УДК 343.9 **DOI: 10.34670/AR.2026.21.72.064**

Киберпреступность: актуальность угрозы и перспективы борьбы с ней

Багрецов Дмитрий Николаевич

Кандидат филологических наук, старший преподаватель,
Уральский юридический институт МВД России,
620057, Российская Федерация, Екатеринбург, ул. Корепина, 66;
e-mail: bagretsow75@yandex.ru

Исакова Ирина Викторовна

Старший преподаватель,
Уральский юридический институт МВД России,
620057, Российская Федерация, Екатеринбург, ул. Корепина, 66;
e-mail: Isakova-1@yandex.ru

Аннотация

Киберпреступность становится все более серьезной угрозой для индивидуальных пользователей, компаний и даже государств. С развитием цифровых технологий и увеличением числа подключений к интернету, объемы и сложность кибератак значительно возросли. Это приводит к потере конфиденциальной информации, финансовым потерям и нанесению вреда репутации организаций. В этой связи разработка и реализация эффективных мер по борьбе с киберпреступностью являются критически важными для сохранения безопасности данных. Государства и частный сектор ищут новые подходы и технологии для предотвращения и реагирования на киберугрозы, что требует международного сотрудничества и обмена опытом.

Для цитирования в научных исследованиях

Багрецов Д.Н., Исакова И.В. Киберпреступность: актуальность угрозы и перспективы борьбы с ней // Вопросы российского и международного права. 2026. Том 16. № 1А. С. 530-537. DOI: 10.34670/AR.2026.21.72.064

Ключевые слова

Киберпреступность, цифровизация, безопасность, интернет, искусственный интеллект, киберугрозы, защита информации.

Введение

Киберпреступность становится все более серьезной угрозой для жизнедеятельности современного общества, приводя к значительным изменениям в способах ведения бизнеса, управления государственными и международными процессами, а также в повседневном общении людей. Как следствие, киберпространство становится не только ресурсом безграничных возможностей, но и ареной для различных противоправных действий, известных как киберпреступность. Этот термин охватывает широкий спектр деятельности, варьирующейся от мошенничества в интернете и взлома данных до распространения вирусов и кибершпионажа.

Развитие технологий, таких как Интернет вещей [Витвицкая, Витвицкий, Исакова, 2023; Что такое интернет вещей? www] (IoT), искусственный интеллект (ИИ) и большие данные, открыли новые горизонты для киберпреступников. Использование этих технологий позволяет совершать преступления с большей степенью анонимности и трудноуловимости. Проблема усугубляется тем, что многие киберпреступления имеют транснациональный характер, что делает сложным привлечение виновных к ответственности из-за различий в юрисдикциях и законодательствах разных стран.

Киберпреступность оказывает значительное негативное влияние на экономику и общественную безопасность. Она угрожает конфиденциальности личных данных, стабильности банковских и финансовых систем и даже национальной безопасности. По оценкам, общемировые затраты на борьбу с киберпреступностью будут продолжать расти, достигая огромных сумм в будущем.

Борьба с киберпреступностью включает не только технические, но и правовые, организационные аспекты [Афанасьева, Гончарова, Шиян, 2019]. Всё большее значение приобретает международное сотрудничество в обмене информацией, правоохранительных практиках и создании общих стандартов безопасности. Однако, несмотря на прогресс в этих направлениях, проблема киберпреступности остается актуальной и требует постоянного адаптирования и инноваций в стратегиях обеспечения кибербезопасности.

Таким образом, понимание сущности киберпреступности и масштабов угрозы, которую она представляет, а также разработка эффективных мер борьбы с этим явлением [Демидов, Костенников, Куракин, 2016] становятся критически важными компонентами обеспечения стабильности и безопасности в цифровую эпоху. В этом контексте признание киберпреступности как серьезной угрозы на глобальном уровне является первым шагом к формированию единой международной повестки в области её предотвращения и пресечения.

Основные виды и методы киберпреступлений

Киберпреступность охватывает широкий спектр правонарушений, осуществляемых при помощи или с целью повреждения компьютерных систем, сетей и цифровых технологий. Рассмотрим основные виды и методы киберпреступлений, которые в настоящее время представляют существенную угрозу для частных лиц, бизнеса и государственных структур.

