

## КИБЕРБЕЗОПАСНОСТЬ И ЕЁ РОЛЬ В ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СТРАНЫ CYBERSECURITY AND ITS ROLE IN THE ECONOMIC SECURITY OF THE COUNTRY

**БАГДАСАРОВА Анаид Эдуардовна,**

кандидат юридических наук, доцент кафедры экономической безопасности и права РГАУ-МСХА им. К.А. Тимирязева.

127434, Россия, г. Москва, Тимирязевская ул., д. 49.

E-mail: a.bagdasarova@rgau-msha.ru;

**BAGDASAROVA Anaid Eduardovna,**

Candidate of Legal Sciences, Associate Professor of the Department of Economic Security and Law

K.A. Timiryazev Russian State Agrarian University-Moscow Agricultural Academy.

127434, Russia, Moscow, Timiryazevskaya str., 49.

E-mail: a.bagdasarova@rgau-msha.ru

**Краткая аннотация.** В условиях стремительного развития цифровых технологий и увеличения числа киберугроз кибербезопасность становится важнейшим аспектом экономической безопасности страны. Статья рассматривает взаимосвязь между кибербезопасностью и экономической стабильностью, анализируя влияние кибератак на ключевые сектора экономики, такие как финансы, энергетика и инфраструктура. Особое внимание уделяется современным вызовам, с которыми сталкиваются государственные и частные организации в области защиты информации, а также мерам, необходимым для повышения уровня киберзащиты. В статье также рассматриваются международный опыт и практика в области кибербезопасности, подчеркивающие необходимость сотрудничества между государственными структурами, бизнесом и научным сообществом для обеспечения устойчивого развития и защиты национальных интересов.

**Abstract.** With the rapid development of digital technologies and the increasing number of cyber threats, cybersecurity is becoming an essential aspect of the country's economic security. The article examines the relationship between cybersecurity and economic stability, analyzing the impact of cyber attacks on key sectors of the economy such as finance, energy and infrastructure. Special attention is paid to the modern challenges faced by public and private organizations in the field of information protection, as well as measures necessary to increase the level of cyber protection. The article also examines international initiatives and best practices in the field of cybersecurity, emphasizing the need for cooperation between government agencies, business and the scientific community to ensure sustainable development and protect national interests.

**Ключевые слова.** Кибербезопасность, экономическая безопасность, кибератаки, информационные технологии, защита информации, критическая инфраструктура, инновации в киберзащите.

**Keywords.** Cybersecurity, economic security, cyber attacks, information technology, information security, critical infrastructure, innovations in cyber defense.

**Для цитирования:** Багдасарова А.Э. Кибербезопасность и её роль в экономической безопасности страны // Право и государство: теория и практика. 2025. № 5. С. 153-156. [http://doi.org/10.47643/1815-1337\\_2025\\_5\\_153](http://doi.org/10.47643/1815-1337_2025_5_153).

**For citation:** Bagdasarova A.E. Cybersecurity and its role in the economic security of the country // Law and state: theory and practice. 2025. No. 5. pp. 153-156. [http://doi.org/10.47643/1815-1337\\_2025\\_5\\_153](http://doi.org/10.47643/1815-1337_2025_5_153).

**Статья поступила в редакцию: 16.05.2025**

В современном информационном обществе, в котором растет зависимость экономической системы от цифровой техники, защита информационной системы и информации от кибератак становится важнейшей частью охраны государственной безопасности. Сейчас взаимосвязь кибербезопасности и экономической безопасности играет важную роль в устойчивом развитии страны, в целом экономики [4].

Кибератаки могли бы нанести вред любому сектору экономики, поскольку электронные системы применяются по всему миру, однако существуют некоторые секторы, которые, как правило, подвергаются им в большей мере:

- банки, финансовые учреждения и платежные системы;
- онлайн-магазины и другие организации, осуществляющие онлайн-продажу, оказываются подвергнуты атакам злоумышленников, цель которых –получить доступ к платежным данным клиентов или кража личных данных;
- кибератаки, направленные на предприятия, пытаются нарушить процесс производства. Такие угрозы могут иметь серьезные негативные последствия, возникающие в процессе производства, дизайном продукции и передовыми технологиями;
- компании телекоммуникаций подвергаются угрозам в сети, поскольку они являются ключевыми лицами для передачи данных и связи организаций и населения;
- медицинские организации имеют большое количество информации, в том числе медицинских записей и личных данных пациентов, которые делают их привлекательными для хакеров;
- в кибератаках на госучреждения могут быть различные причины, от кражи скрытых данных до нарушений функционирования госсистем.

