

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2026, Том 18, № 1 / 2026, Vol. 18, Iss. 1 <https://esj.today/issue-1-2026.html>

URL статьи: <https://esj.today/PDF/76ECVN126.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Сигалов, А. С. Организационно-экономический механизм обеспечения безопасности предпринимательских сетей в цифровой среде / А. С. Сигалов, Н. В. Капустина // Вестник евразийской науки. — 2026. — Т. 18. — № 1. — URL: <https://esj.today/PDF/76ECVN126.pdf>.

For citation:

Sigalov A.S., Kapustina N.V. Organizational and economic mechanism for ensuring the security of business networks in the digital environment. *The Eurasian Scientific Journal*. 2026;18(1): 76ECVN126. Available at: <https://esj.today/PDF/76ECVN126.pdf>. (In Russ., abstract in Eng.).

УДК 338.24:004.056

Сигалов Александр Станиславович

ФГБОУ ВО «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет)», Москва, Россия
Аспирант кафедры «Финансов, бухгалтерского учета и экономической безопасности»
E-mail: sigalov2012@inbox.ru

Капустина Надежда Валерьевна

ФГАОУ ВО «Российский университет транспорта РУТ (МИИТ)», Москва, Россия
Профессор кафедры «Экономика транспортной инфраструктуры и управление строительным бизнесом»
Доктор экономических наук, доцент
E-mail: kuzminova_n@mail.ru

Организационно-экономический механизм обеспечения безопасности предпринимательских сетей в цифровой среде

Аннотация. Трансформация архитектуры предпринимательских структур от иерархических моделей к сетевым формам организации бизнеса в условиях цифровизации экономики порождает качественно новые вызовы и угрозы экономической безопасности, требующие разработки инновационных защитных механизмов, интегрирующих технологические, экономические и институциональные компоненты. Исследование направлено на выявление и систематизацию элементов организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей, функционирующих в цифровом пространстве и подверженных воздействию киберугроз. Предметная область охватывает теоретико-методологические основания, институциональные механизмы и практический инструментарий защиты сетевых бизнес-структур от экономических рисков цифровой среды. В работе проанализированы фундаментальные теории экономической безопасности, концептуальные модели сетевой экономики, методологические подходы к управлению киберрисками и инновационные решения в области защиты критической информационной инфраструктуры. Прослежена эволюция научных представлений об экономической безопасности от классических концепций защиты материальных активов к холистическим моделям обеспечения устойчивости цифровых экосистем в условиях перманентных киберугроз. Идентифицированы и классифицированы ключевые компоненты организационно-экономического механизма: технологическая инфраструктура (системы искусственного интеллекта, блокчейн-платформы, квантовая криптография), экономический инструментарий (страхование киберрисков, инвестиционные программы, система санкций), организационно-управленческие практики (политики безопасности, риск-

менеджмент, развитие компетенций) и институциональная среда (нормативное регулирование, стандартизация, международная координация). Предложенная интегративная модель раскрывает многоуровневую архитектуру взаимодействия гетерогенных элементов механизма, где технологические инновации формируют базис защиты, экономические инструменты создают мотивационную основу и ресурсное обеспечение, а институциональные факторы определяют регуляторные рамки безопасного функционирования предпринимательских сетей. Научная новизна заключается в комплексной систематизации факторов обеспечения экономической безопасности сетевых предпринимательских структур в цифровом пространстве, выявлении специфических особенностей трансформации защитных механизмов в условиях платформенной экономики и разработке интегративной модели, синтезирующей технологические, экономические и институциональные компоненты. Практическая значимость определяется применимостью разработанных положений для формирования корпоративных стратегий кибербезопасности, проектирования систем защиты предпринимательских экосистем и совершенствования регуляторной среды цифровой экономики.

Ключевые слова: экономическая безопасность; предпринимательские сети; цифровая среда; кибербезопасность; организационно-экономический механизм; цифровые экосистемы; управление рисками; блокчейн; искусственный интеллект; платформенная экономика; критическая информационная инфраструктура

Введение

Цифровая трансформация глобальной экономики катализировала беспрецедентные изменения в архитектуре предпринимательских структур, характеризующиеся переходом от традиционных иерархических моделей к сетевым формам организации бизнеса, функционирующим на основе цифровых платформ и экосистем, при чем согласно исследованию McKinsey Global Institute, к 2025 году около 30 % корпоративного дохода в мире будут генерировать цифровые бизнес-экосистемы, достигнув объема в \$60 трлн и увеличив свою долю в мировой экономике с текущих 1–2 % до 30 %.¹ Формирование предпринимательских сетей в цифровой среде сопровождается экспоненциальным ростом киберугроз и экономических рисков, при чем по данным аналитического центра InfoWatch, объем утечек персональных данных россиян за 2023 год вырос на 60 % по сравнению с 2022 годом, а малый бизнес стал вдвое чаще терять конфиденциальную информацию, причем из российских организаций за 2023 год утекло 95 крупных баз данных — на 28 % больше, чем в 2022 году.² Российский рынок информационной безопасности демонстрирует устойчивый рост, достигнув в 2024 году объема 339 млрд рублей с приростом 27 % по сравнению с предыдущим годом, что обусловлено возросшим количеством киберугроз, процессами импортозамещения и ужесточением регуляторных требований к защите данных.³

¹ Ведомости&. Как экосистемы меняют быт, покупки и коммуникацию потребителей. — [Электронный ресурс] Режим доступа: URL: <https://www.vedomosti.ru/partner/articles/2021/12/21/901904-ekosistemi-menyayut> (дата обращения 07.09.2025).

² ComNews. Утечки персданных россиян в 2023 г. кратно возросли и в 2024 г. не планируют снижаться. — [Электронный ресурс] Режим доступа: URL: <https://www.comnews.ru/content/231983/2024-03-12/2024-w11/1008/utechki-persdannyykh-rossiyan-2023-g-kratno-vozrosli-i-2024-g-ne-planiruyut-snizhatsya> (дата обращения 07.09.2025).

³ TAdviser. Информационная безопасность (рынок России). — [Электронный ресурс] Режим доступа: URL: [https://www.tadviser.ru/index.php/Статья:Информационнаябезопасность\(рынок_России\)](https://www.tadviser.ru/index.php/Статья:Информационнаябезопасность(рынок_России)) (дата обращения 07.09.2025).

Трансформация предпринимательских структур в направлении создания цифровых экосистем и платформенных решений порождает качественно новые вызовы для обеспечения экономической безопасности, требующие переосмысления традиционных подходов к защите бизнеса и разработки инновационных организационно-экономических механизмов, при чем согласно исследованию Positive Technologies, в III квартале 2024 года количество кибератак в России увеличилось на 15 % по сравнению с аналогичным периодом 2023 года, а средняя стоимость утечки данных для организаций достигла \$4,88 миллиона.⁴ Формирование национальной программы «Цифровая экономика Российской Федерации» создало институциональную основу для развития систем обеспечения информационной безопасности, включая федеральный проект «Информационная безопасность», предусматривающий выделение 12,21 млрд рублей в 2025 году на развитие инфраструктуры кибербезопасности.⁵

Актуальность темы исследования определяется несколькими взаимосвязанными факторами, формирующими современный контекст функционирования предпринимательских структур в цифровой экономике и требующими системного научного осмысления механизмов обеспечения их экономической безопасности. Масштабное распространение сетевых форм организации бизнеса создает новые вызовы для обеспечения экономической безопасности, при чем согласно данным исследования Spektr, по итогам 2024 года лидерами экосистемного рынка в России остаются Сбер и Яндекс по охвату и наполнению основных b2c-направлений, за ними следуют VK, МТС и Т-Банк, причем активнее всего сервисы открывались в вертикалях финансов, развлечений, покупок и образования.⁶ Цифровизация предпринимательской деятельности сопровождается ростом киберугроз и экономических потерь от инцидентов информационной безопасности, при чем по данным Kaspersky, 75 % от всех утечек информации в российских компаниях в 2024 году произошли из-за человеческого фактора, а 44 % представителей российского бизнеса назвали причиной утечек неумышленные действия сотрудников.⁷ Развитие регуляторной среды в области защиты данных и кибербезопасности требует от предпринимательских структур внедрения комплексных систем обеспечения экономической безопасности, при чем с 1 января 2025 года установлен запрет на использование импортных средств защиты информации, а на отдельные виды технически сложных товаров должны быть установлены российские программы для ЭВМ, включая средства антивирусной защиты.⁸

Научная проблема заключается в недостаточной теоретической проработанности организационно-экономических механизмов обеспечения экономической безопасности предпринимательских сетей в условиях цифровой трансформации, а также в отсутствии комплексной модели, интегрирующей технологические, экономические, организационные и институциональные аспекты защиты сетевых бизнес-структур от киберугроз и экономических рисков цифровой среды.

