

УДК 343.3

DOI: 10.34670/AR.2026.25.61.054

**Правовая неопределённость при квалификации кибератак по
статьям 272 и 273 УК РФ****Милаева Майя Юрьевна**

Кандидат юридических наук, доцент,
кафедра «Безопасность в цифровом мире»,
Московский государственный технический
университет им. Н.Э. Баумана
(национальный исследовательский университет),
105005, Российская Федерация, Москва, 2-я Бауманская ул., 5/ 1;
e-mail: milaeva-bmstu@mail.ru

Колмакова Милена Владимировна

Студент,
Московский государственный технический
университет им. Н.Э. Баумана
(национальный исследовательский университет),
105005, Российская Федерация, Москва, 2-я Бауманская ул., 5/ 1;
e-mail: kolmakovamv@student.bmstu.ru

Аннотация

В работе рассматривается проблема правовой неопределённости при квалификации кибератак по статьям 272 и 273 Уголовного кодекса Российской Федерации. Утверждается, что сложность уголовно-правовой оценки соответствующих деяний обусловлена комплексным характером и технической неоднородностью кибератак, при которых вредоносное программное обеспечение может одновременно выступать как самостоятельный элемент преступного поведения и как средство неправомерного доступа к компьютерной информации. Анализируются положения Пленума Верховного Суда Российской Федерации, позиции исследователей, представленные в научной литературе, а также отдельные материалы судебной практики. На основе статистических данных показано преобладание преступлений, квалифицируемых по статье 272 УК РФ, при сравнительно низкой доле применения статьи 273 УК РФ. Зафиксирован рост числа преступлений в сфере компьютерной информации и в особенности тех, что совершены с использованием вредоносного программного обеспечения. Сделан вывод о необходимости дополнительной конкретизации подходов к квалификации кибератак, в том числе посредством нормативного определения их понятия и учёта роли специальных знаний при правоприменении. Предлагаются дополнения статей Уголовного кодекса Российской Федерации.

Для цитирования в научных исследованиях

Милаева М.Ю., Колмакова М.В. Правовая неопределённость при квалификации кибератак по статьям 272 и 273 УК РФ // Вопросы российского и международного права. 2026. Том 16. № 7А. С. 523-533. DOI: 10.34670/AR.2026.25.61.054

Ключевые слова

Компьютерная атака, вредоносное программное обеспечение, неправомерный доступ к информации, преступления в сфере компьютерной информации, уголовно-правовая квалификация, кибербезопасность, специальные знания.

Введение

Современные кибератаки (или же компьютерные атаки) нередко носят комплексный характер и включают в себя несколько взаимосвязанных действий: разработку вредоносного программного обеспечения (далее – вредоносное ПО), его распространение, получение неправомерного доступа к информационным системам, а также последующее извлечение, модификацию или блокирование данных. В связи с этим возникает вопрос о правильной уголовно-правовой квалификации таких действий.

В законодательстве уголовная ответственность за указанные деяния предусмотрена статьями «Неправомерный доступ к компьютерной информации» (272 УК РФ [Уголовный кодекс РФ, 1996]) и «Создание, использование и распространение вредоносных компьютерных программ» (273 УК РФ [Уголовный кодекс РФ, 1996]). При этом в практике Верховный Суд РФ рекомендует применять идеальную совокупность для одного фактического деяния, чтобы учесть все аспекты преступного поведения несмотря на то, что оно является единой атакой с использованием одного инструмента. По мнению Председателя Следственного комитета Российской Федерации А.И. Бастрыкина [Бастрыкин, 2026], сложности расследования преступлений в сфере компьютерной информации во многом обусловлены их трансграничным характером.

В действующем российском праве отсутствует закрепленное на законодательном уровне определение «киберпреступности» – вместо этого в законе использована категория «преступления в сфере компьютерной информации». В научной литературе неоднократно отмечалось, что отсутствие единого понятийного аппарата осложняет как теоретическое осмысление соответствующих деяний, так и их квалификацию в правоприменительной практике [Суслов, Милаева, 2026].

