

УДК 343.1**Развитие деятельности правоохранительных органов РФ при
расследовании киберпреступлений****Ивахненко Вячеслав Юрьевич**

Выпускник,

Московский университет им. С.Ю. Витте,

115432, Российская Федерация, Москва, 2-й Кожуховский проезд, 12с1;

E-mail: ivahnenko.veaceslav@yandex.ru

Аннотация

Рост киберпреступности является одной из актуальных проблем современного общества, особенно в условиях стремительной информатизации, которая охватывает все сферы жизни, это явление связано не только с увеличением числа пользователей интернет-технологий и цифровых сервисов, но и с развитием технологий, посредством которых возможно осуществлять преступные действия. В статье рассматриваются актуальные проблемы киберпреступности в современных условиях, акцентируя внимание на увеличении угроз, связанных с развитием цифровых технологий и интернет-сервисов. Кроме того, анализируется разнообразие форм киберпреступлений, включая кражу личных данных, мошенничество. Особое внимание уделяется роли прокуратуры в борьбе с данными преступлениями, а также значимости координации между правоохранительными органами. Рассмотрены примеры расследований киберпреступлений и предложены рекомендации по повышению эффективности работы прокуратуры в данной сфере.

Для цитирования в научных исследованиях

Ивахненко В.Ю. Развитие деятельности правоохранительных органов РФ при расследовании киберпреступлений // Вопросы российского и международного права. 2025. Том 15. № 1А. С. 377-383.

Ключевые слова

Законодательство, защита информации, инновационные методы расследования, интернет, информационные технологии, правовые средства, правовое регулирование, правоприменительная практика, прокуратура, прокурорский надзор, риски киберпреступности, киберпреступность.

Введение

В условиях современных реалий, статистика преступлений с использованием информационно-телекоммуникационных технологий в России достигла рекордных значений. Так, в 2023 году из 1 947 161 зарегистрированных преступлений, 676 951 связаны с киберпреступностью, что составляет значительную долю в 29,7% от общего числа, эти данные говорят о том, что цифровая среда становится не только площадкой для развития технологий и коммуникации, но и пространством, где злоумышленники могут действовать с большой эффективностью и анонимностью [МВД РФ, 2023].

В 2024 году на долю интернет-преступлений из 765,4 тысяч зарегистрированных преступлений с января по декабрь 2024 года пришлось 649,1 тыс. случаев, что на 23% больше, чем в 2023 году, примечательно, что более 84% всех зарегистрированных преступлений были совершены через сети, что очевидно указывает на тенденцию использования интернета как основного инструмента для осуществления незаконной деятельности. Глава МВД России отметил, что в числе пострадавших от киберпреступлений оказываются не только физические, но и юридические лица, включая государственные структуры, причиняемый киберпреступлением ущерб серьезно затрагивает экономику страны и имущественные права граждан [ТАСС, 2024].

Основная часть

В целях обеспечения национальных интересов, в том числе, безопасности граждан и государства, Указом Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» определено «создание и развитие систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления, а также повышения эффективности государственного управления, на законодательном уровне» [Указ Президента РФ № 203, 2017].

В целях формирования единообразной правоприменительной практики, 26 апреля 2024 года в Московской академии Следственного комитета имени А.Я. Сухарева прошла II Международная научно-практическая конференция на тему «Проблемы противодействия киберпреступности», в которой участники обсудили актуальные вопросы борьбы с киберпреступлениями. В свете современных реалий, когда треть всех зарегистрированных преступлений в России связаны с использованием информационно-коммуникационных технологий, а 75% из них остаются нераскрытыми, данное мероприятие приобрело особую значимость.

На конференции были рассмотрены вопросы о необходимости совершенствования уголовного и уголовно-процессуального законодательства, направленного на защиту граждан от преступлений, связанных с использованием интернета и мобильной связи, основополагающим является адаптация законов к новым условиям, включая использование цифровых финансовых технологий.

Также была отмечена необходимость систематизации судебной практики и установления единых подходов к квалификации новых видов преступлений, таких как публичное распространение заведомо ложной информации об использовании Вооруженных Сил

Российской Федерации – ст.207.3 Уголовного кодекса Российской Федерации (далее – УК РФ) [УК РФ, 1996 (ред. 2024)].