⁴ РБК Тренды. Технологии против угроз: 7 трендов кибербезопасности в 2025 году. — [Электронный ресурс] Режим доступа: URL: <https://trends.rbc.ru/trends/industry/678f84c69a79478682c0120b> (дата обращения 07.09.2025).

⁵ TAdviser. Информационная безопасность цифровой экономики России. — [Электронный ресурс] Режим доступа: URL: <https://tadviser.ru/index.php/Статья:ИнформационнаябезопасностьцифровойэкономикиРоссии> (дата обращения 07.09.2025).

⁶ Spektr. Исследование: крупнейшие российские цифровые экосистемы 2024–2025. — [Электронный ресурс] Режим доступа: URL: <http://spektr.team/tpost/g8cbrog511-issledovanie-krupneishie-rossiiskie-tsif> (дата обращения 07.09.2025).

⁷ Коммерсантъ. Кибербезопасность 2025: актуальные риски и тренды. — [Электронный ресурс] Режим доступа: URL: https://events.kommersant.ru/nov/events/2025-04-29_kiberbezopasnost-2025-aktualnye-riski-i-trendy/ (дата обращения 07.09.2025).

⁸ УЦСБ. Обзор изменений в законодательстве ИТ и ИБ за июль 2024 года. — [Электронный ресурс] Режим доступа: URL: <https://www.ussc.ru/news/novosti/obzor-izmeneniy-v-zakonodatelstve-za-iyul-2024-goda/> (дата обращения 07.09.2025).

Объектом исследования выступает система экономической безопасности предпринимательских сетей, функционирующих в условиях цифровой экономики.

Предметом исследования являются теоретические подходы, методологические основания и практические инструменты формирования организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей в цифровой среде.

Цель исследования — проведение комплексного теоретико-методологического анализа организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей и разработка интегративной модели защиты сетевых бизнес-структур в условиях цифровой трансформации.

Задачи исследования:

1. Проанализировать эволюцию теоретических подходов к обеспечению экономической безопасности предпринимательских структур в контексте перехода к сетевым формам организации бизнеса и цифровой трансформации экономики.
2. Систематизировать и классифицировать компоненты организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей в цифровой среде.
3. Разработать интегративную модель организационно-экономического механизма, учитывающую взаимосвязь технологических, экономических, организационных и институциональных факторов обеспечения безопасности.

Научная новизна исследования заключается в выявлении и систематизации комплекса взаимосвязанных компонентов организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей, включающего технологические инновации (блокчейн, искусственный интеллект, криптография), экономические инструменты (страхование, инвестиции, санкции) и институциональные факторы (регулирование, стандарты, международное сотрудничество), а также в разработке интегративной модели, синтезирующей различные теоретические подходы и учитывающей специфику функционирования сетевых структур в цифровой экономике.

Практическая значимость работы определяется возможностью применения разработанных теоретических положений и методологических подходов для формирования корпоративных стратегий кибербезопасности, проектирования эффективных систем защиты предпринимательских экосистем, создания регуляторной среды, поддерживающей безопасное развитие цифровой экономики, а также развития компетенций специалистов по обеспечению экономической безопасности в цифровой среде.

1. Методы и материалы

Методологическую основу исследования составляют фундаментальные принципы системного анализа, позволяющие рассматривать организационно-экономический механизм обеспечения экономической безопасности предпринимательских сетей как сложную многоуровневую систему взаимосвязанных технологических, экономических, организационных и институциональных компонентов.

Теоретическим базисом выступают классические концепции экономической безопасности, изложенные в Стратегии экономической безопасности Российской Федерации на период до 2030 года, определяющей экономическую безопасность как состояние защищенности национальной

экономики от внешних и внутренних угроз⁹, теории сетевой экономики и платформенных решений, концепции управления киберрисками и современные подходы к защите критической информационной инфраструктуры.

В качестве основных методов исследования использован комплекс теоретических и эмпирических методов, включающий контент-анализ научной литературы по проблематике экономической безопасности и кибербезопасности предпринимательских структур, компаративный анализ различных моделей организации защиты цифровых экосистем и платформенных решений, метод систематизации и классификации для выявления и группировки компонентов организационно-экономического механизма, а также методы концептуального моделирования для разработки интегративной модели обеспечения экономической безопасности предпринимательских сетей в цифровой среде.

Эмпирическую базу исследования составили данные международных организаций (ОЭСР, Всемирный банк, Всемирный экономический форум), национальных статистических служб (Росстат, ФНС России), результаты исследований ведущих консалтинговых компаний (McKinsey, Deloitte, PwC, KPMG), аналитические отчеты специализированных компаний в области кибербезопасности (Kaspersky, Positive Technologies, InfoWatch), корпоративные отчеты и кейсы трансформации ведущих российских цифровых экосистем (Сбер, Яндекс, VK, МТС), а также актуальные исследования академических институтов (Институт экономики РАН, НИУ ВШЭ, РЭУ имени Г.В. Плеханова).

Теоретической базой выступают труды отечественных исследователей, посвященные различным аспектам механизмов обеспечения экономической безопасности предприятий и регионов. Фундаментальные вопросы разработки системы индикаторов экономической безопасности предприятия раскрываются в работе В.В. Познякова, Н.В. Капустиной, О.А. Аничкиной и соавторов [1], где авторы исследуют современные особенности формирования индикативной системы. Н.В. Капустина [2] развивает данное направление, проводя комплексный анализ аспектов обеспечения экономической безопасности предпринимательской деятельности и ее индикаторов.

Системный подход к исследованию детерминант развития экономики и общества в условиях глобальных изменений представлен в коллективной монографии В.И. Авдийского, О.А. Аничкиной, А.С. Апачанова и соавторов [3], которая создает теоретическую основу для понимания современных вызовов экономической безопасности.

Стратегические аспекты обеспечения экономической безопасности в условиях новых вызовов исследуются В.О. Бессарабовым и А.П. Лутай [4], которые анализируют стратегии и механизмы защиты предприятий от современных угроз. В.А. Артамонов [5] проводит оценку механизма обеспечения экономической безопасности предприятия, акцентируя внимание на практических инструментах. Н.А. Сушко [6] рассматривает информационно-аналитическое обеспечение механизма воспроизводства основных фондов с целью обеспечения экономической безопасности предприятия, подчеркивая важность управления материальными активами.

Особое место в современных исследованиях занимает роль цифровизации в трансформации механизмов обеспечения экономической безопасности. Е.И. Кузнецова и О.В. Сараджева [7] исследуют роль цифровизации в трансформации институционального механизма обеспечения экономической безопасности региона, раскрывая потенциал цифровых технологий в системе защиты экономических интересов.

⁹ КонсультантПлюс. Экономическая безопасность это. — [Электронный ресурс] Режим доступа: URL: <https://www.consultant.ru/law/podborki/jekonomicheskayabezopasnostjeto/> (дата обращения 07.09.2025).

