Вопросы обеспечения кибербезопасности в сфере предпринимательской деятельности

Короткова Ольга Валерьевна
кандидат юридических наук, доцент, доцент кафедры предпринимательского и корпоративного права, Московский государственный юридический университет имени О.Е. Кутафина, ovkorotkova@msal.ru

Статья посвящена анализу взаимосвязи кибербезопасности, экономической безопасности и предпринимательской активности в условиях структурной трансформации российской экономики. Целью исследования выступает выявление институциональных и функциональных противоречий, возникающих между государственным регулированием рисков и целями бизнеса в условиях киберугроз. Киберугрозы представляют проблему не только для крупных корпораций и правительств, но и для небольших компаний. Недавние исследования показали, что малый бизнес особенно сильно подвержен кибератакам и во многом из-за того, что не обладает ресурсами для эффективной защиты. В статье делается вывод, что кибербезопасность бизнеса – задача первостепенной важности, но текущий ландшафт угроз постоянно меняется, поэтому сориентироваться и понять, с чего начать, бывает непросто. Чтобы помочь вам, мы предлагаем ряд рекомендаций по защите малого бизнеса от киберугроз.
Ключевые слова: экономическая безопасность, кибербезопасность, кибератаки, предпринимательские риски, санкционное давление, импортозамещение, адаптационные стратегии бизнеса, государственное регулирование.

Анализ экономической безопасности в современной России показал, что кибербезопасность перестала быть опцией — это обязательное условие для выживания и устойчивого развития любого бизнеса. Для малого и среднего бизнеса кибератака всё чаще становится фатальным событием. В 2025 году почти половина атак на компании были успешными и приводили к сбоям, причём более 70% инцидентов были направлены на полное уничтожение или шифрование данных [2, С. 37-42].

Проблема сегодняшнего дня заключается в том, что существующие научные подходы зачастую рассматривают безопасность бизнеса либо с позиций государственного макрорегулирования, либо через призму корпоративного риск-менеджмента, оставляя за пределами анализа взаимопроникновение публичных и частных интересов в условиях новой реальности [9, С. 180-185].

В сложившихся экономических условиях важным становится анализ связи государственной политикой обеспечения экономической безопасности и возможностей защиты российского бизнеса от киберугроз.

Как отмечает в своих работах И.А. Иваненко экономическая безопасность интерпретируется первой через качественные характеристики институциональной среды, за счёт чего защищённость бизнеса рассматривается как функция от степени зрелости законодательной базы и формальных регуляторных норм [4, С. 96-102].

Недостаточная развитость институтов восполняется избыточным контрольно-надзорным давлением, а это определяет повышение трансакционных издержек бизнеса и последующее снижение деловой активности. Рискологическая школа рассматривает разрушение конкурентных преимуществ, финансовой неустойчивости, при условии того, что внешняя природа шоков не рассматривается.

При этом, подход «безопасность через развитие», в том случае, когда хозяйствующий субъект теряет право определяться как защищённый при условии того, что, стабильность его положения обеспечивается отказом от модернизационных процессов и сокращением доли рынка [8, С. 849-864]. Также, избыточное смещение в сторону протекционистских инструментов приводит к состоянию «стагнационная безопасность», когда номинальное устранение угроз неизбежно ведёт к деградации основных производственных фондов.

Трансформация российской экономики в 2022–2025 годах носит характер не временного кризиса, а глубинной структурной перестройки [10, С. 123]. Санкционное давление затронуло критически важные для бизнеса сферы, в том числе логистику, финансовые транзакции и доступ к критическим технологиям. В ответ на это предпринимательское сообщество продемонстрировало «вынужденное инноваторство», когда ограничения стимулируют не свёртывание деятельности, а поиск альтернативных бизнес-моделей [1, С. 41-50].

В системе обеспечения экономической безопасности сферы предпринимательской деятельности государственная политика в анализируемый период в основном опиралась на ужесточение нормативного поля в сфере персональных данных, критической информационной инфраструктуры и валютного контроля [5, С. 152]. Для корпоративного сектора это привело к росту отчётности и необходимостью содержания громоздких юридических подразделений.

Так, по мнению И.А. Иваненко сегодня сформировалась институциональная ловушка, при которой сформировалась высокая степень формальной защищённости [4, С. 96-102]. Бюрократизация антикризисных мер приводит к тому, что решение о внедрении новой технологической линии, содействующей усилению обеспечения кибербезопасности в сфере бизнеса откладывается из-за процедур согласования специальных разрешений.

