Научная статья
https://doi.org/:10.29039/2312-7937-2025-2-119-124
EDN: https://elibrary.ru/crcnuy

Калашников Игорь Владимирович
кандидат юридических наук, доцент
Московский университет МВД России имени В.Я. Кикотя
(Москва, Россия)

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРЕДУПРЕЖДЕНИЕ ОТДЕЛЬНЫХ ВИДОВ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. *Киберпреступность остается одной из наиболее острых угроз безопасности для общества и государства, в российском обществе в настоящее время прослеживается тенденция к увеличению проникновения преступных угроз в информационно-телекоммуникационное пространство. Киберпреступность наносит значительный ущерб экономике и обществу. Среди наиболее распространенных категорий киберпреступлений в России — незаконный доступ к компьютерной информации, распространение вредоносного программного обеспечения и мошенничество в сфере информационных технологий. Законодательство Российской Федерации сталкивается с рядом вызовов, которые требуют усовершенствования. Основная проблема заключается в недостаточности норм, учитывающих особенности цифровой среды. В России киберпреступления подразделяются на несколько категорий, и только часть из них попадает в статистику МВД, что затрудняет оценку их реального распространения и влияния на экономику. Такая динамика требует не только усиленной работы правоохранительных органов, но и применения более сложных технологий для борьбы с этим видом преступности.*

Ключевые слова: *сайты сети Интернет, киберпреступления, информационные технологии, технологии VPN, TOR, информационно-телекоммуникационное пространство, нарушение авторских и смежных прав, предупреждение и пресечение киберпреступлений*

Для цитирования: *Калашников И.В. Криминологическая характеристика и предупреждение отдельных видов киберпреступлений // Вестник ВИПК МВД России. 2025. № 2(74). С. 119-124; https://doi.org/:10.29039/2312-7937-2025-2-119-124.*

KALASHNIKOV IGOR V.
PhD, associate professor
Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot
(Moscow, Russia)

CRIMINOLOGICAL CHARACTERISTICS AND PREVENTION OF CERTAIN TYPES OF CYBERCRIMES

Abstract. *Cybercrime remains one of the most acute security threats to society and the state; in Russian society, there is currently a tendency for criminal threats to increase their penetration into the information and telecommunications space. Cybercrime causes significant damage to the economy and society. Among the most common categories of cybercrime in Russia — illegal access to computer information, distribution of malicious software and fraud in the field of information technology. The legislation of the Russian Federation faces a number of challenges that require improvement. The main problem is the insufficiency of norms that take into account the specifics of the digital environment. In Russia, cybercrimes are divided into several categories, and only some of them are included in the statistics of the Ministry of Internal Affairs, which makes it difficult to assess their actual distribution and impact on the economy. Such dynamics require not only increased work by law enforcement agencies, but also the use of more complex technologies to combat this type of crime.*

Keywords: *Internet sites, cybercrimes, information technologies, VPN technologies, TOR, information and telecommunications space, violation of copyright and related rights, prevention and suppression of cybercrimes*

For citation: *Kalashnikov I.V. Criminological characteristics and prevention of certain types of cybercrimes // Vestnik Advanced Training Institute of the MIA of Russia. 2025. № 2(74). P. 119-124; https://doi.org/:10.29039/2312-7937-2025-2-119-124.*

В современных условиях достижения технологического прогресса оказывают существенное влияние на все сферы жизни общества. Этому влиянию также подвержено такое социальное явление, как преступность. В течение последних лет в российском обществе прослеживается тенденция к увеличению проникновения преступных угроз в информационно-телекоммуникационное пространство, в частности в сети Интернет [1, с. 101].

Сегодня киберпреступность остается одной из наиболее острых угроз безопасности для общества и государства. По данным МВД России, за последние годы масштабы киберпреступлений значительно возросли, и их количество продолжает расти. В январе-декабре 2024 года зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе-декабре 2023 года до 40,0%.