Концептуальные основы механизма обеспечения экономической безопасности предприятия анализирует Т.А. Юсупова [8], систематизируя ключевые элементы защитного механизма. И.И. Сальников и Д.П. Маширов [9] детально исследуют содержание и инструменты механизма обеспечения экономической безопасности предприятия, предлагая практический инструментарий.

Специфические механизмы обеспечения экономической безопасности рассматриваются в ряде работ. Н.Н. Ощепкова [10] анализирует конкурентоспособность как механизм обеспечения экономической безопасности, подчеркивая рыночные аспекты защиты. Ю.С. Холопова и Н.Н. Поташкова [11] исследуют укрепление финансовой устойчивости как механизм обеспечения экономической безопасности предприятия, акцентируя внимание на финансовых инструментах защиты. О.А. Аничкина, А.В. Бекетов и Т.Н. Коротких [12] рассматривают механизмы функционирования системы обеспечения продовольственной безопасности России в экономическом аспекте, демонстрируя отраслевую специфику обеспечения безопасности.

Таким образом, анализ представленных научных трудов демонстрирует многоаспектность проблематики формирования организационно-экономического механизма обеспечения безопасности предпринимательских сетей в цифровой среде, охватывая индикативные системы, стратегические подходы, институциональные механизмы и роль цифровизации в трансформации защитных инструментов.

Информационной основой исследования послужили научные публикации в ведущих российских журналах по экономической безопасности, управлению и информационным технологиям, материалы профессиональных конференций по кибербезопасности и цифровой трансформации, нормативные правовые акты Российской Федерации в области информационной безопасности и защиты данных, а также актуальные данные о развитии рынка кибербезопасности и предпринимательских экосистем в России и мире за период 2023–2025 годов.

Для анализа российской специфики использованы данные исследований Центра стратегических разработок, Ассоциации ФинТех, Российской ассоциации криптоэкономики, искусственного интеллекта и блокчейна (РАКИБ), материалы специализированных изданий (TAdviser, ComNews, CNews), отчеты российских компаний-лидеров в области кибербезопасности.

2. Результаты и обсуждение

Формирование современной парадигмы обеспечения экономической безопасности предпринимательских сетей в цифровой среде представляет собой комплексный процесс трансформации традиционных подходов к защите бизнеса под влиянием технологических инноваций, изменения архитектуры предпринимательских структур и эволюции угроз в киберпространстве, при чем каждый этап цифровизации экономики привносит качественно новые элементы в понимание природы экономических рисков и механизмов их минимизации. Теоретические основания современных подходов к экономической безопасности в цифровую эпоху восходят к фундаментальным работам по теории экономической безопасности, рассматривающей защищенность экономических систем от внешних и внутренних угроз как базовое условие устойчивого развития, однако современная интерпретация данной теории в контексте цифровой трансформации существенно расширяет понимание экономической безопасности, включая в нее не только защиту материальных активов и финансовых ресурсов, но и обеспечение информационной безопасности, защиту интеллектуальной собственности, сохранность данных и непрерывность бизнес-процессов в условиях киберугроз.

Анализ эволюции предпринимательских структур от традиционных иерархических моделей к сетевым формам организации бизнеса демонстрирует фундаментальные изменения в архитектуре экономических взаимодействий, при чем согласно исследованию АНО

«Цифровая экономика», объем вложений в отечественные ИТ-решения вырос с 441,4 млрд рублей на конец 2022 года до 586,9 млрд рублей к декабрю 2023 года, а в России насчитывалось 19,1 тыс. ИТ-компаний, формирующих основу цифровой инфраструктуры предпринимательских сетей.¹⁰ Предпринимательские сети в цифровой среде характеризуются высокой степенью взаимозависимости участников, использованием общих технологических платформ, интенсивным обменом данными и формированием экосистемных связей, что создает как новые возможности для развития бизнеса через синергетические эффекты и экономию на масштабе, так и порождает системные риски, связанные с возможностью каскадного распространения киберугроз по всей сети.

Современная архитектура киберугроз для предпринимательских сетей представляет собой сложную многоуровневую систему рисков, включающую технические угрозы (вредоносное программное обеспечение, DDoS-атаки, эксплуатация уязвимостей), социально-инженерные атаки (фишинг, претекстинг, бейтинг), инсайдерские угрозы (умышленные и неумышленные действия сотрудников) и угрозы, связанные с цепочками поставок, при чем согласно исследованию ЦСР «Северо-Запад» и Positive Technologies, к 2027 году российские компании будут нуждаться в 235 000–260 000 экспертов по кибербезопасности, а дефицит специалистов снизится до 23–25 %.¹¹ Специфика угроз для предпринимательских сетей заключается в их системном характере, когда компрометация одного участника сети может привести к нарушению функционирования всей экосистемы, при чем исследование Kaspersky ICS-CERT зафиксировало во втором квартале 2024 года рост атак на промышленные системы управления, что свидетельствует о целенаправленном воздействии киберпреступников на критическую инфраструктуру предпринимательских сетей.¹²

Технологическая составляющая организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей базируется на интеграции передовых цифровых технологий, среди которых особое место занимают системы на основе искусственного интеллекта и машинного обучения, при чем согласно данным Venture Guide, за три квартала 2024 года в России совершено 28 сделок с участием компаний, занимающихся искусственным интеллектом и машинным обучением, с общим объемом инвестиций \$14,11 млн, что свидетельствует о признании критической важности данных технологий для обеспечения безопасности.¹³ Применение искусственного интеллекта в системах экономической безопасности позволяет автоматизировать процессы мониторинга, обнаружения и реагирования на киберугрозы в режиме реального времени, минимизируя масштаб потенциального воздействия и обеспечивая возможность превентивного реагирования на основе предиктивной аналитики.¹⁴

¹⁰ НИУ ВШЭ. Белая книга цифровой экономики 2023. — [Электронный ресурс] Режим доступа: URL: https://files.data-economy.ru/Docs/White_paper_2023_.pdf (дата обращения 07.09.2025).

¹¹ Сбер. Защита бизнеса от киберугроз в 2025 году. — [Электронный ресурс] Режим доступа: URL: <https://sber.pro/publication/na-shag-vpered-i-hakerov-kak-zaschitit-biznes-ot-kiberugroz-v-2025-godu/> (дата обращения 07.09.2025).

¹² Хабр. Что ждёт сферу кибербезопасности в 2025 году: тренды, технологии и ключевые навыки. — [Электронный ресурс] Режим доступа: URL: <https://habr.com/ru/companies/netologyru/articles/900718/> (дата обращения 07.09.2025).

¹³ ComNews. Искусственный интеллект и машинное обучение лидируют по объему венчурных инвестиций в 2024 г. — [Электронный ресурс] Режим доступа: URL: <https://www.comnews.ru/content/235954/2024-10-29/2024-w44/1007/iskusstvennyy-intellekt-i-mashinnoe-obuchenie-lidiruyut-obemu-venchurnykh-investitsiy-2024-g> (дата обращения 07.09.2025).

¹⁴ Kaspersky. Искусственный интеллект и машинное обучение в кибербезопасности. — [Электронный ресурс] Режим доступа: URL: <https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity> (дата обращения 07.09.2025).

В таблице 1 представлен сравнительный анализ основных технологических решений для обеспечения экономической безопасности предпринимательских сетей в цифровой среде.

