СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1 СОСТАВ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 5

1.1 Компьютерная информация и основание её правовой охраны 5

1.2 Неправомерность доступа и обязательные последствия 7

1.3 Вина и признаки квалифицированных составов 10

ГЛАВА 2 РАЗГРАНИЧЕНИЕ СОСТАВОВ В СУДЕБНОЙ ПРАКТИКЕ 12

2.1 Доступ к чужому аккаунту и пределы служебных полномочий . 12

2.2 Вредоносная информация и нарушение правил эксплуатации 15

2.3 Имущественные посягательства и самостоятельность информационного вреда 18

2.4 Конфиденциальные сведения и граница специального состава .. 20

2.5 Сопоставление оснований судебных решений 22

ЗАКЛЮЧЕНИЕ 25

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 27

ВВЕДЕНИЕ

Успешный вход в информационную систему ещё не означает, что пользователь вправе распоряжаться её данными. Сохранённый в браузере пароль позволяет открыть чужую почту без обхода технической защиты. Сотрудник с рабочей учётной записью может найти сведения об абоненте, хотя частный запрос знакомого не относится к его обязанностям. В таких случаях суду приходится устанавливать, какое именно действие было разрешено. Этим объясняется сложность квалификации по статье 272 УК РФ: факт авторизации и правомерность доступа требуют разной оценки.

Признание доступа неправомерным не завершает квалификацию. Для оконченного преступления по статье 272 нужно установить предусмотренное законом последствие для компьютерной информации. Использование полученных сведений может затем нарушить тайну частной жизни, коммерческую тайну или имущественные права. Суд проверяет признаки каждого посягательства и решает вопрос о совокупности. Бытовое обозначение случившегося как «взлома» здесь мало помогает: оно ничего не говорит о предмете доступа и результате действий.

Работа посвящена вопросу о том, как суды отличают доступ без права от смежных составов. Её цель — выявить критерии разграничения и проверить их на опубликованных судебных актах. Для этого рассматриваются предмет охраны статьи 272, неправомерность доступа и его обязательные последствия. Затем сопоставляются действия постороннего пользователя и сотрудника с доступом к служебным ресурсам, а также основания отдельной квалификации и совокупности преступлений.

Объект исследования — общественные отношения в сфере уголовно-правовой охраны компьютерной информации. Предмет исследования составляют признаки неправомерного доступа и критерии его разграничения с использованием вредоносной информации, нарушением правил эксплуатации, имущественными посягательствами и незаконным обращением с конфиденциальными сведениями. Анализ ограничен этими

вопросами и не охватывает все преступления, совершаемые с применением информационных технологий.

Методы исследования — формально-юридический анализ норм и разъяснений Верховного Суда, сравнительное изучение судебных актов. Дела сопоставляются по правовому режиму информации, полномочиям пользователя, способу обращения к данным, последствиям, умыслу и смежной квалификации.

Эмпирическую основу составляют восемь приговоров и одно апелляционное постановление. В них рассмотрены действия с электронной почтой, социальными сетями, служебными базами, учётными записями государственных услуг и системой спутникового телевидения. Апелляционный акт позволяет подробно изучить основания исключения статьи 272 при сохранении ответственности по статье 273. Подборка служит для сопоставления правовых аргументов; оценивать по ней распространённость отдельных способов преступления было бы некорректно.

Законодательство рассматривается по состоянию на 5 октября 2026 года с учётом статьи 272.1 УК РФ, введённой Федеральным законом от 30 ноября 2024 года № 421-ФЗ. Приговоры, описывающие более ранние деяния, позволяют изучить признаки неправомерности и последствий доступа. Однако при квалификации новых действий с персональными данными требуется учитывать специальную норму[1]. Поэтому в анализе отдельно указываются дата решения и время совершения деяния.

Обезличенные сведения не восстанавливаются. Особый порядок рассмотрения дела ограничивает анализ доказательств. Даты решений приводятся по текстам актов; расхождения с карточками публикации отмечены в списке источников.

---

[1] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

ГЛАВА 1 СОСТАВ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Компьютерная информация и основание её правовой охраны

Компьютерная информация определяется формой представления сведений, а не видом устройства, на котором они находятся. Предметом доступа могут быть данные, обрабатываемые смартфоном, сервером или другим соответствующим устройством. В обвинении нужно указать эти данные и совершённую с ними операцию. Название оборудования само по себе не раскрывает предмет преступления[2].

По статье 6 Федерального закона № 149-ФЗ обладатель информации определяет условия доступа в пределах, установленных законом. Доступ охватывает получение и использование сведений, а их защита включает больше, чем ограничение круга читателей [3]. В частности, разрешение прочитать запись может не распространяться на её изменение, копирование для личных целей или передачу. Объём полномочий следует соотносить с той операцией, которая вменяется обвиняемому.

Пункт 3 постановления Пленума № 37 относит к охраняемой как информацию со специальным режимом конфиденциальности, так и сведения, целостность либо доступность которых защищены средствами, установленными обладателем [4]. Конфиденциальность ограничивает круг получателей, целостность защищает данные от неразрешённых изменений, доступность позволяет законному пользователю работать с ними. Если эпизод затронул несколько этих интересов, обвинение должно раскрыть каждое нарушение через обстоятельства дела.

Открытость сведений для чтения не даёт разрешения изменять исходные данные или лишать других пользователей доступа. При этом

---

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Примечание 1 к ст. 272.
[3] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Ст. 2, 6, 16.
[4] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 о преступлениях в сфере компьютерной информации. П. 3.

электронная форма записи ещё не объясняет, почему информация охраняется уголовным законом. Суду необходимо назвать основание охраны и показать, как оно относится к спорной операции. Без этого рассуждение становится замкнутым: неправомерность выводится из охраняемости, а охраняемость — из предполагаемого нарушения.

Т. В. Якушева и С. А. Горовой предлагают сузить предмет статьи 272 до информации, обеспечивающей функционирование компьютера, и программного обеспечения. По их мнению, сведения, уже защищённые нормами о частной жизни или тайне, должны охраняться соответствующими специальными составами [5]. Эта позиция позволяет поставить вопрос о дублировании уголовно-правовой защиты, однако не описывает действующее содержание статьи. Приговоры о копировании почты и карточек абонентов показывают, что суды применяют статью 272 и к содержательной информации, а не только к программному коду[6].

