**УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES**

**DOI: https://doi.org/10.60797/LAW.2025.6.2**

# ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТИ «ИНТЕРНЕТ» НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ ОБЩЕСТВА

Научная статья

**Сардак Д.Б.[1, *]**

[1] Волгодонский филиал Ростовского юридического института МВД России, Волгодонск, Российская Федерация

* Корреспондирующий автор (sdb07[at]mail.ru)

**Аннотация**

В статье рассматриваются актуальные проблемы противодействия преступлениям, совершаемым с использованием информационных технологий и сети «Интернет», на современном этапе развития общества. Анализируются основные факторы, способствующие росту киберпреступности, включая недостаточное законодательное регулирование, технические сложности расследования, низкий уровень цифровой грамотности населения и отставание правоохранительных органов. Особое внимание уделяется вопросам международного сотрудничества, совершенствования нормативно-правовой базы и технического оснащения силовых структур. В завершении статьи предложены комплексные меры по повышению эффективности борьбы с киберпреступностью, включая совершенствование законодательства, развитие международного взаимодействия, модернизацию правоохранительных органов и повышение цифровой грамотности граждан.

**Ключевые слова:** киберпреступность, информационные технологии, цифровая безопасность, законодательное регулирование, правоохранительные органы, фишинг, вредоносное ПО, даркнет, международное сотрудничество, цифровая грамотность.

# PROBLEMS OF COUNTERING CRIMES COMMITTED THROUGH THE USE OF INFORMATION TECHNOLOGY AND THE INTERNET AT THE CURRENT STAGE OF SOCIAL DEVELOPMENT

Research article

**Sardak D.B.[1, *]**

[1] Volgodonsk branch of the Rostov Law Institute of the Ministry of Internal Affairs of Russia, Volgodonsk, Russian Federation

* Corresponding author (sdb07[at]mail.ru)

**Abstract**

The article examines the current problems of countering crimes committed with the use of information technology and the Internet at the current stage of development of society. It analyses the main factors contributing to the growth of cybercrime, including insufficient legislative regulation, technical difficulties of investigation, low level of digital literacy of the population and falling behind law enforcement agencies. Special attention is paid to international co-operation, improvement of the legal framework and technical equipment of law enforcement agencies. The paper concludes by proposing comprehensive measures to improve the effectiveness of the fight against cybercrime, including improving legislation, developing international cooperation, modernising law enforcement agencies and increasing the digital literacy of citizens.

**Keywords:** cybercrime, information technology, digital security, legislative regulation, law enforcement, phishing, malware, darknet, international co-operation, digital literacy.

## Введение

Современное общество характеризуется повсеместной цифровизацией, что влечёт за собой не только технологические преимущества, но и новые угрозы в сфере преступности. Информационные технологии стали неотъемлемой частью жизни граждан, бизнеса и государственных структур, однако их использование также открывает возможности для киберпреступников. С каждым годом фиксируется рост числа преступлений, совершаемых в цифровой среде, включая мошенничество, кражу персональных данных, взлом корпоративных сетей и распространение вредоносного программного обеспечения.

Одной из ключевых проблем противодействия таким преступлениям является их трансграничный характер, усложняющий юрисдикционные вопросы и координацию между правоохранительными органами разных стран. Кроме того, преступники используют современные технологии для сокрытия своей личности, что затрудняет их выявление и привлечение к ответственности. Важную роль в распространении киберпреступности играет также низкий уровень цифровой грамотности населения, что делает пользователей уязвимыми перед различными видами атак.

В данной статье рассматриваются актуальные проблемы противодействия преступлениям, совершаемым с использованием информационных технологий, анализируются методы борьбы с ними и предлагаются возможные пути решения с учётом правовых, технических и организационных аспектов.

## Методы и принципы исследования

При написании статьи использованы следующие методы исследования: анализ нормативно-правовых актов, регулирующих сферу информационной безопасности; сравнительный анализ международного опыта борьбы с

киберпреступностью; экспертное интервьюирование специалистов в области цифровой безопасности; статистический анализ данных о преступлениях в сфере информационных технологий.

Принципы исследования: системный подход, позволяющий рассматривать проблему в комплексе; научная объективность, обеспечивающая достоверность выводов; междисциплинарность, объединяющая правовые, технические и социальные аспекты.