Важно помнить, что киберпреступления не только влекут за собой финансовые потери, но также имеют много других негативных последствий. К ним можно отнести ущерб репутационного характера, который повлияет на доверие компаний и государства, и потерю персональных данных, нарушение прав граждан. Все эти аспекты объединяют в себе серьезные задачи для экономической и общественной жизни [2].

Экономическая безопасность определяется как способность экономики обеспечивать устойчивое развитие, противостоять внутренним и внешним угрозам, сохранять стабильность и обеспечивать рост благосостояния населения. Эффективное управление кибербезопасностью способствует обеспечению экономической безопасности, предотвращая возможные потери от кибератак и сохраняя стабильность информационных систем. Становится очевидным, что в ближайшие годы сохранится прогресс данного явления, требуя от государств и хозяйствующих субъектов непрерывного совершенствования мер по защите данных. С учетом вышесказанного, следует отметить важное значение правового регулирования и международного сотрудничества в области кибербезопасности, которые помогают эффективно противостоять угрозам в данной сфере.

Создание правового фундамента для обеспечения кибербезопасности в Российской Федерации выступает одной из главных задач

нормативного регулирования, которое направлено на защиту безопасности государства, хозяйствующих субъектов и всех граждан. В рамках этой задачи разрабатывается и принимается соответствующее законодательство, которое определяет обязанности организаций и граждан в области обеспечения кибербезопасности, а также устанавливает механизмы контроля и ответственности за совершение правонарушений и преступлений. Регулирование выполняется на различных уровнях – международном и государственном.

Основными документами, определяющими подходы к обеспечению кибербезопасности в Российской Федерации, являются:

1. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» данный закон устанавливает основные принципы и подходы к обеспечению кибербезопасности в России [3].
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает определения основных понятий, связанных с информацией, информационными технологиями и защитой информации, а также устанавливает правила и принципы организации, хранения, передачи, обработки и защиты информации [1].
3. Стратегия национальной безопасности Российской Федерации документ, который определяет цели и задачи в области кибербезопасности, а также основные направления развития киберинфраструктуры страны [7].
4. Доктрина информационной безопасности Российской Федерации устанавливает цель, основные принципы и задачи обеспечения информационной безопасности в стране [4].
5. Национальная стратегия развития киберинтеллекта Российской Федерации определяет основные цели и приоритеты развития киберинтеллектуальных возможностей. Ее основная задача заключается в обеспечении информационной безопасности и защите интересов государства в киберпространстве [5].
6. Национальная программа «Цифровая экономика Российской Федерации» представляет собой стратегический документ, разработанный с целью стимулирования развития цифровой экономики в России. Она определяет меры и задачи для достижения этой цели.

Из вышеупомянутого можно сделать выводы о задачах кибербезопасности: защита государственной и частной информационной системы от кибератак, предотвращение утечки конфиденциальных данных, обеспечение надежности электронной торговли и банковских операций, защита инфраструктуры страны, в том числе энергетических систем, транспортной и коммуникационной инфраструктуры.

Для России, одной из крупнейших кибердержав мира, проблемы кибербезопасности являются стратегически важным фактором обеспечения обороны государства и безопасности, эффективного экономического и социально-экономического развития. В связи с этим необходимо постоянное наблюдение за преступлениями в этой сфере и анализ событий, для выявления потенциальных угроз [6].

Под кибербезопасностью понимают потенциальные события или действия, направленные на уничтожение информационных систем, компьютеров, сетей или данных. Угрозы кибербезопасности могут иметь разные цели, например, кража личных данных, вымогательство, шпионаж, саботаж и др. Есть ряд опасностей, которые могут негативно сказаться на экономической безопасности:

1. Мошенничества в сфере финансов – это преступные действия, направленные на получение нелегальной выгоды или на обман других лиц в финансовой операции. Одним из самых распространенных способов обмана является создание ложных страниц сайтов. Под видом официального сайта или электронной почты злоумышленникам открывается доступ к личным данным, банковским счетам и кредитным картам.
2. Разработка вредоносного программного обеспечения. Злонамеренные программы, такие как вирусы, могут заражать компьютеры и сеть, вызывая вывод из строя важнейших инфраструктурных систем типа электросети и транспортных систем. Возможными последствиями этой ситуации является серьезный финансовый ущерб и нарушения бизнес-процесса.
3. Взлом компьютерных систем и сетей является процессом взлома информации, которую можно использовать в различных целях, например, для получения конфиденциальных сведений, торговых тайн, политического вмешательства или хищения интеллектуальных прав.
4. Социальная инженерия является приемом влияния на поведение и мышление людей, чтобы незаконно получать конфиденциальные информационные ресурсы или неправомерные выгоды. Социальная инженерия использует манипуляционные, обманные, психологические методы для того, чтобы убедить лицо предоставить доступ к информации, паролям или совершить конкретные действия.
5. Кибертерроризм – серьезная угроза экономическим системам и правовым системам. Данное явление может быть связано с атаками на критическую инфраструктуру, например, электросети и финансовые системы.

