

БЕРБЕРОВА Алие Длыверовна,
студентка 3 курса заочной формы обучения
Российский государственный университет
правосудия имени В.М. Лебедева,
e-mail: mail@law-books.ru

ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ДОКАЗЫВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. ВЫЯВЛЕНИЕ ТЕНДЕНЦИЙ РАЗВИТИЯ И РАЗРАБОТКА СПОСОБОВ ИХ УСТРАНЕНИЯ

АННОТАЦИЯ. В статье проводится анализ правоприменительных сложностей, возникающих при квалификации преступлений, предусмотренных Главой 28 Уголовного кодекса Российской Федерации, а также при формировании доказательственной базы по делам о компьютерных посягательствах. Рассмотрены статистические показатели роста киберпреступности за 2023-2025 гг. Выявлены проблемы изъятия, фиксации и экспертной оценки электронной информации в условиях её нематериальной природы и легкости уничтожения. Предложены направления совершенствования законодательства и следственной практики, включая унификацию понятийного аппарата и внедрение специализированных цифровых протоколов осмотра.

КЛЮЧЕВЫЕ СЛОВА: компьютерная информация, киберпреступность, квалификация преступлений, цифровые доказательства, уголовный процесс, компьютерная криминалистика, судебная экспертиза.

BERBEROVA Alie Dlaverovna,
3rd-year student of distance learning
Russian State University of Justice named after V.M. Lebedev

PROBLEMS OF CLASSIFICATION AND PROVING CRIMES IN THE FIELD OF COMPUTER INFORMATION. IDENTIFICATION OF DEVELOPMENT TRENDS AND DEVELOPMENT OF METHODS TO ADDRESS THEM

ANNOTATION. The article analyzes the legal and enforcement challenges that arise when classifying crimes under Chapter 28 of the Criminal Code of the Russian Federation, as well as when forming the evidentiary base in cases involving computer related offenses. The statistical indicators of the growth of cybercrime for 2023–2025 are examined. Problems are identified regarding the seizure, recording, and expert assessment of electronic information given its intangible nature and the ease with which it can be destroyed. Directions for improving legislation and investigative practice are proposed, including the unification of the conceptual framework and the introduction of specialized digital inspection protocols.

KEY WORDS: computer information, cybercrime, crime classification, digital evidence, criminal procedure, computer forensics, forensic examination.

По мере того как экономика и повседневная жизнь всё сильнее уходят в цифровизацию, всё очевиднее становится, насколько важна компьютерная информация как объект уголовной защиты. Сейчас IT-преступления принимают самые разные формы: это и незаконный доступ к информационным системам, и кража или уничтожение данных, и запуск вредоносных программ, и применение искусственного интеллекта и генеративных моделей в преступных целях. Поэтому такие деяния всё сложнее верно квалифицировать и доказывать. Разница между законными действиями и преступлением становится всё более размытой, возникают новые виды правонаруше-

ний, а доказательства часто существуют только в цифровом виде, из-за чего для их изучения требуются особые процедуры и экспертизы.

В России в 2024 году было зафиксировано 765,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что превысило показатели 2023 года на 13,1 процента. В период с января по декабрь 2024 года в России было зафиксировано 765,4 тысячи киберпреступлений, что на 13,1% больше, чем за аналогичный период 2023 года, а их доля среди всех зарегистрированных преступлений увеличилась с 34,8% в 2023 году до 40% в 2024 году [2]. Официальный представитель МВД

России отмечала, что 40 процентов всех преступлений в 2024 году совершены с использованием информационно-телекоммуникационных технологий [5].

Президент страны в марте 2025 года публично зафиксировал масштаб материального ущерба: ущерб от киберпреступлений в России в 2024 году составил около 200 млрд рублей, среди пострадавших порядка 25% пенсионеров [7]. Тревожнее другое обстоятельство. Раскрываемость киберпреступлений упала до 23%, а их число продолжает расти [7]. Получается парадоксальная ситуация - государство фиксирует растущий поток преступлений, но раскрывает лишь чуть более пятой их части, и это при том, что доля таких деяний в структуре всей преступности приблизилась к отметке в две пятых.

