3. Савенкова И.В., Добродомова Т.Н., Оценка развития приграничных регионов РФ в новых условиях развития экономики // Материалы X Международной научно-практической конференции. ЭКОНОМИКА УСТОЙЧИВОГО РАЗВИТИЯ РЕГИОНА: ИННОВАЦИИ, ФИНАНСОВЫЕ АСПЕКТЫ, ТЕХНОЛОГИЧЕСКИЕ ДРАЙВЕРЫ РАЗВИТИЯ В СФЕРЕ ТУРИЗМА И ГОСТЕПРИИМСТВА. Ялта, 28–31 марта 2023 года

УДК 349.6:004

ФОРМИРОВАНИЕ БЕЗОПАСНОЙ ПРАВОВОЙ И ИНФОРМАЦИОННОЙ СРЕДЫ ДЛЯ БИЗНЕСА В ПРОСТРАНСТВЕ РФ

А.А. Капустина,
М.Ю. Михайличенко,
Д.К. Пахомова
г. Белгород, Россия
Белгородский государственный
национальный исследовательский университет

Даннаястатья сосредоточена на задачах обеспечения надежной юридической и цифровой инфраструктуры для ведения коммерческой деятельности на территории России. В статье анализируются ключевые элементы законодательной базы, регламентирующей деловую активность. Значительное внимание уделено формированию такой информационной среды, которая будет характеризоваться открытостью, простотой доступа и защищенностью бизнес-операций.

Ключевые слова:*правовая безопасность, информационная безопасность, бизнес-среда, правовое регулирование, цифровая трансформация.*

FORMATION OF A SECURE LEGAL AND INFORMATION ENVIRONMENT FOR BUSINESS IN THE RUSSIAN FEDERATION

A.A. Kapustina,
M.Y. Mikhailichenko,
D.K. Pakhomova
Belgorod, Russia
Belgorod State
National Research University

This article focuses on the challenges of providing a reliable legal and digital infrastructure for conducting business in Russia. The article analyzes the key elements of the legislative framework governing business activity. Considerable attention is paid to the formation of such an information environment, which will be characterized by openness, ease of access and security of business operations.

Keywords: *legal security, information security, business environment, legal regulation, digital transformation.*

Развитие цифровых технологий привело к росту числа кибератак и хищению информации, ставящих под угрозу стабильность и конкурентоспособность бизнеса. Безопасность информации стала ключевым фактором устойчивого экономического роста и социальной стабильности [1, с.222].

Правовая основа информационной безопасности оказывает непосредственное влияние на принятие решений руководством компаний и способность обеспечивать сохранность важных данных. Проблема формирования комплексной системы информационной безопасности приобретает особую остроту в свете возросшей роли цифрового пространства[1, с.222].

Особую сложность формирование комплексной системы информационной безопасности приобретает в условиях значительной региональной дифференциации Российской Федерации. Экономические условия, уровень технологического развития, концентрация различных отраслей и, как следствие, профиль киберугроз существенно различаются от региона к региону. Это ставит перед малыми и средними предприятиями, работающими в разных субъектах РФ, неоднородные вызовы, требующие адаптированных подходов к защите информации.

Российская экономика характеризуется значительным числом малых и средних предприятий, находящихся в зоне повышенного риска ввиду отсутствия достаточных внутренних ресурсов для защиты своей информации. Тем не менее, именно этот сегмент играет важную роль в экономике страны, создавая рабочие места и обеспечивая рост валового продукта. Именно поэтому тема обеспечения информационной безопасности становится актуальной и важной задачей для государства и научного сообщества [3, с. 248].

Информационная безопасность рассматривается как одна из ключевых составляющих общего понятия экономической безопасности.

Она включает в себя комплекс мер и средств, обеспечивающих защиту данных, сетей и систем, используемых в бизнесе. Научные исследования в данной области показывают, что существует взаимосвязь между эффективностью управления информационной безопасностью и общей производительностью бизнеса [3, с. 387].