Таблица 1

**Сравнительный анализ технологических решений
обеспечения экономической безопасности предпринимательских сетей**

Технология	Характеристики и возможности	Преимущества для безопасности	Ограничения и риски	Экономические показатели	Примеры внедрения
Искусственный интеллект и ML	Автоматизация обнаружения угроз, предиктивная аналитика, поведенческий анализ, обработка больших данных	Скорость реагирования увеличивается на 90 %, точность обнаружения угроз до 95 %, снижение false positive на 60 %	Необходимость больших объемов данных для обучения, риски adversarial атак, высокие требования к вычислительным ресурсам	Инвестиции в ИИ для безопасности: \$34 млн в 2024 г., ROI 200–300 % за 2–3 года	Сбер (использует ИИ в 85 % процессов), Kaspersky (AI-powered антивирус), MTC (платформа для AI-разработки)
Блокчейн и распределенные реестры	Неизменность записей, децентрализация, криптографическая защита, смарт-контракты	Защита от захвата мощностей 76 %, исключение единой точки отказа, прозрачность транзакций	Масштабируемость (1–100 тыс. транзакций/сек к 2024), энергопотребление, регуляторная неопределенность	Потенциальный эффект для экономики РФ: 1,6 трлн руб. к 2024 г., необходимые инвестиции: 78 млрд руб.	Мастерчейн (ФинТех), ВТБ (цифровые закладные), Waves Enterprise
Квантовая криптография	Абсолютная защита канала связи, обнаружение попыток перехвата, квантовое распределение ключей	Теоретически невзламываемая защита, соответствие ГОСТ Р 34.11-2012, 34.10-2012	Дальность передачи (до 100 км), стоимость оборудования, сложность интеграции	Инвестиции в исследования: 700 млн руб., рынок к 2030 г.: \$25 млрд	Ростелеком (квантовые сети), РЖД (защита каналов), Сбер (пилотные проекты)
Zero Trust Architecture	Непрерывная верификация, микросегментация сети, принцип наименьших привилегий	Снижение площади атаки на 70 %, минимизация lateral movement, защита от инсайдеров	Сложность внедрения, изменение бизнес-процессов, необходимость реинжиниринга	Затраты на внедрение: 5–10 % ИТ-бюджета, снижение инцидентов на 50 %	Microsoft (Zero Trust модель), Google (BeyondCorp), Яндекс (микросервисная архитектура)
SIEM и SOAR системы	Централизованный мониторинг, корреляция событий, автоматизация реагирования	Сокращение времени обнаружения с дней до минут, автоматизация 80 % рутинных задач	Высокая стоимость лицензий, необходимость квалифицированного SOC, большое количество ложных срабатываний	Рынок SIEM в РФ: 25 млрд руб., рост 30 % в год	Positive Technologies (MaxPatrol), Kaspersky (KUMA), крупные банки и телеком

Составлено автором на основе анализа материалов¹⁵

Блокчейн-технологии и системы распределенного реестра представляют особый интерес для обеспечения экономической безопасности предпринимательских сетей благодаря своим уникальным характеристикам, обеспечивающим неизменность данных, децентрализацию управления и криптографическую защиту транзакций, при чем согласно дорожной карте

¹⁵ CNews. Российским блокчейн-разработчикам нужно 80 млрд руб. — [Электронный ресурс] Режим доступа: URL: <https://www.cnews.ru/articles/2019-08-27rossijskimblokchejnrazrabotchikam> (дата обращения 07.09.2025).

TAdviser. Тенденции развития технологий искусственного интеллекта в России. — [Электронный ресурс] Режим доступа: URL: <https://tadviser.ru/index.php/Статья:ТенденцииразвитиятехнологийискусственногointellektaвРоссии.ОбзорTAdviser2025> (дата обращения 07.09.2025).

Anti-Malware. Тренды рынка кибербезопасности в России: прогноз на 2024–2025 гг. — [Электронный ресурс] Режим доступа: URL: <https://www.anti-malware.ru/analytics/TechnologyAnalysis/Cybersecurity-market-trends-2024-2025> (дата обращения 07.09.2025).

развития технологий распределенного реестра в России, к 2024 году планировалось достижение скорости обработки 100 тысяч транзакций в секунду и создание 50 запатентованных технологий организации и синхронизации данных.¹⁶ Внедрение блокчейн-решений в предпринимательских сетях позволяет создать доверенную среду для автоматизации бизнес-процессов и взаимодействия контрагентов без необходимости привлечения посредников, при чем платформа «Мастерчейн», разработанная Ассоциацией ФинТех, стала первой в России блокчейн-платформой, прошедшей сертификацию в ФСБ России и использующей ГОСТ-криптографию для обеспечения защищенного обмена финансовыми сообщениями.¹⁷

Экономическая составляющая организационно-экономического механизма обеспечения безопасности предпринимательских сетей включает комплекс финансовых инструментов и экономических стимулов, направленных на создание устойчивой системы финансирования мероприятий по защите от киберугроз и компенсации потенциальных потерь, при чем согласно данным правительства РФ, на разработки в области искусственного интеллекта для целей безопасности в 2024 году было запланировано выделить около 5,2 млрд рублей, а к 2025 году внедрение технологий ИИ должно принести компаниям РФ около 1 трлн рублей дополнительного дохода. Страхование киберрисков становится критически важным элементом экономической защиты предпринимательских сетей, позволяя перенести часть финансовых рисков на страховые компании и обеспечить финансовую устойчивость в случае реализации киберугроз, при чем российский рынок киберстрахования демонстрирует устойчивый рост, хотя и отстает от мировых показателей по уровню проникновения.

Инвестиционная политика в области обеспечения экономической безопасности предпринимательских сетей характеризуется необходимостью балансирования между затратами на превентивные меры защиты и потенциальными потерями от реализации киберугроз, при чем исследования показывают, что компании, инвестирующие 5–10 % ИТ-бюджета в кибербезопасность, достигают снижения количества инцидентов на 50 % и сокращения времени восстановления после инцидентов на 70 %.¹⁸ Экономические санкции и штрафы за нарушение требований по защите данных создают дополнительные стимулы для инвестиций в безопасность, при чем в России значительно увеличились штрафы за утечки данных, причем оборотные штрафы существенно превышают ранее установленные пределы административных взысканий, что заставляет компании более серьезно относиться к вопросам защиты информации.¹⁹

Организационная составляющая механизма обеспечения экономической безопасности предпринимательских сетей охватывает систему управленческих практик, процедур и политик, направленных на создание эффективной системы управления рисками и обеспечения непрерывности бизнеса в условиях киберугроз, при чем согласно исследованию Harvard Business Publishing, 70 % организаций считают критически важным развитие лидерских

¹⁶ CNews. Блокчейн принесет российской экономике 1,6 триллиона. — [Электронный ресурс] Режим доступа: URL: <https://www.cnews.ru/news/top/2019-07-17blokcheinprinesetrossijskojekonomike16trillionov> (дата обращения 07.09.2025).

¹⁷ ФинТех. Блокчейн — технология распределенного реестра. — [Электронный ресурс] Режим доступа: URL: <https://www.fintechru.org/press-center/news/bolshe-chem-prosto-bitkoin-zachem-nuzhen-blokcheyn/> (дата обращения 07.09.2025).

¹⁸ Kickidler. Кибербезопасность компании: основные риски и методы защиты. — [Электронный ресурс] Режим доступа: URL: <https://www.kickidler.com/ru/info/ugrozyi-kiberbezopasnosti-biznesa-i-kak-ot-nix-zashhititsya.html> (дата обращения 07.09.2025).

¹⁹ КонсультантПлюс. Информационная безопасность. — [Электронный ресурс] Режим доступа: URL: https://www.consultant.ru/law/podborki/informacionnaya_bezopasnost/ (дата обращения 07.09.2025).