Сегодня, в сложившихся экономических условиях требуется переход от жёсткой модели обеспечения безопасности к сервисной модели. Вместо наращивания количества запретов и штрафных санкций за их неисполнение регулятору целесообразно создавать инфраструктуру безопасности, доступную хозяйствующим субъектам на рыночных условиях. Это касается государственных центров мониторинга киберугроз, предоставляющих услуги бизнесу по подписке, что значительно экономит ресурсы отдельных предприятий [6, С. 52-57].

Современные кибератаки отличаются изощренностью и комплексным воздействием. Злоумышленники редко преследуют одну цель; чаще они стремятся нанести максимальный ущерб, сочетая кражу данных, шифрование систем и нарушение бизнес-процессов. На первый план выходят атаки через цепочки поставок, когда взлом менее защищенного подрядчика или поставщика услуг становится троянским конем для проникновения в более крупную компанию. Ожидается, что в 2026 году ярко проявятся тренды 2025-го: рост мощности и продолжительности DDoS-атак, а также увеличение доли целевых атак. Этот тренд подтверждается прогнозом Positive Technologies, согласно которому автоматизация и AI-модели делают сложные целенаправленные угрозы более доступными, постепенно стирая границу между массовыми и целевыми атаками, в том числе использующими уязвимости нулевого дня.

Кибератаки могут нанести ущерб вашим данным и оборудованию и привести к финансовым потерям. Кроме того, злоумышленники могут проникнуть в корпоративную сеть и использовать в преступных целях следующую информацию:

- списки клиентов;
- данные банковских карт клиентов;
- банковские реквизиты компании;
- структуры ценообразования;
- документация по разработке продуктов;
- планы развития бизнеса;
- описания производственных процессов;
- другие виды интеллектуальной собственности.

Такая атака ставит под угрозу не только вашу компанию. Злоумышленники могут использовать скомпрометированную сеть как ворота в сети других компаний, в цепочках поставок которых вы участвуете. В этих условиях необходимо:

1. Обучать сотрудников. Сотрудники могут сделать ваш бизнес уязвимым. Хотя точная статистика по странам и отраслям отличается, очевидно, что множество утечек данных происходят по вине сотрудников компаний, которые умышленно или просто по неосторожности предоставляют киберпреступникам доступ к корпоративным сетям.
2. Проводить оценку рисков. Оцените потенциальные риски, угрожающие безопасности сетей, систем и информации вашей компании. Определив и проанализировав возможные угрозы, вы сможете разработать план по устранению уязвимостей в системе безопасности. Проведя анализ и выявив потенциальные угрозы, используйте полученную информацию для разработки или уточнения своей стратегии безопасности. Регулярно пересматривайте и обновляйте стратегию.
3. Использовать антивирусное ПО.
4. Вовремя обновлять ПО. Как и антивирус, все рабочие программы необходимо поддерживать в актуальном состоянии. Поставщики программного обеспечения регулярно его обновляют, чтобы повысить эффективность или добавить исправления, устраняющие уязвимости. Необходимы резервные копии файлов
5. Проводить шифровку важной информации. Если компания регулярно имеет дело с данными банковских карт и счетов или другой конфиденциальной информацией, рекомендуется использовать программу, которая обеспечивает шифровку данных.
6. Защитить сеть.
7. Обновлять пароли.

Следует отметить, что по мере роста вашего бизнеса вам понадобятся услуги поставщика таких защитных решений, которые будут расти вместе с вами. Обратите внимание на компании, предлагающие полный ряд систем безопасности для бизнеса, в том числе и тех, которые могут потребоваться вам в будущем.

Еще большее значение кибербезопасность приобретает в условиях повсеместного перехода на удаленную работу. Многие небольшие компании постоянно используют облачные технологии и инструменты для проведения онлайн-собраний, рассылки рекламы, закупок и продаж, взаимодействия с клиентами и поставщиками и проведения банковских операций [7, С. 137]. Чтобы не допустить финансового и репутационного ущерба, данные и облачные системы необходимо защищать от несанкционированного доступа и утечек.

В современной России идёт формирование новой модели взаимосвязи экономической безопасности и бизнес деятельности [3, С. 25-27]. На государственном уровне необходимо институциональное признание компромисса «кибербезопасность – эффективность» как нормативного принципа. При проведении оценки регулирующего воздействия нормативных актов в сфере безопасности следует оценивать не только предотвращённый ущерб, но и упущенную выгоду бизнеса от внедрения ограничений и дополнительных требований.

