УДК 343.3/7
ББК 67.408.135.1

НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ПРАВОВЫЕ, ТЕХНИЧЕСКИЕ И СОЦИАЛЬНЫЕ АСПЕКТЫ[1]

А. С. Соколов, А. В. Кулаевский, Д. С. Яковлев
Алтайский государственный университет (Барнаул, Россия)

Статья посвящена исследованию проблемы неправомерного доступа к компьютерной информации — одной из ключевых угроз современному обществу. Авторы детально изучают содержание ст. 272 Уголовного кодекса Российской Федерации, определяющей ответственность за незаконные манипуляции компьютерными данными: получение, использование, уничтожение, блокировку, изменение или копирование защищенной законом информации.

Особое внимание уделено динамике данного вида преступности, судебной практике и рекомендациям Верховного Суда Российской Федерации, направленным на обеспечение единообразия судебных решений и правильного толкования норм права.

Уделяется внимание сравнению российского уголовного законодательства с аналогичными нормами зарубежных государств азиатского региона, где подобные правонарушения получили широкое распространение.

Исследуются особенности доказывания по делам о нарушениях информационной безопасности, акцентируется внимание на роли технических специалистов-экспертов.

Обосновывается позиция о принятии комплексных мер противодействия киберпреступности, включающих совершенствование нормативной базы, развитие технического обеспечения защиты информации, внедрение специализированных образовательных программ и информированность населения относительно рисков и способов предотвращения правонарушений в цифровом пространстве.

Ключевые слова: неправомерный доступ к компьютерной информации, цифровые технологии, кибербезопасность, преступность, киберпреступления

ILLEGAL ACCESS TO COMPUTER INFORMATION IN THE CONTEXT OF DIGITAL TRANSFORMATION: LEGAL, TECHNICAL AND SOCIAL ASPECTS

A. S. Sokolov, A. V. Kulaevsky, D. S. Yakovlev
Altai State University (Barnaul, Russia)

The article is devoted to the study of the problem of unauthorized access to computer information, one of the key threats to modern society. The authors study in detail the content of article 272 of the Criminal Code of the Russian Federation, which defines responsibility for the illegal manipulation of computer data: obtaining, using, destroying, blocking, modifying or copying legally protected information. Special attention is paid to the dynamics of this type of crime, judicial practice and recommendations of the Supreme Court of the Russian Federation aimed at ensuring uniformity of judicial decisions and the correct interpretation of legal norms. Attention is paid to the comparison of Russian criminal legislation with similar norms of foreign countries in the Asian region, where such offenses are widespread. The article examines the specifics of evidence in cases of information security violations, with special attention being paid to the role of technical

[1] Исследование выполнено за счет гранта Российского научного фонда № 25–28–02532.

experts. The article substantiates the position on taking comprehensive measures to counter cybercrime, including improving the regulatory framework, developing technical support for information protection, introducing specialized educational programs and informing the public about the risks and ways to prevent offenses in the digital space.

Keywords: illegal access to computer information, digital technologies, cybersecurity, crime, cybercrimes

Doi: https://doi.org/10.14258/ralj(2026)2.18

Неправомерный доступ к компьютерной информации является одним из самых опасных преступлений на сегодняшний день. Повышенная общественная опасность обусловлена тотальной цифровизацией публичных и частных отношений, вследствие чего противоправное воздействие на информационные системы способно причинять существенный вред не только отдельным субъектам, но и значимым социальным институтам. В условиях быстрого развития технологий и цифровизации данный вид преступлений достигает угрожающих масштабов. Неправомерный доступ к компьютерной информации определяется в ст. 272 УК РФ как уничтожение, блокирование, модификацию либо копирование компьютерной информации [1].

Основными формами неправомерного доступа являются использование программных средств для несанкционированного входа в системы, а также физическое вторжение в места хранения информации. Статистические данные подтверждают снижение числа подобных преступлений с 20 в 2024 г. до трех зафиксированных случаев в 2025 г. При этом изменилась структура потерпевших: в настоящее время среди них преобладают юридические лица. Так, из 28 преступлений, зарегистрированных в 2025 г., девять были совершены в отношении организаций, а общий размер причиненного им ущерба составил около 100 тыс. руб. В предшествующие периоды подобные эпизоды в статистике не фиксировались [2].

Правовые последствия неправомерного доступа актуализируют необходимость мониторинга и обеспечения защиты данных. Наказание за такие деяния варьируется от штрафов до тюремного заключения в зависимости от отягчающих обстоятельств. За совершение преступления, предусмотренного ст. 272 УК РФ, может быть назначен штраф 200 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок [1]. Общественное беспокойство по поводу киберпреступлений также реализуется через обращения граждан в правоохранительные органы, что свидетельствует о растущей обеспокоенности общества.

Неправомерный доступ к компьютерной информации влечет серьезные риски для экономики и общества. Уничтожение либо блокирование данных нередко становится причиной значительных финансовых убытков, подрывает доверие к информационным технологиям и снижает их инвестиционную привлекательность. Поэтому важно не только привлекать к ответственности преступников, но и разрабатывать эффективные механизмы предотвращения подобных деяний.

Важной задачей остается повышение уровня информированности граждан о способах защиты своих данных и осознание потенциальных рисков при использовании интернет-ресурсов. Образование и осведомленность о кибербезопасности могут значительно сократить количество жертв неправомерного доступа, а также поспособствовать созданию безопасной цифровой среды для всех.

Следует учитывать, что ответственность по ст. 272 УК РФ может усиливаться с учетом конкретных обстоятельств дела. В частности, если неправомерный доступ использовался как способ совершения мошенничества, содеянное подлежит дополнительной квалификации, например по ст. 159.6 УК РФ [1]. Это подтверждает необходимость комплексной оценки всех фактических данных: цифровые посягательства становятся более технологичными, а способы их совершения — более вариативными, что усложняет правовую квалификацию.