Как видно из рисунка 1, составленной на основе данных открытых статистических источников [Уголовное судопроизводство: данные о назначенном наказании, www.anip-press.ru], в отличие от стабильно растущей динамики осужденных по ст. 272 УК РФ, показатели по ст. 273 УК РФ с каждым годом снижаются. Это позволяет предположить, что деяния, связанные с использованием вредоносного программного обеспечения, в правоприменительной практике нередко оцениваются преимущественно через призму неправомерного доступа к компьютерной информации.

Актуальность рассматриваемой проблемы подтверждается и статистикой издания «ТАдвизер» («TAdviser») [Число киберпреступлений в России, www.tadviser.ru]: в 2025 году в сфере компьютерной информации зарегистрировано 61137 преступлений, из которых 58782 эпизода связаны с неправомерным доступом к компьютерной информации. Одновременно отмечается существенный рост преступлений, связанных с созданием, использованием и распространением компьютерных программ: их количество увеличилось на 96,4% и достигло 607 эпизодов.

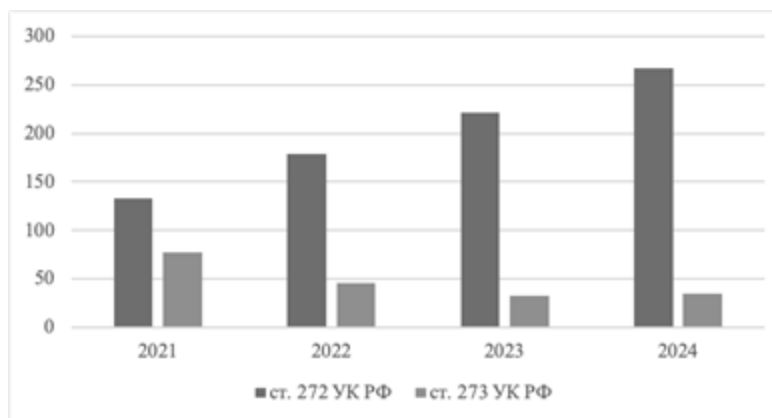


Рисунок 1- Динамика роста осуждённых по статьям 272 и 273 УК РФ в 2021-2024 гг.

Существенное преобладание преступлений, квалифицируемых по статье 272 УК РФ, при относительно небольшом числе деяний, попадающих под признаки статьи 273 УК РФ, может свидетельствовать о том, что использование вредоносного программного обеспечения в ряде случаев воспринимается правоприменителем преимущественно как способ совершения неправомерного доступа, а не как самостоятельное преступление.

На основании Постановления Пленума Верховного Суда РФ от 15.12.2022 №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» [Постановление Пленума Верховного Суда РФ № 37, 2022], судам следует учитывать, что, в случае использования вредоносной компьютерной программы для осуществления неправомерного доступа к компьютерной информации, повлекшего наступление последствий, предусмотренных ст. 272 УК РФ, действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ (согласно пункту 15 Постановления Пленума). Однако такой подход подвергается критике в научной, поскольку не всегда учитывает роль вредоносного ПО в механизме преступления и приводит к неверной квалификации содеянного. Исследователи склоняются к мнению, что кибератаки следует квалифицировать преимущественно по ст. 273 УК РФ, однако нам представляется более обоснованным подход Пленума Верховного Суда РФ, поскольку он позволяет более полно оценить их правовую природу.

Настоящее исследование посвящено анализу квалификационных сложностей при разграничении составов, предусмотренных ст. 272 и 273 УК РФ, в условиях стремительного развития компьютерных атак, а также разработке предложений по унификации правоприменительной практики.

Основная часть

Несмотря на наличие официальных разъяснений Пленума Верховного Суда Российской Федерации, практика свидетельствует о сохраняющихся трудностях как в применении института идеальной совокупности, так и при разграничении ст. 272 и 273 УК РФ.