Литература

1. Варнавский В. Г. Государственно-частное партнерство: некоторые вопросы теории и практики / В. Г. Варнавский // Мировая экономика и международные отношения. 2011. № 9.
2. Дарькина М.М., Короткова О.В. Правовое регулирование безопасности предпринимательской деятельности в условии цифровизации экономики: монография / О.В. Короткова, М.М. Дарькина. Москва: РУСАЙНС, 2025. 68 с.
3. Жариков А.А. Правовое регулирование безопасности предпринимательской деятельности: учебное пособие по специальности 40.05.04 (Судебная и прокурорская деятельность)/ А. А. Жариков.Вологда: Фонд развития филиала МГЮА имени О. Е. Кутафина в г. Вологде. 2020.
4. Иваненко И. А. «Институциональные ловушки» в странах с переходной экономикой / И. А. Иваненко // Ученые записки Крымского инженерно-педагогического университета. 2020. № 2 (68).
5. Короткова О.В. Отдельные вопросы противодействие легализации (отмыванию) денежных средств, направляемых на финансирование терроризма/ Вестник Московской академии Следственного комитета Российской Федерации. 2020.№2 (24).
6. Короткова О.В. Правовое регулирование безопасности предпринимательской деятельности: учебное пособие/ О.В. Короткова, М.: РУСАЙНС: 2022.
7. Короткова О.В. Особенности научного подхода в сфере обеспечения безопасности бизнеса//Современная

наука: актуальные проблемы теории и практики. 2022, № 7.

8. Митяков С. Н. Эмпирический анализ краткосрочных индикаторов экономической безопасности / С. Н. Митяков, Е. А. Назарова // Экономическая безопасность. 2023. Т. 6, № 3.

9. Сугарова И. В. Управление рисками в системе экономической безопасности предприятия / И. В. Сугарова // Вестник Ростовского государственного экономического университета (РИНХ). 2025. Т. 32, № 3.

10. Эскиндаров М.А. Развитие предпринимательства: концепции, цифровые технологии, эффективная система: монография / под ред. М.А. Эскиндарова. 2-е изд. М.: Дашков и К, 2020. 605 с.

Issues of cybersecurity in the field of business activities

Korotkova O.V.
Law at the Kutafin Moscow State Law University

The article analyzes the relationship between cybersecurity, economic security, and entrepreneurial activity in the context of the structural transformation of the Russian economy. The goal of the study is to identify the institutional and functional contradictions that arise between government risk regulation and business goals in the face of cyber threats. Cyber threats pose a challenge not only for large corporations and governments, but also for small businesses. Recent studies have shown that small businesses are particularly vulnerable to cyberattacks, largely due to their lack of resources for effective protection. The article concludes that business cybersecurity is a top priority, but the current threat landscape is constantly changing, making it difficult to know where to start. To help you, we offer a set of recommendations for protecting small businesses from cyber threats.

Keywords: economic security, cybersecurity, cyberattacks, business risks, sanctions pressure, import substitution, business adaptation strategies, and government regulation.

References

1. Varnavsky, V. G. Public-Private Partnership: Some Issues of Theory and Practice / V. G. Varnavsky // World Economy and International Relations. – 2011. No. 9.
2. Darkina, M.M., Korotkova, O.V. Legal Regulation of Business Security in the Context of Digitalization of the Economy: A Monograph / O.V. Korotkova, M.M. Darkina. Moscow: RUSAYNS, 2025. 68 p.
3. Zharikov A.A. Legal regulation of business security: a textbook for the specialty 40.05.04 (Judicial and Prosecutorial Activity)/ A. A. Zharikov. Vologda: Development Fund of the Vologda Branch of the Kutafin Moscow State Law University. 2020.
4. Ivanenko I. A. "Institutional Traps" in Countries with Economies in Transition / I. A. Ivanenko // Scientific Notes of the Crimean Engineering and Pedagogical University. – 2020. – No. 2 (68).
5. Korotkova O.V. Separate Issues of Countering the Legalization (Money Laundering) of Funds Used to Finance Terrorism./ Bulletin of the Moscow Academy of the Investigative Committee of the Russian Federation. 2020. No. 2 (24).
6. Korotkova O.V. Legal Regulation of Business Security: A Study Guide/ O.V. Korotkova, Moscow: RUSAYNS: 2022. Pp. 58-61.
7. Korotkova O.V. Features of the Scientific Approach in the Field of Business Security//Modern Science: Current Issues of Theory and Practice. 2022, No. 7.
8. Mityakov S. N. Empirical Analysis of Short-Term Economic Security Indicators / S. N. Mityakov, E. A. Nazarova // Economic Security. – 2023. – Vol. 6, No. 3.
9. Sugarova I. V. Risk Management in the Economic Security System of an Enterprise / I. V. Sugarova // Vestnik Rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINKh). 2025. Vol. 32, No. 3.
10. Eskindarov M.A. Development of Entrepreneurship: Concepts, Digital Technologies, and an Effective System: Monograph / Ed. by M.A. Eskindarov. 2nd ed. Moscow: Dashkov i K, 2020. 605 p.