Кроме того, особое внимание было уделено практическому опыту работы следователей, действующих в условиях специальной военной операции, была подчеркнута необходимость активизации работы по повышению квалификации сотрудников правоохранительных органов в области цифровой безопасности, что является важным шагом к эффективной борьбе с киберпреступностью.

Отметим, что Генеральный прокурор Российской Федерации в 2024 году также заявил о низкой раскрываемости IT-преступлений в России, что подчеркивает серьезные проблемы в системе борьбы с преступлениями, связанными с использованием технологий и интернет-пространства. Проблемы касаются не только недостаточной эффективности работы следственных органов, но и общей структуры взаимодействия между различными ведомствами, включая органы прокуратуры. На сегодняшний день раскрываемость IT-преступлений остается критически низкой, что ставит под сомнение способности правоохранительных органов в борьбе с киберпреступностью, уровень раскрываемости, который не превышает 27% в последние годы и составил 25,9% в 2024 году, указывает на то, что, несмотря на наличие специальных подразделений, систему борьбы с IT-преступлениями необходимо пересматривать [Петропавловск-Камчатский горсуд, 2024].

Также генпрокурором была определена проблема электронного взаимодействия между правоохранительными органами и организациями финансового рынка, сотовыми операторами, длительное получение оперативно-значимой информации затрудняет раскрытие преступлений, создавая дополнительные преграды в борьбе с киберугрозами, кроме того, слабая структура расследования способствует росту преступности и уменьшает доверие общества к правоохранительной системе.

Представляется, для улучшения ситуации необходимо не только повышение уровня раскрываемости IT-преступлений, но и реформа всей системы, которая включает в себя смену подходов к оперативной деятельности, увеличение кооперации между различными ведомствами, улучшение электронного документооборота и более эффективная работа специализированных подразделений, а также применение новых методов с использованием информационных технологий для успешного противодействия и пресечения преступной деятельности. Технологический прогресс требует от правоохранительных органов гибкости и адаптивности, которые на данный момент явно недостаточны, что создает пробелы в системе и способствует дальнейшему развитию киберпреступности.

Проблема низкой раскрываемости IT-преступлений в России заключается в нескольких ключевых аспектах. Во-первых, это не достаточное ведение в компетенциях и знаниях по информационным технологиям, отсутствие использования новых подходов в подразделениях уполномоченных на осуществление оперативно-разыскной деятельности, что затрудняет понимание механик и методов киберпреступлений, а также зачастую невозможность анализа преступной деятельности и оперативного реагирования на угрозы. Во-вторых, недостаточная подготовленность следственных органов и их сотрудников к расследованию сложных киберпреступлений. В-третьих, существует недостаток эффективного взаимодействия между различными ведомствами и организациями, что усложняет обмен критически важной информации, которая часто необходима для расследования преступлений или проведения оперативно-разыскных мероприятий, она поступает слишком поздно или вообще недоступна, что снижает шанс на раскрытие преступления или на качественную подготовку и дальнейшее

проведение оперативно-разыскных мероприятий.

К тому же, процесс расследования IT-преступлений, а также оперативное сопровождение таких преступлений зачастую не учитывает уникальные особенности цифровой среды. Последствия кибератак могут быть быстрыми и разрушительными, и в таких условиях важно применять нестандартные подходы, и адаптивные методики. А это требует не только специального обучения, но и внедрения новых технологий, позволяющих оперативно собирать и анализировать информацию.

Пути решения этих проблем могут включать несколько направлений. Во-первых, необходимо инвестировать в обучение и переподготовку сотрудников правоохранительных органов в области IT и кибербезопасности. Регулярные тренинги, курсы и семинары помогут повысить уровень знаний и навыков среди следственных работников и оперативных сотрудников. Важно также развивать сотрудничество с учебными заведениями и частным сектором, чтобы обеспечить доступ к современным методам и технологиям.

Во-вторых, требуются изменения в законодательной и организационной области, касающейся обмена информацией. Установление четких и быстрых каналов коммуникации между различными государственными структурами и частными компаниями, работающими в сфере IT, позволит оперативно реагировать на возникающие угрозы. Это также включает в себя создание единой базы данных по киберпреступлениям, которая была бы доступна для анализа и статистики.

Дополнительно, важно создавать межведомственные рабочие группы, которые будут заниматься анализом и разработкой новых методов борьбы с киберпреступностью, такие группы должны включать представителей правоохранительных органов, юридических структур и специалистов в области информационных технологий, что даст возможность взглянуть на проблемы с разных точек зрения и выработать комплексные решения.