В большинстве случаев неправомерный доступ к компьютерной информации осуществляется с использованием вредоносного программного обеспечения – согласно анализу

экспертов «Группы Позитив» («Positive Technologies») [CODE RED 2026, www.ptsecurity.com], проведённому в 2025 году, до 71% киберпреступлений. В таком случае вредоносное ПО выступает не только самостоятельным объектом уголовно-правовой оценки, но и инструментом получения доступа к компьютерной информации. В результате возникает вопрос: подлежит рассматривать содеянное как единое преступление и квалифицировать по статье 273 УК РФ или как совокупность преступлений, предусмотренных статьями 272 УК РФ и 273 УК РФ, что совпадает с разъяснением Пленума.

В этой связи представляется необходимым рассмотреть особенности компьютерных атак как формы преступного деяния. Анализ их внутренней структуры, характера и роли вредоносного ПО в механизме совершения преступления позволит точнее определить причины возникающих трудностей.

Особенности компьютерных атак как формы преступного деяния

В отличие от часто встречаемых в практике преступлений, объективная сторона которых зачастую выражается в одном действии, компьютерные атаки, как правило, включают совокупность взаимосвязанных действий, направленных на неправомерное воздействие на компьютерную информацию, информационные системы и средства их защиты, а также создание самого способа доступа к этим структурам и данным – вредоносного программного обеспечения. При этом отдельные этапы кибератак могут осуществляться как одним лицом, так и группой лиц, а также совпадать по времени, что дополнительно усложняет их уголовно-правовую оценку.

Ключевым элементом механизма компьютерной атаки выступает вредоносное программное обеспечение, которое в одних случаях выступает как самостоятельный объект уголовно-правовой оценки, образуя состав преступления по ст. 273 УК РФ, в иных – инструментом получения неправомерного доступа к компьютерной информации. Указанная двойственность обуславливает ключевую особенность кибератак: одно фактическое деяние может одновременно содержать признаки нескольких составов преступлений. При этом разграничение зависит от роли вредоносного ПО в механизме атаки, которая не всегда очевидна для правоприменителя.

Дополнительно следует учитывать, что атаки всё чаще реализуются в условиях высокой автоматизации и распределённости. Распространение моделей «вредоносного ПО как сервиса» (RaaS), использование ботнетов и облачных инфраструктур приводит к тому, что отдельные стадии атаки могут выполняться различными субъектами, зачастую находящимися в разных юрисдикциях. Это затрудняет установление роли каждого участника и усложняет квалификацию деяния в рамках классических конструкций уголовного права, ориентированных на индивидуализированное поведение субъекта.

Исследование кибератак не должно ограничиваться исключительно анализом действий виновного лица. В криминологии обоснованно указывается, что изучение личности и поведения потерпевшего позволяет глубже понять причины и условия совершения преступлений, а также разработать более эффективные меры их предупреждения [Карасева, 2007]. Применительно к преступлениям в сфере компьютерной информации это означает необходимость учитывать ещё и уровень защищённости информационной системы, соблюдение требований информационной безопасности и действий пользователей, которые могли способствовать реализации преступного умысла.

Следовательно, специфика компьютерных атак как формы преступного деяния требует не только описания их технического механизма, но и анализа уголовно-правовых подходов.

Сравнение позиции Верховного Суда РФ и научного подхода

В пункте 15 Постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по делам о преступлениях в сфере компьютерной информации» конкретизируется, что, когда вредоносная компьютерная программа использовалась для осуществления неправомерного доступа к компьютерной информации и это повлекло наступление последствий, предусмотренных частью 1 статьи 272 УК РФ, действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ.

Позиция Верховного Суда РФ исходит из разграничения объектов охраны и различий в юридической конструкции составов преступлений: статья 272 УК РФ защищает порядок доступа к информации, в то время как статья 273 УК РФ предотвращает распространение вредоносных программ. В результате использование вредоносного ПО для получения доступа к информации рассматривается как два самостоятельных преступления, каждое из которых подлежит отдельной правовой оценке.