Практически все такие преступления (98,7%) выявляются органами внутренних дел. Почти половина таких преступлений (48,2%) относится к категориям тяжких и особо тяжких (369,3 тыс.; +7,8%), четыре преступления из пяти (84,8%) совершаются с использованием сети Интернет (649,1 тыс.; +23,2%), почти половина (45,2%) – средств мобильной связи (346,0 тыс.; +14,3%). Почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества: 486,3 тыс. (+2,3%), почти каждое восьмое (12,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 94,6 тыс. (+16,1%) [2, с. 3].

Эти данные подчеркивают необходимость разработки и внедрения новых мер, направленных на предупреждение и пресечение киберпреступлений. Повышенная угроза наблюдается и на уровне отдельных регионов России, где прирост случаев киберпреступности достигает от 75 до 117% в Ненецком автономном округе, Ингушетии и других субъектах федерации. Такая динамика требует не только усиленной работы правоохранительных органов, но и применения более сложных технологий для борьбы с этим видом преступности.

Термин «киберпреступление» в уголовном праве напрямую не используется, но в законодательстве Российской Федерации закреплен ряд преступлений, связанных с использованием информационных технологий, которые в целом можно отнести к киберпреступлениям. Ключевыми правовыми актами в данной сфере являются Уголовный кодекс Российской Федерации (УК РФ), который предусматривает ответственность за преступления в сфере компьютерной информации, и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регулирующий вопросы доступа, хранения и защиты информации.

В 28 главе УК РФ «Преступления в сфере компьютерной информации» определяются основные составы преступлений, связанных с неправомерным доступом к компьютерной информации. Статья 272 УК РФ, в частности, устанавливает ответственность за неправомерный доступ к компьютерной информации, если это повлекло за собой уничтожение, блокирование, модификацию или копирование данных. Эти нормы позволяют квалифицировать действия, связанные с кражей информации или вмешательством в работу ИТ-систем, как преступные.

Для определения особенностей киберпреступлений важно обратиться к их классификации. С точки зрения российской уголовной доктрины, преступления в сфере ИТТ можно разделить на несколько категорий:

Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.Эта группа преступлений, предусмотренных ст. 272-274 УК РФ, включает такие деяния, как неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи информации (ст. 274)[1]. Эти преступления направлены на вмешательство в работу ИТ-систем и могут нанести ущерб, как отдельным пользователям, так и крупным организациям, включая государственные учреждения.

Мошенничество с использованием информационных технологий. Кибермошенничество включает в себя широкий спектр преступлений, нацеленных на обман пользователей с целью получения их личной информации или денежных средств. Статья 159.6 УК РФ («Мошенничество в сфере компьютерной информации») является основным нормативным актом, регулирующим такие деяния. Примером может служить фишинг — распространенная форма кибермошенничества, при которой преступник создает поддельные сайты или отправляет фальшивые электронные письма, чтобы обманом заставить пользователей предоставить свои данные.

Преступления против частной жизни, совершаемые с использованием ИТТ. Важной категорией киберпреступлений является вмешательство в частную жизнь граждан через несанкционированный сбор и распространение их персональных данных. Такие преступления регулируются ст. 137 УК РФ («Нарушение неприкосновенности частной жизни»)[2], которая предусматривает ответственность за сбор и распространение сведений о частной жизни гражданина без его согласия. Особую угрозу в этой категории представляют действия, связанные с использованием социальных сетей и других платформ для получения и распространения личных данных пользователей.

Преступления, связанные с нарушением авторских прав. Незаконное использование объектов интеллектуальной собственности, таких как программное обеспечение, музыка, фильмы, литература и другие продукты, защищенные авторским правом, также составляет отдельную категорию киберпреступлений. Такие действия регулируются ст. 146 УК РФ («Нарушение авторских и смежных прав»). Незаконное копирование, распространение и продажа цифрового контента являются широко распространенными преступлениями, которые наносят значительный ущерб правообладателям и экономике в целом.