Фишинг – один из наиболее распространённых видов атак, целью которого является получение конфиденциальных данных (логины, пароли, данные банковских карт) путём их "выуживания" из пользователей. Злоумышленники используют электронные письма, сообщения в социальных сетях или текстовые сообщения, маскируясь под надёжные источники, такие как банки, социальные сети или почтовые службы.

Вредоносное ПО (малварь), от английского «malicious software», включая вирусы, троянские кони и шпионское ПО, представляет собой программы или коды, разработанные для внедрения или повреждения компьютерной системы без ведома пользователя. Получив контроль над системой, киберпреступники могут красть личные данные, использовать компьютер для различных мошеннических операций или же включать компьютер в состав ботнета для совершения DDoS-атак.

Атаки "отказ в обслуживании" (DDoS) заключаются в перегрузке целевых серверов, систем или сетей большим количеством запросов, из-за чего легитимные пользователи не могут получить доступ к услугам. Это может быть направлено на вымогательство или просто на разрушение конкурентов или нежелательных сервисов.

Рэнсомвар или вымогательское ПО – это тип вредоносного ПО, которое блокирует доступ к системе или шифрует данные с требованием выкупа за восстановление доступа. Атаки рэнсомвара могут быть нацелены как на индивидуальных пользователей, так и на крупные корпорации, причиняя значительный экономический ущерб.

Кибершпионаж включает в себя использование цифровых технологий для получения секретной или защищенной информации без разрешения владельца. Часто это связано с государственными структурами, но также распространено среди крупных корпораций.

Социальная инженерия — это метод, при котором преступники манипулируют людьми, чтобы вынудить их раскрыть конфиденциальную информацию. Методы могут варьироваться от простых обманов до сложных многоэтапных атак, где злоумышленник может выступать в роли доверенного лица или авторитета.

Эти виды и методы киберпреступлений демонстрируют разнообразие и сложность угроз, с которыми сталкиваются пользователи в современном цифровом мире. Важно отметить, что по мере развития технологий киберпреступники находят новые способы атак и эксплуатации технологических уязвимостей, что требует постоянной вигилантности и адаптации со стороны оборонных систем.

Современные угрозы и их влияние на общество

Киберпреступность в современном мире принимает всё более сложные и масштабные формы [Витвицкая, Витвицкий, Исакова, 2023], представляя серьезную угрозу как для отдельных пользователей, так и для крупных организаций и государства в целом. За последние годы число атак в киберпространстве значительно возросло, их цели и методы становятся всё более разнообразными.

Основные современные угрозы включают использование вредоносного программного обеспечения, атаки на критическую инфраструктуру, фишинг, кражу данных и кибершпионаж. Вредоносное ПО, включая трояны и вирусы, продолжает быть распространенным способом заражения компьютерных систем с целью кражи чувствительной информации, требования выкупа или просто дестабилизации работы организаций.

Фишинговые атаки обычно нацелены на получение персональных данных пользователей, таких как логины и пароли, путем отправки поддельных сообщений, имитирующих законные запросы от знакомых организаций. Такие материалы часто содержат ссылки на вредоносные сайты или вложения, которые, будучи открытыми, активируют механизмы утечки данных [Канубриков, Османов, 2023].

Кража данных из крупных корпораций и правительственных организаций оказывает значительное воздействие на экономическую и политическую стабильность страны.

Последствия таких атак могут включать потерю корпоративных секретов, интеллектуальной собственности и чувствительной информации граждан. Кроме того, влияние на рынки может быть мгновенным, снижая доверие инвесторов и влекущее за собой колебания акционерной стоимости компаний [Нейберт, 2023].

Другой важной ареной киберпреступности является кибершпионаж, который включает хищение данных не только для экономической выгоды, но и для политического давления или стратегического преимущества. Государственно-поддерживаемые хакерские операции могут целиться в электоральные системы, государственные организации и даже силы обороны, что является особенно тревожным в свете возрастающих международных напряженностей [Немов, 2017].

