич ВАСИЛЕНКО
Генеральный директор, ООО «Солид Бренч» (Ереван, Армения). Адрес: Республика Армения, Ереван, Н. Зарян 22А, e-mail: dreaktor0@gmail.com

Аннотация

Цель исследования состояла в определении роли и места информационной безопасности в системе экономической безопасности предприятий в современных условиях, а также выявлении направлений интеграции мер по обеспечению информационной безопасности в общую систему защитных мер. **Методологическую основу** составили общенаучные методы познания (анализ, синтез, обобщение, сравнение), а также системный и структурно-функциональный подходы, позволившие комплексно отразить взаимодействие экономической и информационной составляющих. Выявлены три подхода к исследованию экономической безопасности предприятия, что позволило определить место информационной безопасности в деятельности современных предприятий. Предложено авторское определение информационной безопасности предприятия, учитывающее ее взаимосвязь с общим уровнем экономической безопасности и отражающее ее значимость для решения задач функционирования современных предприятий. Показана ключевая роль информационной безопасности в рамках каждого из выделенных подходов. **В выводах** отмечается, что уточнение информационной составляющей экономической безопасности расширяет представления о ее структуре и сущности, позволяя рассматривать информационные риски как один из ключевых факторов устойчивости предприятия в современных условиях. При разработке стратегий экономической безопасности следует проводить дополнительную оценку уровня информационной безопасности, что особенно важно в условиях повышенных внешних угроз и санкционного давления. Перспективы развития данной темы связаны с формированием комплексных методологических основ интеграции информационной безопасности во все уровни экономической безопасности предприятия, а также проведением сравнительного анализа состояния и проблем информационной безопасности предприятий в контексте их экономической безопасности по отраслям или странам.

Ключевые слова

информационная составляющая экономической безопасности, киберугрозы, санкционное давление, управление информационными рисками, устойчивость предприятия

Для цитирования: Барабанова М.И., Василенко Б.Г. Информационная безопасность в структуре экономической безопасности современных предприятий // Ученые записки Международного банковского института. 2026. № 3 (57). С. 45-65. EDN: RNARFS.

Финансирование: Настоящее исследование не получило внешнего финансирования.

Code of scientific specialty: 5.2.3
UDC: 338.246.87: 004.056
EDN: RNARFS

INFORMATION SECURITY IN THE STRUCTURE OF ECONOMIC SECURITY OF MODERN ENTERPRISES

Marina Ivanovna BARABANOVA, Candidate of Economic Sciences, Associate Professor
Vice-Rector for Academic Activities, Autonomous non-profit organization of higher education «International Banking Institute named after Anatoly Sobchak» (Saint Petersburg, Russia). Address: 191023, Nevsky prospect, 60, Saint Petersburg, Russia, e-mail: barabanova@ibispb.ru
Boris Gennadievich VASILENKO
CEO, Solid Branch LLC (Yerevan, Armenia). Address: Republic of Armenia, Yerevan, N. Zaryan 22A, e-mail: dreaktor0@gmail.com

Abstract

The article substantiates the relevance of information security for improving the economic security of an enterprise in modern conditions. The methodological framework includes an analysis of scientific literature, systematic and comparative approaches that allow a comprehensive reflection of the interaction of economic and informational components. Three different approaches to the study of the economic security of an enterprise have been identified, which made it possible to consider the place of information security in the work of modern enterprises. The author's definition of enterprise information security is proposed, taking into account the relationship with the general level of economic security and reflecting the importance of information security for solving the tasks of modern enterprises. The key importance of information security within the framework of the selected approaches is shown. The theoretical value of the research lies in complementing the scientific discourse by clarifying the content of economic security in terms of the information component, which expands the understanding of the structure and essence of economic security, allowing information risks to be considered as one of the key

factors influencing the sustainability of the enterprise. The practical significance of the results obtained lies in the possible application of the main provisions and conclusions by enterprises when developing economic security strategies, including assessing the level of information security, which is especially important in conditions of increased external threats and sanctions pressure. The prospects for the development of this topic are related to the formation of a comprehensive methodological framework for integrating information security into all levels of economic security of an enterprise, as well as conducting a comparative analysis of the state and problems of information security of enterprises in the context of their economic security by industry or country.

Keywords

information component of economic security, cyber threats, sanctions pressure, information risk management, enterprise sustainability

For citation: Bararbanova M.I., Vasilenko B.G. Information security in the structure of economic security of modern enterprises // Uchenye zapiski Mezhdunarodnogo bankovskogo instituta [Proceedings of the International Banking Institute]. 2026. 3 (57). pp. 45-65 (in Russ.). EDN: RNARFS.

Funding: This research received no external funding.

Введение

В современных условиях хозяйствования, связанных с нарастанием технологических изменений, международной напряженности, задачами импортозамещения экономическая безопасность предприятия приобретает особую значимость. Представляя собой многогранный феномен, экономическая безопасность предприятия выстраивается, как правило, в форме иерархической системы и чаще всего описывается через совокупность функциональных элементов, позволяющих непосредственное осуществление соответствующих защитных механизмов.