В научной литературе данная позиция оценивается неоднозначно. Ряд исследователей указывает на риск избыточного применения совокупности преступлений, поскольку в условиях реальных кибератак вредоносное ПО нередко выступает способом реализации неправомерного доступа.

В.Ф. Щепельков, анализируя Постановление Пленума Верховного Суда РФ [Щепельков, 2023] отмечает, что применение идеальной совокупности может приводить к избыточной уголовно-правовой оценке одного фактического деяния, и квалификация должна осуществляться по одной из статей: преимущественно по 272 УК РФ, так как основное значение имеет неправомерный доступ к компьютерной информации.

Исследуя особенности состава компьютерных преступлений, И.А. Клепицкий указывает на запутанность в определении способов и последствий таких деяний и толковании признаков «правомерности» в ст. 272 УК РФ и «несанкционированности» в ст. 273 УК РФ [Клепицкий, 2025]. В ряде случаев, рассмотренных автором, к компьютерным преступлениям относились действия, не представляющие реальной общественной опасности (например, вмешательство в программное обеспечение с согласия владельца), что свидетельствует о риске расширительного толкования уголовно-правовых норм. В связи с этим, предлагается чётко определить критерии вреда и квалифицировать деяния по ст. 273 УК РФ в отдельных случаях.

Определяющим критерием разграничения составов преступлений должен быть способ проникновения в информационную систему – такую позицию высказывает Р.С. Поздышев [Поздышев, 2023]. В случае, если доступ осуществляется без использования вредоносного ПО (например, с применением полученных учетных данных), содеянное подлежит квалификации по части 2 статьи 272 УК РФ. В случае, когда доступ к информации осуществляется посредством использования программы, предназначенной для несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации средств защиты, то деяние попадает под признаки части 2 статьи 273 УК РФ. В подобных ситуациях вредоносная ПО выступает ключевым инструментом совершения преступления, и потому данная норма должна иметь приоритетное значение при квалификации деяния. Автор отмечает, что использование вредоносного ПО нередко приводит к наступлению последствий, указанных в ст. 272 УК РФ – в таком случае возможно применение совокупности преступлений как дополнительной уголовно-правовой оценки.

Обзор научной литературы свидетельствует, что сложности квалификации обусловлены не

только конструкцией статей 272 и 273 УК РФ, но и отсутствием единых подходов к определению самих преступлений в сфере компьютерной информации. В исследованиях отмечается необходимость законодательного закрепления соответствующего понятийного аппарата, что позволило бы обеспечить более последовательное разграничение смежных составов преступлений [Миронов, Милаева, 2024].

Вместе с тем позиция Верховного Суда Российской Федерации в целом является обоснованной, поскольку учитывает сложный характер рассматриваемых деяний. Однако её применение на практике требует рассмотрения технической специфики компьютерных атак, в частности роли вредоносного ПО в механизме их совершения. Универсальное применение конструкции совокупности без анализа указанных обстоятельств может приводить к формальному подходу к квалификации и нивелировать различия между способом совершения преступления и самостоятельным преступным деянием.

Анализ судебной практики

При квалификации преступлений, связанных с неправомерным доступом к компьютерной информации и использованием вредоносного ПО, суды сталкиваются с рядом сложностей. Несмотря на разъяснения, содержащиеся в Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37, единообразие правоприменительной практики в данной сфере пока не достигнуто.

В подтверждение изложенных выводов обратимся к материалам уголовного дела, рассмотренного Владимирским областным судом в апелляционном порядке от 9 сентября 2025 года [Апелляционное постановление Владимирского областного суда, 2025]. В суде первой инстанции осужденный был признан виновным по ч. 1 ст. 272 УК РФ, а также в покушении на распространение и использование компьютерной информации, предназначенной для нейтрализации средств защиты (ч. 1 ст. 273 УК РФ).

Содержание дела сводится к неправомерному модифицированных смарт-карт для доступа к спутниковому телевидению, содержащих изменённые сведения о подписках и сроках их действия, что позволяло получать доступ к закрытым пакетам телеканалов без внесения абонентской платы. Проведённые экспертизы установили, что содержащаяся на картах информация позволяла нейтрализовать средства защиты и осуществлять копирование данных, необходимых для дешифрования спутникового канала.