Сужение предмета статьи 272 оставило бы без самостоятельной оценки нарушение режима данных, если дополнительное посягательство на тайну не доказано или совершено другим лицом. Научное предложение в этом случае расходится с действующим подходом судов. При наличии признаков смежного состава их нужно исследовать отдельно, сохраняя проверку оснований ответственности за доступ.

Закон № 152-ФЗ определяет персональные данные через их связь с прямо или косвенно определяемым физическим лицом и устанавливает требование конфиденциальности [7]. При квалификации по статье 272 выясняются также компьютерная форма сведений, полномочия пользователя и последствие операции. Затем решается вопрос о применимости статьи

[5] Якушева Т. В., Горовой С. А. Неправомерный доступ к компьютерной информации: проблемы квалификации // Проблемы правовой и технической защиты информации. 2024. № 12. С. 117–118.
[6] Приговор Оренбургского районного суда Оренбургской области от 27 февраля 2025 г. по делу № 1-12/2025 (1-314/2024). Приговор Реутовского городского суда Московской области от 18 июля 2024 г. по делу № 1-118/2024.
[7] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Ст. 3, 7.

272.1. Отнесение данных к персональным помогает установить режим охраны, но не отвечает на остальные вопросы.

Для признания сведений коммерческой тайной требуется установленный правовой режим. Закон № 98-ФЗ предусматривает меры по его введению и обязанности работника по соблюдению[8]. При обвинении по статье 183 УК РФ суд проверяет, относятся ли спорные сведения к такой тайне. У статьи 272 могут быть и другие основания охраны, в частности законодательные ограничения доступа к абонентским данным. Поэтому одни и те же сведения способны стать предметом двух составов при разных условиях ответственности.

1.2 Неправомерность доступа и обязательные последствия

Пункт 5 постановления № 37 связывает неправомерность доступа с отсутствием согласия обладателя и необходимых полномочий либо с нарушением порядка, установленного нормативными правовыми актами[9]. Способ входа помогает установить эти обстоятельства. Однако и при подборе пароля, и при использовании сохранённой сессии, и при штатной авторизации суд выясняет, на какие действия пользователь имел право.

В научной дискуссии предлагается разграничивать незаконный вход и неправомерную операцию после законного входа. С. А. Катаев считает проблематичным применение статьи 272 к служебному пользователю, которому ресурс изначально доступен, и связывает эту трудность с границей статьи 274[10]. Такой подход выявляет реальную опасность: квалификация может подменить отсутствие права на доступ простым нарушением трудовой дисциплины. Но из наличия действующего логина ещё не следует право на любой поиск и любое копирование.

---

[8] Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Ст. 10, 11.
[9] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 о преступлениях в сфере компьютерной информации. П. 5.
[10] Катаев С. А. Проблемы уголовно-правовой квалификации ответственности за неправомерный доступ к компьютерной информации // Молодой учёный. 2025. № 24 (575). С. 363–364.

Разрешённую операцию следует описывать достаточно точно. Сотрудник вправе открыть карточку клиента для обслуживания, но частный запрос к той же карточке может выходить за его полномочия. Пароль остаётся прежним; меняется цель и основание обращения к базе. Если же право на операцию сохранялось, а нарушен порядок эксплуатации оборудования, оценка зависит от признаков соответствующего состава. Расширительное толкование неправомерности доступа способно скрыть это различие.

А. О. Аргучинская обращает внимание на роль локальных актов и предлагает уточнить разъяснения о неправомерном доступе[11]. Такие акты могут закреплять перечень разрешённых сотруднику действий. Их содержание нужно читать вместе с законодательством и условиями согласия обладателя: внутренний запрет не устанавливает уголовной ответственности. В служебных делах имеет значение связь нарушенной инструкции с режимом данных и пределами предоставленного доступа.

Для оконченного состава статья 272 предусматривает «уничтожение, блокирование, модификацию либо копирование» информации[12]. Перечень закрыт, поэтому в обвинении должно быть названо и описано конкретное последствие. Недостаточно сообщить, что пользователь вошёл в чужую систему. Нужно показать, что изменилось в самих данных или в возможности законного пользователя работать с ними.

Пункт 6 постановления № 37 требует установить причинную связь и описать все связанные последствия[13]. Если смена пароля вызвала блокирование, суд раскрывает связь между действием и утратой доступа. При оценке модификации необходимо отделять вмешательство обвиняемого от обычных технических процессов. Обновление данных после входа ещё не

[11] Аргучинская А. О. Некоторые проблемные аспекты уголовной ответственности за неправомерный доступ к компьютерной информации // Актуальные исследования. 2024. № 21 (203). Ч. III. С. 12.
[12] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ч. 1 ст. 272.
[13] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 о преступлениях в сфере компьютерной информации. П. 6.

объясняет, какие изменения вызвало лицо и почему они имеют уголовно-правовое значение.

Векленко и Локнов, а также Якушева и Горовой предлагают включить несанкционированное ознакомление в диспозицию статьи 272 [14]. Это предложение изменить закон, а не описание действующего основания ответственности. Когда доказано только чтение сведений, возможна проверка иного состава или признаков покушения. Чтобы признать копирование, суду нужно установить воспроизведение информации; появление текста на экране не позволяет считать этот вопрос решённым.

И. Н. Мосечкин рассматривает уничтожение, блокирование и модификацию данных способами, не связанными с неправомерным доступом, и предлагает отдельно криминализировать такое воздействие [15]. Эта дискуссия обращает внимание на предел статьи 272. Вред данным и доступ к ним представляют разные элементы состава. Даже существенные последствия для потерпевшего не восполняют отсутствие установленного неправомерного доступа.

Вопрос об общественной опасности не сводится к перечню операций. А. Г. Антонов и Д. В. Крюков критикуют уголовно-правовую оценку блокирования, которое не сопровождается иным значительным вредом, и связывают опасность подобных деяний с возможностью дальнейшего причинения вреда другим отношениям[16]. Их вывод относится к обоснованию криминализации и соразмерности. Из него нельзя вывести, что восстановимая блокировка всегда исключает состав действующей статьи.

---

[14] Якушева Т. В., Горовой С. А. Неправомерный доступ к компьютерной информации: проблемы квалификации // Проблемы правовой и технической защиты информации. 2024. № 12. С. 118. Векленко С. В., Локнов А. И. Совершенствование уголовно-правового противодействия неправомерному доступу к компьютерной информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 1 (75). С. 14.

