УДК 338

ЭКОНОМИЧЕСКАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВОЗМОЖНОСТИ И РИСКИ

Леонтьева С.М.

Старший преподаватель

Кафедра «Экономика и финансы»

Пермский национальный исследовательский политехнический университет,

Пермь, Россия

Мухина Е.Р.

Доцент, к.э.н.

Кафедра «Экономика и управление промышленным производством»

Пермский национальный исследовательский политехнический университет

Пермь, Россия

Литвинова А.А.

студент гр. ПИФ-24-1бз

Пермский национальный исследовательский политехнический университет

Пермь, Россия

Аннотация

Актуальность исследования обусловлена тем, что информационные ресурсы становятся важным экономическим активом. Нарушения в сфере информационной безопасности могут привести к значительным экономическим потерям, подрыву доверия и дестабилизации ключевых процессов в государстве и обществе. В статье отражена взаимосвязь экономической и информационной безопасности в условиях активной цифровизации бизнеса, финансовых систем и государственного управления, выявлены основные возможности и риски, проанализированы современные тенденции и стратегии

обеспечения безопасности. Определены методы и инструменты обеспечения экономической и информационной безопасности. В заключении статьи предложены рекомендации по совершенствованию системы обеспечения экономической и информационной безопасности.

Ключевые слова: экономическая и информационная безопасность, риски, возможности, цифровые технологии.

ECONOMIC AND INFORMATION SECURITY: OPPORTUNITIES AND RISKS

Leontyeva S.M.
Senior Lecturer
Department of Economics and Finance
Perm National Research Polytechnic University,
Perm, Russia

Mukhina E.R.
Associate Professor, PhD in Economics
Department of Economics and Industrial Management
Perm National Research Polytechnic University
Perm, Russia

Litvinova A.A.
Student, Group PIF-24-1bz
Perm National Research Polytechnic University
Perm, Russia

Abstract

the relevance of this study stems from the fact that information resources are becoming a vital economic asset. Information security breaches can lead to significant economic losses, undermine trust, and destabilize key processes in the state and society. This article examines the relationship between economic and information security in the context of the active digitalization of business, financial systems, and public administration. It identifies key opportunities and risks, and analyzes current security trends and strategies. It also identifies methods and tools for ensuring economic and information security. The article concludes with recommendations for improving economic and information security systems.

Keywords: economic and information security, risks, opportunities, digital technologies.

В условиях стремительного развития цифровых технологий, глобальной интеграции и усиления конкуренции обеспечение экономической и информационной безопасности приобретает всё большее значение как для отдельных компаний, так и для национальной и международной экономики в целом [5]. Экономическая и информационная безопасность являются ключевыми составляющими национальной безопасности любого государства [14].

В условиях глобализации, цифровизации и ускоряющихся темпов научно-технологического прогресса вопросы защиты экономической стабильности и информационного пространства приобретают первостепенное значение. Эффективное обеспечение безопасности в этих сферах предполагает комплексный подход, объединяющий правовые, организационные, технические и кадровые меры [7]. Экономическая безопасность - это состояние защищённости экономики от внутренних и внешних угроз, способное обеспечить устойчивое развитие, экономический суверенитет и высокий

уровень жизни населения. Угрозы экономической безопасности могут быть как внешнего (санкции, торговые войны, глобальные кризисы), так и внутреннего характера (коррупция, теневой сектор, инфляция, недостаток инвестиций и инноваций) [1].

В таблице 1 представлены основные методы обеспечения экономической безопасности.

Таблица 1. – Методы обеспечения экономической безопасности (составлено авторами).

Методы	Мероприятия
Государственное регулирование экономики	Проведение сбалансированной денежно-кредитной политики (управление ключевой ставкой, уровень инфляции, валютное регулирование). Бюджетная политика (эффективное распределение доходов и расходов бюджета, сокращение дефицита). Налоговая политика (установление справедливой налоговой нагрузки, борьба с уклонением от уплаты налогов).
Поддержка отечественного производства	Предоставление субсидий и государственных гарантий стратегически важным отраслям. Импортозамещение и протекционистские меры, направленные на снижение зависимости от внешних рынков. Создание благоприятного инвестиционного климата.
Развитие инноваций и внедрение новых технологий	Формирование наукоёмкой экономики и стимулирование научно-технического прогресса. Поддержка стартапов и малого технологического бизнеса через гранты, акселераторы, технопарки. Развитие цифровой экономики и ИТ-инфраструктуры.
Противодействие коррупции и теневой экономике	Повышение прозрачности бюджетных процессов и госзакупок. Ужесточение наказаний за финансовые и экономические преступления. Цифровизация государственного управления и внедрение технологий электронной отчетности и контроля.
Международное сотрудничество	Участие в международных экономических организациях (ВТО, ЕАЭС и др.). Привлечение иностранных инвестиций. Подписание двусторонних и многосторонних соглашений о совместных проектах, развитии торговли и технологического обмена.

