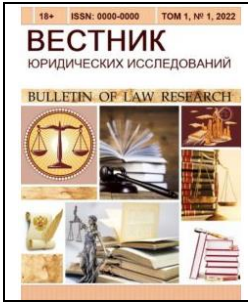

*Научно-исследовательский журнал «**Вестник юридических исследований / Bulletin of Law Research**»*
https://blr-journal.ru
2025, Том 4, № 3 / 2025, Vol. 4, Iss. 3 https://blr-journal.ru/archives/category/publications
Научная статья / Original article
УДК 338.1

Киберугрозы как ключевые угрозы экономической безопасности в условиях современного мира

[1] Кравчук Е.А., [1] Селезнёв Р.Н.,
[1] Российский государственный университет правосудия имени В.М. Лебедева

Аннотация: данная статья посвящена исследованию киберугроз как одних из глобальных угроз, которые влияют на экономическую безопасность в условиях всеобщей цифровизации. Ускорение развития информационно-коммуникационных технологий (ИКТ) оказывает значительное влияние на различные сферы деятельности человечества, обеспечивая новые возможности для экономического и социального развития, но вместе с этим растет число угроз экономической безопасности, которые связаны с использованием ИКТ. Данная работа предусматривает статистику роста количества зарегистрированных фактов совершения киберпреступлений. Работа рассматривает виды киберугроз, такие как утечка конфиденциальной информации, взлом аккаунтов в социальных сетях и другие формы несанкционированного вмешательства в информационные системы. Исследуются существующие трудности и актуальные вызовы в обеспечении защиты критически важных объектов инфраструктуры и коммерческих структур. Также данная статья включает рекомендации по укреплению экономической безопасности в сфере цифровизации. В статье приводятся реальные примеры известных кибератак начала XXI века, подчеркивая значимость проблем кибербезопасности. Результаты исследования могут быть использованы для разработки практических мер по повышению устойчивости экономики к киберугрозам и обеспечению ее стабильного развития в условиях цифровизации.

Ключевые слова: киберугрозы, цифровизация, экономическая безопасность, технологии, федеральный закон, кибербезопасность, киберпреступления

Для цитирования: Кравчук Е.А., Селезнёв Р.Н. Киберугрозы как ключевые угрозы экономической безопасности в условиях современного мира // Вестник юридических исследований. 2025. Том 4. № 3. С. 123 – 127.

Поступила в редакцию: 16 февраля 2025 г.; Одобрена после рецензирования: 18 апреля 2025 г.; Принята к публикации: 22 мая 2025 г.

Cyber threats as key threats to economic security in the modern world

[1] Kravchuk E.A., [1] Seleznev R.N.,
[1] Russian State University of Justice named after V.M. Lebedev

Abstract: this article is devoted to the study of cyber threats as one of the global threats that affect economic security in the context of universal digitalization. The acceleration of the development of information and communication technologies (ICTs) has a significant impact on various spheres of human activity, providing new opportunities for economic and social development, but at the same time, the number of threats to economic security associated with the use of ICTs is growing. This work provides statistics on the increase in the number of reported cases of cybercrime. The work examines types of cyber threats, such as the leakage of confidential information, hacking of accounts on social networks and other forms of unauthorized interference in information systems. The article

examines the existing difficulties and current challenges in ensuring the protection of critical infrastructure and commercial structures. This article also includes recommendations on strengthening economic security in the field of digitalization. The article provides real-life examples of well-known cyber attacks of the early 21st century, emphasizing the importance of cybersecurity issues. The research results can be used to develop practical measures to increase the resilience of the economy to cyber threats and ensure its stable development in the context of digitalization.

Keywords: cyber threat, digitalization, economic security, technology, federal law, cybersecurity, cybercrimes

For citation: Kravchuk E.A., Seleznev R.N. Cyber threats as key threats to economic security in the modern world. Bulletin of Law Research. 2025. 4 (3). P. 123 – 127.

The article was submitted: February 16, 2025; Approved after reviewing: April 18, 2025; Accepted for publication: May 22, 2025.

Введение

Современный мир стремительно переходит от индустриального общества к информационному (постиндустриальному), где информация становится ключевым ресурсом. Цифровые технологии меняют способы управления экономическими процессами, формирования финансовых потоков и ведение бизнеса. Это создает как огромные возможности для экономического роста, так и значительные риски для стабильности национальных экономик. В процессе глобализации и цифровизации экономика все чаще сталкивается с новыми киберугрозами. Эффективное противостояние этим рискам не может обойтись без надежной правовой базы, которая способна адаптироваться к быстро меняющимся условиям.