Атаки на критическую инфраструктуру представляют собой особо опасное направление киберпреступности. Они могут включать атаки на системы управления энергосетями, водоснабжением, транспортом и здравоохранением. Нападения такого рода способны привести не только к экономическому ущербу, но и к непоправимым последствиям для здоровья и безопасности человека.

Эти угрозы неизбежно влияют на социальное взаимодействие внутри общества, увеличивая уровень недоверия и создавая атмосферу страха и неопределенности среди граждан. Предприятия и частные лица вынуждены увеличивать расходы на защиту информационной безопасности, что в свою очередь может замедлить темпы развития и инноваций [Немов, 2017].

Таким образом, современные киберугрозы не только наносят значительный экономический ущерб, но и провоцируют глубокие социальные изменения, влияющие на все аспекты жизни современного общества. Эффективная борьба с киберпреступностью требует не только развития новых технологий и методов защиты, но и международного сотрудничества, усиления правовой базы и повышения информационной культуры среди населения. В противном случае, риски и последствия кибератак будут только усиливаться.

Текущие методы и технологии борьбы с киберпреступностью

В борьбе с киберпреступностью используются различные методы и технологии, каждый из которых имеет свои особенности и области применения. Одним из наиболее эффективных подходов является использование систем обнаружения и предотвращения вторжений (IDS/IPS). Эти системы непрерывно мониторят сетевой трафик на предмет подозрительной активности и могут автоматически блокировать атаки или предупреждать администраторов о возможных угрозах.

Еще одна распространенная мера — применение фаерволов, которые могут быть настроены для контроля доступа на основе установленных правил безопасности. Современные фаерволы обладают глубокими возможностями инспекции, что позволяет им не только блокировать несанкционированный трафик, но и анализировать проходящие через них данные на предмет вредоносного содержимого.

Метод шифрования данных также является ключевым в предотвращении несанкционированного доступа к информации. В случае утечки шифрованные данные остаются недоступными для злоумышленников без соответствующего ключа. Средства шифрования используются как в масштабах отдельных устройств, так и для защиты передаваемых данных, например, в интернет-банкинге или при онлайн-транзакциях.

Биометрическая аутентификация — это еще один метод повышения уровня безопасности, путем использования уникальных физических характеристик человека, таких как отпечатки

пальцев, распознавание лица или радужная оболочка глаза. Эта технология обеспечивает высокий уровень защиты от несанкционированного доступа и все чаще внедряется в мобильные устройства и системы доступа.

Кроме того, для борьбы с киберпреступностью активно используются средства искусственного интеллекта и машинного обучения, которые способны анализировать большие объемы данных и выявлять сложные паттерны поведения, которые могут указывать на кибератаки. Эти технологии помогают предсказать и предотвратить атаки до того, как они причинят ущерб.

Также необходимо упомянуть о регистрации и аудите событий безопасности, которые представляют собой детализированное логирование, регистрацию действий пользователей и системных процессов. Это позволяет оперативно отслеживать необычные или подозрительные действия и реагировать на них в кратчайшие сроки.

В совокупности все эти технологии и методы создают многоуровневую защитную систему, которая способна значительно снизить риски кибератак и минимизировать их последствия. Однако поскольку технологии постоянно развиваются, необходимо регулярно обновлять и адаптировать системы кибербезопасности для защиты от новых, все более изощренных угроз.

Перспективы развития и рекомендации по противодействию угрозам

Скорость развития технологий обуславливает непрерывное появление новых видов киберугроз [Число киберпреступлений в России, www; Киберпреступность. Модуль 2, www], что требует от государственных и частных структур одновременно реагировать на текущие вызовы и антиципировать будущие угрозы. В этом контексте, перспективы развития методов борьбы с киберпреступностью и рекомендации по противодействию угрозам становятся крайне актуальными.

Прежде всего, необходима интеграция усилий на национальном и международном уровнях. Эффективное противодействие киберпреступности возможно только при условии активного взаимодействия правоохранительных агентств, технологических компаний, финансовых институтов и образовательных учреждений. Важным шагом стала бы разработка и ратификация новых международных договоров, направленных на борьбу с киберпреступлениями, а также обновление существующих соглашений в свете последних технологических достижений.