**Основные результаты**

В последние годы в России наблюдается значительный рост числа киберпреступлений. Согласно данным МВД РФ, в 2024 году зарегистрировано 765,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что составляет около 40% от общего числа зарегистрированных преступлений [1]. Это на 13,1% больше по сравнению с 2023 годом. В 2023 году количество киберпреступлений достигло 677 тысяч случаев, что на 29,7% превышает показатели предыдущего года [2]. За этот период киберпреступники похитили около 156 миллиардов рублей, при этом в суд было направлено более 161 тысячи дел, и к уголовной ответственности привлечено 105 тысяч человек [3].

Особое внимание привлекает рост числа фишинговых атак. В 2023 году в России и странах СНГ было обнаружено более 29 тысяч фишинговых доменов, тогда как годом ранее их количество составляло около 20 тысяч [4]. Это свидетельствует о повышенной активности киберпреступников в сфере онлайн-мошенничества. Аналитический отчет компании F.A.C.C.T. за 2023–2024 годы также подтверждает тенденцию увеличения киберпреступной активности в России и странах СНГ [5]. В отчете подчеркивается необходимость усиления мер по противодействию киберугрозам, включая развитие технологий кибербезопасности и повышение осведомленности пользователей о современных методах защиты информации.

На взгляд автора, в нашей стране правовое регулирование киберпреступности сталкивается с рядом проблем, связанных с отсутствием четкой классификации и определения таких преступлений в законодательстве. Это приводит к неоднородности судебной практики и затрудняет привлечение виновных к ответственности. Как пример из судебной практики можно привести дело о несанкционированном доступе к информационной системе: В данном случае речь идет о деле, рассмотренном Верховным Судом Российской Федерации, в котором обвиняемый К. был признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, что повлекло за собой модификацию этой информации. Одно из преступлений было совершено из корыстной заинтересованности. Суд столкнулся с трудностями в квалификации преступления и вынесении приговора из-за отсутствия конкретных норм, определяющих ответственность за подобные действия [6].

Вторым примером можно привести дело о распространении вредоносного программного обеспечения: В данном случае речь идет о деле Андрея Коваленко, рассмотренном в Краснодарском крае. В августе 2023 года Темрюкский районный суд признал Коваленко виновным в распространении вредоносного программного обеспечения (ч. 2 ст. 273 УК РФ), неправомерном обороте средств платежей (ч. 1 ст. 187 УК РФ) и финансировании экстремистской организации (ч. 1 ст. 282.3 УК РФ). Однако приговор был обжалован, и в декабре 2023 года Краснодарский краевой суд отправил дело на пересмотр из-за ошибок в постановлении суда первой инстанции [7]. Этот случай иллюстрирует сложности, возникающие при квалификации преступлений, связанных с распространением вредоносного ПО, и необходимость точного соблюдения процессуальных норм для вынесения обоснованных приговоров.

К рассматриваемой в исследовании проблеме в последнее время проявляет интерес все больше и больше отечественных ученых и авторов. П.Н. Кобец в работе «Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт» отмечает, что ежегодный рост киберпреступлений угрожает безопасности страны, однако уголовно-правовые составы преступлений в этой сфере остаются недостаточно разработанными, что затрудняет их пресечение [8] А.А. Карцхия в статье «Правовые аспекты современной киберпреступности» подчеркивает, что отсутствие четкого законодательного определения киберпреступлений и их классификации приводит к проблемам в правоприменительной практике и необходимости совершенствования нормативно-правовой базы [9].

Одной из проблем борьбы с киберпреступлениями с которой сталкиваются правоохранительные органы выступает техническая сложность расследования и использование преступниками технологий анонимизации, таких как VPN и даркнет. В частности, в ходе расследования дела о распространении вредоносного ПО было установлено, что злоумышленники использовали сети Tor для скрытия своей деятельности, что затруднило их идентификацию. Например, в 2017 году математик Дмитрий Богатов был арестован по подозрению в призывах к массовым беспорядкам, которые были опубликованы с использованием сети Tor. Следствию удалось выяснить, что Богатов использовал браузер Tor, что затруднило установление, была ли публикация осуществлена непосредственно с его компьютера. В мае 2018 года уголовное дело против него было прекращено из-за недостаточности доказательств [10]. Этот пример демонстрирует, как использование технологий анонимизации, таких как Tor, усложняет идентификацию злоумышленников и сбор доказательств, что является серьёзной проблемой для правоохранительных органов при расследовании киберпреступлений. Дополнительно преступники всё чаще применяют шифрование данных и системы удалённого управления вредоносными программами, что усложняет их обнаружение.