Преступления в сфере ИТТ обладают рядом специфических особенностей, которые отличают их от традиционных форм преступности и требуют особого подхода к их расследованию и предотвращению:

анонимность – преступники могут скрывать свое местонахождение и личность, используя технологии VPN, TOR и другие средства для анонимного доступа в интернет, что значительно осложняет их выявление. В России анонимность остается одной из главных проблем при расследовании киберпреступлений, особенно в случаях, когда преступники находятся за пределами страны;

глобальный характер – поскольку преступления совершаются в сети Интернет, границы государств для них практически не имеют значения. Примером может служить международная сеть преступников, использующих фальшивые сайты для выманивания средств у пользователей из разных стран;

использование вредоносного программного обеспечения – современные преступники используют специальные программы для взлома систем, кражи данных и распространения вирусов. Например, программа-вымогатель (ransomware) шифрует данные на компьютере жертвы и требует выкуп за их восстановление. В ст. 273 УК РФ оговаривается уголовная ответственность за разработку и распространение такого ПО;

---

[1] Уголовный кодекс Российской Федерации: Федер. закон от 13.06.1996 № 63-ФЗ: принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г.: посл .ред. // КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid=m9trmlgnrg740440851 (дата обращения 2.02.2025).

[2] Там же.

быстрая эволюция преступных технологий – преступники регулярно обновляют свои методы, адаптируясь к новым средствам защиты. Такая динамика требует от правоохранительных органов постоянного совершенствования их технической оснащенности и подготовки специалистов;

сложности в доказывании и идентификации – в отличие от традиционных преступлений, киберпреступления часто требуют специальных знаний для расследования, так как доказательства могут находиться в цифровом виде и быть защищены от несанкционированного доступа.

Несмотря на наличие базовых норм, регулирующих ответственность за преступления в сфере ИТТ, законодательство РФ сталкивается с рядом вызовов, которые требуют усовершенствования. Основная проблема заключается в недостаточности норм, учитывающих особенности цифровой среды. В частности, следует отметить:

Необходимость в совершенствовании правовой базы для борьбы с новыми формами киберпреступлений, такими как атаки с использованием искусственного интеллекта и облачных технологий.

Отсутствие механизмов быстрой адаптации к изменениям в цифровой сфере, законодательство в этой области нередко отстает от реальных событий, что создает «серые зоны», в которых киберпреступники могут действовать безнаказанно.

Проблемы международного сотрудничества, международные договоры и соглашения, такие как Конвенция о киберпреступности Совета Европы, помогают координировать усилия стран, но их исполнение сталкивается с трудностями. В частности, Россия не ратифицировала данную конвенцию, что создает дополнительные преграды в обмене данными с зарубежными правоохранительными органами[1].

В рамках предупреждения отдельных видов киберпреступлений необходимо отметить, что в России принимаются меры по укреплению правовой и технической базы для борьбы с киберпреступлениями. Доктрина информационной безопасности, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646[2], определяет основные направления государственной политики в области информационной безопасности, включая защиту критически важных информационных структур и обеспечение безопасности персональных данных. Кроме того, программа «Цифровая экономика Российской Федерации», утвержденная постановлением Правительства РФ от 28 июля 2017 г., также направлена на развитие цифровой инфраструктуры и повышение устойчивости киберугроз.

Таким образом, несмотря на активные меры по противодействию киберпреступности, данная сфера требует постоянного внимания, законодательного и технического обновления, а также тесного международного сотрудничества для эффективного противодействия глобальным угрозам.

Анализ статистических данных о киберпреступлениях представляет собой важную задачу, которая требует тщательного подхода и использования надежных источников информации. Для этого необходимо опираться на данные, собираемые и публикуемые как государственными, так и международными организациями. В России основной массив статистических данных по преступности, в том числе в сфере информационных технологий, предоставляется Министерством внутренних дел Российской Федерации (МВД России) и Федеральной службой государственной статистики (Росстат). Ежегодные отчеты и доклады этих ведомств позволяют отслеживать динамику киберпреступности и выделять наиболее значимые изменения и тенденции.