2025 год принес неожиданный перелом тенденции. По данным замглавы МВД Андрея Храпова, в 2025 году в России зафиксировано 663 тыс. киберпреступлений, что на 12% меньше, чем в 2024 году [6]. При этом число случаев неправомерного доступа к компьютерным данным сократилось на 44%, то есть до 58 тыс.; количество краж сократилось в 2025 году на 23,8%, до 80 тыс. случаев; число случаев мошенничества снизилось на 9%, до 344 тыс. [6]. Снижение выглядит обнадеживающе, впрочем, оно не отменяет структурной проблемы: доля мошенничеств и хищений в общей массе киберпреступлений остается доминирующей, а именно на эту категорию правоприменители тратят наибольшие процессуальные ресурсы. По данным за одиннадцать месяцев 2025 года, основной массив правонарушений, почти две трети (63,4%), по-прежнему составляют хищения и мошенничества - зарегистрировано 397,4 тысячи таких случаев [4].

Региональная картина неоднородна, и это тоже показатель системной проблемы, а не просто статистическая деталь. В 2024 году наибольшее количество IT-преступлений было зафиксировано в Мордовии, Марий Эл и Татарстане, где доля киберпреступлений составила более 63%, 62% и 57% соответственно [8]. Регионы с наименьшей долей демонстрируют совершенно иную картину: наименьшие показатели зафиксированы в Республиках Северного Кавказа, что косвенно указывает на неравномерность цифровизации инфраструктуры и, соответственно, неравномерность распределения нагрузки на следственные органы разных субъектов Федерации.

Практика правоприменения в сфере Главы 28 УК РФ сталкивается с устойчивым противоречием: закон описывает конкретные технологические явления, а технологии меняются быстрее, чем формулировки статей. Как отмечается в одной из работ, посвященных критическому анализу составов Главы 28, использование в правовых документах ссылок на частные технологические решения рискует описывать только существующие на определенный момент технологии и по-

следствия их неправомерного применения, что не выглядит предусмотрительным с учетом динамики технологического развития [1]. Отсюда вытекает вывод о необходимости пересмотра терминологии Уголовного кодекса с целью адекватного парирования угроз в сфере компьютерной информации [1].

Латыпова Э.Ю., исследовавшая проблемы квалификации преступлений Главы 28 УК РФ, фиксирует парадоксальную ситуацию роста числа зарегистрированных деяний на фоне сохраняющихся квалификационных сложностей. По ее данным, количество зарегистрированных правонарушений, совершенных с использованием информационно-телекоммуникационных технологий, постоянно увеличивается, а за первое полугодие 2024 года было зафиксировано 152,4 тысячи преступлений, связанных с использованием компьютерной информации, что на 22,7 процента больше по сравнению с аналогичным периодом прошлого года [3]. Автор напоминает, что преступления в области компьютерной информации регулируются главой 28 Уголовного кодекса Российской Федерации [3], однако именно относительная лаконичность этой главы, состоящей всего из четырех статей, порождает необходимость постоянного обращения к смежным нормам.

Ключевая проблема лежит на стыке статьи 159.6 и статьи 272 УК РФ. Мошенничество в сфере компьютерной информации выделено законодателем в отдельный состав, но границы этого состава остаются дискуссионными. Правоприменительная практика показывает следующее наблюдение: анализ судебных решений по ст. 159.6 УК РФ демонстрирует, что данное преступление не может быть отнесено ни к одной из традиционных форм хищения, а предусмотренные меры наказания не соответствуют степени его общественной опасности. Здесь, впрочем, стоит сделать оговорку - подобное расхождение между санкцией и реальной степенью общественной опасности деяния касается не только мошенничества, но и большинства составов главы 28, поскольку законодатель до сих пор не выработал единой шкалы оценки тяжести цифровых посягательств.

Существует и вторая линия квалификационных затруднений, связанная с разграничением статей 272 и 273 УК РФ. Неправомерный доступ к охраняемой законом информации нередко сопровождается использованием вредоносного программного обеспечения, и следователю приходится решать, какая из норм отражает основное содеянное, а какая - вспомогательный способ достижения преступного результата. Практика криминалистического анализа киберпреступлений указывает, что рост количества киберпреступлений требует определения субъекта криминалистической характеристики указанной категории преступлений и разработки методических ре-

комендаций по расследованию для повышения эффективности работы правоохранительных органов. Проблема здесь не столько в отсутствии норм, сколько в отсутствии унифицированной методики их применения на местах - у следователя в Казани и у следователя в Мурманске может сложиться разное понимание того, какой состав является приоритетным при совпадении признаков нескольких статей.