В последнее время информационные угрозы стали неотъемлемой частью геополитической борьбы и экономического соперничества. Шпионаж, хакерские атаки, утечки данных и киберпреступность могут причинить

существенный ущерб государствам, компаниям и частным лицам. Информационная безопасность — это состояние защищённости информационной среды общества, отдельных лиц и государства от внешних и внутренних угроз, обеспечивающее качество, доступность, достоверность и конфиденциальность информации, а также устойчивость и целостность информационных систем [6].

В таблице 2 представлены методы обеспечения информационной безопасности.

Таблица 2. – Методы обеспечения информационной безопасности (составлено авторами).

Методы	Мероприятия
Технические меры защиты	Внедрение современных средств защиты информации: антивирусные программы, межсетевые экраны (firewall), системы предотвращения и обнаружения вторжений (IDS/IPS). Использование криптографических методов защиты. Обеспечение безопасной работы внутрисетевых и корпоративных систем.
Организационные меры	Разработка и внедрение политик информационной безопасности (инструкции по работе с данными, права доступа, резервное копирование). Формирование информационной культуры и контроль за соблюдением политики безопасности. Разделение ответственности между структурными подразделениями и контроль доступа к чувствительной информации.
Правовые меры	Разработка и применение законодательства в сфере защиты данных (например, Федеральный закон РФ «О персональных данных», закон «О государственной тайне»). Регулирование использования интеллектуальной собственности и защиты авторских прав. Привлечение к ответственности за киберпреступления, мошенничество.

Следует отметить, что экономическая и информационная безопасность глубоко взаимосвязаны. Утечка конфиденциальных данных, утраты коммерческой тайны или атаки на финансовые институты могут привести к серьёзным экономическим потерям. Кроме того, цифровизация экономики влечёт за собой расширение спектра угроз — от кибератак на банки и

стратегические объекты инфраструктуры до цифрового шпионажа и распространения фейковой информации, влияющей на поведение инвесторов и потребителей [10].

В свою очередь, снижение уровня экономической безопасности может способствовать росту киберугроз из-за нехватки средств на технологии защиты и квалифицированных людей.

Таким образом, экономическая безопасность неразрывно связана с информационной. Информационные активы (базы данных, цифровая инфраструктура, ПО и коммуникационные сети) - играют важнейшую роль в обеспечении функционирования государственных структур, бизнеса и финансовых институтов. Нарушения в их работе могут привести к большим экономическим потерям. Примеры таких угроз включают кибератаки на банки, утечки персональных данных, цифровое мошенничество и манипулирование экономической информацией. Обеспечение информационной безопасности - неотъемлемая часть стратегии общей экономической безопасности государства.

В таблице 3 представлены риски экономической и информационной безопасности.

Таблица 3 - Риски экономической и информационной безопасности (составлено авторами).

Риски экономической безопасности	Риски информационной безопасности
Финансовые риски (инфляция, колебания валютных курсов, банковские кризисы)	Кибератаки (вирусы, трояны, программы-вымогатели, DDoS-атаки)
Макроэкономические риски (рецессия, стагнация, дефицит бюджета)	Утечки данных (инсайдерские утечки, взломы, несанкционированный доступ)
Технологические риски (отставание от мировых лидеров, зависимость от импорта технологий)	Социальная инженерия (фишинг, обман, манипуляции)
Геополитические риски (торговые войны, санкции, политическая нестабильность)	Вредоносное программное обеспечение (ПО)
Коррупция и теневая экономика	Ошибки в конфигурации информационных систем
Криминальные риски (мошенничество, хищения, рейдерство)	Недостаточная осведомлённость пользователей о правилах информационной безопасности

Обеспечение экономической и информационной безопасности требует скоординированных усилий государства, бизнеса и гражданского общества, а также баланса между обеспечением безопасности и соблюдением прав и свобод личности. Инструменты обеспечения экономической и информационной безопасности представлены в таблице 4.

Таблица 4 - Инструменты обеспечения экономической и информационной безопасности.