[15] Мосечкин И. Н. О криминализации деяний, направленных на уничтожение, блокирование или модификацию компьютерной информации // Всероссийский криминологический журнал. 2024. Т. 18. № 5. С. 482–493. DOI: 10.17150/2500-4255.2024.18(5).482-493.

[16] Антонов А. Г., Крюков Д. В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего её блокирование // Ленинградский юридический журнал. 2021. № 2 (64).. DOI: 10.35231/18136230_2021_2_168. С. 174–177.

1.3 Вина и признаки квалифицированных составов

Субъективная сторона статьи 272 требует оценки того, как лицо воспринимало свои полномочия и последствия действий. Ошибка в объёме разрешения или технический сбой могут иметь значение для вывода о вине. Суд сопоставляет поведение пользователя с известными ему ограничениями: что он намеревался получить, почему обратился к сведениям и какие последствия охватывались его умыслом. Наличие компьютерных навыков этой оценки не заменяет.

Уголовная ответственность по статье 272 наступает с шестнадцати лет[17]. Для основного состава специальная должность не требуется. При вменении использования служебного положения суд устанавливает, какую возможность дали работа, полномочия или должностное влияние. Важно показать их участие в получении неправомерного доступа, а не ограничиться указанием места работы обвиняемого.

Корыстная заинтересованность описывает мотив, использование служебного положения — способ совершения преступления. При доступе ради обещанного вознаграждения могут присутствовать оба признака. Если сотрудник выполнил частную просьбу без оплаты, оценка использования должности всё равно сохраняет значение. Выражение «служебная выгода» смешивает эти обстоятельства и потому не подходит для их обоснования.

Крупный ущерб и корыстная заинтересованность названы в статье 272 как альтернативные признаки; денежный порог ущерба установлен примечанием к главе[18]. Квалификация по мотиву не означает, что суд установил ущерб такого размера. При анализе дел это различие сохраняется: ни строгость наказания, ни предположение о рыночной стоимости сведений не служат доказательством имущественного последствия.

До выбора части статьи 272 проверяется оговорка о случаях, предусмотренных статьёй 272.1. Закон № 421-ФЗ выделил незаконное

[17] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ст. 20.
[18] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ч. 2 ст. 272 и примечание 2.

обращение с компьютерной информацией, содержащей персональные данные, полученной неправомерным доступом или иным незаконным путём [19]. Для выбора нормы существенны происхождение сведений и характер обращения с ними. Установленные факты соотносятся с признаками специального состава.

Применимая редакция закона определяется временем деяния с учётом правил об обратной силе. Приговор 2026 года может относиться к доступу, совершённому до введения статьи 272.1. В таком случае используются статьи 9 и 10 УК РФ; значение законодательного изменения оценивается применительно к положению конкретного лица[20]. Появление новой нормы само по себе не даёт основания ни для безусловной переквалификации, ни для вывода о полной декриминализации прежнего поведения.

Признаки оконченного состава статьи 272 связаны между собой, но каждый требует обоснования. Обвинение должно раскрывать охраняемую информацию, отсутствие права на спорную операцию, последствие и причинную связь, вину и квалифицирующие обстоятельства. Их соотношение показано на рисунке 1. В судебных делах следующей главы видно, какие доказанные факты позволяют сохранить квалификацию, а какие пробелы ведут к её исключению.

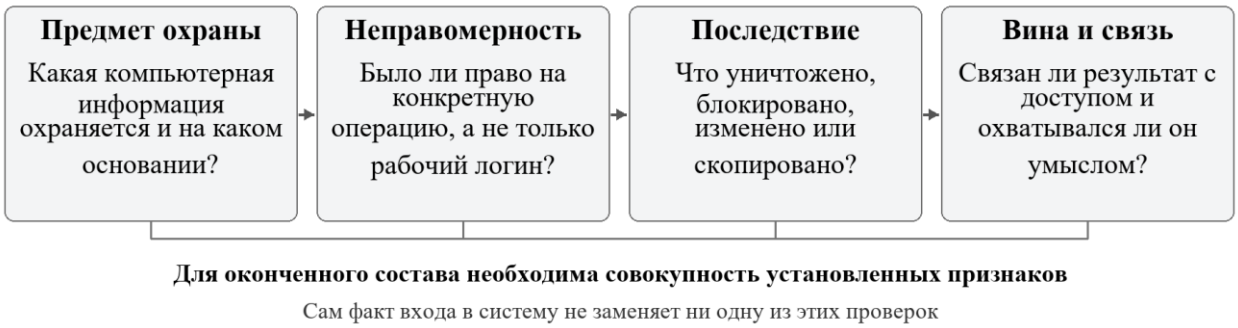


Рисунок 1 — Признаки оконченного состава неправомерного доступа

Источник: составлено по нормам и разъяснениям, рассмотренным в работе.[21]

[19] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».
[20] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ст. 9, 10.
[21] УК РФ. Ст. 272; постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. П. 3–7.

ГЛАВА 2 РАЗГРАНИЧЕНИЕ СОСТАВОВ В СУДЕБНОЙ ПРАКТИКЕ

2.1 Доступ к чужому аккаунту и пределы служебных полномочий

Приговор Оренбургского районного суда от 27 февраля 2025 года по делу № 1-12/2025 показывает, что технически доступный почтовый ящик не обязательно доступен юридически. В браузере ноутбука подсудимой сохранились данные входа в почту бывшего супруга. Обвинение связывало доступ с отсутствием его согласия, а копирование — с фотографированием содержания писем и отправкой фотографий третьему лицу. Подсудимая утверждала, что потерпевший ранее разрешал пользоваться ящиком и сообщил пароль. Суд отверг эту версию после исследования показаний и письменных доказательств и квалифицировал действия по части 1 статьи 272 УК РФ[22].

В этом деле открытая почтовая сессия создавала возможность прочитать письма, а спор касался разрешения бывшего супруга. Суд установил осознанное обращение к охраняемым сведениям и их воспроизведение, не связывая неправомерность с обязательным подбором пароля или применением специальной программы. Фотографии писем позволили описать последствие доступа. Поэтому обвинение вышло за пределы утверждения о том, что подсудимая увидела чужую переписку.