Зарубежные ученые сосредоточились преимущественно на изучении отдельных компонентов системы информационной безопасности. Например, широко используются модели оценки рисков и формализованные подходы к выбору средств защиты. Однако, несмотря на высокую степень детализации предлагаемых моделей, отмечается отсутствие целостного подхода к оценке и мониторингу информационной безопасности на уровне предприятий [2, с. 111].

Проблема усугубляется значительным разрывом в уровне цифровизации и доступности ИТ-специалистов между центральными и периферийными регионами. Если компании в Москве, Санкт-Петербурге или Татарстане имеют относительно больший доступ к ресурсам и компетенциям, то малые предприятия в малых городах и сельской местности зачастую лишены даже базовых возможностей для организации защиты. Это создает «цифровое неравенство» в сфере безопасности и делает региональный бизнес более уязвимым.

Российские специалисты обращают внимание на проблему несоответствия нормативных требований уровню технологического прогресса. Законодательство часто отстает от реальных потребностей бизнеса, вызывая трудности с внедрением новейших технологий. Российским ученым удается лучше учитывать национальные особенности ведения бизнеса. Но исследования зачастую ограничиваются единичными примерами конкретных компаний и отраслей, что снижает общую обоснованность сделанных выводов [2, с. 111].

Основные недостатки, отмечаемые в литературе представлены на рисунке 1 [5, с. 35]:

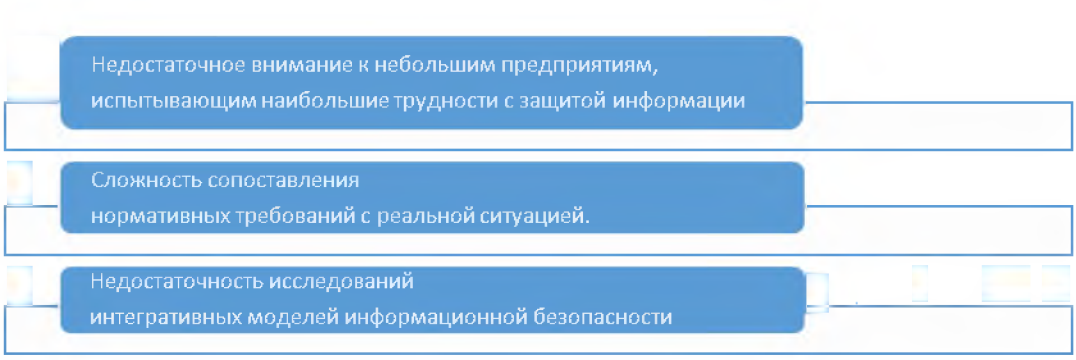


Рисунок 1 – Основные недостатки, отмечаемые в литературе

Эти факторы определяют необходимость продолжения исследований в области построения надежных систем защиты данных и информации, адаптированных к российским условиям.

Методология настоящего исследования основана на системном подходе, включающем сравнительный анализ международного опыта и отечественных разработок. Использованы методы документального анализа, сравнительного анализа и моделирования. Исследовательская работа выполнена в три этапа:

1. Сбор первичной информации. Анализ действующей нормативной базы, профессиональных отчетов и научных публикаций.

2. Оценка текущего состояния. Выявлены ключевые показатели информационной безопасности российских предприятий и проанализирована практика их применения.

3. Разработка рекомендаций. Разработаны практические рекомендации по укреплению правовой и технологической составляющей информационной безопасности бизнеса.

4. **Учет региональной специфики при разработке и внедрении стандартов.** Федеральным органам власти совместно с региональными администрациями целесообразно разрабатывать типовые, но адаптируемые модели систем информационной безопасности. Эти модели должны учитывать:

- **Отраслевую структуру экономики региона** (например, акцент на защиту интеллектуальной собственности для инновационных кластеров или на обеспечение бесперебойности технологических процессов для агропромышленных предприятий).
- **Развитие региональной ИТ-инфраструктуры.**
- Создание **межрегиональных центров компетенций** для поддержки МСП в вопросах ИБ, особенно в регионах с низкой концентрацией специалистов.