Угрозы, изложенные выше, являются одной из основных угроз кибербезопасности, но список неполный, поскольку данная сфера развивается в ускоренном режиме. Все эти риски могут спровоцировать серьезные экономические потери, потери доверия, нарушение бизнес процессов. Следовательно, обеспечение кибербезопасности становится жизненно важной задачей для гарантирования экономической стабильности [8].

Нельзя не согласиться с высказыванием Антропова К. Ю., Ахмадеева Р. Г., Косова М. Е., которые писали: «основной упор кибератак делается на коммерческие организации с целью получения соответствующей информации или получения каких-либо предпочтений». Действительно, в результате комплексного анализа доминирующими факторами киберпреступности выступают сферы личных данных граждан, корпоративных учетов и конфиденциальной информации о коммерческой деятельности предприятий, а также данные о банковских картах физических лиц. Соответственно, современная киберугроза глубже проникает в экономические и предпринимательские структуры, что требует серьезного пересмотра государственных стратегий по обеспечению информационной безопасности. В этом контексте особое внимание нужно уделить охране критически важных объектов инфраструктуры [11].

В связи с этим нужно выделить конкретные киберугрозы, которые присутствуют в качестве угрозы экономической безопасности страны:

1. Уязвимость критической инфраструктуры.

Критическая инфраструктура, включая энергетику, транспорт и связь, становится основной мишенью для кибератак. Например, в 2021 году атака на Colonial Pipeline в США привела к остановке работы крупнейшего нефтепровода, что вызвало панику и рост цен на топливо. В России подобные угрозы также актуальны, особенно в условиях цифровизации энергетических систем и транспортных сетей.

2. Недостаточная защита персональных данных.

Утечки персональных данных граждан становятся все более частыми. Например, в 2023 году произошла утечка данных клиентов крупного российского банка, что привело к финансовым потерям и утрате доверия к учреждению. Проблема усугубляется слабой осведомленностью населения о правилах кибергигиены.

3. Недостаток квалифицированных кадров.

В России наблюдается дефицит специалистов в области кибербезопасности. По данным исследования РАЭК, только 30% компаний имеют в штате достаточно квалифицированных сотрудников для защиты от кибератак. Это делает организации уязвимыми перед сложными угрозами, такими как целевые атаки (APT).

4. Недостаточная координация между государственными и частными структурами.

Многие компании неохотно делятся информацией о кибератаках, опасаясь репутационных потерь. Это затрудняет оперативное реагирование на угрозы и разработку эффективных мер защиты.

5. Рост киберпреступности в финансовом секторе.

Финансовые организации сталкиваются с увеличением числа атак, таких как фишинг, мошенничество с использованием социальной инженерии и атаки на платежные системы. Например, в 2022 году в России было зафиксировано более 1,5 млн случаев мошенничества с использованием банковских карт. Анализ угроз в сети свидетельствует о том, что киберпреступления являются серьезной проблемой для международной и национальной экономической безопасности. Постоянное развитие технических средств, используемых злоумышленниками для осуществления атак, обуславливает необходимость активного и комплексного подхода в реализации защитных мер для обеспечения стойкости и безопасности информационной инфраструктуры.

В России обеспечивают кибербезопасность соответствующие государственные органы и структуры, в числе которых, можно выделить следующие: Федеральная служба безопасности (ФСБ), Министерство внутренних дел (МВД), Министерство цифрового развития, связи и массовых коммуникаций (Минцифры), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Центр по противодействию киберпреступности и другие. Кроме того, разрабатывается и активно применяется законодательство, направленное на обеспечение безопасности в киберпространстве.

Помимо принятия внутренних мер, Россия активно взаимодействует с другими странами и международными организациями в области обеспечения кибербезопасности. В рамках такого сотрудничества обмениваются информацией об угрозах, разрабатываются совместные механизмы реагирования на кибератаки и проводятся совместные тренировки и учения [12].