Отдельно нужно упомянуть проблему квалификации деяний, связанных с применением искусственного интеллекта при совершении компьютерных преступлений. Тема пока разработана слабо, хотя отдельные авторы уже фиксируют, что традиционная конструкция составов главы 28 плохо приспособлена для описания ситуаций, когда программный агент действует автономно или полуавтономно, без прямого волевого контроля человека в момент совершения технической операции. Насколько эта проблема станет масштабной в ближайшие пять-семь лет - вопрос открытый, и однозначного ответа современная доктрина пока не предлагает.

Доказывание по делам о компьютерных преступлениях устроено иначе, чем по большинству традиционных составов. Информация нематериальна, легко копируется, легко изменяется и легко уничтожается - причем часто без физического доступа к устройству, дистанционно, одной командой. Именно поэтому в литературе появилось устойчивое предложение о введении отдельной процессуальной категории. Один из авторов, анализирувавших закрепление цифровой информации в УПК РФ, отмечает, что в статье анализируются проблемы, связанные с закреплением в Уголовно-процессуальном кодексе РФ категорий, коррелирующих с цифровой информацией, и на этом основании предлагается введение нового следственного действия - осмотр цифровой информации, а также закрепление понятия «цифровые доказательства», с обязательным участием специалиста при производстве такого осмотра и введением нового обязательного случая назначения судебной экспертизы при работе с цифровой информацией.

Действующее регулирование опирается на достаточно широкую формулировку. Согласно статье 74 действующего Уголовно-процессуального кодекса, доказательства определяются как любые сведения, на основе которых устанавливаются обстоятельства, подлежащие доказыванию по уголовному делу, что теоретически позволяет использовать электронную информацию в любой ее форме [9]. Проблема, однако, не в тексте нормы, а в правоприменительной практике ее реализации: следователи по инерции продолжают требовать материализации электронных данных - распечатки, записи на оптический диск, - хотя цифровая инфраструктура давно генерирует объемы информации, несопоставимые с возможностями бумажного протоколирования.

Форензика - то есть компьютерная криминалистика в узком смысле - остается ключевым, но недостаточно развитым инструментом доказывания. Один из исследователей современных методов форензики фиксирует, что важными условиями для предотвращения и успешного расследования компьютерных преступлений является совершенствование правовой базы и развитие компьютерной криминалистики, добавляя, что грамотный сбор цифровых доказательств позволяет восстановить картину происшествия и выявить предпосылки его возникновения. Практика, впрочем, демонстрирует иное: не во всех регионах есть достаточное число сертифицированных специалистов, способных провести полноценный форензик-анализ на месте происшествия, и это создает серьезный разрыв между теоретической полнотой процессуальных возможностей и их реальной реализуемостью.

Здесь стоит привести данные о разнородности региональной ситуации. Доля киберпреступлений в отдельных субъектах Федерации превышает 60 процентов от всей регистрируемой преступности [8], и очевидно, что нагрузка на экспертные подразделения в таких регионах кратно выше среднероссийской. Возникает вопрос - способна ли текущая штатная численность экспертов-криминалистов, специализирующихся на цифровых следах, обеспечить своевременное производство исследований по каждому такому делу? Ответ, судя по показателю раскрываемости в 23 процента [7], скорее отрицательный.

Есть и чисто технологическая сложность, связанная с трансграничным характером многих цифровых следов. Сервер может находиться за пределами Российской Федерации, провайдер - отказывать в оперативном предоставлении данных, а срок хранения логов на стороне оператора связи - истекать раньше, чем следователь успевает направить соответствующий запрос. Мессенджеры стали, пожалуй, самым проблемным каналом с точки зрения доказывания: как показывают данные за одиннадцать месяцев 2025 года, ключевым каналом для противоправных действий остаются мессенджеры, с их помощью совершено 244,6 тысячи преступлений, что на 17,5% больше показателя за январь-ноябрь 2024 года [4]. Получение переписки из зарубежных мессенджеров по официальным каналам международной правовой помощи занимает месяцы, тогда как злоумышленник успевает скрыть следы за считанные часы.

