НАУЧНАЯ СТАТЬЯ
УДК 343.9

Криминалистические аспекты борьбы с основными видами киберпреступлений

Станислав Юрьевич БУЛОЧНИКОВ ✉, Сергей Александрович ПОТАПОВ
ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина»
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33
✉ bulochnikov03@mail.ru

Аннотация. Киберпреступность представляет собой доминирующую угрозу, характеризующуюся ростом, усложнением методов и диверсификацией. Целью исследования является анализ криминалистических аспектов противодействия ей. На основе анализа статистики МВД РФ и научных публикаций установлено, что эффективное расследование требует развития цифровой криминалистики. Ключевыми элементами являются работа с цифровыми следами, использование специализированного ПО, искусственного интеллекта, блокчейна, а также специализированная подготовка кадров. Разработана таблица, систематизирующая методы расследования для таких видов преступлений, как финансовое мошенничество и кибервымогательство. Результаты подтверждают, что успешное противодействие возможно лишь при интеграции традиционных криминалистических подходов с современными цифровыми технологиями и компетенциями.

Ключевые слова: киберпреступность, цифровая криминалистика, расследование, цифровые следы, искусственный интеллект

Для цитирования: *Булочников С.Ю., Потапов С.А.* Криминалистические аспекты борьбы с основными видами киберпреступлений // Державинский форум. 2025. Т. 9. № 4. С. 430-436.

ORIGINAL ARTICLE
UDC 343.9

Criminalistic aspects of combating the main types of cybercrime

Stanislav Yu. BULOCHNIKOV ✉, Sergey A. POTAPOV
Derzhavin Tambov State University
33 Internatsionalnaya St., Tambov, 392000, Russian Federation
✉ bulochnikov03@mail.ru

Abstract. Cybercrime is a dominant threat characterized by growth, increasing sophistication, and diversification. The purpose of the study is to analyze the criminalistic aspects of countering it. Based on the analysis of statistics of the Ministry of Internal Affairs of the Russian Federation and scientific publications, it has been established that effective investigation requires the development of digital forensics. The key elements are working with digital footprints, using specialized software, artificial intelligence, blockchain, as well as specialized training. A table has been developed that systematizes investigative methods for such types of crimes as financial fraud and cyber extortion. The results con-

firm that successful counteraction is possible only with the integration of traditional forensic approaches with modern digital technologies and competencies.
Keywords: cybercrime, digital forensics, investigation, digital footprints, artificial intelligence

For citation: Bulochnikov, S.Yu., & Potapov, S.A. (2025). Criminalistic aspects of combating the main types of cybercrime. *Derzhavinskii forum = Derzhavin Forum*, vol. 9, no. 4, pp. 430-436.

ВВЕДЕНИЕ

Современное общество существует в двух взаимосвязанных реальностях: физической и цифровой. И если в первой правоохранительная система за столетия выработала отработанные механизмы реагирования, то во второй она зачастую действует с запаздыванием. Киберпреступность, используя анонимность, скорость и безграничность глобальной сети, демонстрирует угрожающие темпы роста. Фишинг, кражи криптовалют, атаки, взломы корпоративных систем – это уже не сюжеты фантастических фильмов, а повседневные угрозы. Ключевой проблемой в борьбе с ними является не столько отсутствие законодательной базы, сколько сложность применения классических криминалистических методик к цифровым следам. Таким образом, ядром любого успешного расследования киберпреступления становится цифровая криминалистика. Необходимо рассмотреть ключевые криминалистические аспекты и инструменты, позволяющие дешифровать цифровые улики, реконструировать механизм преступления и обеспечить неотвратимость наказания для злоумышленников, действующих в киберпространстве.