Материалы и методы исследований

В качестве методологической основы исследования использованы методы системного анализа и статистического анализа для выявления и оценки ключевых киберугроз, которые оказывают влияние на экономическую безопасность. Применялся анализ нормативно-правовых актов и стратегических документов, регулирующих сферу кибербезопасности, также были изучены научные публикации. Эмпирическую базу исследования составили данные о кибератаках, собранные из открытых источников.

Результаты и обсуждения

Стоит отметить слова Тима Бернерс-Ли: «Интернет должен быть местом, где люди могут безопасно обмениваться информацией. Защита от киберугроз – это общая ответственность». Из его высказывания можно сделать вывод, что киберугрозы являются особой опасностью в Интернете и нужна необходимость коллективных усилий в обеспечении безопасности. Киберугрозы – это любые потенциальные угрозы, направленные на нарушение конфиденциальности, целостности и доступности информационных систем, сетей и данных, которые могут исходить от различных источников, включая хакеров, инсайдеров, преступные группы, случайные ошибки пользователей [3].

За последние десятилетия наблюдается устойчивый рост количества зарегистрированных фактов совершения киберпреступлений. По данным МВД, в 2024 году в России было зарегистрировано 765,4 тысячи случаев киберпреступлений, что составляло 40% от всех преступлений, выявленных в стране [8]. По данным компании «Лаборатория Касперского», за 12 месяцев 2024 года в России было зафиксировано 1 812 562 707 случаев кибератак. Рост числа инцидентов, которые направлены на мобильные устройства под управлением ОС Android – данных случаев было зафиксировано на 12% больше, чем в 2023 году [1]. По подсчетам RED Security, число кибератак на российские компании в 2024 возросло году выросло в 2,5 раза по сравнению с 2023 годом – почти до 130 000 [10]. Большинство данных правонарушений совершается профессиональными группами преступников, которые действуют согласовано и организовано. Выделим следующие категории:

- похищение конфиденциальной информации (сведений ограниченного пользования, коммерческой и государственной тайн, взлом базы данных компании, содержащей личные данные пользователей);
- Malware [3] (предназначены для повреждения, уничтожения или несанкционированного доступа к системам и данным, например, WannaCry (программа-вымогатель), Keylogger (шпионское ПО));
- осуществление мошеннических операций с использованием платежных систем и электронных денег;
- несанкционированный доступ к информационным ресурсам (взлом)
- создание фальшивых сайтов известных брендов и сервисов;
- шантаж владельцев аккаунтов социальных сетей и мессенджеров.

Кибератаки стали одним из наиболее опасных факторов риска для экономической безопасности, и их влияние продолжает расти в условиях глобализации и цифровизации. Отметим несколько ключевых аспектов, подчеркивающие данную угрозу:

- утечка конфиденциальной информации, включая данные клиентов или интеллектуальную собственность, которая наносит ущерб репутации компании и влечет за собой юридические последствия;
- кибератаки могут привести к финансовым потерям из-за кражи средств, вымогательства и затрат на восстановление систем;
- прерывание бизнес-процессов, так как кибератаки могут привести к замедлению и остановку работу предприятий, что может негативно сказаться на доходах и производительности;
- частые кибератаки могут ухудшить репутацию предприятия, так как клиенты, инвесторы и партнеры могут потерять доверие к компании, если им станет известно о кибератаке, что может привести к упадку бизнеса, а также к юридическим и финансовым последствиям [9, с. 15];
- компании, которые стали жертвами кибератак, могут потерять свою конкурентоспособность на рынке, что влияет на экономику.