Анализ научной литературы по рассматриваемой проблематике показывает, что исследования преимущественно концентрируются на финансовых [8], кадровых [6], правовых [17], а также некоторых других вопросах [2, 10, 11], принимая во внимание инновационную [12] и стратегическую направленности [13]. При детальном рассмотрении функциональных блоков экономической безопасности можно убедиться, что информационная составляющая, несмотря на свою критическую важность для решения задач обеспечения безопасности

предприятия, освещается недостаточно. Ее анализ носит преимущественно фрагментарный характер, отсутствует систематизированная проработка угроз, не определяются достаточные оценочные индикаторы, которые позволили бы сопоставлять уровень информационной защиты с другими функциональными составляющими. Вместе с тем, как показывает практика, инциденты, связанные с нарушением конфиденциальности и целостности данных, могут приводить к значительным финансовым и репутационным потерям [15].

В условиях стремительной цифровизации [9] и усиления киберугроз, в том числе обусловленных усилением международной геополитической нестабильности [16], информационная безопасность превращается в базовый элемент экономической устойчивости предприятий. В связи с этим обоснование ее места и функций в общей системе экономической безопасности на корпоративном уровне приобретает особую теоретическую и практическую значимость.

Цель настоящего исследования заключалась в обобщении существующих подходов к трактовке экономической безопасности предприятия, что позволило бы уточнить роль и статус информационной безопасности в современных хозяйственных условиях, а также определить возможные каналы ее встраивания в целостную систему защитных механизмов.

Материалы и методы

В качестве объекта исследования была выбрана экономическая безопасность предприятия в целом, включая все ее функциональные аспекты, освещенные в научных работах (финансовая, кадровая, технологическая и другие составляющие). Предметом исследования стали место и роль информационной безопасности в этой многокомпонентной системе, а также ее влияние на устойчивость предприятия и преодоление потенциальных угроз.

Методологической основой исследования послужили: анализ литературы и систематизация научных материалов по экономической безопасности; метод обобщения и сравнительный анализ для сопоставления различных точек зрения; структурно-функциональный анализ, позволяющий рассматривать информационную безопасность как часть единой системы; системный подход, необходимый для выявления взаимосвязей между различными функциональными компонентами экономической безопасности.

Результаты

Подходы к исследованию экономической безопасности предприятия

Анализ существующих авторских позиций позволил обобщить их в трех укрупненных подходах исследования экономической безопасности, каждый из которых по-своему демонстрирует значимость информационной защиты для современных предприятий:

– трактовка экономической безопасности предприятия как целостного, системного образования (подход 1);

– подход, акцентирующий внимание на внешних условиях среды хозяйствования предприятия (подход 2);

– направление, сосредоточенное на одной либо нескольких функциональных подсистемах экономической безопасности (подход 3).

Обоснованность **первого подхода** заключается в том, что экономическая безопасность предприятия не может быть сведена к одной или нескольким узким функциональным плоскостям. Напротив, подавляющее число исследователей настаивает на необходимости системного охвата, который объединяет несколько взаимосвязанных элементов.

В проанализированных научных источниках [16, 18] среди ключевых функциональных компонентов экономической безопасности предприятия чаще всего выделяются следующие:

– финансовая (обеспечивает устойчивость и платежеспособность);

– информационная (включает защиту данных, коммерческой тайны, цифровую безопасность);

– интеллектуально-кадровая (связана с квалификацией и благонадежностью персонала, а также с защитой интеллектуальной собственности);

– технико-технологическая (ориентирована на состояние и безопасность производственного процесса, инновации, технологические ресурсы);

– политико-правовая (обеспечивает соблюдение законодательных норм, организацию правовой защиты интересов предприятия);

– экологическая (формирует условия для устойчивого развития с учетом требований по охране окружающей среды);

– силовая (охватывает механизмы физической защиты и противодействия преступным действиям).

При этом ряд авторов [19] подчеркивает, что каждая из перечисленных составляющих может быть дополнена или объединена с другими в зависимости от отраслевой специфики и текущих стратегических задач предприятия.

В рамках первого подхода исследуется широкий круг вопросов, отражающих различные аспекты системного подхода экономической безопасности. Так, например, анализируется роль экономической безопасности в системе национальных приоритетов и подчеркиваются меры по защите интересов на корпоративном уровне [4], уделяется внимание концептуальным положениям интегрированной системы безопасности предприятия, включающей определение целей, принципов, объектов и субъектов, а также стратегии и тактики обеспечения экономической безопасности, охватываются вопросы системного моделирования процессов экономической безопасности, предлагают алгоритмы действий и стратегий, ориентированных на все функциональные компоненты [19]. Ряд научных работ раскрывают экологическую составляющую в общем комплексе безопасности [5], а также затрагивают правовые и административные механизмы [3]. Отмечаются нарастающая значимость цифрового фактора в структуре комплексной безопасности [9, 16].