На основании обнародованных МВД РФ в конце января 2025 года данных можно констатировать, что киберпреступность в России не только сохраняет свои масштабы, но и демонстрирует устойчивый и опасный рост, становясь структурным элементом всей преступной среды. Ключевым индикатором является тот факт, что в 2024 г. было зафиксировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что составляет примерно 40 % от общего числа всех противоправных деяний в стране. Это означает, что практически каждое второе преступление теперь имеет цифровую составляющую. В динамике наблюдается значительное увеличение: общее количество киберпреступлений выросло на 13,1 % по сравнению с предыдущим годом. Особую тревогу вызывает качественная трансформация киберпреступности в сторону большей тяжести. Так, в ИТ-сфере было совершено 369,3 тыс. тяжких и особо тяжких преступлений, что на 7,8 % больше чем годом ранее и именно этот фактор в значительной степени повлиял на общий рост числа тяжких и особо тяжких преступлений в России на 4,8 % за 2024 год[1].

Детальная структура киберпреступности раскрывает ее основные векторы. Абсолютным лидером является мошенничество: за год выявлено 380,3 тыс. случаев по статьям 159, 159.3, 159.6 УК РФ. Почти сопоставимы по масштабам кражи (статья 158 УК РФ) – 105,9 тыс. случаев, и преступления в сфере компьютерной информации (глава 28 УК РФ) – 105,8 тыс. случаев. Значительный сегмент занимает незаконный оборот наркотиков, осуществляемый с использованием IT-технологий (статья 228.1 УК РФ) – около 94,6 тыс. деяний. Также в цифровом пространстве фиксируются такие опасные преступления, как изготовление порнографических материалов (более

[1] Tadviser. МВД составило рейтинг регионов РФ с самым высоким уровнем ИТ-преступности. URL: https://vk.cc/cRJPGZ (дата обращения: 27.08.2025).

3,5 тыс. фактов по статье 242 УК РФ), публичные призывы к терроризму (898 случаев по статье 205.2 УК РФ) и экстремизму (447 случаев по статье 280 УК РФ), а также незаконная организация азартных игр (368 случаев по статье 171.2 УК РФ).

Во-первых, киберпреступность превратилась из периферийной в доминирующую угрозу, определяющую общий криминогенный фон в стране. Во-вторых, наблюдается четкая тенденция не только к количественному росту, но и к качественному усугублению: преступления в IT-сфере становятся более тяжкими, что прямо влияет на общий уровень общественной безопасности. В-третьих, структура киберпреступности демонстрирует ее диверсификацию: от массовых имущественных преступлений (мошенничество, кражи) до крайне опасных деяний, угрожающих основам государственной безопасности и общественной нравственности (терроризм, экстремизм, распространение наркотиков и запрещенного контента). Это свидетельствует о том, что цифровая среда стала универсальным инструментом и платформой для совершения практически всех видов преступлений, что требует адекватного и комплексного противодействия со стороны правоохранительных органов, включая развитие специальных подразделений, совершенствование законодательной базы и внедрение передовых технологий для прогнозирования, предотвращения и раскрытия таких преступлений.

Транснациональный характер, высокая латентность и постоянная эволюция методов атак создают беспрецедентные вызовы для правоохранительных органов. В этих условиях традиционные подходы к расследованию зачастую оказываются малоэффективными, что обуславливает настоятельную потребность в развитии специализированного криминалистического инструментария.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Рост количества и сложности противоправных деяний в цифровой сфере по данным Азизова А.А. и Хорошилова А.С. закономерно порождает уязвимость пользователей и требует адекватного ответа со стороны правоохранительной системы, насыщенной инновационными продуктами и технологиями [1].

Одной из центральных проблем является сама природа киберпреступлений. Как справедливо отмечают Азизов А.А. и Хорошилов А.С., главной характеристикой, определяющей противоправные деяния как киберпреступление, является их совершение с помощью сетевых и компьютерных технологий. При этом, за исключением отдельных преступлений против жизни и здоровья, в наши дни все разновидности преступлений могут быть совершены при помощи компьютера. Среди многообразия киберпреступлений исследователи выделяют такие основные виды, как корыстные киберпреступления (финансовое мошенничество, кибервымогательство, фишинг), кибершпионаж и кибербуллинг. Особую актуальность, по мнению К.Н. Бакеевой, приобретают различные виды мошенничества платежными картами, распространение вредоносных программ, хищение средств с банковских счетов, а также противоправные действия с использованием блокчейна, искусственного интеллекта и криптовалют [2].