Низкий уровень цифровой грамотности населения так же очень сильно влияет на рассматриваемую нами проблему. Исследования Лаборатории Касперского показали, что 45% пользователей не распознают фишинговые и используют слабые пароли для защиты своих данных. Это делает их лёгкими жертвами злоумышленников. В июне 2024 года «Лаборатория Касперского» проанализировала 193 миллиона паролей, обнаруженных в публичном доступе на даркнет-ресурсах, и выяснила, что почти половину из них (45%) мошенники могут подобрать менее чем за минуту [11]. В совместном исследовании «Лаборатории Касперского» и Почты Mail, опубликованном в октябре 2024 года, выяснилось, что почти каждый четвертый опрошенный (24%) не уверен в надежности созданных им паролей для важных сервисов, таких как мессенджеры и социальные сети [12]. Эти данные подчеркивают необходимость

повышения цифровой грамотности населения, особенно в вопросах создания и использования надежных паролей, а также распознавания фишинговых атак. Рекомендую обновить соответствующий раздел статьи, чтобы отразить эти актуальные статистические данные.

Кроме того техническое оснащение правоохранительных органов в области кибербезопасности отстаёт от современных угроз. В связи с этим необходима модернизация специализированных подразделений и привлечение к расследованию специалистов в области IT и информационной безопасности.

**Обсуждение**

В ходе обсуждения выявленных проблем становится очевидным, что борьба с киберпреступностью требует комплексного подхода. Важно не только совершенствовать законодательство и усиливать правоохранительные органы, но и развивать международное сотрудничество, внедрять инновационные технологии и повышать осведомлённость граждан. Основные направления решения проблемы должны включать в себя: создание единой международной платформы для обмена данными о киберугрозах; развитие образовательных программ по цифровой грамотности для широких слоёв населения; расширение полномочий правоохранительных органов в сфере расследования киберпреступлений; совершенствование механизмов защиты персональных данных на государственном и корпоративном уровнях.

Только комплексный подход, включающий все указанные меры, позволит снизить уровень киберпреступности и обеспечить цифровую безопасность в современном обществе.

**Заключение**

Таким образом, подводя итоги нашего исследования мы видим, что киберпреступность является одной из основных угроз современному обществу, и для эффективной борьбы с ней необходимо внедрять комплексный подход. В первую очередь стоит сосредоточиться на реформировании законодательства, а именно внести новые статьи в Уголовный кодекс РФ, которые позволят более точно квалифицировать преступления, связанные с цифровыми угрозами. Но для этого важно разработать чёткие формулировки таких преступлений, как фишинг, создание вирусов, кража личных данных в интернете и других, чтобы правоохранительные органы могли оперативно реагировать на такие преступления. Как пример можно привести ст. 272.1 «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения», которая введена в УК РФ Федеральным законом от 30.11.2024 № 421-ФЗ. Ответственность по данной статье предусмотрена за незаконное использование или передачу (распространение, предоставление, доступ), сбор или хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем; а также за те же деяния, совершенные в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных или биометрические персональные данные.

Следующим выводом нашего исследования является тот факт, что эффективная борьба с киберпреступностью невозможна без активного международного сотрудничества, поэтому на наш взгляд наряду с внесением изменений в УК, важно усилить взаимодействие с правоохранительными органами других стран и международными организациями, такими как Интерпол и Европол. Создание глобальной базы данных с информацией о киберугрозах и преступниках позволит быстро реагировать на инциденты и обеспечивать координацию действий между странами. Поэтому здесь же необходимо усилить техническое оснащение правоохранительных органов, предоставив им инструменты для мониторинга интернет-пространства, включая даркнет, а также для анализа больших данных с использованием искусственного интеллекта.