Ключевое достоинство первого из выделенных подходов к экономической безопасности заключается в его системном характере, который позволяет охватить взаимосвязи между разнородными сферами, такими как финансы, кадры, информация, экология и т.п. Эта многоаспектность способствует уточненной идентификации рисков и угроз, гибкой подстройке под меняющуюся внешнюю среду, в том числе санкционные ограничения или технологические изменения, а также закладывает фундамент для долгосрочной устойчивости предприятия.

Вместе с тем системный подход к экономической безопасности предприятия имеет и определенные недостатки. Так, внедрение комплексных защитных механизмов сопряжено с крупными административными и финансовыми расходами [19]. Кроме того, требуется налаживание непрерывного взаимодействия между профильными специалистами, что во многих ситуациях усложняет управленческие процедуры. И, наконец, унифицированная методика, отражающая

особенности каждой функциональной области в настоящее время еще отсутствует, из-за чего возможна несогласованность при выборе оценочных критериев и способов измерения и оценки уровня экономической безопасности.

Второй подход к экономической безопасности предприятия фокусирует внимание на специфике внешнего контекста функционирования предприятия, и в первую очередь, на явлениях цифровизации и санкционных барьерах. Как показывает практика, оба эти фактора напрямую затрагивают вопросы информационной безопасности.

В эпоху цифровизации, когда хозяйственные операции все чаще переносятся в Интернет-пространство, предприятиям необходимо принимать во внимание новые возникающие опасности и вызовы. Цифровые инструменты, с одной стороны, предоставляют дополнительные возможности для роста и укрепления конкурентоспособности, но с другой – порождают риски, обусловленные уязвимостью информационных систем [9]. Противодействие им требует специализированного набора средств, таких как оперативного анализа на базе актуальных данных, создания системы мониторинга операций, применения программно-аппаратных решений в области киберзащиты и сертификационных механизмов. Это, в свою очередь, формирует требования к системе обеспечения информационной безопасности предприятия. В рамках систематического подхода к управлению цифровыми угрозами значительное внимание уделяется национальным программам импортозамещения в области программного обеспечения, позволяющим снизить зависимость критически важных технологий от зарубежных поставщиков [16]. Подобные шаги способствуют укреплению стабильности и уменьшению вероятности негативного внешнего воздействия или диверсий в сфере информационно-коммуникационных технологий.

Санкции в настоящее время стали одним из главных источников вызовов для экономической безопасности как на уровне национальной экономики, так и на уровне отдельных предприятий. В исследованиях по данной теме [1, 17] санкционное влияние трактуется как внешний фактор, способный перекрыть доступ к капиталу, передовым технологиям и сырьевым ресурсам. Среди основных последствий экономических санкций для предприятий выделяются:

– сокращение или потеря источников внешнего финансирования;

– перебои в поставках необходимых ресурсов, в том числе технологических компонентов;

– ограничение рынков сбыта, снижение экспортных возможностей;

– рост транзакционных издержек из-за сложностей с проведением валютных операций.

В ответ на эти вызовы предлагаются следующие меры:

– развитие импортозамещения и повышение доли отечественных технологий (что перекликается и с цифровой экономикой);

– диверсификация поставщиков и рынков сбыта;

– усиление финансовой устойчивости за счет резервирования капитала и использования внутренних источников инвестирования;

– создание структурированных механизмов мониторинга внешнеэкономических рисков и автоматизации управленческих решений.

Таким образом, второй подход к экономической безопасности предприятия, ориентированный на учет внешних факторов хозяйствования, фокусируется на двух важных направлениях. Первое направление предполагает приспособление предприятий к цифровым условиям и минимизации рисков в информационной сфере. Второе направление нацелено на формирование стратегий, позволяющих противостоять санкционным ограничениям, что подразумевает комплексное управление внешнеэкономическими угрозами и перенастройку деятельности в сторону создания прочной внутренней основы. Перечисленные в изученных публикациях способы (от внедрения инструментов цифровой защиты для запуска программ импортозамещения) дают предприятиям возможность повышать собственную экономическую безопасность и сохранять рыночные позиции даже при нестабильной внешней обстановке.

В рамках **третьего подхода** к экономической безопасности предприятия основное внимание уделяется углубленной проработке отдельных функциональных областей, каждая из которых располагает уникальными оценочными критериями, механизмами обеспечения и спектрами угроз. Приведем краткую характеристику наиболее значимых направлений, выделенных на основе проанализированных материалов.

Финансовая составляющая экономической безопасности предприятия сфокусирована на обеспечении устойчивости и ликвидности организации, а также на управлении рисками, связанными с денежными потоками и инвестициями. В рамках данного подхода рассматривается значение непрерывного мониторинга финансовых показателей, в том числе состояния баланса и внешних факторов, влияющих на устойчивость предприятия [8], подчеркивается важность управления финансовыми рисками в страховом рынке, указывая на необходимость системных мер против внешнего и внутреннего давления, в том числе санкционного, для сохранения финансовой стабильности [13].