Сохранённая авторизация могла остаться как после разрешённого пользования почтой, так и после незакрытой сессии. Отсюда необходимость проверить версию защиты о прежнем согласии. Техническая возможность входа не оспаривалась; выяснялось право читать и воспроизводить письма. Конституционная охрана тайны переписки объясняет защищаемый интерес[23], тогда как отсутствие согласия и копирование устанавливаются по обстоятельствам эпизода.

---

[22] Приговор Оренбургского районного суда Оренбургской области от 27 февраля 2025 г. по делу № 1-12/2025 (1-314/2024).

[23] Конституция Российской Федерации, принята 12 декабря 1993 г. Ст. 23.

Следственный эксперимент в приговоре использован для проверки версии о пароле. Он позволял оценить конкретный технический довод: могла ли указанная комбинация символов использоваться в сервисе. Вопрос о согласии обладателя решался на основе других обстоятельств. Поэтому убедительность решения связана с общей оценкой версии защиты и следов фотографирования и передачи писем, а не только с результатом эксперимента.

Охрана переписки и частной жизни могла поставить вопрос о статьях 137 и 138, однако суд рассматривал обвинение по статье 272. Приговор подтверждает возможность установить этот состав при доступе через сохранённую сессию и копировании писем посредством фотографирования. Делать из него общий вывод о неприменимости смежных статей оснований нет: самостоятельный вопрос о такой квалификации в деле не разрешён.

Иная конфигурация полномочий раскрыта в приговоре Реутовского городского суда от 18 июля 2024 года по делу № 1-118/2024. Работник салона связи пользовался собственной учётной записью в системе обслуживания. По описанию суда, он обращался к карточкам абонентов по просьбам посторонних лиц за обещанное вознаграждение, фотографировал экран и передавал снимки. Правила работодателя разрешали работу с данными для обслуживания клиента и запрещали частный поиск и передачу. Суд применил часть 3 статьи 272; дело рассмотрено в особом порядке[24].

Реутовское дело отличается от почтового эпизода тем, что пользователь имел штатный доступ к системе. Неправомерность суд связал с обращениями вне служебной задачи. Собственная учётная запись разрешала обслуживать клиентов, но не давала права искать сведения по просьбам посторонних и передавать их за вознаграждение. Таким образом, предметом оценки стал объём служебного разрешения, а не способ преодоления защиты.

[24] Приговор Реутовского городского суда Московской области от 18 июля 2024 г. по делу № 1-118/2024.

Закон о связи устанавливает ограниченный режим абонентской информации, а инструкция определяет разрешённые сотруднику операции[25]. В приговоре эти основания соотнесены с частными запросами к базе. Фотографирование описывает копирование, обещанное вознаграждение — корыстную направленность. Судебная квалификация опирается на получение и воспроизведение конкретных сведений за пределами полномочий сотрудника.

Особый порядок рассмотрения Реутовского дела не даёт возможности проследить спор о доказательствах каждой операции. Приговор полезен для изучения принятой квалификации служебного доступа, но его аргументацию нельзя без проверки переносить на любое нарушение инструкции. В другом деле потребовалось бы заново установить режим информации и содержание предоставленных работнику полномочий.

Приговор Октябрьского районного суда г. Рязани по делу № 1-90/2024 показывает другую форму использования служебного положения. Согласно опубликованному тексту, оперуполномоченный по частной просьбе знакомого получал и копировал сведения из ведомственных ресурсов без служебной необходимости. Использовались данные входа других сотрудников и обусловленная должностью возможность воздействовать на лиц, имевших доступ. Суд прямо связал часть 3 статьи 272 с этим использованием служебного положения. Корыстное вознаграждение не положено в основу квалификации; мотив описан как неправильно понятая дружба[26].

Возражение Катаева о границе статей 272 и 274 позволяет проверить, достаточно ли определённо суд описал запрещённое действие. В рассмотренных служебных делах речь идёт о частных запросах и копировании вне полномочий сотрудника. Это отличается от обычного начала рабочего сеанса. Убедительность квалификации зависит от того,

[25] Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Ст. 53. Приговор Реутовского городского суда Московской области от 18 июля 2024 г. по делу № 1-118/2024.
[26] Приговор Октябрьского районного суда г. Рязани по делу № 1-90/2024 (1-431/2023).

насколько точно установлено разрешение на конкретную операцию. При расплывчатом описании обязанностей сохраняется риск подмены уголовно значимой неправомерности нарушением трудовой дисциплины[27].

2.2 Вредоносная информация и нарушение правил эксплуатации

Статья 273 отличается от статьи 272 прежде всего предметом запрета. Она оценивает обращение с программой или иной компьютерной информацией, заведомо предназначенной для несанкционированного воздействия. Статья 272 требует установить неправомерный доступ к охраняемым данным и результат такого доступа. Поэтому наличие вредоносного средства не является готовым доказательством второго состава. Совокупность возможна, когда признаки обоих преступлений установлены самостоятельно[28].

В приговоре Ковровского городского суда от 27 февраля 2025 года по делу № 1-150/2025 рассмотрено использование модифицированных смарт-карт для получения доступа к закрытым спутниковым каналам без абонентской платы. Суд описал изменённые сведения о подписках, не соответствовавшие данным оператора, и доступ посредством копирования и обработки служебной информации. Действия квалифицированы по частям 2 статей 272 и 273. Применительно к статье 273 предметом стала иная компьютерная информация; дело рассмотрено в особом порядке[29].

Ковровское дело расширяет круг рассматриваемых предметов доступа: служебные сообщения системы условного доступа имеют собственное назначение и режим охраны. Смарт-карта объясняет механизм действий, тогда как правовая оценка относится к её данным. Суд описал отличие изменённой информации от сведений оператора и её использование для несанкционированного получения доступа. Эти обстоятельства позволяют

---

[27] Катаев С. А. Проблемы уголовно-правовой квалификации ответственности за неправомерный доступ к компьютерной информации // Молодой учёный. 2025. № 24 (575). С. 362–365.
[28] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ст. 272, 273.
[29] Приговор Ковровского городского суда Владимирской области от 27 февраля 2025 г. по делу № 1-150/2025.

обсуждать каждый состав отдельно от самого наличия материального носителя.