Первое, что напрашивается само собой - унификация понятийного аппарата Главы 28 УК РФ с последующей синхронизацией терминологии УПК РФ. Разрозненность формулировок «компьютерная информация», «информационно-телекоммуникационная сеть» и «электронный документ» порождает споры на уровне квалификации, которые можно снять законодательным путем, не дожидаясь очередного постановления Пленума

Верховного Суда. Насколько быстро законодатель пойдет на такой шаг - вопрос политической воли, а не юридической техники.

Второе направление касается именно процессуальной формы работы с цифровыми доказательствами. Введение самостоятельного следственного действия - осмотра цифровой информации - выглядит логичным продолжением идеи, уже прозвучавшей в профильной литературе. Такая мера позволила бы закрепить обязательное участие специалиста уже на стадии первичного осмотра, а не только при последующей экспертизе, что снизило бы риск утраты доказательственного значения информации из-за неправильных технических действий следователя на месте происшествия.

Третье направление - развитие ведомственной инфраструктуры цифровой криминалистики на региональном уровне, причем с учетом фактической нагрузки, а не формальной штатной численности. Регионы с долей киберпреступности выше 50 процентов [8] нуждаются в опережающем финансировании экспертных подразделений, тогда как равномерное распределение ресурсов без учета региональной специфики консервирует существующий разрыв между регистрацией и раскрытием дел.

Четвертое - работа с зарубежными операторами связи и мессенджерами требует не столько новых норм внутреннего права, сколько ускоренных межведомственных и межгосударственных процедур обмена данными, поскольку доля преступлений, совершаемых через мессенджеры, продолжает расти [4] быстрее, чем совершенствуются механизмы международного взаимодействия.

Пятое, менее очевидное направление связано с подготовкой кадров. Цифровизация криминалистики, как отмечается в одной из недавних работ, является комплексным многовекторным явлением и осуществляется в трех основных направлениях: через упрощение существующих подходов, повышение эффективности имеющихся подходов и формирование новых подходов в деятельности сотрудников правоохранительных органов [1]. Формирование новых подходов невозможно без подготовки следователей и экспертов, обладающих не только юридической, но и технической квалификацией - а таких специалистов на всю страну по-прежнему ощутимо не хватает, особенно в отдаленных субъектах Федерации.

Снижение показателей киберпреступности в 2025 году [6] дает определенный повод для сдержанного оптимизма, однако делать далеко иду-

щие выводы о переломе тенденции пока рано. Слишком велика инерция статистики предыдущих лет, слишком неравномерна региональная картина, и слишком многое зависит от того, удастся ли синхронизировать законодательные новации с реальной практикой их применения на местах.

Таким образом, проблематика квалификации и доказывания преступлений в сфере компьютерной информации демонстрирует устойчивый разрыв между темпами технологических изменений и скоростью адаптации уголовного и уголовно-процессуального законодательства. Рост числа зарегистрированных деяний, зафиксированный статистикой МВД за 2023-2024 годы [2, 5], сменился умеренным снижением в 2025 году [6], но структурная нагрузка на правоприменителей от этого не уменьшилась - доля хищений и мошенничеств в общем массиве киберпреступности остается доминирующей [4], а раскрываемость остается непропорционально низкой относительно масштаба причиняемого ущерба [7].

Квалификационные сложности сосредоточены преимущественно на стыке смежных составов главы 28 УК РФ и статьи 159.6 УК РФ, а также в отсутствии единой терминологической базы, способной охватывать новые технологические явления без постоянной корректировки текста закона [1, 3]. Доказательственные барьеры связаны с нематериальной природой цифровых следов, недостаточной процессуальной регламентацией их фиксации и хронической нехваткой квалифицированных специалистов в области компьютерной криминалистики на региональном уровне [8].

Практическая значимость представленного анализа состоит в том, что предложенные направления - унификация терминологии, введение самостоятельного следственного действия по осмотру цифровой информации, дифференцированное распределение экспертных ресурсов и ускорение международного информационного обмена - формируют реалистичную дорожную карту для законодателя и правоприменителя. Дальнейшие исследования целесообразно сосредоточить на эмпирическом анализе региональной судебной практики по статьям 272-274 УК РФ за 2024-2026 годы, а также на изучении квалификационных последствий использования систем искусственного интеллекта при совершении компьютерных преступлений - теме, которая пока остается на периферии отечественной уголовно-правовой доктрины, но, по всей видимости, приобретет центральное значение в ближайшие годы.