Кадровая составляющая экономической безопасности предприятия охватывает вопросы надежности и квалифицированности персонала, а также минимизации угроз, связанных с мошенничеством, хищениями или несанкционированным доступом к конфиденциальным данным. Так, например, в исследовании [6] представлена модель оценки благонадежности сотрудников, особо актуальная для предприятий критической информационной инфраструктуры. Такая модель позволяет идентифицировать потенциальные угрозы со стороны персонала и своевременно реагировать на риски внутреннего характера.

Обоснование выделения производственной (промышленной) компоненты в структуре экономической безопасности предприятия связано с тем, что хозяйственные операции в этой сфере сопряжены с технологическими и организационными рисками, способными подорвать финансовую устойчивость компании. В русле данной трактовки промышленное предприятие воспринимается как многоканальная система, испытывающая воздействие широкого спектра внешних и внутренних факторов [1]. При этом производственный блок предполагает диагностику эндогенных и экзогенных вызовов и угроз, также разработку мер по обеспечению безопасности ключевых технологических звеньев.

Правовая составляющая кадровой безопасности предприятия охватывает как внутрикорпоративные нормы и договорные отношения, так и соблюдение требований действующего законодательства. В работах, посвященных этой тематике, рассматриваются организационно-административные вопросы функционирования правоохранительных структур при противодействии коррупционным проявлениям и иным экономическим правонарушениям [3].

Данное направление акцентирует внимание на роли юридического инструментария и государственного надзора в защите предпринимательских интересов.

Технологическая составляющая экономической безопасности предприятия увязывается с внедрением инноваций, обновлением производственных мощностей и применением прогрессивных технологических и организационных решений. В работе [12] подчеркивается, что инновационная направленность служит важнейшим условием укрепления экономической защищенности. Первостепенное значение здесь приобретает мониторинг технологических вызовов и угроз и своевременное финансирование научно-исследовательских проектов. Использование системы показателей и пороговых значений для оценки технологической безопасности позволяет на ранних стадиях выявлять слабые места в производственном аппарате предприятия [18].

Инновационная составляющая нацелена на создание и внедрение новых продуктов, управленческих подходов и технологических схем, что непосредственно определяется конкурентоспособность и долгосрочную стабильность компаний. Акцент делается на значимости стратегического менеджмента в инновационной сфере, особенно актуальной для нефтегазового сектора в контексте глобальных энергетических трансформаций [14]. Этот подход предполагает не только оценку рисков внедрений новаций, но и выявление резервов для усиления экономических позиций предприятия благодаря научно-техническому прогрессу.

Экологическая составляющая исходит из того, что вредное воздействие на природную среду может оборачиваться дополнительными расходами, штрафными санкциями и репутационным потерями. В работе [2] изложены концептуальные подходы к моделированию эколого-экономической безопасности в кризисных условиях, где природоохранные индикаторы рассматриваются как элемент общей устойчивости региона и хозяйствующих субъектов. В работах [5, 7] предлагаются методы анализа рисков загрязнения окружающей среды и интеграции систем экологического мониторинга в повседневную практику функционирования предприятий с целью предотвращения аварийных ситуаций.

Итак, третий из рассматриваемых подходов – фокусировка на отдельных функциональных составляющих экономической безопасности предприятий – дает

возможность более предметно изучить приоритетные сферы детальности предприятий и подобрать адекватные механизмы защиты. Каждая из перечисленных составляющих вносит свой вклад в общий контур экономической безопасности и нуждается в скоординированном взаимодействии, с учетом как внутренней специфики предприятия, так и внешних вызовов.

В таблице 1 представлены результаты сравнительного анализа основных характеристик предлагаемых подходов к исследованию экономической безопасности предприятия.

Таблица 1 - Сравнительный анализ предлагаемых подходов к исследованию экономической безопасности предприятия

Подход	Достоинства	Недостатки
1. Системный	Системный охват, учет взаимосвязей, гибкость, долгосрочная устойчивость	Крупные административные и финансовые расходы, сложность координации, отсутствие унифицированной методики
2. Внешнесредовой	Учет цифровизации и санкций, адаптация к внешним условиям	Ограниченность внутренними факторами, недостаточная проработка функциональных аспектов
3. Функциональный	Глубокий анализ отдельных подсистем, конкретные механизмы защиты	Риск фрагментарности, отсутствие целостной картины, необходимость координации

Источник: составлено авторами.

Информационная безопасность в системе экономической защиты предприятия

В научной литературе, затрагивающей вопросы экономической безопасности предприятия, информационная защита часто трактуется как одна из функциональных подсистем наравне с финансовой, кадровой и технологической и т.п. При этом подчеркивается значимость сохранности данных в условиях цифрового пространства, а также необходимость всестороннего анализ угроз и уязвимостей, порождаемых быстрым техническим прогрессом и нестабильностью нормативно-правового поля. В частности, в исследовании [9] представлен методический инструментарий для системной оценки опасностей в информационной среде, учитывающий как стремительное обновление технологий, так и подвижность регуляторных требований.