Разграничение требует сопоставлять предмет посягательства, действия и обязательные признаки каждого состава. Основные различия сведены в таблицу 1.

Таблица 1 — Основания разграничения статьи 272 и смежных составов

Норма УК РФ	Что устанавливается отдельно	Граница со статьёй 272
Статья 273	Заведомое предназначение программы или иной информации для запрещённого воздействия	Средство воздействия не доказывает самостоятельный доступ и его последствия
Статья 274	Нарушенные правила, обязанность их соблюдать, последствия и крупный ущерб	Нарушение правил законным пользователем отличается от отсутствия права на операцию
Статьи 159 и 159.6	Обман человека либо вмешательство в процесс обработки информации для завладения имуществом	Цифровой способ хищения не заменяет признаков вреда компьютерной информации
Статья 183	Режим охраняемой тайны, способ её получения или разглашения и иные признаки выбранной части	Копирование и разглашение могут образовать совокупность при доказанности обоих составов
Статьи 137 и 138	Личная или семейная тайна либо тайна переписки; способ посягательства	Конфиденциальность данных сама по себе не устанавливает эти специальные составы
Статья 272.1	Персональные данные, незаконное происхождение, предусмотренные действия и исключения	Проверяется специальная норма с учётом времени деяния и оговорки в статье 272

Источник: сопоставление норм УК РФ и разъяснений Верховного Суда.[30]

Другой результат отражён в апелляционном постановлении Свердловского областного суда от 7 мая 2024 года по делу № 22-3412/2024. Нижестоящий суд признал руководителя виновным по статьям 272 и 273 за действия, связанные с применением программы-патчера к релизам «1С». Областной суд сохранил квалификацию подстрекательства к использованию вредоносной программы. Осуждение по статье 272 он отменил, прекратив дело в этой части за отсутствием состава. Мотивированное постановление изготовлено 13 мая 2024 года[31].

---

[30] УК РФ. Ст. 137, 138, 159, 159.6, 183, 272–274; постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. П. 12, 15, 16; постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48. П. 20, 21.

[31] Апелляционное постановление Свердловского областного суда от 7 мая 2024 г. по делу № 22-3412/2024.

Апелляционный суд обратил внимание на правомерное получение программ, характер защиты программного кода и отсутствие в обвинении доступа к бухгалтерским данным. Также он указал на дефект описания последствия: изменение исполняемых файлов было одновременно представлено как способ преодоления защиты и как результат доступа. Иные изменения, копирование или блокирование информации не получили самостоятельного описания [32] . Таким образом, исключение статьи 272 основано на проверке конкретного обвинения, а не на признании любой модификации программы допустимой.

Апелляция потребовала объяснить, какая охраняемая информация стала предметом неправомерного доступа и какое последствие вызвал именно этот доступ. Ответственность за участие в использовании вредоносной программы сохранилась, однако её признаки не восполнили пробелы обвинения по статье 272. Для разграничения оказалось решающим различие между нейтрализацией программной защиты и самостоятельным нарушением режима данных.

Статья 1280 ГК РФ регулирует определённые действия правомерного владельца экземпляра программы или базы данных [33] . Областной суд обратился к ней при оценке доступа к полученной программе и охраняемых отношений. Значение этой ссылки ограничено обстоятельствами обвинения. Она не даёт общего разрешения обходить защиту; сохранение квалификации по статье 273 также исключает вывод о законности всех действий подсудимого.

Статья 274 образует ещё одну границу. В её основном составе необходимы нарушение указанных законом правил, информационное последствие и крупный ущерб. Пункт 12 постановления № 37 требует установить конкретные правила и обязанность лица их соблюдать; локальные акты могут учитываться при предусмотренной разъяснением связи с

[32] Апелляционное постановление Свердловского областного суда от 7 мая 2024 г. по делу № 22-3412/2024.
[33] Гражданский кодекс Российской Федерации. Часть четвёртая: Федеральный закон от 18 декабря 2006 г. № 230-ФЗ. Ст. 1280.

законодательством [34] . Отсюда нельзя вывести, что наличие инструкции автоматически исключает статью 272 либо что всякое её нарушение позволяет применить статью 274.

Самостоятельного приговора по статье 274 в изученной подборке нет. Разграничение с ней основано на законе и разъяснениях Пленума; служебные дела позволяют изучить применение статьи 272, но не судебное исключение статьи 274 при тех же обстоятельствах. Материал поэтому недостаточен для вывода об единообразии практики на этой границе.

2.3 Имущественные посягательства и самостоятельность информационного вреда

Приговор Промышленного районного суда г. Оренбурга от 28 февраля 2024 года по делу № 1-133/2024 описывает захват профиля социальной сети. Подсудимая получила чужие учётные данные, изменила пароль, отправляла сообщения от имени владельца с целью обмана другого пользователя и затем удалила переписку. Суд признал блокирование, модификацию и уничтожение информации и применил часть 2 статьи 272. Производство по обвинению в мошенничестве по части 1 статьи 159 прекращено вследствие истечения срока давности[35].

Прекращение преследования за мошенничество в Оренбургском деле не затронуло оценку действий с аккаунтом. Смена пароля и удаление переписки получили самостоятельную квалификацию. При этом срок давности является указанным судом основанием прекращения имущественного обвинения. Он не означает, что обман признан недоказанным. Различие между процессуальным решением и оценкой обстоятельств важно сохранить при сопоставлении составов.

Пункты 20 и 21 постановления Пленума № 48 различают целенаправленное вмешательство в процесс обработки информации,

[34] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 о преступлениях в сфере компьютерной информации. П. 12.
[35] Приговор Промышленного районного суда г. Оренбурга от 28 февраля 2024 г. по делу № 1-133/2024.

использование чужих учётных данных и обман посредством ложных сведений в сети[36]. В частности, для статьи 159.6 необходимо воздействие, нарушающее установленный процесс и позволяющее завладеть имуществом. Штатное изменение записи о счёте вследствие использования чужой авторизации не считается само по себе таким воздействием. Это разъяснение препятствует квалификации по одному цифровому внешнему признаку.

Иную имущественную ситуацию содержит приговор Южно-Сахалинского городского суда от 11 марта 2024 года по делу № 1-435/2024. После получения доступа к чужим ресурсам подсудимый использовал персональные сведения для оформления займа от имени другого человека. Суд описал обман сотрудника микрофинансовой организации и квалифицировал имущественное деяние по части 1 статьи 159, а эпизоды доступа — по части 2 статьи 272. Дело рассмотрено в особом порядке[37].