Не менее важным представляется повышение цифровой грамотности населения, введение образовательных программ, начиная с ранних этапов обучения, поскольку это поможет гражданам лучше защищать себя в интернете. Обучение основам кибербезопасности должно стать неотъемлемой частью школьного образования, а также проводится активное информирование граждан о новых угрозах и способах защиты. Для бизнеса необходимо внедрять меры, стимулирующие внедрение передовых технологий защиты данных. Важно создать систему сертификаций безопасности и предложить налоговые льготы компаниям, которые обеспечивают высокие стандарты защиты информации.

Таким образом, только совместные усилия государства, международных организаций, бизнеса и граждан смогут значительно снизить уровень киберпреступности. Для этого требуется не только совершенствование законодательства, но и внедрение инновационных технологий, усиление сотрудничества на международной арене и повышение осведомлённости населения о рисках в цифровой среде.

**Конфликт интересов**

Не указан.

**Рецензия**

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

**Conflict of Interest**

None declared.

**Review**

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

## Список литературы / References

1. В России в 2024 году IT-преступления достигли пика за последние пять лет // ТАСС. — URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 10.02.2025).

2. Число киберпреступлений в России выросло на 30% в 2023 году // Телеспутник. — URL: https://telesputnik.ru/materials/gov/news/chislo-kiberprestupleniy-v-rossii-vyroslo-na-30-v-2023-godu (дата обращения: 19.02.2025).

3. В России резко выросло число киберпреступлений // The Moscow Times. — URL: https://www.moscowtimes.ru/2024/05/29/vrossii-rezko-viroslo-chislo-kiberprestuplenii-a132273 (дата обращения: 12.02.2025).

4. Киберпреступность в России и СНГ 2023–2024 // ICT.Moscow. — URL: https://ict.moscow/research/kiberprestupnost-v-rossii-i-sng-2023-2024/ (дата обращения: 19.02.2025).

5. Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023–2024 // FACCT. — URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (дата обращения: 19.02.2025).

6. Верховный Суд рассмотрел дело о неправомерном получении доступа к компьютерной информации игровой консоли // Legal Bulletin Online. — URL: https://legalbulletin.online/verhovnyj-sud-rassmotrel-delo-o-nepravomernom-poluchenii-dostupa-k-kompjuternoj-informacii-igrovoj-konsoli/ (дата обращения: 19.02.2025).

7. Суд из-за ошибок в приговоре отправил на пересмотр дело краснодарского хакера о рассылке вредоносного ПО и донатах ФБК // Zona.Media. — URL: https://zona.media/news/2023/12/11/kovalenko (дата обращения: 19.02.2025).

8. Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // Научный вестник Омской академии МВД России. — 2022. — № 2(85). — URL: https://cyberleninka.ru/article/n/pravovye-osnovy-preduprezhdeniya-kiberprestupleniy-otechestvennyy-i-zarubezhnyy-opyt (дата обращения: 17.02.2025).

9. Карцхия А.А. Правовые аспекты современной киберпреступности / А.А. Карцхия // Правовая информатика. — 2023. — № 1. — URL: https://cyberleninka.ru/article/n/pravovye-aspekty-sovremennoy-kiberprestupnosti (дата обращения: 17.02.2025).

10. В России за использование анонимного браузера Tor действительно могут наказать // IB-Bank. — URL: https://ib-bank.ru/bisjournal/news/9367 (дата обращения: 19.02.2025).

11. Лаборатория Касперского проверила 193 миллиона паролей на устойчивость к взлому: результат неутешительный // Лаборатория Касперского. — URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-proverila-193-milliona-parolej-na-ustojchivost-k-vzlomu-rezultat-neuteshitelnyj (дата обращения: 19.02.2025).

12. Четверть россиян не уверены в безопасности созданных ими паролей // Лаборатория Касперского. — URL: https://www.kaspersky.ru/about/press-releases/chetvert-rossiyan-ne-uvereny-v-bezopasnosti-sozdannyh-imi-parolej (дата обращения: 19.02.2025).