Первоначально органами предварительного расследования действия обвиняемого были квалифицированы по более тяжким составам преступлений, предусмотренным ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ, однако в ходе судебного разбирательства государственный обвинитель переквалифицировал действия подсудимого, смягчив обвинение. Апелляционная инстанция указала на неполноту исследования обстоятельств дела и признала такое изменение необоснованным. Приговор был отменён, а дело направлено на новое рассмотрение. Этот случай наглядно демонстрирует, что суд и сторона обвинения испытывают затруднения при определении уголовно-правовой оценки подобных действий.

Различия в квалификации на разных стадиях уголовного судопроизводства, а также вмешательство апелляционной инстанции подтверждает, что существующие правовые конструкции требуют дополнительного разъяснения с учётом технической специфики компьютерных атак.

Показательным также является Кассационное определение Верховного Суда Российской Федерации №77-УД25-1-К1 от 17 апреля 2025 года [Кассационное определение Верховного Суда РФ № 77-УД25-1-К1, 2025], в рамках которого действия виновного лица были

квалифицированы по совокупности преступлений, предусмотренных частью 1 статьи 272 и частью 1 статьи 273 УК РФ. Судом установлено, что лицо осуществляло неправомерный доступ к компьютерной информации с использованием программных средств, направленных на преодоление механизмов защиты. Рассмотренное дело содержит системную проблему правоприменения в сфере компьютерных преступлений, где одно фактическое деяние требует квалификации по совокупности статей, учитывая использование вредоносного ПО как инструмента совершения преступления.

Существенное значение при рассмотрении дела имели результаты судебной компьютерно-технической экспертизы: определение функций примененных программных средств и указание на наличие признаков вредоносного ПО, что выходит за пределы общеправовой оценки. Анализ содержания судебного акта показывает, что квалификация содеянного не носила формальный характер и требовала от суда детального исследования технической стороны совершённого деяния. Указанные сложности объясняются также особенностями законодательной конструкции составов преступлений в сфере компьютерной информации. Как отмечается в научной литературе, многие уголовно-правовые нормы данной группы обладают сходными признаками объективной стороны, вследствие чего без установления их особенностей корректная квалификация деяния существенно затрудняется [Суслов, Милаева, 2026].

Таким образом, если неправомерный доступ к компьютерной информации совершен средствами с признаками вредоносного ПО, то действия лица подлежат рассмотрению по совокупности преступлений, предусмотренных статьями 272 и 273 УК РФ. В случае отсутствия таковых признаков квалификация может ограничиваться только статьей 272 УК РФ. Указанная правовая позиция соответствует разъяснениям, данным в Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37. Вместе с тем сам факт необходимости привлечения специальных знаний и проведения экспертизы свидетельствует о сложности правовой оценки подобных деяний и отсутствии очевидных критериев разграничения составов преступлений.

Анализ судебной практики указывает на необходимость разработки предложений, направленных на уточнение и адаптацию законодательства к особенностям современных компьютерных атак. В этой связи представляется обоснованным рассмотреть возможные направления совершенствования квалификации соответствующих деяний.

Направления совершенствования уголовно-правовой квалификации кибератак

Представляется целесообразным дополнить действующие нормы Уголовного кодекса Российской Федерации и разъяснения Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 года.

Во-первых, следует ввести примечание к ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», которое будет предусматривать освобождение от уголовной ответственности лиц, предотвративших последствия неправомерного доступа к информации. Такое решение будет основываться на принципе справедливости и направлено на поощрение активных действий, предотвращающих причинённый ущерб. Это позволит стимулировать инициативность и готовность лиц, допустивших неправомерный доступ к информации, принимать меры для устранения последствий своих действий.

Примечания. <...> 1. Лицо, предотвратившее последствия неправомерного доступа к компьютерной информации, освобождается от уголовной ответственности, если это не противоречит общественным интересам, в том числе принципу справедливости.