На макроуровне государство является постоянной мишенью кибератак извне, и до 15% от общего объема таких атак направлено на государственные учреждения. Это подчеркивает необходимость разработки четкой и скоординированной стратегии борьбы с киберпреступностью со стороны органов государственной власти. В качестве основы для этой стратегии на законодательном уровне была разработана Доктрина информационной безопасности страны, в которой кибербезопасность выделена как важный компонент, учитывающий национальные интересы, виды угроз и стратегические цели, направленные на обеспечение информационной безопасности [9].

Противодействие угрозам кибербезопасности на уровне государства включает в себя ряд мероприятий, которые направлены на предотвращение, обнаружение и реагирование на возможные атаки в Сети на экономику страны. Можно выделить следующие ключевые меры:

1. Создание централизованной системы мониторинга киберугроз.

Необходимо разработать единую платформу для сбора и анализа данных о кибератаках, которая будет интегрирована с системами государственных органов и частных компаний. Это позволит оперативно выявлять угрозы и координировать действия по их устранению.

2. Ужесточение требований к защите персональных данных.

Предлагается внести изменения в законодательство, обязывающие компании внедрять современные методы шифрования и аутентификации. Также необходимо ввести обязательное обучение сотрудников компаний правилам кибергигиены.

3. Развитие образовательных программ в области кибербезопасности.

Для решения проблемы нехватки кадров следует расширить программы подготовки специалистов в вузах и создать систему непрерывного обучения для сотрудников IT-отделов. Важно также стимулировать молодежь к выбору профессий в сфере кибербезопасности через гранты и стипендии.

4. Стимулирование обмена информацией между компаниями и государством.

Для повышения прозрачности и оперативности реагирования на угрозы предлагается ввести систему поощрений для компаний, которые добровольно сообщают о кибератаках. Это может включать налоговые льготы или снижение страховых взносов.

5. Разработка национальной стратегии по защите финансового сектора.

Необходимо создать специализированный орган, который будет координировать действия банков, платежных систем и регуляторов для предотвращения мошенничества. Также важно внедрить технологии искусственного интеллекта для анализа транзакций и выявления подозрительных операций.

## 6. Укрепление международного сотрудничества.

Россия должна активнее участвовать в международных инициативах по борьбе с киберпреступностью, таких как Конвенция Совета Европы о киберпреступности. Это позволит обмениваться опытом и оперативно реагировать на трансграничные угрозы.

Международное сотрудничество способствует более эффективной борьбе с киберпреступностью, особенно в тех странах, где отсутствуют необходимые ресурсы, что создает проблемы как для соседей, так и для международного сообщества в целом [10].

Крайне необходимо улучшить сбор актуальной статистической информации национальными органами. Дальнейшая стандартизация данных об угрозах и координация требований к кибербезопасности значительно повысит уровень защиты, особенно в таких критически важных секторах, как финансы.

Без таких мер киберпреступность будет стремительно развиваться на фоне роста числа подключенных устройств и ценности онлайн-операций. Улучшение сбора данных о киберпреступлениях необходимо для эффективного решения этой проблемы и обоснования необходимости выделения дополнительных ресурсов. Однако сбор данных может быть политически чувствительным вопросом, так как жертвы часто предпочитают не сообщать о киберпреступлениях. Кроме того, может быть сложно количественно оценить стоимость нематериальных товаров и услуг, а также некоторых киберфинансовых преступлений, таких как манипуляции на фондовом рынке.

Подводя итог можно сказать, что существует тесная связь между кибербезопасностью и экономической безопасностью. Недостаточный уровень обеспечения кибербезопасности может серьезно повлиять на экономическую стабильность и безопасность хозяйствующих субъектов и государства.

В современном информационном обществе практически все экономические субъекты зависят от применения информационных систем и сети Интернет, постоянно сталкиваются с угрозами кибератак и другими преступными действиями посредством Сети. Эффективное управление кибербезопасностью становится неотъемлемым условием для обеспечения стабильности и устойчивого экономического роста, создает благоприятную экономическую среду, способствует привлечению инвестиций и способствует развитию цифровых технологий.