Инструменты обеспечения экономической безопасности	Инструменты обеспечения информационной безопасности
Анализ рисков и уязвимостей экономики как на макроуровне и микроуровне	Проведение анализа рисков и угроз, в том числе внешних (хакерские атаки, кибершпионаж) и внутренних (недобросовестные сотрудники, ошибки в конфигурациях)
Прогнозирование социально-экономического развития и моделирование возможных стресс-сценариев	Разработка и внедрение комплексной политики информационной безопасности предприятий и государственных организаций
Разработка и реализация стратегий экономической безопасности — например, Стратегия экономической безопасности Российской Федерации до 2030 года	Непрерывный мониторинг IT-систем и аудит информационной безопасности, включая регулярное тестирование на проникновение (penetration testing)
Создание национальных систем мониторинга ключевых экономических показателей, таких как ВВП, уровень безработицы, инфляция, инвестиционная активность и др.	Создание центров оперативного реагирования на инциденты информационной безопасности (CERT/SOC)
Повышение уровня экономического образования и квалификации кадров в сфере управления, международной торговли, макроэкономического регулирования	Обучение сотрудников правилам безопасной работы с информационными системами, повышение квалификации IT-специалистов
	Применение международных стандартов в области информационной безопасности (например, ISO/IEC 27001)

В последние годы Россия сталкивается с рядом вызовов в сфере экономической и информационной безопасности, связанных с геополитической напряжённостью, санкционным давлением, ростом киберпреступности и необходимостью обеспечения технологической независимости [4]. Государство уделяет этим вопросам приоритетное внимание, разрабатывая и реализуя комплекс мер, направленных на укрепление экономической устойчивости и

повышение уровня информационной безопасности. Рассмотри динамику ключевых показателей за период 2023-2025 гг. (таблица 5).

Таблица 5 – Динамика ВВП, инфляции и уровня безработицы (составлено на основании источников [2,8]).

Год	ВВП, трлн. руб.	Инфляция, в %	Безработица, в %
2023	141	7,4	3,2
2024	201,152	9,5	2,5
2025	221,8	6	2,2

Номинальный объём ВВП России в 2023 году, по первой оценке Росстата, составил 141 трлн. рублей. В 2024 году, согласно второй оценке Росстата, ВВП увеличился и достиг 201,152 трлн. рублей в текущих ценах. По прогнозу Минэкономразвития России, в 2025 году объём ВВП может составить 221,8 трлн. рублей, что указывает на положительную динамику развития экономики в условиях внешнеполитического и санкционного давления [11]. Инфляция, оставаясь важнейшим показателем макроэкономической стабильности, в 2023 году достигла 7,4%. В 2024 году инфляция значительно ускорилась и составила 9,5%, что связано, в том числе, с геополитическими рисками, ослаблением рубля и ростом потребительского спроса [8]. Вместе с тем к концу декабря инфляция ожидается на уровне около 6%, что свидетельствует о стабилизации ценовой динамики. Рынок труда также демонстрирует устойчивость: к концу 2025 года безработица достигла исторически минимального уровня - 2,2%, отражая восстановление экономики, рост занятости и расширение деловой активности.

Обратим внимание на показатели информационной безопасности. С распространением цифровых технологий и ростом онлайн-сервисов в России наблюдается значительное увеличение числа преступлений, совершённых с использованием информационно-телекоммуникационных технологий. Так в

2023 году в России было зарегистрировано почти 700 тысяч киберпреступлений [10], при этом их доля в общем количестве всех преступлений выросла с 25,3% до 33,3%. Это говорит о том, что каждое третье преступление в стране совершается с использованием ИТ-инструментов. В 2024 году количество киберпреступлений продолжило расти. Согласно официальной статистике, за январь-декабрь было зафиксировано 765,4 тысячи таких правонарушений, что на 13,1% превышает показатель 2023 года. Основную массу составляют преступления, связанные с интернет-мошенничеством, хищениями денежных средств с банковских счетов, фишингом, кражами и продажей персональных данных. В 2025 году ситуация продолжает усугубляться. По оценке RED Security SOC, только за третий квартал 2025 года в России было зафиксировано свыше 42 тысяч кибератак, что на 73% больше, чем за аналогичный период прошлого года [10]. Рост числа киберпреступлений и атак на критически важные объекты подчеркивает необходимость усиления мер по обеспечению информационной безопасности на государственном и корпоративном уровнях, а также повышения цифровой грамотности населения [4]. Учитывая современные вызовы, вопрос кибербезопасности становится стратегическим направлением в обеспечении национальной безопасности России [14].

В таблице 6 приведены данные о динамике доли отечественного программного обеспечения на российском рынке, а также объёмах инвестиций в сферу информационной безопасности за 2023–2025 годы.

Таблица 6 – Доля отечественного программного обеспечения и объём инвестиций в информационную безопасность в России в период 2023-2025 гг. (составлено авторами на основании источников [3,13]).