Следующим важным аспектом является разработка технологических решений для защиты от кибератак. Искусственный интеллект и машинное обучение могут играть ключевую роль в разработке систем автоматического обнаружения и предотвращения киберугроз на ранней стадии. Применение алгоритмов глубокого обучения для анализа паттернов использования данных может помочь в идентификации ненормального поведения или потенциальных угроз.

Обучение и повышение осведомленности о кибербезопасности также остается приоритетным направлением. Регулярные тренинги и курсы для сотрудников всех уровней, включая управленческий состав, могут существенно уменьшить риски киберинцидентов. Особое внимание следует уделить созданию программ обучения для молодежи, так как она активно использует новые технологические платформы и часто становится целью для киберпреступников [Что такое интернет вещей?, www; ChatGPT и борьба с преступностью, 2023].

Не менее важна работа над созданием нормативных рамок. Современные законодательные инициативы должны не только ограничивать действия киберпреступников, но и способствовать созданию безопасной киберсреды. Возможные меры включают ужесточение наказаний за киберпреступления, улучшение процедур регистрации и контроля над киберпространством, а

также усиление требований к кибербезопасности у банков, IT-компаний и других организаций, подверженных высокому риску атак.

Заключение

В заключение важно подчеркнуть, что борьба с киберпреступностью требует не только технологических и правовых рамок, но и культурного изменения в отношении защиты данных. Создание культуры кибербезопасности, когда каждый пользователь сети осознает возможные риски и знает, как минимизировать их, станет ключом к обеспечению более безопасного киберпространства.

Библиография

1. Афанасьева О.Р., Гончарова М.В., Шиян В.И. Криминология и предупреждение преступлений. Учебник и практикум для СПО. Москва: Юрайт, 2019. 360 с.
2. Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. С. 20.
3. Демидов Ю.Н., Костенников М.В., Куракин А.В. Административная деятельность органов внутренних дел: учебник: в 2 ч. Часть 1: Общая часть. Домодедово: ВИПК МВД России, 2016. 285 с.
4. Канубриков В.А., Османов М.М. Соотношения понятий «киберпреступление» и «киберпреступность» в контексте исследования борьбы с киберпреступностью // Право и управление. 2023. № 2. URL: https://cyberleninka.ru/article/n/sootnosheniya-ponyatiy-kiberprestuplenie-ikiberprestupnost-v-kontekste-issledovaniyaborby-s-kiberprestupnostyu
5. Киберпреступность. Модуль 2. Основные виды киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности. URL: https://docs.yandex.ru/docs/view?tm=1737193546&tld=ru&lang=ru&name=Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf&text...
6. Ларина Е., Овчинский В. ChatGPT и борьба с преступностью // Завтра. 22 мая 2023. URL: https://zavtra.ru/blogs/chatgpt_i_bor_ba_s_prestupnost_yu
7. Нейберт А.Е. Киберпреступность как глобальная угроза: проблемы правоприменения // Международный научно-исследовательский журнал. 2023. № 12 (138). URL: https://research-journal.org/archive/12-138-2023-december/10.23670/IRJ.2023.138.94
8. Немов М.В. Киберпреступность как новая криминальная угроза // Эпоха науки. 2017. № 9. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnayaugroza-1
9. Число киберпреступлений в России // TADVISER. URL: https://www.tadviser.ru/index.php...
10. Что такое интернет вещей? Определение и описание // Лаборатория Касперского. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-iot

Cybercrime: The Relevance of the Threat and Prospects for Combating It

Dmitrii N. Bagretsov

PhD in Philology,
Senior Lecturer,
Ural Law Institute of the Ministry of Internal Affairs of Russia,
620057, 66, Korepina str., Yekaterinburg, Russian Federation;
e-mail: bagretsow75@yandex.ru

Irina V. Isakova

Senior Lecturer,
Ural Law Institute of the Ministry of Internal Affairs of Russia,
620057, 66, Korepina str., Yekaterinburg, Russian Federation;
e-mail: Isakova-1@yandex.ru

Abstract

Cybercrime is becoming an increasingly serious threat for individual users, companies, and even states. With the development of digital technologies and the increase in the number of internet connections, the volume and complexity of cyberattacks have grown significantly. This leads to the loss of confidential information, financial losses, and damage to the reputation of organizations. In this regard, the development and implementation of effective measures to combat cybercrime are critically important for maintaining data security. States and the private sector are seeking new approaches and technologies to prevent and respond to cyber threats, which requires international cooperation and the exchange of experience.