Также стоит отметить, что, в связи с высоким уровнем анонимности криптовалюта среди преступников занимает весомую роль, поскольку большинство виновных противоправных деяний совершается непосредственно с использованием данной технологии. Нельзя не отметить, что до 2021 года криптовалюта не была закреплена на нормативно-правовом уровне, тогда как в 2021 году законодатель признал ее средством платежа, урегулировав особенности ее применения в связи с принятием закона Федерального закона №259-ФЗ «О цифровых финансовых активах и цифровой валюте» [Федеральный закон № 259-ФЗ, 2020 (ред. 2024)].

Технология блокчейн, на которой основаны криптовалюты создает определенные сложности для правоохранительных органов, поскольку обеспечивает децентрализованный и анонимный характер транзакций, что затрудняет идентификацию пользователей, совершающих операции с цифровыми активами, что также вызывает проблемы при расследований преступлений, вместе с тем, судебная практика показывает, что раскрываемость таких преступлений имеет место быть (приговор от 18 июля 2024 г. по делу № 1-535/2024). Представляется, целесообразно проводить анализ блокчейна, что позволяет отслеживать транзакции и выявлять паттерны, которые могут указать на владельцев адресов, а также анализ сетевого трафика для определения IP-адреса, что также способствует связке транзакций с конкретными устройствами.

В целях эффективности раскрытия преступлений в сфере незаконного оборота наркотиков, учитывая латентный характер деяний, совершенных, в том числе, посредством использования сети-Интернет, автор настоящего исследования в качестве новеллы предлагает ввести в рамках уголовно-процессуального законодательства проведение экспертизы с использованием методов

интернет-разведки (разведки по открытым источникам) для унификации лица осуществляющего противоправные действия. Обоснованием нововведения выступает пример, когда В. Сакраменто (штат Калифорния, США) к тюремному сроку приговорили наркодилера, которого поймали благодаря фотографии его ладони с размещенной на ней наркотическими веществами. Суть примера, совместная операция Управления по борьбе с наркотиками США, Почтовой службы США, Налогового управления, Службы маршалов и обычных полицейских под названием «Тёмное золото». «Суть «Тёмного золота»: агенты под прикрытием изображали в даркнете специалистов по отмыванию денег, предлагая обменять биткойны продавцов на реальные деньги. Эту систему придумали в 2016 после ареста человека, который предоставлял аналогичные услуги наркодилерам. Операция привела к аресту более 40 человек, конфискации наркотиков и 30 миллионов долларов в криптовалюте. Также федеральные агенты обнаружили 3,6 миллиона долларов в наличных и золотых слитках» [TJ, 2024]. В марте 2018 года сотрудник главного следственного подразделения Департамента внутренней безопасности США Арон Манн (Aron Mann) рассматривал данные по деятельности продавца наркотиков в даркнете на площадке «Dream Market» под ником «Canna_Bars», к этому моменту площадка была закрыта властями Нидерландов, однако Манну были доступны сведения с данной площадки, «среди прочей информации спецагент обнаружил ссылку на фотохостинг Imgur: там оказался целый альбом с фотографиями марихуаны в высоком качестве. В альбоме — восемь вроде бы обычных фото. Но на одном из них Canna_Bars держал наркотики в руке — и на снимке отчётливо видны отпечатки пальцев» [TJ, 2024]. Что и позволило в дальнейшем при расследовании, определить личность «Canna_Bars» как Хосе Роберт Поррас III (Jose Robert Porras III).

Заключение

Таким образом, полагаем, введение аналогичного института расследования преступлений, позволит сократить незаконный сбыт наркотических средств и психотропных веществ на территории Российской Федерации и повысить раскрываемость преступлений. Кроме того, для повышения эффективности борьбы с IT-преступлениями необходим комплексный подход: улучшение квалификации сотрудников правоохранительных органов, налаживание межведомственного взаимодействия, внедрение современных технологий и создание единой информационной базы, что в итоге поможет снизить уровень киберпреступности в стране и повысить уровень раскрываемости таких преступлений.