В Южно-Сахалинском деле выбор статьи о мошенничестве объясняется механизмом выдачи займа. Суд описал обман относительно личности заявителя и намерения исполнить обязательство. Направление заявки через сайт не изменило этого основания: ресурс использовался для обращения и оформления, а имущество получено посредством введения сотрудника организации в заблуждение. Для статьи 159.6 пришлось бы установить иной характер воздействия на процесс обработки информации.

Приговор Ивановского районного суда от 22 января 2026 года по делу № 1-19/2026 раскрывает похожий способ получения доступа к порталу государственных услуг. Суд описал использование сим-карт и кодов авторизации для восстановления доступа к чужим записям, блокирование информации и копирование сведений для оформления займов. Деяния относятся к октябрю 2023 года; рассмотренное обвинение квалифицировано

[36] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 о мошенничестве, присвоении и растрате (с изменениями от 15 декабря 2022 г.). П. 20, 21.
[37] Приговор Южно-Сахалинского городского суда Сахалинской области от 11 марта 2024 г. по делу № 1-435/2024.

по части 2 статьи 272. В акте отдельно упоминается прежний приговор по иным эпизодам, который не заменяет квалификацию настоящего дела[38].

Ивановское дело показывает значение средства авторизации и времени деяния. Полученный через сим-карту код дал техническую возможность войти, но не подтвердил право действовать от имени обладателя записи. Одновременно приговор 2026 года относится к действиям октября 2023 года. Поэтому его квалификация по статье 272 не свидетельствует о применении этой нормы к поведению после введения статьи 272.1.

Тот же подход необходим при использовании мобильного банка. Если денежные средства изымаются с применением чужой авторизации без незаконного воздействия на программное обеспечение или сеть, Пленум ориентирует на квалификацию хищения как кражи[39]. Но вывод о статье 158 не устанавливает автоматически состав статьи 272. Нужно отдельно показать неправомерный доступ к охраняемой информации и предусмотренное последствие. Одного изменения остатка на счёте вследствие обычной обработки перевода для всей совокупности недостаточно.

При разграничении имущественных составов устанавливаются адресат воздействия и способ завладения деньгами. Обман сотрудника организации, использование чужой авторизации и вмешательство в автоматизированный процесс имеют разные правовые признаки. Для дополнительной оценки по статье 272 нужно описать результат обращения с охраняемыми данными. Такое разделение позволяет обосновать совокупность, не выводя её из одного лишь использования цифрового сервиса.

2.4 Конфиденциальные сведения и граница специального состава

Приговор Усть-Илимского городского суда от 21 августа 2024 года по делу № 1-215/2024 содержит прямую совокупность статей 272 и 183.

---

[38] Приговор Ивановского районного суда Ивановской области от 22 января 2026 г. по делу № 1-19/2026 (1-111/2025).

[39] Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 о мошенничестве, присвоении и растрате (с изменениями от 15 декабря 2022 г.). П. 21.

Работник офиса продаж обращался через собственный логин к абонентским сведениям, фотографировал полученные данные и направлял изображения знакомым. Суд указал на служебные ограничения, подписанные обязательства и режим коммерческой тайны. Действия признаны неправомерным доступом с копированием по части 3 статьи 272 и разглашением доверенных по работе сведений по части 2 статьи 183[40].

В Усть-Илимском деле одна фотография могла участвовать в доказательстве разных действий. Для статьи 272 существенны полномочия на обращение к базе и воспроизведение информации. Статья 183 требует установить режим коммерческой тайны, доверенность сведений либо их известность по работе и передачу без согласия владельца. Способ копирования связывает эпизоды фактически, но правовые основания каждого состава проверяются отдельно.

В Реутовском деле также фигурируют абонентские сведения и фотографирование экрана, однако отдельная квалификация по статье 183 в приговоре не разрешена. Сходства действий недостаточно, чтобы приписать суду вывод о совокупности. Для такой оценки нужно было бы установить режим коммерческой тайны наряду с ограничением доступа к базе. Сравнение двух дел показывает значение именно правового основания охраны сведений.

При применении статей 137 и 138 выясняются содержание сведений и способ посягательства. Конфиденциальные персональные данные могут иметь иной режим, чем личная или семейная тайна либо охраняемая переписка[41]. В почтовом деле суд установил воспроизведение писем. Ответ на вопрос о совокупности зависел бы также от содержания информации и предъявленного обвинения; обязательную дополнительную квалификацию для любого чужого почтового ящика из этого акта вывести нельзя.

---

[40] Приговор Усть-Илимского городского суда Иркутской области от 21 августа 2024 г. по делу № 1-215/2024.

[41] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Ст. 137, 138.

После вступления в силу Закона № 421-ФЗ эта схема требует дополнительного шага. В части 1 статьи 272 прямо оговорено исключение для случаев статьи 272.1. Новая статья регулирует незаконные использование, передачу, сбор и хранение компьютерной информации с персональными данными при указанном законом незаконном происхождении[42]. Поэтому нельзя обосновывать выбор статьи 272 только тем, что практика до изменения закона применяла её к похожим абонентским сведениям.

Примечание 1 к статье 272.1 исключает из её действия обработку данных физическими лицами исключительно для личных и семейных нужд[43]. Чтобы применить это положение, необходимо установить фактическую цель обращения с информацией. Родство с обладателем само по себе такой цели не подтверждает. Даже при неприменимости специальной нормы сохраняется вопрос о праве на доступ и признаках других составов.

Рассмотренные приговоры раскрывают критерии доступа, полномочий и последствий в рамках прежнего регулирования. Отдельного акта о применении статьи 272.1 в подборке нет. Поэтому анализ новой нормы основан на её тексте, а старые решения используются для сравнения признаков. Это ограничение особенно существенно при выборе нормы для деяний с персональными данными после изменения закона.

2.5 Сопоставление оснований судебных решений

При сопоставлении дел различаются основания, от которых зависело решение суда. В почтовом эпизоде проверялось согласие обладателя, в служебных делах — пределы разрешённых операций. Апелляция по программе «1С» сосредоточилась на предмете доступа и его последствиях. В

[42] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».
[43] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

делах о займах и обмане отдельно устанавливался способ завладения имуществом. Сравнение этих оснований приведено в таблице 2.