Укрепление экономической безопасности и преодоление кибератак в условиях цифровизации требует более глубокого и комплексного подхода. Одним из подходов является повышение уровня кибербезопасности, поскольку цифровизация предполагает использование сложных IT-систем и больших объемов данных, что представляет опасность для организаций. Необходимо регулярно оценивать риски с помощью аудитов информационной безопасности, чтобы выявлять слабые места в системах, и создавать резервные копии важных данных, чтобы уменьшить последствия утраты информации. Отметим такой подход, как разработку стратегии управления данных, для которой необходимо обеспечить правовую защиту данных, поскольку важно разрабатывать внутреннюю политику обработки персональных данных и их соответствие законодательству. Например, Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024), согласно которому создается правовая основа обращения с персональными данными физических лиц, также стоит отметить GDPR (General Data Protection Regulation) - законодательный акт Европейского союза, который определяет порядок сбора, обработки, хранения и распространения персональных данных в странах Евросоюза и с участием его граждан [11] (действует с 25.05.2018 года). Так как традиционные нормы могут не учитывать специфику цифровой экономики, поэтому необходимо разрабатывать новые законы и нормативные акты, регулирующие вопросы кибербезопасности, вопросы ответственности за нарушения в данной сфере. В экономической безопасности имеет особое место развитие цифровых компетенций, так как эффективное управление цифровыми процессами требует наличие квалифицированных кадров. Например, развитие цифрового образования повысит уровень квалификации, что позволит увеличить число квалифицированных кадров и повысить их эффективность в работе [2, с. 17]; формирование специализированных подразделений внутри компаний, которые занимаются вопросами цифровизации и информационной безопасности. Также стоит отметить такую рекомендацию, как учет социальных аспектов цифровизации и экономической безопасности, так как процессы цифровизации могут приводить к увеличению социального неравенства и ухудшению качества жизни населения, поэтому, необходимо разрабатывать программы поддержки и обучения населения. Особой важностью укрепления экономической безопасности в условиях цифровизации является международное сотрудничество для создания устойчивых систем от кибератак. Важным аспектом является разработка общих стандартов и протоколов безопасности, позволяющие странам совместно реагировать на кибератаки и обмениваться информацией, которая может помочь минимизировать ущерб от киберугроз.

Среди наиболее известных кибератак можно выделить следующие случаи:

- взлом аккаунтов знаменитостей в Twitter (Илона Маска, Канье Уэста, Барака Обамы и других известных личностей США). Во взломанных аккаунтах мошенники призывали отправлять биткоины на указанный криптокошелек. Пострадали также корпоративные аккаунты Apple и Uber [12];
- атака на ГАС (государственная автоматизированная система Российской Федерации) «Правосудие». В октябре 2024 года хакеры взломали государственную систему, которая используется для управления судебными процессами. Мошенники получили доступ к серверам системы, где хранилась информация о судебных делах, а также данные граждан, участвующих в процессах, что в итоге привело к уничтожению большого количества данных [4];
- в 2014 году хакеры получили доступ к фото и видео знаменитостей, которые хранились в облаке iCloud, тем самым, они попали в сеть. В числе пострадавших оказались: Ким Кардашьян, Кейли Куоко, Дженнифер Лоуренс, Кирстен Дантс, Рианна, Скарлетт Йоханссон, Вайнона Райдер [12];

- 7 мая 2021 года произошла хакерская атака на компанию Colonial Pipeline, которая является оператором крупнейшего нефтепровода в США. В результате этого, данная атака привела к тому, что датчики давления, термостаты, насосы, трубопроводная арматура и другие элементы нефтепровода оказались выведены из строя [5];

- в ноябре 2021 года произошла мощная DDoS-атака на «Госуслуги. Атака мощностью свыше 680 гигабит в секунду привела к временным проблемам с доступом для некоторых пользователей. Отдельно пострадал экспериментальный чат-бот «Макс» [6];

- вирус Stuxnet, предположительно созданный американскими и израильскими спецслужбами, проник на иранские ядерные объекты в 2009 году, вызвав сбои в работе центрифуг. В результате более 1300 центрифуг были повреждены, что существенно замедлило развитие иранской ядерной программы [7].

Выводы

В заключение хотелось бы отметить слова Мартина Навратилова: «Раньше безопасность иногда была неудобством, но теперь она стала постоянной необходимостью». Из данного высказывания можно сделать вывод, что безопасность раньше воспринималась как что-то необязательное или даже мешающее в повседневной жизни, но сейчас безопасность стала важной частью существования. Так, цифровизация экономики создает новые возможности для развития и роста, но одновременно увеличивает риски, которые связаны с киберугрозами. Киберпреступления могут наносить непоправимый ущерб компаниям и государствам, нарушая работу важных инфраструктур, похищая конфиденциальную информацию и финансовые средства, что в итоге может привести к уходу с рынка и потери доверия клиентов. Таким образом, обеспечение кибербезопасности должно стать важной задачей для поддержания стабильности и конкурентоспособности в цифровой экономике.