Во-вторых, в ч. 1 ст. 273 УК РФ следует уточнить, что именно *вредоносные* компьютерные

программы являются объектом уголовной ответственности. Это позволит чётко разграничить преступления, связанные с созданием и распространением программ, наносящих вред информационным системам. Кроме того, предлагается увеличить штрафы и предусмотреть лишение свободы до 8 лет за указанные деяния, чтобы повысить санкции за преступления, связанные с нарушением информационной безопасности.

Далее, в ч. 2 ст. 273 УК РФ целесообразно усилить санкции за крупный ущерб, сговор и совершение деяний организованной группой, чтобы усилить ответственность за совершение преступлений, имеющих широкие последствия для функционирования систем и скоординированных действий преступников. Также предлагается повысить штрафы и продлить сроки лишения свободы до 10 лет.

Кроме того, целесообразно дополнить санкции ст. 273 УК РФ наказанием в виде лишения права занимать определённые должности или заниматься определённой деятельностью для лиц, виновных в создании, использовании и распространении вредоносных программ.

Основным предложением является закрепление на нормативном уровне понятия компьютерной атаки (кибератаки). Логичным является включение соответствующего определения в примечание к ст. 273 УК РФ, что будет способствовать более точному толкованию в правоприменительной практике, а также позволит отразить многоэтапность современных кибератак.

Примечания. 1. Под компьютерной атакой (кибератакой) в настоящей статье понимается совокупность взаимосвязанных действий, направленных на неправомерное воздействие на компьютерную информацию, информационные системы либо на средства их защиты, включающая создание, использование или распространение вредоносного программного обеспечения, а также получение, изменение, блокирование, уничтожение или копирование компьютерной информации.

В-третьих, Постановление Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 года предлагаем дополнить следующим разъяснением:

Если деяние, совершённое с использованием вредоносного ПО, квалифицируется по совокупности преступлений, предусмотренных статьями 272 и 273 УК РФ, то при проведении судебной компьютерно-технической экспертизы, которая подтверждает отсутствие признаков использования вредоносного ПО, деяние подлежит квалификации исключительно по статье 272 УК РФ.

Представляется, что реализация указанных предложений упростит квалификацию, обеспечит единообразие правоприменительной практики и будет учитывать специфику современных компьютерных атак без изменения базовой конструкции действующего уголовного законодательства.

Заключение

В ходе исследования была проанализирована проблема правовой неопределённости при квалификации деяний, связанных с кибератаками, по статьям 272 и 273 УК РФ. Рассмотрены существующие подходы в судебной практике и доктрине, что позволило выявить основные трудности, с которыми сталкивается правоприменитель при квалификации подобных преступлений.

Важным результатом работы является предложение о дополнении статей уголовного законодательства, в частности, закрепление понятия компьютерной атаки (кибератаки). Кроме

того, предложены изменения в статью 273 УК РФ, касающиеся увеличения санкций, включая штрафы и срок лишения свободы, и последствия для лиц, использующих своё служебное положение для совершения преступлений с вредоносными программами. Значимым для судебной практики является уточнение Постановления Пленума Верховного Суда РФ о применении совокупности преступлений, а также дополнение примечания в статью 272 УК РФ, предусматривающее освобождение от уголовной ответственности в случае, если лицо самостоятельно предотвратило последствия неправомерного доступа к информации.

Представляется, что данные изменения позволят обеспечить единообразие практики, связанной с кибератаки и поможет более эффективно бороться с преступлениями в сфере компьютерной информации.

Следует учитывать, что развитие технологий и усложнение моделей совершения подобных преступных деяний опережают темпы адаптации уголовного законодательства, что усиливает выявленные проблемы квалификации и требует их системного осмысления в рамках как правоприменительной, так и научной деятельности.