компетенций для управления безопасностью в условиях цифровой трансформации.²⁰ Формирование культуры кибербезопасности в предпринимательских сетях требует системного подхода к обучению и повышению осведомленности сотрудников, при чем человеческий фактор остается главным источником угроз — в 2024 году 44 % представителей российского бизнеса назвали причиной утечек неумышленные действия сотрудников, а 37 % — спланированные операции персонала.²¹

Институциональная составляющая организационно-экономического механизма формирует правовую и нормативную основу для обеспечения экономической безопасности предпринимательских сетей, при чем в России создана комплексная система нормативного регулирования цифровой среды, включающая федеральные законы «Об информации, информационных технологиях и о защите информации», «О коммерческой тайне», а также специализированные требования ФСТЭК России и ФСБ России по защите информации.²²

Международное сотрудничество в области обеспечения экономической безопасности предпринимательских сетей приобретает особую значимость в условиях трансграничного характера киберугроз и глобализации цифровой экономики, при чем согласно исследованиям ОЭСР, необходима разработка единой методологической основы для измерения цифровой экономики и оценки киберрисков, что позволит обеспечить сопоставимость данных и эффективность международной координации в борьбе с киберпреступностью.²³ Развитие стандартов информационной безопасности играет ключевую роль в формировании единых подходов к защите предпринимательских сетей, при чем в январе 2025 года вступил в силу национальный стандарт ГОСТ Р 71476–2024 «Искусственный интеллект. Концепции и терминология искусственного интеллекта», устанавливающий единую терминологию и подходы к применению ИИ в системах безопасности.²⁴ Специфика российского подхода к обеспечению экономической безопасности предпринимательских сетей обусловлена необходимостью импортозамещения в критических областях информационных технологий и кибербезопасности, при чем форсированное импортозамещение в сфере ИТ продолжилось в 2024 году, а с 1 января 2025 года установлен запрет на использование импортных средств защиты информации для критической инфраструктуры.²⁵ Развитие отечественных решений в области кибербезопасности демонстрирует значительный прогресс, при чем реестр российских программ для ЭВМ и баз данных содержит около 20 тысяч программных продуктов, включая системы защиты информации, платформы управления безопасностью и средства криптографической защиты.²⁶

²⁰ Gazprombank. Распределенный реестр и блокчейн. — [Электронный ресурс] Режим доступа: URL: <https://www.gazprombank.tech/blog/508/> (дата обращения 07.09.2025).

²¹ РБК Тренды. Технологии против угроз: 7 трендов кибербезопасности в 2025 году. — [Электронный ресурс] Режим доступа: URL: <https://trends.rbc.ru/trends/industry/678f84c69a79478682c0120b> (дата обращения 07.09.2025).

²² Министерство экономического развития РФ. Нормативное регулирование цифровой среды. — [Электронный ресурс] Режим доступа: URL: <https://www.economy.gov.ru/material/directions/gosudarstvennoeupravlenie/normativnoeregulirovaniecifrovoysredy/> (дата обращения 07.09.2025).

²³ World Bank. Digital Economy Report. — [Электронный ресурс] Режим доступа: URL: <https://documents1.worldbank.org/curated/en/848071539115489168/pdf/Competing-in-the-Digital-Age-Policy-Implications-for-the-Russian-Federation-Russia-Digital-Economy-Report.pdf> (дата обращения 07.09.2025).

²⁴ Справочно-правовая система по информационной безопасности. Действующие нормативные правовые акты. — [Электронный ресурс] Режим доступа: URL: <https://sps-ib.ru/npa/dejstvujuschie> (дата обращения 07.09.2025).

²⁵ TAdviser. Цифровая экономика России. — [Электронный ресурс] Режим доступа: URL: <https://www.tadviser.ru/index.php/Статья:ЦифроваяэкономикаРоссии> (дата обращения 07.09.2025).

²⁶ Правительство РФ. Программа «Цифровая экономика Российской Федерации». — [Электронный ресурс] Режим доступа: URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf> (дата обращения 07.09.2025).

Таблица 2

Матрица рисков и защитных мер для предпринимательских сетей в цифровой среде

Категория рисков	Специфические угрозы	Потенциальные потери	Защитные меры	Экономические инструменты	Эффективность мер
Технические риски	Ransomware (41 % инцидентов в 2024), DDoS-атаки, эксплуатация уязвимостей, APT-атаки	Средняя стоимость инцидента: \$4,88 млн, простой систем: 21 день, потеря данных	Внедрение EDR/XDR решений, патч-менеджмент, сегментация сети, резервное копирование	Инвестиции: 5–7 % ИТ-бюджета, страхование: до \$100 млн покрытия	Снижение инцидентов на 70 %, восстановление за 4 часа вместо 21 дня
Человеческий фактор	Фишинг (75 % утечек), инсайдеры (37 % случаев), социальная инженерия, ошибки конфигурации	Утечка данных 1 млрд записей в 2023, репутационные потери, штрафы	Security Awareness Training, DLP-системы, принцип наименьших привилегий, 2FA/MFA	Обучение: 50 тыс. руб./сотрудник, DLP: 2–3 млн руб./100 пользователей	Снижение фишинг-кликов с 30 % до 5 %, предотвращение 85 % утечек
Риски цепочек поставок	Компрометация поставщиков, supply chain атаки, зависимость от third-party, shadow IT	Каскадный эффект на всю экосистему, недоступность критических сервисов	Vendor risk management, SBOM-анализ, контрактные SLA, аудит поставщиков	Due diligence: 500 тыс. руб./поставщик, штрафы в контрактах	Выявление 90 % рисков, снижение инцидентов third-party на 60 %
Регуляторные риски	Нарушение 152-ФЗ, GDPR, несоответствие ГОСТ, отсутствие лицензий ФСТЭК	Оборотные штрафы до 5 % выручки, приостановка деятельности, уголовная ответственность	Compliance-программы, DPO, регулярный аудит, сертификация систем	Аудит: 1–2 млн руб./год, сертификация: 3–5 млн руб.	100 % соответствие требованиям, избежание штрафов
Риски ИИ и автоматизации	Adversarial атаки на ML, отравление данных, bias в алгоритмах, потеря контроля	Некорректные решения ИИ, дискриминация клиентов, правовые иски	MLOps, explainable AI, валидация моделей, human-in-the-loop	R&D в AI безопасность: 10–15 % от AI-бюджета	Точность моделей 95 %+, обнаружение 99 % adversarial атак
Инфраструктурные риски	Отказ облачных сервисов, недоступность ЦОД, сбой телеком, энергетические проблемы	Недоступность сервисов, SLA-пенальти, потеря клиентов	Multi-cloud стратегия, георезервирование, автономные системы, BCP/DRP	Резервные мощности: +30 % к основным, DR-site: 50 млн руб.	RPO < 1 час, RTO < 4 часа, доступность 99,99 %

Составлено автором на основе анализа материалов²⁷

Анализ эффективности различных компонентов организационно-экономического механизма демонстрирует синергетический эффект от их комплексного применения, при чем организации, внедряющие интегрированные системы безопасности, сочетающие технологические решения, экономические инструменты и организационные меры, достигают снижения количества успешных кибератак на 80 % и сокращения финансовых потерь от инцидентов безопасности на 65 %.²⁸ Экономическая эффективность инвестиций в обеспечение безопасности предпринимательских сетей подтверждается исследованиями, показывающими, что каждый

²⁷ Коммерсантъ. Кибербезопасность: актуальные риски и тренды. — [Электронный ресурс] Режим доступа: URL: <https://events.kommersant.ru/nov/events/2024-0523-kiberbezopasnost-aktualnye-riski-i-trendy/> (дата обращения 07.09.2025).

ICT-Online. Бизнес-форум «Цифровые экосистемы и сервисы». — [Электронный ресурс] Режим доступа: URL: <https://eventtoday.biz/ecosistems-2024> (дата обращения 07.09.2025).

ТБ Форум. Кибербезопасность 2025. — [Электронный ресурс] Режим доступа: URL: <https://www.tbforum.ru/blog/kiberbezopasnost-2025-regulirovaniye-ugrozy-sertifikatsiya-i-zashchita-dannykh-v-gossektore> (дата обращения 07.09.2025).

²⁸ Positive Technologies. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. — [Электронный ресурс] Режим доступа: URL: <https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-vtoraya/> (дата обращения 07.09.2025).