Исследуемый объект – совокупность элементов и характеристик информационной безопасности в контексте российской действительности. Основная цель исследования – определение оптимальной модели формирования безопасной правовой и информационной среды для бизнеса.

Современные российские законы недостаточны для полноценного отражения изменений, происходящих в области информационных технологий[5, с. 35].

Малые и средние предприятия испытывают серьезные трудности в создании устойчивых систем защиты информации[5, с. 35].

Отсутствует единая концепция интеграции лучших мировых практик и отечественного опыта в единой научно-практической среде[5, с. 35].

Предложено разработать единую концепцию построения безопасной информационной среды. Концепция предусматривает последовательное выполнение ряда шагов:

Определение критериев выбора оптимальных решений в области информационной безопасности.

Установление приоритета интересов потребителей и государства в управлении системой информационной безопасности.

Принятие мер по расширению возможностей малого и среднего бизнеса в вопросах информационной безопасности.

Приводится таблица сравнения уровня информационной безопасности предприятий малого и среднего бизнеса в России и Европе (таблица 1).

Таблица 1

Сравнение уровня информационной безопасности

Показатели	Европа	Россия
Наличие сертифицированной системы информационной безопасности, %	60	20
Инвестиции в средства защиты информации, млн руб./год	Высокие	Умеренные
Количество зарегистрированных инцидентов, шт./год	Среднее	Высокое

Представленная таблица подтверждает необходимость радикального усиления мер информационной безопасности в российских компаниях. Важно отметить, что приведенные средние показатели по России скрывают значительную внутристрановую вариативность. Уровень защищенности компаний в регионах-донорах и крупных индустриальных центрах может быть сопоставим с восточноевропейскими странами, в то время как в депрессивных и сельскохозяйственных регионах он может быть критически низким. Это подтверждает необходимость не просто усиления мер в целом, но и дифференцированного регионального подхода к поддержке бизнеса.

Выделяются две ключевые проблемы, определяющие будущее направление исследований [4, 25]:

1. Необходимость систематизации международных и российских стандартов информационной безопасности[4, 25].

2. Разработка механизма адаптации лучших мировых практик к российскому рынку[4, 25].

Особый интерес вызывает разработка интегрированного подхода к управлению информационной безопасностью, сочетающего принципы государственно-частного партнёрства и применение передовых технологий.

Вывод о необходимости принятия активных мер по повышению уровня информационной безопасности и защиты данных представляется очевидным. В связи с увеличением объемов обрабатываемой информации возрастает угроза потери данных и

мошенничества, что ставит под сомнение успешность бизнеса и экономику страны в целом[4, 25].

Следует отметить, что рассмотренные проблемы носят комплексный характер и требуют междисциплинарного подхода. Инновационный подход к построению системы информационной безопасности подразумевает активное участие государства, общественных институтов и бизнеса в разработке и внедрении новых технологий и концептуальных моделей.

Создание надежного правового и технического фундамента информационной безопасности является необходимым условием стабильного и динамичного развития российского бизнеса. Государству предстоит реализовать целый спектр инициатив, способствующих усилению защиты информации, начиная от совершенствования законодательства и заканчивая разработкой отраслевых стандартов и поощрения внедрения передовых технологий.

Для предприятий малого и среднего бизнеса рекомендуется уделять особое внимание вопросам информационной безопасности, используя доступные средства и профессиональные консультации. Практическими рекомендациями являются регулярный аудит систем защиты, обучение сотрудников правилам работы с конфиденциальной информацией и страхование рисков, связанных с возможным взломом систем и потерей данных.

Реализация государственных инициатив должна учитывать региональный аспект. Субсидирование приобретения средств защиты, образовательные программы для ИТ-специалистов и аудит безопасности для МСП следует внедрять, отталкиваясь от конкретных потребностей и угроз, характерных для каждого субъекта Федерации. Только такой, децентрализованный подход, позволит обеспечить не фрагментарную, а повсеместную укрепление информационной безопасности российского бизнеса.