Важнейшим криминалистическим аспектом выступает работа с цифровыми следами (на ряду с реальными и материальными следами). Островский О.А. определяет киберкриминалистику как скрупулезный процесс извлечения электронных данных в качестве доказательств, основной целью которого является сохранение связной цепочки доказательств и документации для идентификации цифровых преступников. Процесс включает идентификацию, сохранение, ана-

лиз, документирование и представление цифровых доказательств [3]. В свою очередь, Карагулова А.А. и Нежута О.С., подчеркивают, что цифровые следы, являясь криминалистически значимой информацией, занимают особое место, так как их можно отнести как к идеальным, так и к материальным, что дает основание полагать о целесообразности выделения их в особую категорию [4].

Для анализа этих следов применяется широкий арсенал методов и инструментов цифровой криминалистики. Как указывает Бакеева К.Н., к ним относятся изъятие цифровых устройств и носителей информации, анализ цифровых доказательств (включая анализ жестких дисков), использование специальных программных средств (таких как EnCase, FTK, Oxygen Forensic Detective) и экспертиза цифровых доказательств. Саханова Н.Т. и Жумагулов А.Г. относят к перспективным методам использование искусственного интеллекта и машинного обучения для анализа больших объемов данных, выявления мошеннических транзакций и поведения пользователей, а также блокчейн-технологий для обеспечения прозрачности и неизменности записей, отслеживания финансовых операций и защиты доказательств от подделки [5].

Особую роль занимают новые виды преступлений (мошенничества, шантажа и т. п.) с использованием технологии DeepFake («глубокой подделки»). Булочников С.Ю. в своей работе выделяет способы использования этой технологии злоумышленниками и предлагает актуальные способы противодействия им [6]. В частности, отмечаются законопроекты, которые позволят охранять голос граждан от неправомерного использования в системах аудио- видеосинтеза. По мнению автора, в случае принятия законопроектов использование дипфейка в рамках совершения определённых противоправных действий будет квалифицироваться судом как преступление, совершенное с отягчающими обстоятельствами, по которым наказание может быть увеличено. В свою очередь это означает, что криминалисты и профильные эксперты должны обладать необходимыми инструментами и навыками для определения DeepFake-подделок для проведения экспертизы и вынесения соответствующих экспертных заключений.

Существенным криминалистическим аспектом является кадровое и методическое обеспечение борьбы с киберпреступностью. Низкое качество расследования киберпреступлений зачастую связано с отсутствием методических разработок и низкой профессиональной подготовкой следователей. Они отмечают, что лишь 3,5 % следователей обладают минимальными знаниями по специальности «Информатика и вычислительная техника». В этой связи особую роль приобретает важность специализированного обучения сотрудников, включающего изучение методов цифровой криминалистики, анализа вредоносного программного обеспечения и противодействия интернет-мошенничеству, а также необходимость активного привлечения IT-специалистов к расследованию.

Организационно-технический аспект борьбы с киберпреступностью включает создание специализированных киберподразделений и цифровых криминалистических лабораторий, подобных представленной в Казахстане Digital Crime Lab (DCL). Важным направлением является цифровизация самого уголовного процесса, внедрение «электронных уголовных дел» и использование цифровых технологий для фиксации следственных действий, что, по их мнению, способствует систематизации доказательств, упрощению доступа к информации и обеспечению прозрачности процесса.

Эффективное расследование киберпреступлений требует от следователя и криминалиста четкого понимания того, какие цифровые следы характерны для конкретного вида противоправной деятельности, а также какими методами и инструментами следует оперировать для их обнаружения и анализа. Для систематизации этих знаний и наглядного представления взаимосвязей между типом преступления, его цифровыми проявлениями и криминалистическим инструментарием, на основе анализа была разработана сводная таблица (табл. 1).