Библиография

1. Апелляционное постановление Владимирского областного суда от 9 сентября 2025 г. № 22-1795/2025 по делу № 1-109/2024 // СудАкт. URL: sudact.ru/regular/doc/TUxhN6ASZwxs/
2. Бастрыкин А.И. Преступность перетекает в онлайн, но следствие к этому готово: интервью // Следственный комитет Российской Федерации. 2026. URL: <https://sledcom.ru/press/interview/item/2062124/>
3. Карасева М.Ю. Криминологическая характеристика потерпевшего // Актуальные проблемы российского права. 2007. № 1 (4). С. 549–554.
4. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 17 апреля 2025 г. № 77-УД25-1-К1. URL: https://vsrf.ru/lk/practice/stor_pdf/2457588
5. Клепицкий И.А. Компьютерные преступления: вопросы юридической техники // Вектор юридической науки. 2025. № 5. С. 48–57. DOI: 10.17803/2311-5998.2025.129.5.048-057.
6. Миронов Б.А., Милаева М.Ю. Современный взгляд на понятие преступления в сфере компьютерной информации // Скиф. Вопросы студенческой науки. 2024. № 10 (98). С. 248–254.
7. Поздышев Р.С. Вопросы квалификации преступлений в сфере компьютерной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 105–112. DOI: 10.36511/2078-5356-2023-1-105-112.
8. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» // Российская газета. URL: <https://rg.ru/documents/2022/12/28/document-postanovlenie-plenuma-verkhovnogo-suda.html>
9. Суслов Т.В., Милаева М.Ю. Криминологический анализ личности киберпреступника как феномен современного общества // Скиф. Вопросы студенческой науки. 2026. № 1 (113). С. 145–151.
10. Уголовное судопроизводство: данные о назначенном наказании по статьям УК РФ // АПИ-Пресс. URL: <https://stat.anip-precc.pf/stats/ug/t/14/s/17>
11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 10.06.2026 № 164-ФЗ) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891>
12. Число киберпреступлений в России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России
13. Щепельков В.Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6. С. 70–79.
14. CODE RED 2026: Актуальные киберугрозы для российских организаций // Positive Technologies. URL: <https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id3>

Legal Uncertainty in the Qualification of Cyberattacks under Articles 272 and 273 of the Criminal Code of the Russian Federation

Maiya Yu. Milaeva

PhD in Law, Associate Professor,
Department of "Security in the Digital World",
Bauman Moscow State Technical University (National Research University),
105005, 5/1, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: milaeva-bmstu@mail.ru

Milena V. Kolmakova

Student,
Bauman Moscow State Technical University (National Research University),
105005, 5/1, 2-ya Baumanskaya str., Moscow, Russian Federation;
e-mail: kolmakovamv@student.bmstu.ru

Abstract

The paper examines the problem of legal uncertainty in the qualification of cyberattacks under Articles 272 and 273 of the Criminal Code of the Russian Federation. It is argued that the complexity of the criminal law assessment of the relevant acts is due to the complex nature and technical heterogeneity of cyberattacks, in which malicious software can simultaneously act as an independent element of criminal behavior and as a means of unlawful access to computer information. The provisions of the Plenum of the Supreme Court of the Russian Federation, the positions of researchers presented in scientific literature, as well as certain materials of judicial practice are analyzed. Based on statistical data, the predominance of crimes qualified under Article 272 of the Criminal Code of the Russian Federation is shown, with a comparatively low share of the application of Article 273 of the Criminal Code of the Russian Federation. An increase in the number of crimes in the sphere of computer information, and in particular those committed using malicious software, is recorded. A conclusion is made about the need for further concretization of approaches to the qualification of cyberattacks, including by means of a normative definition of their concept and taking into account the role of special knowledge in law enforcement. Amendments to the articles of the Criminal Code of the Russian Federation are proposed.

For citation

Milaeva M.Yu., Kolmakova M.V. (2026) *Pravovaya neopredelennost' pri kvalifikatsii kiberneticheskikh po stat'yam 272 i 273 UK RF* [Legal Uncertainty in the Qualification of Cyberattacks under Articles 272 and 273 of the Criminal Code of the Russian Federation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (7A), pp. 523-533. DOI: 10.34670/AR.2026.25.61.054

Keywords

Computer attack, malicious software, unlawful access to information, crimes in the sphere of computer information, criminal law qualification, cybersecurity, special knowledge.