рубль, вложенный в превентивные меры защиты, позволяет избежать потерь в размере 3–5 рублей от потенциальных инцидентов, при чем возврат инвестиций (ROI) в системы на основе искусственного интеллекта составляет 200–300 % за период 2–3 года.²⁹

В таблице 2 представлена матрица рисков и защитных мер для предпринимательских сетей в цифровой среде.

Развитие предпринимательских экосистем в России демонстрирует формирование уникальных моделей организации бизнеса, сочетающих преимущества сетевой архитектуры с централизованным управлением ключевыми процессами безопасности, при чем крупнейшие российские экосистемы — Сбер, Яндекс, VK, МТС — инвестируют значительные ресурсы в создание собственных систем защиты, включая разработку проприетарных решений в области искусственного интеллекта, создание SOC-центров и внедрение передовых практик управления киберрисками³⁰. Особенностью российских предпринимательских экосистем является их многопрофильность и стремление к созданию замкнутых циклов предоставления услуг, что с одной стороны повышает устойчивость к внешним угрозам за счет контроля всей цепочки создания стоимости, с другой — создает риски концентрации и системной уязвимости при компрометации центральных элементов экосистем.

Роль малого и среднего предпринимательства в формировании устойчивых предпринимательских сетей характеризуется двойственностью — с одной стороны, МСП демонстрируют большую гибкость и адаптивность к изменяющимся условиям цифровой среды, с другой — испытывают острый дефицит ресурсов для обеспечения адекватного уровня экономической безопасности, при чем согласно данным Единого реестра субъектов МСП, на начало 2025 года число зарегистрированных малых и средних предприятий превысило 6,5 млн, а количество самозанятых достигло 10,2 миллиона человек.³¹ Поддержка МСП в области кибербезопасности становится критическим фактором развития предпринимательских сетей, при чем российский рынок информационной безопасности в сегменте малого и среднего бизнеса прогнозируется вырасти более чем в два раза — с 15 млрд до 35-37 млрд рублей к 2030 году, что обусловлено ростом киберугроз и цифровизацией бизнес-процессов.³²

Влияние глобальных технологических трендов на организационно-экономический механизм обеспечения безопасности предпринимательских сетей проявляется в необходимости постоянной адаптации защитных мер к новым типам угроз, при чем развитие квантовых вычислений создает перспективную угрозу для существующих криптографических систем, требуя разработки квантово-устойчивых алгоритмов шифрования, на что планируется выделить 700 млн рублей для исследований в данной области.³³ Развитие технологий 5G и последующих поколений мобильной связи создает новые возможности для построения распределенных предпринимательских сетей с ультранизкой задержкой и высокой пропускной

²⁹ Globus. Главные тренды в AI и ML в 2024 году. — [Электронный ресурс] Режим доступа: URL: <https://globus-ltd.ru/blog/194> (дата обращения 07.09.2025).

³⁰ CDO2DAY. Российские цифровые экосистемы: перспективы развития. — [Электронный ресурс] Режим доступа: URL: <https://cdo2day.ru/analytics/cifrovye-jekosistemy-v-rossii-perspektivy-razvitiya/> (дата обращения 07.09.2025).

³¹ Правительство РФ. Александр Новак: В 2024 году сохраняется тенденция к росту численности МСП. — [Электронный ресурс] Режим доступа: URL: <http://government.ru/news/51693/> (дата обращения 07.09.2025).

³² Первое экономическое издательство. Новосельцева Г.Б., Рассказова Н.В. Перспективы малого бизнеса в цифровой экономике. — [Электронный ресурс] Режим доступа: URL: <https://leconomic.ru/lib/100580> (дата обращения 07.09.2025).

³³ Cognitive RBC. Азы технологии блокчейн. — [Электронный ресурс] Режим доступа: URL: <http://cognitive.rbc.ru/blockchain-basics> (дата обращения 07.09.2025).

способностью, однако одновременно расширяет поверхность атаки и требует разработки специализированных механизмов защиты edge-вычислений и IoT-устройств.³⁴

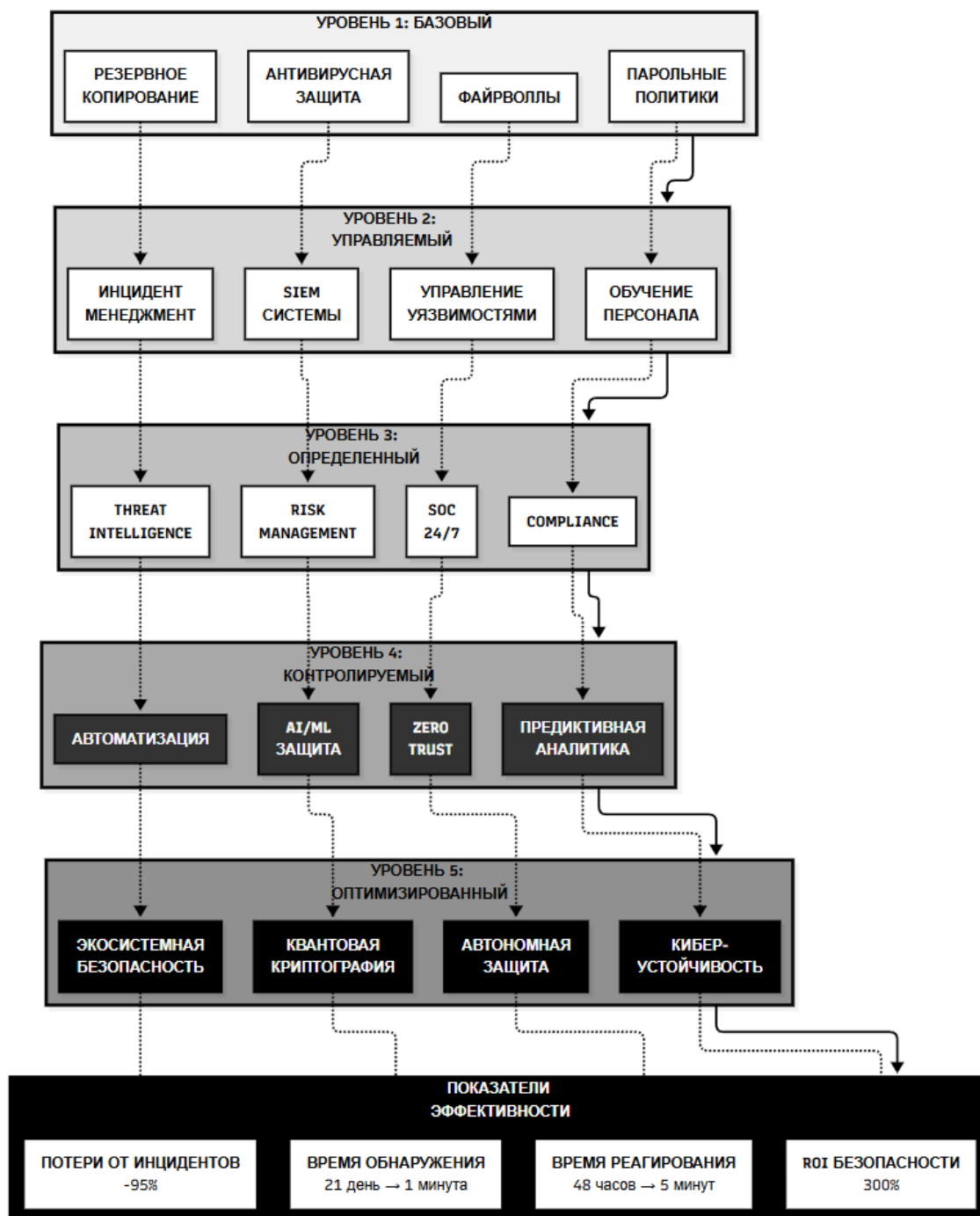


Рисунок 1. Модель зрелости системы обеспечения экономической безопасности предпринимательских сетей (разработано автором на основе анализа материалов³⁵)

³⁴ НИУ ВШЭ. Магистерская программа «Искусственный интеллект». — [Электронный ресурс] Режим доступа: URL: <https://www.hse.ru/ma/mlds/> (дата обращения 07.09.2025).