В работах, анализирующих специфику экономической безопасности в цифровой экономике [16], акцент смещается на критические технологии и средства их защиты, а также на угрозы, связанные с возможными сбоями в работе аппаратных и программных средств. Тем самым, по мнению исследователей, информационная безопасность не сводится только к предотвращению кибератак, но и подразумевает обеспечение непрерывности бизнес-процессов, в том числе через применение механизмов сертификации и контроля отечественных разработок в сфере информационно-коммуникационных технологий. Развитие отечественных предприятий в цифровой экономике требует усиления защиты критически важных информационно-коммуникационных технологий, создания реестра отечественного программного обеспечения и контроля за безопасным использованием аппаратных средств.

Общие черты в трактовках сводятся к признанию стратегического значения информации и инструментов ее защиты для стабильной деятельности предприятия. Различия же сосредоточены на степени технологического акцента – одни авторы считают первостепенным мониторинг киберугроз, другие дополнительно выделяют репутационный риск и нормативно-правовое регулирование как часть информационной безопасности.

Наконец, возрастание роли информационной составляющей экономической безопасности предприятия связывается с тем, что в условиях цифровизации экономической деятельности особую значимость приобретают вопросы защиты конфиденциальных данных и предотвращения кибератак.

Согласно отчету Verizon Data Breach Investigations Report (2023)[11], 74% всех утечек данных связаны с человеческим фактором, а средняя стоимость утечки данных, по данным IBM Cost of a Data Breach Report (2023)[12], достигла 4,45 млн долларов США. Эти данные подтверждают, что информационные риски являются одним из ключевых факторов, влияющих на устойчивость предприятия в современных условиях.

[11]Verizon. 2023 Data Breach Investigations Report (DBIR). URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 14.09.2026).

[12]IBM. Cost of a Data Breach Report 2023. URL: https://www.ibm.com/reports/data-breach (дата обращения: 14.09.2026).

Обобщение теоретических позиций и существующих трактовой информационной безопасности позволило сформулировать определение данного понятия, учитывающие актуальные вызовы, такие как рост числа кибератак, ужесточение санкционных ограничений, участившиеся случаи утечек информации, сбои в работе технологических систем и т.п.

Под информационной безопасностью предприятия следует понимать систему организационных, технико-технологических и правовых мер, которые обеспечивают сохранность как внутренних, так и внешних информационных ресурсов предприятия от несанкционированного проникновения, искажения потери или неправомерного применения, а также гарантируют бесперебойность и устойчивость основных бизнес-процессов в условиях динамично меняющейся экономической конъюнктуры.

В предложенном определении подчеркивается значение двух главных составляющих: обеспечение конфиденциальности и неизменности данных, а также недопущение сбоев в операционной деятельности, что обусловлено необходимостью гибко реагировать на санкционные ограничения и технологические изменения.

В научной литературе и нормативных документах часто используются близкие по смыслу термины: «информационная безопасность», «кибербезопасность», «цифровая безопасность» и «информационная составляющая экономической безопасности». Представляется важным разграничить эти понятия. Информационная безопасность – это состояние защищенности информационной среды, обеспечивающее ее формирование и развитие в интересах субъектов. Кибербезопасность – более узкое понятие, ориентированное на защиту от угроз в киберпространстве, прежде всего техническими средствами. Цифровая безопасность охватывает защиту цифровых активов и инфраструктуры. Информационная составляющая экономической безопасности предприятия – это часть общей системы экономической безопасности, направленная на защиту информационных ресурсов и обеспечение бесперебойности бизнес-процессов. Таким образом, информационная безопасность является более широким понятием по отношению к кибербезопасности, а информационная составляющая

экономической безопасности акцентирует внимание на экономических аспектах защиты информации.

В рамках общей системы экономической безопасности информационная составляющая призвана решать следующие задачи:

– предотвращать нелегитимное распространение коммерчески значимых, финансовых и персональных сведений;

– не допускать искажений в данных, которые могут обернуться денежными потерями или перебоями в работе;

– поддерживать бесперебойный доступ к необходимым информационным ресурсам и сервисам, задействованным в повседневной деятельности;

– способствовать укреплению доверия контрагентов и клиентов, минимизировать репутационные риски, связанные с утечками или хакерскими атаками, и тем самым повышать общую конкурентоспособность организации.

Таким образом, информационная безопасность становится важнейшим условием устойчивой экономической деятельности и одним из ключевых факторов формирования комплексной системы экономической безопасности предприятия.

Например, в 2022 году крупная российская логистическая компания столкнулась с целевой кибератакой, приведшей к остановке операционной деятельности на 48 часов и прямым потерям в размере 120 млн рублей. Внедрение комплексной системы информационной безопасности, включающей мониторинг сетевой активности и обучение персонала, позволило снизить риск повторных инцидентов на 60% и укрепить экономическую устойчивость предприятия. По данным Positive Technologies, в 2023 году количество кибератак на российские компании выросло на 30% по сравнению с 2022 годом, что подтверждает необходимость интеграции информационной безопасности в систему экономической безопасности[13].