Год	Доля отечественного программного обеспечения, в%	Инвестиции в информационную безопасность, млрд. руб.
2023	21	248,5
2024	35-40	339
2025	50	369

В 2023 году доля российского программного обеспечения в структуре рынка офисных решений достигла 21%. Как отмечают аналитики, основным драйвером роста стал переход государственных и госкорпоративных структур на отечественные решения в условиях санкционной изоляции и ограничений на использование зарубежного программного обеспечения. В 2024 году рынок российского программного обеспечения демонстрировал интенсивный рост — по данным Росстата, его объем увеличился на 40% год к году и достиг 4,97 трлн. рублей. Этот рост стал возможным благодаря государственной поддержке импортозамещения, активному развитию отечественных ИТ-продуктов и расширению спроса со стороны частного бизнеса. К 2025 году, доля отечественного программного обеспечения достигла в среднем 50%, что свидетельствует об уверенном продвижении цифрового суверенитета страны. Одновременно наблюдалось увеличение инвестиций в сферу информационной безопасности. В 2023 году объём рынка информационной безопасности составил 248,5 млрд. рублей, увеличившись на 28,5% по сравнению с предыдущим годом. В 2024 году этот показатель вырос до 339 млрд. рублей (+27% к 2023 г.), в том числе за счёт повышения числа киберугроз, цифровизации бизнес-процессов и ужесточения требований к защите информации. По прогнозу ЦСР, в 2025 году объём инвестиций достигнет 369 млрд. рублей. Рост капиталовложений в информационную безопасность отражает стремление государства и бизнеса к снижению уязвимостей цифровой инфраструктуры и усилению технологической независимости [12].

Анализ статистических данных показывает, что в Российской Федерации наблюдается рост киберпреступности, утечек данных, а также увеличение инвестиций в информационную безопасность. Вместе с тем сохраняются проблемы, связанные с санкционным давлением, дефицитом квалифицированных кадров и технологическим отставанием.

В заключении проведенного исследования предлагаются следующие рекомендации по совершенствованию системы обеспечения экономической и информационной безопасности: развитие собственного производства критически важных технологий, усиление мер по защите от киберугроз, подготовка квалифицированных кадров в области экономической и информационной безопасности, повышение осведомлённости населения о правилах информационной безопасности, укрепление международного сотрудничества в сфере экономической и информационной безопасности.

Таким образом, реализация этих мер позволит повысить уровень экономической и информационной безопасности России и обеспечить её устойчивое развитие в долгосрочной перспективе.

Библиографический список

1. Бурдина Л. А. К вопросу об экономической безопасности предприятия: ключевые риски и угрозы в современном мире / Л. А. Бурдина // Современная конкуренция. – 2025. – Т. 19, № 5(107). – С. 90-107.

2. Вести.ру. ВВП России в 2024 [Электронный ресурс]. — URL: https://clc.li/cJDuy (дата обращения: 20.11.2025).

3. Инвестиции в ИБ России [Электронный ресурс]. — URL: https://clc.li/wSUBA (дата обращения: 20.11.2025).

4. Коммерсант. Повышение киберпреступности [Электронный ресурс]. — URL: https://clc.li/zprMr (дата обращения: 25.11.2025).

5. Копылова О. А. Основные подходы к анализу и оценке экономической безопасности предприятия / О. А. Копылова, С. В. Чучкалова // Вектор экономики. – 2025. – № 8(110). – EDN IYZYEI.

6. Крупко О. О. Аудит информационной безопасности и его методы в управлении информационной безопасностью организации / О. О. Крупко, А. В. Шабурова // Интерэкспо Гео-Сибирь. – 2024. – Т. 6. – С. 115-120.

7. Мухина Е. Р., Леонтьева С.М., Базарбаева Д.А. Механизм обеспечения экономической безопасности предприятия машиностроительной отрасли // Управленческий учет. – 2025. – № 4. – С. 307-315.

8. Сберметр. Инфляция и безработица [Электронный ресурс]. — URL: https://clc.li/KlUeT (дата обращения: 29.11.2025).

9. Терентьев Д. Е. Влияние системы искусственного интеллекта в системы защиты информации / Д. Е. Терентьев, А. Л. Ткаченко // Дневник науки. – 2025. – № 1(97). – EDN AHHBCB.

10. Точность. Киберугрозы — [Электронный ресурс]. – URL: https://clc.li/jFSzY (дата обращения: 29.11.2025).

11. Финам. Оценки ВВП 2025 — [Электронный ресурс]. – URL: https://clc.li/IBPTS (дата обращения: 07.12.2025).

12. Форбс. Объём рынка ИБ. — [Электронный ресурс]. URL: https://clc.li/GsVjU (дата обращения: 29.11.2025).

13. Хайтэч. Доля отечественного ПО [Электронный ресурс]. — URL: https://clc.li/Cafjj (дата обращения: 07.11.2025).

14. Чапис М. А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере / М. А. Чапис // Наукосфера. – 2024. – № 6-1. – С. 551-557.