References

1. Appellate ruling of the Vladimir Regional Court dated September 9, 2025, No. 22-1795/2025 in case No. 1-109/2024. (2025). *SudAct*. sudact.ru/regular/doc/TUxuN6ASZwxs/
2. Bastrykin, A.I. (2026) Crime is moving online, but investigators are ready for it: interview. *Investigative Committee of the Russian Federation*. <https://sledcom.ru/press/interview/item/2062124/>
3. Cassation ruling of the Judicial Collegium for Criminal Cases of the Supreme Court of the Russian Federation dated April 17, 2025, No. 77-UD25-1-K1. (2025). https://vsrf.ru/lk/practice/stor_pdf/2457588
4. CODE RED 2026: Current Cyber Threats to Russian Organizations. (2026) *Positive Technologies*. <https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id3>
5. Criminal Code of the Russian Federation dated June 13, 1996, No. 63-FZ (as amended on June 10, 2026, No. 164-FZ). (1996). *Official Internet Portal of Legal Information*. <http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891>
6. Karaseva, M.Yu. (2007). Kriminologicheskaya kharakteristika poterpevshego [Criminological characteristics of the victim]. *Aktual'nye problemy rossiyskogo prava*, (1(4)), 549–554.
7. Klepitsky, I.A. (2025). Komp'yuternye prestupleniya: voprosy yuridicheskoy tekhniki [Computer crimes: issues of legal drafting]. *Vektoryuridicheskoy nauki*, (5), 48–57. DOI: 10.17803/2311-5998.2025.129.5.048-057
8. Mironov, B.A., & Milaeva, M.Yu. (2024). Sovremennyy vzglyad na ponyatie prestupleniya v sfere komp'yuternoy informatsii [A modern view of the concept of computer-related crime]. *Skif. Voprosy studentcheskoy nauki*, (10(98)), 248–254.
9. Number of cybercrimes in Russia. (2026) *TAdviser*. https://www.tadviser.ru/index.php/Article:Number_of_cybercrimes_in_Russia
10. Pozdyshev, R.S. (2023). Voprosy kvalifikatsii prestupleniy v sfere komp'yuternoy informatsii [Issues of qualification of crimes in the sphere of computer information]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii*, (1(61)), 105–112. DOI: 10.36511/2078-5356-2023-1-105-112
11. Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 dated December 15, 2022, “On Certain Issues of Judicial Practice in Criminal Cases Concerning Crimes in the Sphere of Computer Information, as well as Other Crimes Committed Using Electronic or Information and Telecommunication Networks, Including the Internet”. (2022). *Rossiyskaya Gazeta Internet Portal*. <https://rg.ru/documents/2022/12/28/document-postanovlenie-plenuma-verkhovnogo-suda.html>
12. Shchepelkov, V.F. (2023). O kvalifikatsii prestupleniy v sfere komp'yuternoy informatsii (v svete raz'yasneniy Plenuma Verkhovnogo Suda RF) [On the qualification of crimes in the sphere of computer information (in light of the clarifications of the Plenum of the Supreme Court of the Russian Federation)]. *Ugolovnoe pravo*, (6), 70–79.
13. Suslov, T.V., & Milaeva, M.Yu. (2026) Kriminologicheskii analiz lichnosti kiberprestupnika kak fenomen sovremennogo obshchestva [Criminological analysis of the personality of a cybercriminal as a phenomenon of modern society]. *Skif. Voprosy studentcheskoy nauki*, (1(113)), 145–151.
14. Ugolovnoe sudoproizvodstvo: dannye o naznachennom nakazanii po stat'yam UK RF [Criminal proceedings: data on sentences imposed under articles of the Criminal Code of the Russian Federation]. (2026) *API-Press*. <https://stat.anip-precc.φ/stats/ug/t/14/s/17>