Необходимы дальнейшие исследования в области анализа стоимости ущерба от киберинцидентов, а также изучение способов минимизации рисков в зависимости от размеров предприятий и отрасли. Эти меры позволят сформировать надежный фундамент для устойчивого роста экономики и снижения уязвимости бизнеса перед новыми угрозами.

Представленные в исследовании выводы и рекомендации находят свое практическое применение в регионах с особой экономической спецификой, таких как Белгородская область. Для данного региона, характеризующегося развитым агропромышленным комплексом и растущим сектором информационных технологий, вопросы информационной безопасности приобретают особую актуальность.

Региональные особенности Белгородской области создают уникальный профиль киберугроз, требующий адаптации предложенной концепции построения безопасной информационной среды. Особое значение приобретает разработка механизмов государственно-частного партнерства, направленных на поддержку малого и среднего бизнеса в сфере защиты информации.

Опыт реализации предложенных мер в Белгородской области может стать модельным для других регионов России, демонстрируя эффективность интеграции правовых, организационных и технических аспектов информационной безопасности с учетом местной экономической специфики. Это позволит не только усилить защищенность регионального бизнеса, но и создать основу для формирования единого безопасного цифрового пространства страны.

ЛИТЕРАТУРА

1. Информационные технологии в экономике и управлении : учебник для вузов / ответственный редактор В. В. Трофимов. – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 556 с. – (Высшее образование). – ISBN 978-5-534-18678-9. –

Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/568903 (дата обращения: 19.11.2025).

2. Информационные технологии в юридической деятельности : учебник для вузов / под общей редакцией П. У. Кузнецова. – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 396 с. – (Высшее образование). – ISBN 978-5-534-20461-2. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/581423 (дата обращения: 19.11.2025).

3. Кожевникова, Г. П. Информационные системы и технологии в маркетинге : учебник для вузов / Г. П. Кожевникова, Б. Е. Одинцов. – Москва : Издательство Юрайт, 2025. – 444 с. – (Высшее образование). – ISBN 978-5-534-07447-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/560580 (дата обращения: 19.11.2025).

4. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебник для вузов / Н. С. Козырь, Н. В. Седых. – Москва : Издательство Юрайт, 2025. – 170 с. – (Высшее образование). – ISBN 978-5-534-17153-2. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/568566 (дата обращения: 19.11.2025).

5. Правовая статистика : учебник и практикум для вузов / И. Н. Андрюшечкина, Е. А. Ковалев, Л. К. Савюк, Ю. А. Бикбулатов ; под редакцией Л. К. Савюка. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 459 с. – (Высшее образование). – ISBN 978-5-534-17360-4. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/559683 (дата обращения: 19.11.2025).

УДК 339.54

МЕЖДУНАРОДНЫЕ ТРАНСПОРТНЫЕ КОРИДОРЫ КАК ФАКТОР ТРАНСФОРМАЦИИ ЭКОНОМИЧЕСКОГО ПРОСТРАНСТВА

Х. Кереселидзе, Н. Кереселидзе, О.А. Немченко
Россия, Королёв
«Технологический университет имени дважды Героя Советского Союза летчика-космонавта А.А. Леонова» – филиал ФГБОУ ВО «Московский государственный университет геодезии и картографии»

В работе рассматривается роль международных транспортных коридоров как ключевого фактора трансформации экономического пространства в условиях глобализации. Анализируются три стратегически значимых направления – Инициатива «Один пояс – один путь», Транссибирский транспортный коридор и коридор «Север–Юг». Отражено, что их развитие способствует формированию новых логистических центров, перераспределению мировых товаропотоков, усилению значения транзитных территорий и модернизации таможенной инфраструктуры. Особое внимание уделяется влиянию коридоров на совершенствование таможенных процедур, цифровизацию контроля и повышение эффективности международных цепочек поставок. Отмечается, что транспортные коридоры становятся фундаментом новой пространственной организации мировой экономики, определяя вектор развития регионов и характер международного экономического взаимодействия.

Ключевые слова: *Международные транспортные коридоры, экономическое пространство, логистика, таможенное администрирование, Шелковый путь, Транссибирский коридор, Север-Юг.*