Список литературы:

[1] Бахтеев Д.В., Беляков А.А. Векторы цифрового развития криминалистики на примере современных цифровых проектов криминалистического назначения // Сборник трудов конференции. 2024. С. 54-57.

[2] В России в 2024 году IT-преступления достигли пика за последние пять лет // Хабр. 2025. URL: <https://habr.com/ru/news/877022/> (дата обращения: 23.08.2026).

[3] Латыпова Э.Ю. Преступления в сфере компьютерной информации: проблемы квалификации // Международный студенческий научный вестник. 2024. URL: <https://sci-article.ru/stat.php?i=1720588459> (дата обращения: 28.09.2026).

[4] МВД: с начала 2025 года в РФ зарегистрировано 627 тысяч киберпреступлений // Аргументы и Факты. 2025. URL: <https://aif.ru/incidents/mvd-s-nachala-2025-goda-v-rf-zaregistrirovano-627-tysyach-kiberprestupleniy> (дата обращения: 23.09.2026).

[5] МВД: Число обычных преступлений снижается, а киберпреступлений - растёт // Российская газета. 2025. URL: <https://rg.ru/2025/01/20/mvd-chislo-obychnyh-prestuplenij-snizhaetsia-a-kiberprestuplenij-rastet.html> (дата обращения: 23.09.2026).

[6] МВД: число киберпреступлений в России снизилось на 12% в 2025 году // Коммерсантъ. 2026. URL: <https://www.kommersant.ru/doc/8442339> (дата обращения: 23.08.2026).

[7] Путин заявил об ущербе от киберпреступлений в 2024 году на сумму 200 млрд рублей // ComNews. 2025. URL: <https://www.comnews.ru/content/238114/2025-03-05/2025-w10/1009/putin-zayavil-ob-uscherbe-kiberprestupleniy-2024-godu-summu-200-mlrd-rublej> (дата обращения: 23.09.2026).

[8] Статистика киберпреступности в российских регионах: данные МВД за 2024 год // Региональные системы. 2025. URL: <https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/> (дата обращения: 23.08.2026).

[9] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 25.12.2024) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

References:

[1] Bakhteev D.V., Belyakov A.A. Vectors of digital development in forensic science: the case of modern digital forensic projects // Conference Proceedings. 2024. P. 54–57.

[2] IT crimes in Russia reached a five-year high in 2024 // Habr. 2025. URL: <https://habr.com/ru/news/877022/> (accessed: 23.08.2026).

[3] Latypova E.Yu. Crimes involving computer information: issues of legal classification // International Student Scientific Bulletin. 2024. URL: <https://sci-article.ru/stat.php?i=1720588459> (accessed: 28.09.2026).

[4] Ministry of Internal Affairs: 627,000 cybercrimes registered in the Russian Federation since the beginning of 2025 // Argumenty i Fakty. 2025. URL: <https://aif.ru/incidents/mvd-s-nachala-2025-goda-v-rf-zaregistrirovano-627-tysyach-kiberprestupleniy> (accessed: 23.09.2026).

[5] Ministry of Internal Affairs: Number of conventional crimes is decreasing, while cybercrimes are rising // Rossiyskaya Gazeta. 2025. URL: <https://rg.ru/2025/01/20/mvd-chislo-obychnyh-prestuplenij-snizhaetsia-a-kiberprestuplenij-rastet.html> (accessed: 23.09.2026). [6] Ministry of Internal Affairs: Number of cybercrimes in Russia fell by 12% in 2025 // Kommersant. 2026. URL: <https://www.kommersant.ru/doc/8442339> (accessed: 23.08.2026).

[7] Putin stated that cybercrimes caused 200 billion rubles in damages in 2024 // ComNews. 2025. URL: <https://www.comnews.ru/content/238114/2025-03-05/2025-w10/1009/putin-zayavil-ob-uscherbe-kiberprestupleniy-2024-godu-summu-200-mlrd-rublej> (accessed: 23.09.2026).

[8] Cybercrime statistics in Russian regions: Ministry of Internal Affairs data for 2024 // Regional Systems. 2025. URL: <https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/> (accessed: 23.08.2026).

[9] Criminal Procedure Code of the Russian Federation No. 174-FZ dated December 18, 2001 (as amended on December 25, 2024) // Collection of Legislation of the Russian Federation. 2001. No. 52 (Part I). Art. 4921.