Сходные технические действия получили различную оценку, поскольку суды исследовали объём согласия, служебные полномочия, режим охраны и результат доступа. Квалификация по статье 272 требует обоснования всех её признаков. Совокупность возникает при установлении дополнительного посягательства, а выбор специальной нормы зависит от её условий и действия закона во времени. Последовательность этих вопросов представлена на рисунке 2.

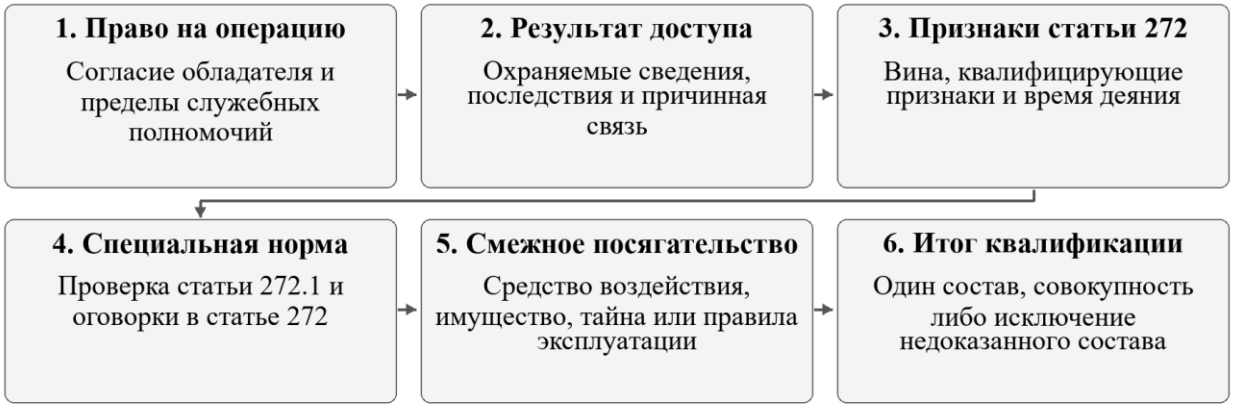


Рисунок 2 — Последовательность проверки основания квалификации

Источник: составлено по нормам и разъяснениям, рассмотренным в работе.[44]

[44] УК РФ. Ст. 9, 10, 272, 272.1; постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. П. 5, 6, 15, 16; апелляционное постановление Свердловского областного суда от 7 мая 2024 г. по делу № 22-3412/2024.

Таблица 2 — Основания разграничения в рассмотренных актах

Дело	Ключевое различие	Принятая квалификация
Почта[45]	Сохранённая сессия не заменяет согласия; фотография подтверждает воспроизведение	Ч. 1 ст. 272
Служебная база[46]	Полномочие ограничено служебной задачей; частный запрос выходит за его пределы	Ч. 3 ст. 272
Социальная сеть[47]	Изменение режима записи оценивается отдельно от обмана адресата	Ч. 2 ст. 272; обвинение по ст. 159 прекращено по давности
Займы[48]	Средство авторизации не даёт права действовать от имени обладателя	Ч. 2 ст. 272; по делу[49] также ч. 1 ст. 159
Коммерческая тайна[50]	Копирование и разглашение требуют разных признаков	Ч. 3 ст. 272 и ч. 2 ст. 183
Смарт-карты[51]	Суд описал средство и доступ к служебной информации	Ч. 2 ст. 272 и ч. 2 ст. 273
Программа «1С»[52]	Недостаток самостоятельных признаков доступа исключает добавление ст. 272	Осуждение по ст. 272 отменено; сохранено подстрекательство к ч. 2 ст. 273

Источник: составлено по опубликованным судебным актам[53].

[45] Приговор Оренбургского районного суда Оренбургской области от 27 февраля 2025 г. по делу № 1-12/2025 (1-314/2024).
[46] Приговор Реутовского городского суда Московской области от 18 июля 2024 г. по делу № 1-118/2024. Приговор Октябрьского районного суда г. Рязани по делу № 1-90/2024 (1-431/2023).
[47] Приговор Промышленного районного суда г. Оренбурга от 28 февраля 2024 г. по делу № 1-133/2024.
[48] Приговор Южно-Сахалинского городского суда Сахалинской области от 11 марта 2024 г. по делу № 1-435/2024. Приговор Ивановского районного суда Ивановской области от 22 января 2026 г. по делу № 1-19/2026 (1-111/2025).
[49] Приговор Южно-Сахалинского городского суда Сахалинской области от 11 марта 2024 г. по делу № 1-435/2024.
[50] Приговор Усть-Илимского городского суда Иркутской области от 21 августа 2024 г. по делу № 1-215/2024.
[51] Приговор Ковровского городского суда Владимирской области от 27 февраля 2025 г. по делу № 1-150/2025.
[52] Апелляционное постановление Свердловского областного суда от 7 мая 2024 г. по делу № 22-3412/2024.
[53] Составлено по приговорам и апелляционному постановлению, приведённым в списке использованных источников под № 11–19.

ЗАКЛЮЧЕНИЕ

Разбор судебных актов позволяет ответить на поставленный вопрос: доступ без права отличают от смежных составов по содержанию разрешённой операции, предмету охраны и наступившему последствию. Успешная авторизация подтверждает техническую возможность входа. Для статьи 272 суд дополнительно устанавливает отсутствие полномочий, изменение состояния охраняемой информации или её копирование, причинную связь и вину. При недостаточном обосновании любого из этих элементов дополнительная квалификация оказывается уязвимой.

В почтовом и служебных делах решающее значение имели границы согласия и полномочий. Сохранённая сессия, собственный рабочий логин или должностное влияние позволяли обратиться к сведениям. Право читать, фотографировать и передавать их суд проверял по обстоятельствам конкретного эпизода. Такой подход требует доказать содержание разрешения, иначе конфликт с обладателем или нарушение инструкции могут ошибочно получить уголовно-правовую оценку.

Апелляционное дело о программе «1С» показало последствия недостаточного разграничения статей 272 и 273. Ответственность за подстрекательство к использованию вредоносной программы сохранилась, а осуждение за доступ было отменено. Признаки средства воздействия не восполнили отсутствие самостоятельного описания предмета доступа и его результата. Этот акт подтверждает необходимость обосновывать каждый состав при вменении совокупности.