Среди международных источников важное место занимают отчёты ООН, Интерпола, а также специализированные исследования частных компаний, занимающихся кибербезопасностью (например, Kaspersky, Symantec, McAfee и др.). Эти компании ежегодно проводят

[1] Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: утверждена Указом Президента Российской Федерации от 12.12.2014 № К 1274 // Гарант: сайт. URL: https://base.garant.ru/71127868 (дата обращения 24.01.2025).

[2] Доктрина информационной безопасности РФ: утв. Указом Президента РФ от 09.09.2000 г. № Пр-1895 // Рос. газ. 2000. № 187. 28 сент.

анализ киберугроз и публикуют подробные отчёты о киберпреступности в различных странах. В условиях глобализации киберпреступлений международные данные необходимы для сравнительного анализа и выявления взаимосвязей и угроз, имеющих международный характер.

Согласно данным МВД России, в последние годы наблюдается устойчивый рост числа преступлений, связанных с информационно-телекоммуникационными технологиями. В 2022 году количество таких преступлений составило 522 тыс., что почти в три раза больше, чем в 2018 году, когда было зафиксировано около 174 тыс. преступлений.

Этот рост обусловлен, с одной стороны, повышенной активностью киберпреступников, использующих сложные технологии и целевые атаки, а с другой — увеличением общего количества пользователей цифровых технологий, что расширяет потенциальную базу жертв киберпреступности.

В 2023 году, согласно отчётам МВД России, зафиксирован рост числа преступлений в сфере ИТТ на 28% только за первое полугодие по сравнению с аналогичным периодом предыдущего года.

В 2024 году зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе-декабре 2023 года до 40,0% [2, с. 3].

Среди наиболее распространенных категорий киберпреступлений в России — незаконный доступ к компьютерной информации, распространение вредоносного ПО и мошенничество в сфере ИТ. Например, число преступлений, связанных с мошенничеством, увеличилось на 25,9% за последние два года, что связано с активным использованием интернет-платформ для кражи средств у граждан.

Киберпреступность в России демонстрирует различия в уровне активности по регионам. Исходя из информации МВД России за 2023 год, наиболее высокий рост числа киберпреступлений был зафиксирован в Ненецком автономном округе (117,5%), Ингушетии (92%), Томской (90,5%) и Ярославской областях (75%).

Такие различия могут быть связаны с особенностями экономического и социального развития регионов, доступностью интернета, уровнем цифровой грамотности населения и другими факторами.

С точки зрения структуры преступности, наибольшее количество киберпреступлений связано с неправомерным доступом к информации и её копированием. Этот тип преступлений включает, например, атаки на базы данных государственных организаций, банков и коммерческих компаний, что приводит к утечке конфиденциальной информации и нанесению значительного экономического ущерба. Второй по распространенности тип преступлений — это мошенничество в интернете, которое стало серьёзной проблемой для всех возрастных групп населения. Преступники используют различные способы социальной инженерии для получения личных данных пользователей, которые впоследствии используются для вымогательства денег или кражи идентичности.

В соответствии с докладом ООН, за последние десять лет киберпреступность вышла на новый уровень из-за активного использования цифровых технологий в личной и профессиональной жизни. ООН отмечает, что число зарегистрированных случаев кибератак и мошенничества в интернете растет по всему миру на 15-20% ежегодно. В странах Европы, США и Азии аналогичные тенденции подтверждаются отчетами Интерпола и Европола, где фиксируются тысячи инцидентов, связанных с кражей данных и шпионажем с помощью ИТТ. Особенно актуальными остаются угрозы атак на критическую инфраструктуру, включая медицинские учреждения и финансовые институты, где кибератаки могут привести к дестабилизации и экономическим потерям[1].

[1] Доклад Генерального Секретаря ООН «Воздействие организованной преступной деятельности на общество в целом» // Материалы комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, L7CN 15/1993/3.

В международной практике также наблюдается тенденция роста преступлений, связанных с программами-вымогателями (ransomware), которые шифруют данные и требуют выкуп за их восстановление. В 2023 году такие инциденты привели к потере миллионов долларов, причём значительная часть атак была направлена на компании и государственные учреждения, нарушая их работу и причиняя серьёзные убытки.