В рамках второго из выделенных нами подходов внимание к вопросам информационной безопасности также носит критический характер. Учитывая факторы цифровой экономики и санкционного давления, многие предприятия

[13] Positive Technologies. Актуальные киберугрозы: 2023 г. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 14.09.2026).

сталкиваются с необходимостью детального сценарного анализа угроз и возможностей. В соответствии с приведенными в контексте данными, подсанкционные ограничения (например, ограничения на доступ к программным и аппаратным ресурсам или финансовым инструментам) становятся дополнительным источником уязвимостей для информационной инфраструктуры.

Опора на четко сформулированное определение информационной безопасности помогает современным предприятиям:

– выстраивать сценарные модели реагирования на внешние риски, возникающие из-за санкции или быстрого развития цифрового рынка;

– вовремя адаптировать системы защиты данных к новым нормативным требованиям, которые меняются под влиянием международных и локальных регуляторов;

– формировать гибкую стратегию выхода на нестабильные рынки и управления поставщиками, учитывая возможные перебои в каналах связи и трансграничных операциях.

Таким образом, при учете внешней среды учет информационной безопасности становится основой для регулярной корректировки мер защиты, эффективного планирования и долгосрочного управления рисками.

Третий выделенный нами подход также может быть обогащен, поскольку информационная безопасность по своей сути тесно связана с обеспечением всех функциональных подсистемам экономической безопасности: финансовой, кадровой, правовой и т.д. Практика функционирования современных предприятий показывает, что защитные инструменты по отношению к информации, связанной с предприятием, должны органично встраиваться в каждую из подсистем.

Примерами реализации такой межфункциональной интеграции могут послужить:

– контроль доступа к банковским счетам и аналитическим системам (финансовая составляющая).

– обучение персонала правилам безопасной работы с корпоративными данными и предотвращение инсайдерских угроз (кадровая составляющая).

– внедрение систем мониторинга сетевой активности, резервное копирование критических данных и сертификация IT-инфраструктуры (технологическая составляющая).

Подобная взаимосвязь повышает устойчивость всей экономической структуры предприятия, так как сбои или утечки в одной из зон безопасности неминуемо отражаются на других аспектах работы организации. В свою очередь сочетание разных функциональных направлений экономической безопасности помогает предприятиям своевременно проводить оценку рисков и предотвращать критические последствия.

Таким образом, предлагаемое определение информационной безопасности имеет практическую значимость в рамках всех выделенных нами подходов (комплексном, с учетом внешней среды и функциональном), позволяя предприятиям выстраивать четкую систему мер для защиты от актуальных цифровых угроз, санкционного давления и внутренних уязвимостей на основе взаимодополняющих принципов и сценариев управления.

Выводы

В результате проведенного исследования удалось выявить три самостоятельных подхода к трактовке экономической безопасности предприятия, что послужило основой для уточнения роли и места информационной составляющей в обеспечении экономической безопасности хозяйствующих субъектов в современных условиях. Кроме того, предложена трактовка информационной безопасности предприятия, которая не только фиксирует ее связь с общим уровнем экономической защищенности, но и подчеркивает ее значимость для выполнения текущих и перспективных задач предприятия.

Дальнейшими задачами исследования проблемы информационной безопасности предприятия авторы видят:

– разработку методики интеграции информационной безопасности в общую модель экономической безопасности предприятия, в которой будут учтены этапы от выявления информационных рисков и уязвимостей до анализа их влияния на основные экономические показатели;

– формирование инструментария для оценки эффективности мер, направленных на обеспечение информационной безопасности, охватывающего

показатели и критерии, позволяющие измерять результативность действующих и планируемых мер в условиях цифровизации и санкционного давления, когда технологические и экономические барьеры могут быстро меняться.

Перспективными направлениями эмпирического анализа могут стать следующие:

– проведение опросов и интервью сотрудников и руководителей предприятий с целью выявления реального уровня информационных рисков с целью сопоставления теоретических предпосылок обеспечения информационной безопасности с практическими сценариями предприятий и сформирования на этой основе более точных индикаторов информационной безопасности предприятий.

– использование сценарного прогнозирования и экономико-математического моделирования для оценки вклада информационной безопасности в общую экономическую безопасность предприятия, что позволит отслеживать влияние изменений в экономической политико-правовой и технологической среде на ключевые показатели работы предприятия.

Одним из возможных направлений дальнейших исследований является проведение сравнительного анализа состояния и проблем информационной безопасности предприятий в контексте их экономической безопасности по отраслям или странам. Это позволит выявить особенности, лучшие практики и предложить адаптированные модели обеспечения экономической безопасности, учитывающие конкретную специфику внешней и внутренней среды конкретных организаций. Подобная сравнительная работа сможет обогатить как теоретические основы, так и практические методы укрепления информационной и экономической безопасности предприятий.