Список источников

1. В «Лаборатории Касперского» посчитали все кибератаки на Россию за 2024 год. // газета.ru. URL: https://www.gazeta.ru/tech/news/2025/01/16/24840404.shtml (дата обращения: 25.01.2025)
2. Иванова Н.М., Жеребцов А.А. Цифровизация экономики и ее влияние на экономическую безопасность России // Контентус. 2023. Т. 4. № 7S. С. 25 – 31.
3. Киберугрозы: виды, примеры и как защититься. // 4BRAIN. URL: https://4brain.ru/internet_security/cyberthreats.php (дата обращения 20.01.2025)
4. Пять крупнейших хакерских атак 2024 года. // Тренды. URL: https://trends.rbc.ru/trends/industry/67613aff9a7947f4d1ea3f71 (дата обращения 20.01.2025)
5. «Робин Гуды» нашего времени: хакеры вывели из строя крупнейший нефтепровод в США // ПРОСТНЬЮС статьи. URL: https://postnews.ru/a/7743 (дата обращения 20.01.2025)
6. Самые крупные хакерские атаки в России с 2021 по 2025 год. // КОМПЬЮТЕРРА. URL: https://www.computerra.ru/309334/samye-krupnye-hakerskie-ataki-v-rossii-s-2021-po-2025-god/ (дата обращения 25.01.2025)
7. Семь громких кибератак в России и в мире. // Финам. URL: https://www.finam.ru/publications/item/sem-gromkix-kiberatak-v-rossii-i-v-mire-20210910-183246/ (дата обращения 25.01.2025)
8. «Статистика киберпреступности в российских регионах: данные МВД за 2024 год». // Региональные системы: URL: https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/ (дата обращения 25.01.2025)
9. Струнин Д.А. Кибератаки и их влияние на цифровую экономику // Молодой ученый. 2023. № 5 (452). С. 15 – 16. URL: https://moluch.ru/archive/452/99590/ (дата обращения: 18.01.2025)
10. Число кибератак на российские компании за год выросло в 2,5 раза. // Бизнес-секреты. URL: https://secrets.tbank.ru/novosti/kiberataky-2024/ (дата обращения: 20.01.2025)
11. GDPR (general data protection regulation) // UNISENDER Словарь маркетолога. URL: https://www.unisender.com/ru/glossary/gdpr/ (дата обращения 18.01.2025)
12. 10 самых громких кибератак XXI века // Тренды. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (дата обращения 20.01.2025)

References

1. Kaspersky Lab counted all cyberattacks on Russia in 2024. gazeta.ru. URL: https://www.gazeta.ru/tech/news/2025/01/16/24840404.shtml (accessed on 25.01.2025)
2. Ivanova N.M., Zherebtsov A.A. Digitalization of the economy and its impact on Russia's economic security. Contentus. 2023. Vol. 4. No. 7S. P. 25 – 31.

3. Cyber threats: types, examples, and how to protect yourself. 4BRAIN. URL: https://4brain.ru/internet_security/cyberthreats.php (accessed on 20.01.2025)
4. The five largest hacker attacks of 2024. Trends. URL: https://trends.rbc.ru/trends/industry/67613aff9a7947f4d1ea3f71 (date of access 01/20/2025)
5. "Robin Hoods" of our time: hackers disabled the largest oil pipeline in the USA. PROSTNEWS articles. URL: https://postnews.ru/a/7743 (date of access 01/20/2025)
6. The largest hacker attacks in Russia from 2021 to 2025. COMPUTERRA. URL: https://www.computerra.ru/309334/samye-krupnye-hakerskie-ataki-v-rossii-s-2021-po-2025-god/ (date of access 01/25/2025)
7. Seven high-profile cyberattacks in Russia and the world. Finam. URL: https://www.finam.ru/publications/item/sem-gromkix-kiberatak-v-rossii-i-v-mire-20210910-183246/ (date of access 01/25/2025)
8. "Cybercrime statistics in Russian regions: data from the Ministry of Internal Affairs for 2024". Regional systems: URL: https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/ (date of access 01/25/2025)
9. Strunin D.A. Cyberattacks and their impact on the digital economy. Young scientist. 2023. No. 5 (452). P. 15 – 16. URL: https://moluch.ru/archive/452/99590/ (date of access: 01.18.2025)
10. The number of cyberattacks on Russian companies has increased by 2.5 times in a year. Business secrets. URL: https://secrets.tbank.ru/novosti/kiberataky-2024/ (date of access 01.20.2025)
11. GDPR (general data protection regulation). UNISENDER Marketer's Dictionary. URL: https://www.unisender.com/ru/glossary/gdpr/ (date of access 01/18/2025)
12. 10 most high-profile cyberattacks of the 21st century. Trends. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (date of access 01/20/2025)

Информация об авторах

Кравчук Е.А., Российский государственный университет правосудия имени В.М. Лебедева

Селезнёв Р.Н., преподаватель, Российский государственный университет правосудия имени В.М. Лебедева