## Список литературы на английском языке / References in English

1. V Rossii v 2024 godu IT-prestupleniya dostigli pika za poslednie pyat' let [In Russia, IT crimes reached a five-year peak in 2024] // TASS. — URL: https://tass.ru/proisshestviya/22978955 (accessed: 10.02.2025). [in Russian]

2. Chislo kiberprestupleniy v Rossii vyroslo na 30% v 2023 godu [Cybercrimes in Russia increased by 30% in 2023] // Telesputnik. — URL: https://telesputnik.ru/materials/gov/news/chislo-kiberprestupleniy-v-rossii-vyroslo-na-30-v-2023-godu (accessed: 19.02.2025). [in Russian]

3. V Rossii rezko vyroslo chislo kiberprestupleniy [Cybercrimes increased sharply in Russia] // The Moscow Times. — URL: https://www.moscowtimes.ru/2024/05/29/vrossii-rezko-viroslo-chislo-kiberprestuplenii-a132273 (accessed: 12.02.2025). [in Russian]

4. Kiberprestupnost' v Rossii i SNG 2023-2024 [Cybercrime in Russia and CIS 2023-2024] // ICT.Moscow. — URL: https://ict.moscow/research/kiberprestupnost-v-rossii-i-sng-2023-2024/ (accessed: 19.02.2025). [in Russian]

5. Kiberprestupnost' v Rossii i SNG. Trendy, analitika, prognozy 2023-2024 [Cybercrime in Russia and CIS. Trends, analytics, forecasts 2023-2024] // FACCT. — URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (accessed: 19.02.2025). [in Russian]

6. Verkhovnyy Sud rassmotrel delo o nepravomernom poluchenii dostupa k komp'yuternoy informatsii igrovoy konsoli [The Supreme Court considered a case of unauthorized access to gaming console computer information] // Legal Bulletin Online. — URL: https://legalbulletin.online/verhovnyj-sud-rassmotrel-delo-o-nepravomernom-poluchenii-dostupa-k-kompjuternoj-informacii-igrovoj-konsoli/ (accessed: 19.02.2025). [in Russian]

7. Sud iz-za oshibok v prigovore otpravil na peresmotr delo krasnodarskogo khakera o rassylke vredonostnogo PO i donatakh FBK [Court sent case of Krasnodar hacker about malware distribution and FBK donations for reconsideration due to sentencing errors] // Zona.Media. — URL: https://zona.media/news/2023/12/11/kovalenko (accessed: 19.02.2025). [in Russian]

8. Kobets P.N. Pravovye osnovy preduprezhdeniya kiberprestupleniy: otechestvennyy i zarubezhnyy opyt [Legal foundations of cybercrime prevention: domestic and foreign experience] / P.N. Kobets // Nauchnyy vestnik Omskoy akademii MVD Rossii [Scientific Bulletin of Omsk Academy of Russian Ministry of Internal Affairs]. — 2022. — № 2(85). — URL: https://cyberleninka.ru/article/n/pravovye-osnovy-preduprezhdeniya-kiberprestupleniy-otechestvennyy-i-zarubezhnyy-opyt (accessed: 17.02.2025). [in Russian]

9. Kartskhiya A.A. Pravovye aspekty sovremennoy kiberprestupnosti [Legal aspects of modern cybercrime] / A.A. Kartskhiya // Pravovaya informatika [Legal Informatics]. — 2023. — № 1. — URL: https://cyberleninka.ru/article/n/pravovye-aspekty-sovremennoy-kiberprestupnosti (accessed: 17.02.2025). [in Russian]

10. V Rossii za ispol'zovanie anonimnogo brauzera Tor deystvitel'no mogut nakazat' [In Russia, using Tor anonymous browser can indeed be punished] // IB-Bank. — URL: https://ib-bank.ru/bisjournal/news/9367 (accessed: 19.02.2025). [in Russian]

11. Laboratoriya Kasperskogo proverila 193 milliona paroley na ustoychivost' k vzlomu: rezul'tat neuteshitel'nyy [Kaspersky Lab tested 193 million passwords for crack resistance: disappointing results] // Laboratoriya Kasperskogo [Kaspersky Lab]. — URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-proverila-193-milliona-parolej-na-ustojchivost-k-vzlomu-rezultat-neuteshitelnyj (accessed: 19.02.2025). [in Russian]

12. Chetvert' rossiyan ne uvereny v bezopasnosti sozdannykh imi paroley [A quarter of Russians are unsure about the security of their created passwords] // Laboratoriya Kasperskogo [Kaspersky Lab]. — URL: https://www.kaspersky.ru/about/press-releases/chetvert-rossiyan-ne-uvereny-v-bezopasnosti-sozdannyh-imi-parolej (accessed: 19.02.2025). [in Russian]