Список источников

1. **Баженов О.В., Блинов И.А.** Исследование проблем влияния экономических санкций на металлургическую отрасль России // Дискуссия. 2025. № 3 (136). С. 69–80. doi: 10.46320/2077-7639-2025-3-136-69-80.
2. **Белоножко М.Л., Барбаков О.М., Овчинникова С.В.** Концептуальные основы моделирования процесса эффективного управления экономико-экологической безопасностью в кризисный период // Экономика: вчера, сегодня, завтра. 2020. Т. 10, № 9-1. С. 425–437. doi: 10.34670/AR.2020.67.54.048.

3. **Быков Б.А.** Проблемы и перспективы административно-правового обеспечения экономической безопасности // Российский научный журнал. 2017. № 3 (56). С. 195–198.
4. **Василенко Н.В.** Структура управления системой экономической безопасности в новых условиях // Экономическая безопасность. 2024. Т. 7, № 12. С. 2989–3006. doi: 10.18334/ecsec.7.12.122270.
5. **Вишняков Я.Д., Киселева С.П., Маколова Л.В. и др.** Эколого-ориентированное развитие предприятий агропромышленного комплекса и опережающая подготовка кадров в области агроэкологического менеджмента // Управление. 2019. Т. 7, № 2. С. 24–32. doi: 10.26425/2309-3633-2019-2-24-32.
6. **Глухарева С.В., Шелупанов А.А., Немирович-Данченко М.М.** Формализованный подход к оценке уровня благонадежности сотрудников предприятий критической информационной инфраструктуры (КИИ) // Перспективы науки. 2023. № 4 (163). С. 17–23.
7. **Головинов О.Н., Ткачева М.В.** Анализ и оценка экологической безопасности как инструмента обеспечения устойчивого развития корпорации // Современная экономика: проблемы и решения. 2024. № 4 (172). С. 86–103. doi: 10.17308/meps/2078-9017/2024/4/86-103.
8. **Грабоздин Ю.П., Татаровский Ю.А.** Анализ платежеспособности и ликвидности бизнеса в управленческом консалтинге // Экономика и предпринимательство. 2021. № 12 (137). С. 1459–1462. doi: 10.34925/EIP.2021.137.12.292.
9. **Графов Ю.Г.** Цифровая устойчивость как условие обеспечения экономической безопасности цифрового предприятия при конкретизации целей национального развития // Индустриальная экономика. 2022. Т. 5, № 2. С. 466–471.
10. **Ковтуненко А.В.** Повышение эффективности консалтинговых услуг в условиях инновационной экономики // Научные труды Вольного экономического общества России. 2010. Т. 137. С. 743–749.
11. **Коробейникова Л.С., Ткачева М.В.** Развитие комплексного экономического анализа экологической устойчивости корпораций. Воронеж: Изд. дом ВГУ, 2022. – 187 с.
12. **Лещенко Ю.Г.** Инновационный вектор в системе экономической безопасности России // Вопросы инновационной экономики. 2019. Т. 9, № 2. С. 301–316. doi: 10.18334/vinec.9.2.40689.
13. **Лобанов С.Ю.** Сущность и содержание финансовой безопасности как объекта научного исследования // Экономика и предпринимательство. 2019. № 1 (102). С. 1228–1232.

14. **Лобов Д.С., Рыбин М.В., Шишонкова Ю.А.** Результативность экосистемы финансовой поддержки инновационной деятельности в РФ на государственном и корпоративном уровнях в нефтегазовой отрасли // Контроллинг. 2022. № 4 (86). С. 26–33.
15. **Матвеева Я.А.** Взаимосвязь конкурентоспособности предприятия и корпоративной социальной ответственности // Современная экономика: проблемы и решения. 2017. № 3 (87). С. 128–141. doi: 10.17308/meps.2017.3/1629.
16. **Моденов А.К., Власов М.П.** Особенности экономической безопасности в цифровой экономике // Петербургский экономический журнал. 2020. № 2. С. 121–134. doi: 10.24411/2307-5368-2020-10015. EDN BPATYU.
17. **Смирнова О.П., Чеснюкова Л.К.** Оценка промышленного потенциала индустриальных регионов России: экономическая безопасность // Национальные интересы: приоритеты и безопасность. 2024. Т. 20, № 4 (433). С. 743–758. doi: 10.24891/ni.20.4.743.
18. **Титоренко А.Г.** Вопросы обеспечения технико-технологической составляющей экономической безопасности предприятия // Символ науки: международный научный журнал. 2018. № 3. С. 44–48.
19. **Ianioglo A.** Comprehensive system of ensuring the economic security of enterprise // Agricultural and Resource Economics: International Scientific E-Journal. 2015. Vol. 1, № 1. P. 69–79. doi: 10.5555/20173155242.