ВЫВОД

Проведенное исследование позволяет констатировать, что киберпреступность в современной России трансформировалась из периферийной в доминирующую угрозу, определяющую общий криминогенный фон. Ее ключевыми характеристиками являются не только стремительный количественный рост, но и качественное усугубление, выражающееся в увеличении доли тяжких и особо тяжких преступлений, а также диверсификация – от массового имущественного мошенни-

Таблица 1
Анализ инструментария цифровой криминалистики для расследования основных видов киберпреступлений
Table 1
Analysis of digital forensics tools for investigating major types of cybercrimes

Вид киберпреступления	Криминалистически значимые цифровые следы	Основные методы расследования
Финансовое мошенничество	– Логи электронной почты и фишинговых сайтов; – История браузера и кеш; – Журналы банковских операций и транзакций в блокчейне; – Файлы-ключи криптокошельков.	– Анализ сетевого трафика; – Криминалистика электронной почты; – Транзакционный анализ (в т. ч. блокчейн); – Изъятие и анализ данных с мобильных устройств.
Кибервымогательство (шифровальщики, DDoS-атаки)	– Исполняемые файлы вредоносного ПО (трояны-шифровальщики); – Логи сетевой активности; – Зашифрованные файлы на диске; – Сообщения с требованиями выкупа.	– Криминалистика вредоносных программ (анализ кода, поведения); – Сетевая криминалистика (анализ входящих / исходящих атак); – Восстановление удаленных и зашифрованных данных.
Преступления с использованием искусственного интеллекта	– Исходные медиафайлы для обучения моделей; – Лог-файлы генеративных алгоритмов; – Метаданные сгенерированного контента; – Сетевой трафик между узлами бот-сети.	– Экспертиза цифровых доказательств на предмет установления подлинности (фото-, видео-, аудиоконтента); – Анализ алгоритмов и исходного кода; – Фоноскопическая и вокалоскопическая экспертиза;

чества до деяний, угрожающих основам государственной безопасности. Борьба с этими вызовами требует комплексного и адекватного криминалистического ответа, ядром которого является цифровая криминалистика.

Как показал анализ, ее эффективность напрямую зависит от трех ключевых аспектов: совершенствования работы с цифровыми следами, которые обладают специфической двойственной природой и требуют выделения в особую категорию криминалистически значимой информации; развития специализированного инструментария, включая активное внедрение искусственного интеллекта для анализа больших данных и блокчейна для обеспечения неизменности доказательств; а также кадрового и организационного обеспечения, которое предполагает специализированную подготовку следователей, привлечение внешних экспертов и создание специализированных киберподразделений.

Таким образом, успешное противодействие киберпреступности возможно лишь при условии интеграции традиционных криминалистических подходов с постоянно обновляемым арсеналом цифровых методов, технологий и компетенций, что позволит обеспечить неотвратимость наказания и эффективную защиту прав граждан и интересов государства в цифровую эпоху.

Список источников

1. *Азизов А.А., Хорошилов А.С.* Перспективы использования современных информационных технологий в криминалистике, направленных на эффективное раскрытие киберпреступлений // Вопросы российской юстиции. 2020. № 9. С. 1052-1060. https://elibrary.ru/chiieq
2. *Бакеева К.Н.* Применение современных методов криминалистики при расследовании киберпреступлений // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: материалы Всерос. науч. конф. обучающихся и молодых ученых с междунар. участием. Самара: Самарский юридический институт ФСИН России, 2023. Ч. 1. С. 37-39. https://elibrary.ru/orvhxv
3. *Островский О.А.* Киберкриминалистика в цифровую эпоху: вызовы и перспективы развития // Юридическая гносеология. 2024. № 5. С. 106-114. https://elibrary.ru/qirrrq
4. *Карагулова А.А., Нежута О.С.* К вопросу об использовании современных технологий в криминалистике при раскрытии и расследовании киберпреступлений // Актуальные проблемы науки и практики: Гатчинские чтения 2023: сб. науч. тр. по материалам X Междунар. науч.-практ. конф. Гатчина: Государственный институт экономики, финансов, права и технологий, 2023. Т. 2. С. 276-278. https://elibrary.ru/jhopyx
5. *Саханова Н.Т., Жумагулов А.Г.* Будущее цифровой криминалистики: новые методы расследования киберпреступлений // Современные проблемы уголовного процесса: пути решения: сб. материалов Междунар. науч.-практ. конф. Уфа: Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2025. С. 276-281. https://elibrary.ru/vemwcy
6. *Булочников С.Ю.* О правотворчестве и правовых новациях в части защиты от утечек персональных данных // Новизна. Эксперимент. Традиции (Н.Экс.Т). 2025. Т. 11, № 1(29). С. 6-15. https://elibrary.ru/vnuymr