For citation

Bagretsov D.N., Isakova I.V. (2026) Kiberprestupnost': aktual'nost' ugrozy i perspektivy bor'by s ney [Cybercrime: The Relevance of the Threat and Prospects for Combating It]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (1A), pp. 530-537. DOI: 10.34670/AR.2026.21.72.064

Keywords

Cybercrime, digitalization, security, internet, artificial intelligence, cyber threats, information protection.

References

1. Afanaseva, O. R., Goncharova, M. V., & Shiyan, V. I. (2019). *Kriminologiya i preduprezhdeniye prestupleniy. Uchebnik i praktikum dlya SPO* [Criminology and crime prevention. Textbook and practicum for vocational education]. Moscow: Yurayt.
2. Demidov, Yu. N., Kostennikov, M. V., & Kurakin, A. V. (2016). *Administrativnaya deyatelnost organov vnutrennikh del: uchebnik: v 2 ch. Chast 1: Obshchaya chast* [Administrative activities of internal affairs bodies: textbook in 2 parts. Part 1: General part]. Domodedovo: VIPK MVD Rossii.
3. Kanubrikov, V. A., & Osmanov, M. M. (2023). Sootnosheniya ponyatiy "kiberprestupleniye" i "kiberprestupnost" v kontekste issledovaniya borby s kiberprestupnostyu [Correlation of the concepts "cybercrime" and "cybercriminality" in the context of studying the fight against cybercrime]. *Pravo i upravleniye*, (2). Retrieved from https://cyberleninka.ru/article/n/sootnosheniya-ponyatiy-kiberprestuplenie-ikiberprestupnost-v-kontekste-issledovaniyaborby-s-kiberprestupnostyu
4. Larina, E., & Ovchinsky, V. (2023, May 22). ChatGPT i borba s prestupnostyu [ChatGPT and the fight against crime]. *Zavtra*. Retrieved from https://zavtra.ru/blogs/chatgpt_i_bor_ba_s_prestupnost_yu
5. Neibert, A. E. (2023). Kiberprestupnost kak globalnaya ugroza: problemy pravoprimeneniya [Cybercrime as a global threat: problems of law enforcement]. *Mezhdunarodnyy nauchno-issledovatelskiy zhurnal*, (12). Retrieved from https://research-journal.org/archive/12-138-2023-december/10.23670/IRJ.2023.138.94
6. Nemov, M. V. (2017). Kiberprestupnost kak novaya kriminalnaya ugroza [Cybercrime as a new criminal threat]. *Epokha nauki*, (9). Retrieved from https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnayaugroza-1
7. [Chislo kiberprestupleniy v Rossii] The number of cybercrimes in Russia. (n.d.). *TADVISER*. Retrieved from https://www.tadviser.ru/index.php...
8. [Chto takoye internet veshchey? Opredeleniye i opisaniye] What is the Internet of Things? Definition and description. (n.d.). *Kaspersky Lab*. Retrieved from https://www.kaspersky.ru/resource-center/definitions/what-is-iot

9. [Kiberprestupnost. Modul 2. Osnovnyye vidy kiberprestupnosti] Cybercrime. Module 2. Main types of cybercrime. (n.d.). *United Nations Office on Drugs and Crime*. Retrieved from https://docs.yandex.ru/docs/view?tm=1737193546&tld=ru&lang=ru&name=Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf&text...
10. Vitvitskaya, S. S., Vitvitsky, A. A., & Isakova, Yu. I. (2023). Kiberprestupleniya: ponyatiye, klassifikatsiya, mezhdunarodnoye protivodeystviye [Cybercrimes: concept, classification, international counteraction]. *Pravovoy poryadok i pravovyye tsennosti*, 20.