References

1. **Bazhenov O.V., Blinov I.A.** [Study of the problems of the impact of economic sanctions on the metallurgical industry of Russia]. Diskussiya, 2025, no. 3(136), pp. 69–80. (In Russ.) doi: 10.46320/2077-7639-2025-3-136-69-80.
2. **Belonozhko M.L., Barbakov O.M., Ovchinnikova S.V.** [Conceptual foundations of modeling the process of effective management of economic and environmental security in a crisis period]. Ekonomika: vchera, segodnya, zavtra, 2020, vol. 10, no. 9-1, pp. 425–437. (In Russ.) doi: 10.34670/AR.2020.67.54.048.
3. **Bykov B.A.** [Problems and prospects of administrative and legal support of economic security]. Rossiiskiy nauchnyy zhurnal, 2017, no. 3(56), pp. 195–198. (In Russ.)
4. **Vasilenko N.V.** [Management structure of the economic security system in new conditions]. Ekonomicheskaya bezopasnost', 2024, vol. 7, no. 12, pp. 2989–3006. (In Russ.) doi: 10.18334/ecsec.7.12.122270.
5. **Vishnyakov Ya.D., Kiseleva S.P., Makolova L.V. et al.** [Ecologically oriented development of agro-industrial complex enterprises and advanced training of

personnel in the field of agroecological management]. Upravlenie, 2019, vol. 7, no. 2, pp. 24–32. (In Russ.) doi: 10.26425/2309-3633-2019-2-24-32.

6. **Glukhareva S.V., Shelupanov A.A., Nemirovich-Danchenko M.M.** [Formalized approach to assessing the level of reliability of employees of critical information infrastructure (CII) enterprises]. Perspektivy nauki, 2023, no. 4(163), pp. 17–23. (In Russ.)
7. **Golovinov O.N., Tkacheva M.V.** [Analysis and assessment of environmental security as a tool for ensuring the sustainable development of a corporation]. Sovremennaya ekonomika: problemy i resheniya, 2024, no. 4(172), pp. 86–103. (In Russ.) doi: 10.17308/meps/2078-9017/2024/4/86-103.
8. **Grabozdin Yu.P., Tatarovskiy Yu.A.** [Analysis of solvency and liquidity of a business in management consulting]. Ekonomika i predprinimatel'stvo, 2021, no. 12(137), pp. 1459–1462. (In Russ.) doi: 10.34925/EIP.2021.137.12.292.
9. **Grafov Yu.G.** [Digital sustainability as a condition for ensuring the economic security of a digital enterprise in the concretization of national development goals]. Industrial'naya ekonomika, 2022, vol. 5, no. 2, pp. 466–471. (In Russ.)
10. **Kovtunenko A.V.** [Improving the efficiency of consulting services in an innovative economy]. Nauchnye trudy Vol'nogo ekonomicheskogo obshchestva Rossii, 2010, vol. 137, pp. 743–749. (In Russ.)
11. **Korobeynikova L.S., Tkacheva M.V.** [Development of comprehensive economic analysis of corporate environmental sustainability]. Voronezh: Izd. dom VGU, 2022, 187 p. (In Russ.)
12. **Leshchenko Yu.G.** [Innovative vector in the system of economic security of Russia]. Voprosy innovatsionnoy ekonomiki, 2019, vol. 9, no. 2, pp. 301–316. (In Russ.) doi: 10.18334/vinec.9.2.40689.
13. **Lobanov S.Yu.** [Essence and content of financial security as an object of scientific research]. Ekonomika i predprinimatel'stvo, 2019, no. 1(102), pp. 1228–1232. (In Russ.)
14. **Lobov D.S., Rybin M.V., Shishonkova Yu.A.** [Effectiveness of the financial support ecosystem for innovation activities in the Russian Federation at the state and corporate levels in the oil and gas industry]. Kontrolling, 2022, no. 4(86), pp. 26–33. (In Russ.)
15. **Matveeva Ya.A.** [Interrelation of enterprise competitiveness and corporate social responsibility]. Sovremennaya ekonomika: problemy i resheniya, 2017, no. 3(87), pp. 128–141. (In Russ.) doi: 10.17308/meps.2017.3/1629.
16. **Modenov A.K., Vlasov M.P.** [Features of economic security in the digital economy]. Peterburgskiy ekonomicheskiy zhurnal, 2020, no. 2, pp. 121–134. (In Russ.) doi: 10.24411/2307-5368-2020-10015. EDN BPATYU.

17. **Smirnova O.P., Chesnyukova L.K.** [Assessment of the industrial potential of industrial regions of Russia: economic security]. Natsional'nye interesy: prioritety i bezopasnost', 2024, vol. 20, no. 4(433), pp. 743–758. (In Russ.) doi: 10.24891/ni.20.4.743.
18. **Titorenko A.G.** [Issues of ensuring the technical and technological component of the economic security of an enterprise]. Simvol nauki: mezhdunarodnyy nauchnyy zhurnal, 2018, no. 3, pp. 44–48. (In Russ.)
19. **Ianioglo A.** Comprehensive system of ensuring the economic security of enterprise. *Agricultural and Resource Economics: International Scientific E-Journal*, 2015, vol. 1, no 1, P. 69–79. doi: 10.5555/20173155242.