³⁵ TAdviser. Блокчейн (Blockchain). — [Электронный ресурс] Режим доступа: URL: [https://www.tadviser.ru/index.php/Статья:Блокчейн_\(Blockchain\)](https://www.tadviser.ru/index.php/Статья:Блокчейн_(Blockchain)) (дата обращения 07.09.2025).

Хабр. Блокчейн для распределенного реестра. — [Электронный ресурс] Режим доступа: URL: <https://habr.com/ru/articles/723530/> (дата обращения 07.09.2025).

Формирование компетенций в области обеспечения экономической безопасности становится критическим фактором успешности предпринимательских сетей, при чем согласно исследованиям, в ИТ-отрасли России работает 857 тысяч человек с ростом показателя на 12,7 % к 2022 году, причем наиболее высокий спрос наблюдается в сегментах разработки и программирования, внедрения и сопровождения ПО, инжиниринга, информационной безопасности и аналитики.³⁶ Образовательные программы в области кибербезопасности и управления рисками демонстрируют взрывной рост, при чем на магистерские программы по искусственному интеллекту и информационной безопасности в 2024 году поступило рекордное количество студентов, что свидетельствует о признании критической важности данных компетенций для будущего развития экономики.³⁷

На рисунке 1 представлена модель зрелости системы обеспечения экономической безопасности предпринимательских сетей.

Представленная модель зрелости иллюстрирует эволюционный путь развития систем обеспечения экономической безопасности предпринимательских сетей от базового уровня реактивной защиты до создания проактивных киберустойчивых экосистем, при чем переход между уровнями требует не только технологических инвестиций в размере 5–15 % от ИТ-бюджета на каждом этапе, но и фундаментальной трансформации организационной культуры, развития новых компетенций и создания систем непрерывного совершенствования процессов безопасности. Перспективы развития организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей связаны с дальнейшей интеграцией передовых технологий, включая развитие автономных систем защиты на основе искусственного интеллекта, способных самостоятельно обнаруживать, анализировать и нейтрализовывать угрозы без участия человека, при чем согласно прогнозам, к 2030 году более 50 % решений по кибербезопасности будут приниматься автоматически системами ИИ.³⁸

Влияние макроэкономических факторов на развитие систем обеспечения экономической безопасности предпринимательских сетей остается существенным, при чем экономическая неопределенность и санкционное давление стимулируют развитие отечественных решений в области кибербезопасности, создавая как вызовы, связанные с ограничением доступа к передовым технологиям, так и возможности для развития национальной индустрии информационной безопасности. Формирование суверенной системы обеспечения экономической безопасности становится стратегическим приоритетом, требующим координации усилий государства, бизнеса и научного сообщества в создании полного цикла разработки и производства средств защиты информации.³⁹

Интеграция концепции устойчивого развития в организационно-экономический механизм обеспечения безопасности предпринимательских сетей приобретает новое измерение, поскольку цифровизация и переход к удаленным форматам работы способствуют

³⁶ Росстат. Малое и среднее предпринимательство в России. — [Электронный ресурс] Режим доступа: URL: <https://rosstat.gov.ru/folder/210/document/13223> (дата обращения 07.09.2025).

³⁷ Мосполитех. Искусственный интеллект и машинное обучение. — [Электронный ресурс] Режим доступа: URL: <https://mospolytech.ru/postupayushchim/programmy-obucheniya/iskusstvennyj-intellekt-i-mashinnoe-obuchenie/> (дата обращения 07.09.2025).

³⁸ Рекламный форум. Искусственный интеллект и бизнес: внедрение и применение ИИ. — [Электронный ресурс] Режим доступа: URL: <https://advertisingforum.ru/blog/primenenie-ii-v-biznese/> (дата обращения 07.09.2025).

³⁹ ComNews. Российские инвесторы вложили в искусственный интеллект и машинное обучение почти \$34 млн — [Электронный ресурс] Режим доступа: URL: <https://www.comnews.ru/content/237389/2025-01-27/2025-w05/1008/rossiyskie-investory-vlozhili-iskusstvenny-intellekt-i-mashinnoe-obuchenie-pochti-34-mln> (дата обращения 07.09.2025).

снижению углеродного следа, при чем полностью цифровые бизнес-процессы могут снизить выбросы CO₂ на 54 %, что делает развитие безопасных цифровых экосистем важным элементом корпоративных ESG-стратегий.⁴⁰ Социальная ответственность в контексте обеспечения экономической безопасности предпринимательских сетей включает защиту персональных данных клиентов и сотрудников, обеспечение цифровой инклюзивности и предотвращение дискриминации при использовании алгоритмов искусственного интеллекта.

Выводы

Проведенный комплексный анализ эволюции теоретических подходов к обеспечению экономической безопасности предпринимательских структур в контексте перехода к сетевым формам организации бизнеса выявил фундаментальную трансформацию парадигмы защиты экономических систем от традиционной модели, фокусирующейся на физической защите активов и периметровой безопасности, к экосистемному подходу, интегрирующему технологические инновации, экономические механизмы и институциональные факторы в единую систему обеспечения устойчивости предпринимательских сетей в цифровой среде. Установлено, что современный этап развития характеризуется формированием качественно новых подходов к экономической безопасности, основанных на принципах Zero Trust, проактивной защиты с использованием искусственного интеллекта и создания киберустойчивых экосистем, способных функционировать в условиях постоянных киберугроз, при чем российский рынок информационной безопасности демонстрирует устойчивый рост в 27 % годовых, достигнув объема 339 млрд рублей в 2024 году. Анализ показал, что эффективность обеспечения экономической безопасности предпринимательских сетей определяется не отдельными технологическими решениями, а системной интеграцией технологических инноваций, экономических инструментов, организационных практик и институциональных механизмов, формирующих многоуровневую систему защиты.

Систематизация и классификация компонентов организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей позволила выделить четыре взаимосвязанных блока: технологический (системы на основе искусственного интеллекта и машинного обучения, блокчейн-платформы, квантовая криптография, архитектура Zero Trust), экономический (инвестиции в безопасность в размере 5–10 % ИТ-бюджета, страхование киберрисков с покрытием до \$100 млн, экономические санкции и штрафы до 5 % от выручки, финансовые резервы), организационный (политики безопасности, системы управления рисками, программы обучения персонала стоимостью 50 тыс. руб. на сотрудника, процедуры реагирования на инциденты) и институциональный (нормативное регулирование, включая 152-ФЗ и требования ФСТЭК, стандарты информационной безопасности ГОСТ, международное сотрудничество, сертификация систем). Выявлено, что наибольший эффект достигается при синергетическом развитии всех компонентов — организации, внедряющие интегрированные системы безопасности, достигают снижения количества успешных кибератак на 80 % и сокращения финансовых потерь от инцидентов на 65 %. Анализ специфики российского контекста показал критическую важность импортозамещения в области средств защиты информации и развития отечественных решений, при чем с 1 января 2025 года установлен запрет на использование импортных средств защиты для критической инфраструктуры, а реестр российских программ содержит около 20 тысяч продуктов.

Разработанная интегративная модель организационно-экономического механизма обеспечения экономической безопасности предпринимательских сетей представляет

⁴⁰ Roscongress. Digital economy report 2024. — [Электронный ресурс] Режим доступа: URL: <https://roscongress.org/en/materials/doklad-o-tsifrovoy-ekonomike-v-2024-godu/> (дата обращения 07.09.2025).