На границе со статьёй 274 выясняется, имел ли пользователь право на спорную операцию и какие правила был обязан соблюдать. Трудовые отношения сами по себе не определяют квалификацию. В работе эта граница рассмотрена по нормам и разъяснениям Пленума: отсутствие отдельного приговора по статье 274 в подборке не позволяет сделать вывод о единообразии судебных решений.

В имущественных эпизодах выбор нормы зависел от способа получения денег. Обман человека, использование чужой авторизации и вмешательство в обработку данных требуют разной оценки. Обращение через сайт не давало достаточного основания для статьи 159.6. Одновременно доказанные действия с аккаунтом могли сохранить квалификацию по статье 272, даже если преследование за мошенничество прекращалось по сроку давности.

Усть-Илимский приговор позволил проследить совокупность доступа и разглашения коммерческой тайны. Её основанием стали установленные признаки обоих преступлений, а не только закрытый характер базы. При разграничении со статьями 137, 138 и 183 определяются вид охраняемой тайны, полномочия лица и дальнейшее обращение со сведениями. Поэтому похожие действия с абонентскими данными не обязательно получают одинаковую дополнительную квалификацию.

После введения статьи 272.1 выбор нормы для действий с персональными данными требует учитывать специальный состав и оговорку в статье 272. Ранние приговоры сохраняют значение для анализа доступа, но не раскрывают практику новой статьи. Применимая редакция определяется временем деяния и правилами действия закона, что особенно наглядно видно в Ивановском приговоре 2026 года о событиях 2023 года.

Таким образом, квалификация начинается с установления охраняемых сведений и права на конкретную операцию. Затем оцениваются последствия, причинная связь и вина, после чего проверяются признаки смежного преступления и условия специальной нормы. Этот порядок помогает объяснить различия между рассмотренными решениями. Выводы относятся к отобранным делам и позволяют сопоставить судебные аргументы, но не оценить распространённость каждого подхода во всей российской практике.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Дата обращения к электронным источникам — 5 октября 2026 года. Реквизиты судебных актов приводятся по их тексту; расхождения с карточками публикации отмечены отдельно.

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Положения, действующие на 5 октября 2026 г. Электронный текст.

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ. Ст. 2, 6, 9, 16. Электронный текст.

3. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ. Ст. 3, 7. Электронный текст.

4. О коммерческой тайне: Федеральный закон от 29 июля 2004 г. № 98-ФЗ. Ст. 10, 11. Электронный текст.

5. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ. Ст. 53. Электронный текст.

6. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30 ноября 2024 г. № 421-ФЗ. Электронный текст.

7. Гражданский кодекс Российской Федерации. Часть четвёртая: Федеральный закон от 18 декабря 2006 г. № 230-ФЗ. Ст. 1261, 1280. Электронный текст.

8. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. Ст. 23. Электронный текст.

9. 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 от 15 декабря 2022 г. № 37. Электронный текст.

10. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48, с изменениями от 15 декабря 2022 г. П. 20, 21. Электронный текст.

11. Приговор Оренбургского районного суда Оренбургской области от 27 февраля 2025 г. по делу № 1-12/2025 (1-314/2024). В карточке публикации указана дата 26 февраля 2025 г. Электронный текст.

12. Приговор Реутовского городского суда Московской области от 18 июля 2024 г. по делу № 1-118/2024. В карточке публикации указана дата 17 июля 2024 г. Электронный текст.

13. Приговор Октябрьского районного суда г. Рязани по делу № 1-90/2024 (1-431/2023). Карточка публикации датирована 18 января 2024 г.; дата в тексте обезличена. Электронный текст.

14. Приговор Промышленного районного суда г. Оренбурга от 28 февраля 2024 г. по делу № 1-133/2024. В карточке публикации указана дата 27 февраля 2024 г. Электронный текст.

15. Приговор Южно-Сахалинского городского суда Сахалинской области от 11 марта 2024 г. по делу № 1-435/2024. В карточке публикации указана дата 10 марта 2024 г. Электронный текст.

16. Приговор Ивановского районного суда Ивановской области от 22 января 2026 г. по делу № 1-19/2026 (1-111/2025). В карточке публикации указана дата 21 января 2026 г. Электронный текст.

17. Приговор Усть-Илимского городского суда Иркутской области от 21 августа 2024 г. по делу № 1-215/2024. В карточке публикации указана дата 20 августа 2024 г. Электронный текст.

18. Приговор Ковровского городского суда Владимирской области от 27 февраля 2025 г. по делу № 1-150/2025. В карточке публикации указана дата 26 февраля 2025 г. Электронный текст.

19. Апелляционное постановление Свердловского областного суда от 7 мая 2024 г. по делу № 22-3412/2024. Мотивированное постановление изготовлено 13 мая 2024 г.; в карточке публикации указана дата 12 мая 2024 г. Электронный текст.

20. Якушева Т. В., Горовой С. А. Неправомерный доступ к компьютерной информации: проблемы квалификации // Проблемы правовой и технической защиты информации. 2024. № 12. С. 116–119. Электронный текст.

21. Векленко С. В., Локнов А. И. Совершенствование уголовно-правового противодействия неправомерному доступу к компьютерной информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 1 (75). С. 9–15. Электронный текст.

22. Аргучинская А. О. Некоторые проблемные аспекты уголовной ответственности за неправомерный доступ к компьютерной информации // Актуальные исследования. 2024. № 21 (203). Ч. III. С. 12–13. Электронный текст.

23. Катаев С. А. Проблемы уголовно-правовой квалификации ответственности за неправомерный доступ к компьютерной информации // Молодой учёный. 2025. № 24 (575). С. 362–365. Электронный текст.

24. Антонов А. Г., Крюков Д. В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации, повлекшего её блокирование // Ленинградский юридический журнал. 2021. № 2 (64). С. 168–179. DOI: 10.35231/18136230_2021_2_168. Электронный текст.

25. Мосечкин И. Н. О криминализации деяний, направленных на уничтожение, блокирование или модификацию компьютерной информации // Всероссийский криминологический журнал. 2024. Т. 18. № 5. С. 482–493. DOI: 10.17150/2500-4255.2024.18(5).482-493. Электронный текст.