Несмотря на значительный объем данных о киберпреступлениях, их анализ затруднён из-за нескольких факторов. Прежде всего, не все киберпреступления регистрируются в официальной статистике, поскольку значительная часть инцидентов остаётся неизвестной правоохранительным органам из-за нежелания пострадавших организаций сообщать о случаях утечек данных или атак. Проблема «темного числа» преступлений, то есть случаев, о которых не сообщается официальным органам, особенно актуальна для киберпреступности.

Кроме того, различия в методах учета преступлений между странами и организациями осложняют сопоставление данных и их интеграцию для получения полной картины. Например, в международных отчетах часто приводится только общее количество инцидентов, в то время как структура и типы киберпреступлений могут существенно различаться. В России киберпреступления подразделяются на несколько категорий, и только часть из них попадает в статистику МВД, что затрудняет оценку их реального распространения и влияния на экономику.

Киберпреступность наносит значительный ущерб экономике и обществу. Прямые убытки от кибератак включают расходы на восстановление данных, повышение безопасности и компенсации пострадавшим пользователям. Например, компании, подвергшиеся атакам вымогателей, вынуждены тратить значительные средства на восстановление утраченной информации и восстановление своей репутации, особенно если пострадали данные клиентов.

Непрямые убытки включают потерю доверия к цифровым сервисам и снижение активности пользователей в интернете. Если пользователи не чувствуют себя в безопасности, они могут отказаться от использования определенных услуг, что приводит к потере доходов для компаний.

Одним из наиболее значительных последствий киберпреступлений является их воздействие на государственный бюджет. Для эффективной борьбы с киберугрозами государствам необходимо выделять значительные средства на обучение специалистов в области кибербезопасности. Это включает в себя как подготовку новых кадров, так и повышение квалификации уже работающих специалистов. Кроме того, требуется разработка и внедрение современных технологий защиты информации, что также требует значительных финансовых вложений.

Анализ динамики киберпреступности показывает, что угроза будет сохраняться и в дальнейшем, а рост числа преступлений продолжится. Эксперты прогнозируют, что в 2024 году количество киберпреступлений в мире может увеличиться на 15-20%, что обусловлено развитием технологий, которые становятся доступными не только законопослушным гражданам, но и преступникам. Ситуация требует совершенствования законодательства, усиления международного сотрудничества и внедрения передовых технологий для предотвращения и расследования киберпреступлений.

Таким образом, статистический анализ демонстрирует, что киберпреступность является серьезной угрозой, и её распространение требует постоянного мониторинга, улучшения мер защиты и повышения цифровой грамотности среди населения.

Список источников

1. Калашников И.В., Калашникова Л.Н. Криминологическая характеристика и прогнозирование отдельных видов киберпреступлений, совершаемых в информационнотелекоммуникационном пространстве на территории Российской Федерации // Криминологический журнал. 2024. № 2.

2. Состояние преступности в России за январь-декабрь 2024 года: сборник. – М.: ГИАЦ МВД России, 2024.

3. Криминология: учебное пособие / Г.А. Аванесов, Е.А. Антонян, С.В. Иванцов [и др.]. – 8-е изд., перераб. и доп. – М.: Юнити-Дана, 2023.

4. Калашников И.В. Личность преступника, совершающего преступления в сфере экономики с использованием информационно-телекоммуникационных технологий // Актуальные вопросы предупреждения преступлений в сфере информационно-телекоммуникационных технологий: криминологический и виктимологический аспекты: сб. науч. тр. Всероссийской науч.-практ. конф.: – М.: МосУ МВД России им. В.Я. Кикотя, 2022.

Информация об авторе:

И.В. Калашников, *заместитель начальника кафедры криминологии*

About the author:

I.V. Kalashnikov, *Deputy Head of the Department of Criminology*

Статья поступила в редакцию 17.03.2025