**Список литературы:**

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.
2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности». Собрание законодательства Российской Федерации. 2010. № 1. Ст. 2.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4736.
4. Указ Президента РФ от 5 декабря 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.
5. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.
6. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». Собрание законодательства Российской Федерации. 2021. № 16. Ст. 2746.
7. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». Собрание законодательства Российской Федерации. 2021. № 27. Ст. 5351.
8. Кузнецов, А. В. Кибербезопасность: вызовы и угрозы. Москва: Издательство "Наука", 2021.
9. Громов, И. А. Кибербезопасность: теория и практика защиты информации. Санкт-Петербург: Питер, 2022.
10. Лебедев, С. В. Киберугрозы и их влияние на экономическую безопасность России. Вестник информационной безопасности. 2022. № 1(1). С. 12-20.
11. Антропов К. Ю., Ахмадеев Р. Г., Косов М. Е. Кибербезопасность и сохранение цифрового суверенитета экономики // Вестник экономической безопасности. 2021. № 5. С. 268–273. <https://doi.org/10.24412/2414-3995-2021-5-268-273>.
12. Архипцев, И. Н. Кибербезопасность и компьютерная грамотность в правоохранительных органах / [И. Н. Архипцев и др.] // Проблемы в российском законодательстве. 2021. Т. 14. № 4. С. 276–279.
13. Богданов, Ю. М. Мониторинг кибербезопасности сложных информационных и управляющих систем критической инфраструктуры / Ю. М. Богданов, А. Л. Огарок, С. А. Селиванов // Информатизация и связь. 2021. № 1. С. 142–150.
14. Горохова, С. С. Искусственный интеллект: инструмент обеспечения кибербезопасности финансовой сферы или киберугроза для банков / С. С. Горохова // Банковское право. 2021. № 1. С. 35–46.
15. Гукешоков, М. Х. Тенденции развития права в условиях цифровой реальности / [М. Х. Гукешоков и др.] // Финансовая экономика. 2021. № 3. С. 145–149.

**References:**

1. Federal Law No. 149-FZ of 27.07.2006 "On Information, Information Technologies and Information Protection". Collection of legislation of the Russian Federation. 2006. No. 31. Art. 3448.
2. Federal Law No. 390-FZ dated December 28, 2010 "On Security". Collection of legislation of the Russian Federation. 2010. No. 1. Art. 2.
3. Federal Law No. 187-FZ dated July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation". Collection of legislation of the Russian Federation. 2017. No. 31. Article 4736.
4. Decree of the President of the Russian Federation dated December 5, 2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation". Collection of legislation of the Russian Federation. 2016. No. 50. Art. 7074.
5. Decree of the President of the Russian Federation dated 10.10.2019 No. 490 "On the development of artificial intelligence in the Russian Federation". Collection of legislation of the Russian Federation. 2019. No. 41. St. 5700.
6. Decree of the President of the Russian Federation dated 04/12/2021 No. 213 "On Approval of the Fundamentals of the State Policy of the Russian Federation in the field of international information security". Collection of legislation of the Russian Federation. 2021. No. 16.
7. Decree of the President of the Russian Federation dated 07/02/2021 No. 400 "On the National Security Strategy of the Russian Federation". Collection of legislation of the Russian Federation. 2021. No. 27. Art. 5351.
8. Kuznetsov, A.V. Cybersecurity: challenges and threats. Moscow: Nauka Publishing House, 2021.
9. Gromov, I. A. Cybersecurity: theory and practice of information protection. Saint Petersburg: Peter, 2022.
10. Lebedev, S. V. Cyber threats and their impact on Russia's economic security. Bulletin of Information Security. 2022. No. 1(1). pp. 12-20.
11. Antropov K. Yu., Akhmedeev R. G., Kosov M. E. Cybersecurity and preservation of digital sovereignty of the economy // Bulletin of Economic Security. 2021. No. 5. pp. 268-273. <https://doi.org/10.24412/2414-3995-2021-5-268-273>.
12. Arkhipcev, I. N. Cybersecurity and computer literacy in law enforcement agencies / [I. N. Arkhipcev et al.] // Gaps in Russian legislation. 2021. Vol. 14. No. 4. pp. 276-279.
13. Bogdanov, Yu. M. Monitoring cybersecurity of complex information and control systems of critical infrastructure / Yu. M. Bogdanov, A. L. Ogarok, S. A. Selivanov // Informatization and communications. 2021. No. 1. pp. 142-150.
14. Gorokhova, S. S. Artificial intelligence: a tool for ensuring cybersecurity of the financial sector or a cyber threat for banks / S. S. Gorokhova // Banking law. 2021. No. 1. pp. 35-46.
15. Gukeshokov, M. H. Trends in the development of law in digital reality / [M. H. Gukeshokov et al.] // Financial Economics. 2021. No. 3. pp. 145-149.