многоуровневую архитектуру, где внешние факторы цифровой трансформации (развитие цифровой экономики с прогнозируемым объемом \$60 трлн к 2025 году, эволюция киберугроз с ростом атак на 15 % в 2024 году, ужесточение регуляторных требований, технологические инновации) создают импульс для трансформации систем защиты, которая реализуется через взаимодействие четырех ключевых блоков механизма, результируя в повышении экономической устойчивости, защищенности активов, обеспечении непрерывности бизнеса и конкурентоспособности предпринимательских сетей. Модель демонстрирует нелинейный характер развития систем безопасности с пятью уровнями зрелости — от базового с временем обнаружения угроз 21 день до оптимизированного с обнаружением за 1 минуту, при чем переход между уровнями требует инвестиций 5–15 % ИТ-бюджета и обеспечивает возврат инвестиций 200–300 % за 2–3 года. Выявлены критические факторы успешности реализации модели, включая необходимость преодоления кадрового дефицита (потребность в 235–260 тыс. специалистов к 2027 году), развитие компетенций в области искусственного интеллекта и машинного обучения (рост числа специалистов на 12,7 % в год), создание культуры кибербезопасности (снижение фишинг-кликеров с 30 % до 5 % после обучения).

Общие выводы исследования свидетельствуют о формировании новой парадигмы обеспечения экономической безопасности предпринимательских сетей в цифровой среде, характеризующейся переходом от реактивных мер защиты к проактивным системам на основе искусственного интеллекта, от периметровой безопасности к модели Zero Trust, от изолированных решений к экосистемному подходу, интегрирующему технологические, экономические, организационные и институциональные компоненты в единый механизм обеспечения устойчивости. Выявленные закономерности и разработанная модель создают методологическую основу для проектирования эффективных систем защиты предпринимательских экосистем, однако их успешное применение требует учета специфики конкретных предпринимательских сетей, отраслевых особенностей и уровня цифровой зрелости организаций, при чем ключевым фактором успеха является способность к непрерывной адаптации и эволюции защитных механизмов в ответ на динамично меняющийся ландшафт киберугроз и технологические инновации в области как атакующих, так и защитных технологий.

ЛИТЕРАТУРА

1. Современные особенности разработки системы индикаторов экономической безопасности предприятия / В.В. Позняков, Н.В. Капустина, О.А. Аничкина [и др.] // Вестник евразийской науки. — 2024. — Т. 16, № S1. — EDN DWYLNPN.
2. Капустина, Н.В. Анализ аспектов обеспечения экономической безопасности предпринимательской деятельности и ее индикаторы / Н.В. Капустина // Вестник евразийской науки. — 2023. — Т. 15, № S4. — EDN BQWVCL.
3. Детерминанты развития экономики и общества в условиях глобальных изменений / В.И. Авдийский, О.А. Аничкина, А.С. Апачанов [и др.]. — Курск: ЗАО «Университетская книга», 2025. — 361 с. — EDN TLTSKI.
4. Бессарабов, В.О. К вопросу о стратегиях и механизмах обеспечения экономической безопасности предприятий в условиях новых вызовов / В.О. Бессарабов, А.П. Лутай // Финансовые рынки и банки. — 2025. — № 7. — С. 24–29. — EDN VWVIRL.
5. Артамонов, В.А. Оценка механизма обеспечения экономической безопасности предприятия / В.А. Артамонов // Вестник науки. — 2024. — Т. 4, № 12(81). — С. 71–76. — EDN VOQYYM.

6. Сушко, Н.А. Информационно-аналитическое обеспечение механизма воспроизводства основных фондов с целью обеспечения экономической безопасности предприятия / Н.А. Сушко // Вестник Керченского государственного морского технологического университета. — 2024. — № 4. — С. 195–202. — EDN DWTRPJ.
7. Кузнецова, Е.И. Роль цифровизации в трансформации институционального механизма обеспечения экономической безопасности региона / Е.И. Кузнецова, О.В. Сараджева — DOI 10.24412/2414-3995-2023-4-159-162. // Вестник экономической безопасности. — 2023. — № 4. — С. 159–162 — EDN JATRYM.
8. Юсупова, Т.А. Механизм обеспечения экономической безопасности предприятия / Т.А. Юсупова — DOI 10.18411/trnio-11-2023-182. // Тенденции развития науки и образования. — 2023. — № 103-3. — С. 209–211 — EDN WXRWOP.
9. Сальников, И.И. Содержание и инструменты механизма обеспечения экономической безопасности предприятия / И.И. Сальников, Д.П. Маширов — DOI 10.21295/2223-5639-2024-2-118-128 // Вестник Белгородского университета кооперации, экономики и права. — 2024. — № 2(105). — С. 118–128. — EDN SZXGBN.
10. Ощепкова, Н.Н. Конкурентоспособность как механизм обеспечения экономической безопасности / Н.Н. Ощепкова // Прогнозирование инновационного развития национальной экономики в рамках рационального природопользования: Материалы II Всероссийской с международным участием научно-практической конференции, Пермь, 27 декабря 2023 года. — Пермь: Пермский государственный национальный исследовательский университет, 2024. — С. 32–40. — EDN АНННАК.
11. Холопова, Ю.С. Укрепление финансовой устойчивости как механизм обеспечения экономической безопасности предприятия / Ю.С. Холопова, Н.Н. Поташкова // Финансовая экономика. — 2018. — № 5. — С. 867–870. — EDN YVJXAL.
12. Аничкина, О.А. Механизмы функционирования системы обеспечения продовольственной безопасности России (экономический аспект) / О.А. Аничкина, А.В. Бекетов, Т.Н. Коротких — DOI 10.14451/1.226.11. // Экономические науки. — 2023. — № 226. — С. 11–20 — EDN WPRFUI.

Sigalov Alexander Stanislavovich

Moscow State University of Technology and Management named after K.G. Razumovsky (First Cossack University),
Moscow, Russia
E-mail: sigalov2012@inbox.ru

Kapustina Nadezhda Valerievna

Russian University of Transport (MIIT), Moscow, Russia
E-mail: kuzminova_n@mail.ru

Organizational and economic mechanism for ensuring the security of business networks in the digital environment

Abstract. The transformation of business architecture from hierarchical models to networked business structures in the context of economic digitalization is generating fundamentally new challenges and threats to economic security, requiring the development of innovative protective mechanisms that integrate technological, economic, and institutional components. This study aims to identify and systematize the elements of the organizational and economic mechanism for ensuring the economic security of business networks operating in the digital space and exposed to cyberthreats. The subject area covers theoretical and methodological foundations, institutional mechanisms, and practical tools for protecting networked business structures from the economic risks of the digital environment. The paper analyzes fundamental theories of economic security, conceptual models of the network economy, methodological approaches to cyber risk management, and innovative solutions for protecting critical information infrastructure. It traces the evolution of scientific understanding of economic security from classical concepts of protecting tangible assets to holistic models for ensuring the resilience of digital ecosystems in the face of persistent cyberthreats. The key components of the organizational and economic mechanism are identified and classified: technological infrastructure (artificial intelligence systems, blockchain platforms, quantum cryptography), economic instruments (cyber risk insurance, investment programs, sanctions system), organizational and managerial practices (security policies, risk management, competency development), and the institutional environment (regulation, standardization, international coordination). The proposed integrative model reveals a multi-level architecture of interaction between the mechanism's heterogeneous elements, where technological innovations form the basis of protection, economic instruments create the motivational foundation and resource provision, and institutional factors determine the regulatory framework for the safe functioning of entrepreneurial networks. The scientific novelty lies in the comprehensive systematization of factors ensuring the economic security of network entrepreneurial structures in the digital space, the identification of specific features of the transformation of protective mechanisms in the context of a platform economy, and the development of an integrative model synthesizing technological, economic, and institutional components. The practical significance is determined by the applicability of the developed provisions for the formation of corporate cybersecurity strategies, the design of systems for protecting entrepreneurial ecosystems, and the improvement of the regulatory environment of the digital economy.

Keywords: economic security; entrepreneurial networks; digital environment; cybersecurity; organizational and economic mechanism; digital ecosystems; risk management; blockchain; artificial intelligence; platform economy; critical information infrastructure