References

1. Azizov A.A., Khoroshilov A.S. (2020). Prospects for the use of modern information technologies in criminalistics aimed at effective detection of cybercrime. *Voprosy rossiiskoi yustitsii= Issues of Russian Justice*, no. 9, pp. 1052-1060. (In Russ.) https://elibrary.ru/chiieq

2. Bakeeva K.N. (2023). The use of modern forensic methods in the investigation of cybercrimes. *Materialy Vserossiiskoi nauchnoi konferentsii obuchayushchikhsya i molodykh uchenykh s mezhdunarodnym uchastiem «Problemy i perspektivy razvitiya ugolovno-ispolnitel'noi sistemy Rossii na sovremennom etape»: in 3 pts. = Proceedings of the All-Russian Scientific Conference of Students and Young Scientists with International Participation "Problems and Prospects of Development of the Russian Penal System at the Present Stage": in 3 pts*. Samara, Samara Law Institute of the Federal Penitentiary Service of Russia Publ., pt. 1, pp. 37-39. (In Russ.) https://elibrary.ru/orvhxv
3. Ostrovskii O.A. (2024). Cybercriminalism in the digital age: challenges and development prospects. *Yuridicheskaya gnoseologiya = Legal Epistemology*, no. 5, pp. 106-114. (In Russ.) https://elibrary.ru/qirrrq
4. Karagulova A.A., Nezhuta O.S. (2023). On the use of modern technologies in criminology in the detection and investigation of cybercrimes. *Sbornik nauchnykh trudov po materialam 10 Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Aktual'nye problemy nauki i praktiki: Gatchinskie chteniya 2023»: v 2 t. = Collection of Scientific Papers Based on the Materials of the 10th International Scientific and Practical Conference "Current Problems of Science and Practice: Gatchina Readings 2023". in 2 vols*. Gatchina, State Institute of Economics, Finance, Law and Technology Publ., vol. 2, pp. 276-278. (In Russ.) https://elibrary.ru/jhopyx
5. Sakhanova N.T., Zhumagulov A.G. (2025). The future of digital forensics: new methods of cybercrime investigation. *Sbornik materialov Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Sovremennye problemy ugolovnogo protsessa: puti resheniya» = Collection of Materials of the International Scientific and Practical Conference "Modern Problems of the Criminal Process: Solutions"*. Ufa, Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation Publ., pp. 276-281. (In Russ.) https://elibrary.ru/vemwcy
6. Bulochnikov S.Yu. (2025). On law-making and legal innovations in terms of protection against personal data leaks. *Novizna. Eksperiment. Traditsii (N.Eks.T) = Novelty. Experiment. Traditions (N.Ex.T)*, vol. 11, no. 1 (29), pp. 6-15. (In Russ.) https://elibrary.ru/vnuymr

Информация об авторах

Булочников Станислав Юрьевич, студент института права и национальной безопасности, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, bulochnikov03@mail.ru

Потапов Сергей Александрович, кандидат юридических наук, доцент, доцент кафедры Уголовно-правовых дисциплин, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, potapov.1995@yandex.ru.

Information about the authors

Stanislav Yu. Bulochnikov, Student of Law and National Security Institute, Derzhavin Tambov State University, Tambov, Russian Federation, bulochnikov03@mail.ru

Sergey A. Potapov, Cand. Sci. (Law), Associate Professor, Associate Professor of the Criminal Law Disciplines Department, Derzhavin Tambov State University, Tambov, Russian Federation, potapov.1995@yandex.ru

Статья поступила в редакцию / The article was submitted 03.10.2025
Одобрена после рецензирования / Approved after reviewing 26.11.2025
Принята к публикации / Accepted for publication 28.11.2025