Библиография

1. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 25.10.2024) // Российская газета, № 173, 06.08.2020.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 08.01.2025) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.
3. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: указ Президента РФ от 09.05.2017 № 203 // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 10.05.2017.
4. В России в 2024 году IT-преступления достигли пика за последние пять лет // URL: <https://tass.ru/proisshestviya/22978955> (дата обращения: 12.02.2025).
5. В Генпрокуратуре заявили о низкой раскрываемости киберпреступлений в России // URL: <https://ria.ru/20241010/kiberprestuplenie-1977431676.html> (дата обращения: 12.02.2025).
6. Петропавловск-Камчатский городской суд (Камчатский край): приговор № 1-535/2024 от 18 июля 2024 г. по делу № 1-535/2024 // URL: <https://sudact.ru> (дата обращения: 12.02.2025).

7. Ошибка Canna_Bars: история о продавце наркотиков из даркнета, которого вычислили по отпечаткам пальцев с фото <https://tjournal.ru/internet/215105-oshibka-canna-bars-istoriya-o-prodavce-narkotikov-iz-darkneta-kotorogo-vychislili-po-otpechatkam-palcev-s-foto> (дата обращения: 05.02.2025).
8. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2023 года. URL: <https://мвд.рф/reports/item/47055751/> (дата обращения 24.02.2025).

Enhancing the Activities of Russian Law Enforcement Agencies in Investigating Cybercrimes

Vyacheslav Yu. Ivakhnenko

Graduate,
Moscow Witte University,
115432, 12, building 1, 2nd Kozhukhovskiy Proezd, Moscow, Russian Federation;
e-mail: ivakhnenko.vyacheslav@yandex.ru

Abstract

The rise of cybercrime is one of the most pressing challenges facing modern society, particularly in the context of rapid digitalization affecting all spheres of life. This phenomenon is driven not only by the growing number of internet users and digital services but also by advancements in technology that facilitate criminal activities. The article examines current issues in cybercrime, highlighting the increasing threats associated with the development of digital technologies and online services. Additionally, it analyzes various forms of cybercrime, including identity theft and fraud. Special attention is given to the role of the Prosecutor's Office in combating these crimes and the importance of interagency coordination among law enforcement bodies. The study reviews case examples of cybercrime investigations and provides recommendations for improving the efficiency of prosecutorial efforts in this field.

For citation

Ivakhnenko V.Yu. (2025) *Razvitie deyatel'nosti pravookhranitel'nykh organov RF pri rassledovanii kiberprestupleniy* [Enhancing the Activities of Russian Law Enforcement Agencies in Investigating Cybercrimes]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (1A), pp. 377-383.

Keywords

Legislation, information security, innovative investigation methods, internet, information technology, legal measures, legal regulation, law enforcement practice, Prosecutor's Office, prosecutorial supervision, cybercrime risks, cybercrime.

References

1. On Digital Financial Assets, Digital Currency and Amendments to Certain Legislative Acts of the Russian Federation: Federal Law No. 259-FZ dated 07/31/2020 (as amended on 10/25/2024) // *Rossiyskaya Gazeta*, No. 173, 08/06/2020.
2. Criminal Code of the Russian Federation No. 63-FZ dated 06/06/1996 (as amended on 12/28/2024) (with amendments and additions, intro. effective from 08.01.2025) // Collection of legislation of the Russian Federation, 17.06.1996, No. 25, art. 2954.
3. On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030: Decree of the

-
- President of the Russian Federation dated 05/09/2017 No. 203 // Official Internet Portal of Legal Information <http://www.pravo.gov.ru> , 05/10/2017.
4. In Russia in 2024, IT crimes reached a peak over the past five years // URL: <https://tass.ru/proisshestiya/22978955> (date of request: 12.02.2025).
 5. The Prosecutor General's Office announced the low detection rate of cybercrimes in Russia // URL: <https://ria.ru/20241010/kiberprestuplenie-1977431676.html> (date of request: 12.02.2025).
 6. Petropavlovsk-Kamchatsky City Court (Kamchatka Territory): Verdict No. 1-535/2024 of July 18, 2024 in case No. 1-535/2024 // URL: <https://sudact.ru> (date of access: 02/12/2025).
 7. Canna_Bars error: a story about a drug dealer from the darknet who was identified by fingerprints from a photo <https://tjournal.ru/internet/215105-oshibka-canna-bars-istoriya-o-prodavce-narkotikov-iz-darkneta-kotorogo-vychislili-po-otpechatkam-palcev-s-foto> (date of request: 02/05/2025).
 8. Brief description of the state of crime in the Russian Federation in January - December 2023. URL: <https://мвд.рф/reports/item/47055751> / (accessed 24.02.2025).