Существенное значение имеет и введение в 2024 г. ст. 272.1 УК РФ, предусматривающей ответственность за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной

информации, содержащей персональные данные, а также за создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения [1]. Указанная новелла подчеркивает приоритет охраны информации в цифровом обществе. При квалификации соответствующих деяний необходимо учитывать не только национальные нормы, но и международные правовые акты в сфере информационной безопасности, поскольку они также влияют на выбор правовой оценки и меры ответственности.

Анализ практики показывает: при рассмотрении дел по ст. 272 УК РФ суды должны опираться на совокупность профильных нормативных источников, что особенно важно в условиях роста числа и разновидностей правонарушений в цифровой среде. В целом уголовно-правовая природа деяний, подпадающих под ст. 272 УК РФ, остается многоаспектной и требует детального исследования каждого элемента состава преступления. Динамика цифровых технологий предопределяет постоянное обновление законодательства и адаптацию правоприменительных подходов на стадиях расследования и судебного рассмотрения.

Значимую роль в обеспечении единообразия судебной практики играет Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 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”». Документ системно разъясняет применение норм, предусмотренных ст. 272, 273, 274, 274.1 УК РФ, и ориентирован на единообразное толкование закона в условиях стремительного технологического развития.

Постановление акцентирует необходимость углубленной оценки доказательств по делам о неправомерном доступе, поскольку такие преступления имеют одновременно правовую и техническую специфику. В этой связи особое значение приобретают современные методы анализа цифровой информации, позволяющие достоверно установить обстоятельства нарушения. Среди ключевых подходов выделяется требование тщательно выяснять, каким способом и с какой целью обвиняемый получил доступ к данным. Иными словами, мотив и цель действий рассматриваются как существенные элементы квалификации.

Кроме того, Пленум обращает внимание на особенности функционирования электронных систем и механизмов защиты информации, что требует постоянного обновления профессиональных компетенций как судей, так и иных участников процесса. Отдельно подчеркивается: ссылки на «обоснованность» несанкционированного доступа не могут приниматься во внимание, если установлен прямой умысел на совершение преступления [3]. Следовательно, установление умысла выступает центральным критерием правовой оценки содеянного и способствует повышению правовой определенности.

Практическая значимость указанных разъяснений подтверждается судебными делами. Так, по делу № 1–226/2023, рассмотренному Пролетарским районным судом г. Тулы, оценивалась квалификация действий подсудимого по совокупности преступлений, предусмотренных ч. 1 ст. 273 и ч. 1 ст. 137 УК РФ. Существенным для правовой оценки стало установление последствий неправомерного доступа, включая копирование и модификацию сведений [4]. Для применения ст. 272 УК РФ суду потребовалось доказать причинно-следственную связь между действиями лица и конкретным результатом (например, блокированием или уничтожением компьютерной информации), а также учитывать легальное определение компьютерной информации как любых сведений в форме электрических сигналов независимо от способа их хранения, обработки и передачи [3; 4].

Сопоставимые выводы содержатся и в решении по делу № 1–439/2023 Ленинского районного суда г. Владимира, где также рассматривались вопросы неправомерного доступа и модификации охраняемой законом компьютерной информации. Суд установил умышленный характер действий подсудимого и наличие подтвержденных последствий, что непосредственно повлияло на квалификацию деяния и перспективу уголовного преследования [5].

Анализ судебной практики показывает, что неправомерный доступ может быть квалифицирован как оконченное преступление в случаях, когда созданы вредоносные программы, позволяющие получить доступ к компьютерной информации. Судебные решения в таких делах строго следят за тем,

чтобы квалификация преступления соответствовала фактическим обстоятельствам и правовым нормам [6].

Защита прав потерпевших от неправомерного доступа к компьютерной информации возникает как критически важная задача в условиях роста компьютерной преступности. Применение ст. 272 УК РФ позволяет квалифицировать действия таких преступников, однако это не всегда просто. Для начала уголовного преследования достаточно установить, что был создан фрагмент вредоносной программы, позволяющей осуществить неправомерный доступ к защищенной информации. Если создание программы не завершено, действия таких лиц могут быть квалифицированы как создание иной вредоносной информации.

Интересен зарубежный опыт квалификации действий по неправомерному доступу к компьютерной информации. В зарубежном законодательстве стран Азии «неправомерный доступ к компьютерной информации» квалифицируется как преступление против компьютерной системы, данных. Для квалификации необходимо наличие умысла, отсутствие правомерного доступа, наличие действий по обходу системы безопасности, а также выполнение действий для получения, копирования данных и нацеленных на причинение вреда системе безопасности.

К примеру, в Японии законом о запрете несанкционированного доступа к компьютерам (Acton Prohibition of Unauthorized Computer Access) закрепляется понятие «несанкционированный доступ» (unauthorized access) в качестве уголовно наказуемого деяния. За неправомерный доступ предусмотрено наказание до 3 лет лишения свободы или штраф [7].

В Сингапуре законом о неправомерном использовании компьютеров и кибербезопасности (Computer Misuse and Cybersecurity Act) регламентируются неправомерные действия, направленные на получение доступа к компьютерному устройству без установленного разрешения. Законом устанавливается наказание до 5000 долларов или до 2 лет лишения свободы [8].

Индия также в разделе 66 Закона об информационных технологиях (Information Technology Act) устанавливает уголовную ответственность за доступ к компьютерной информации обманным путем. Законом предусмотрено наказание до 3 лет или штраф [9].

В Китае законодатель устанавливает классификацию неправомерного доступа к компьютерной информации. В ст. 285 Уголовного закона упоминается ответственность за различные действия: незаконное вторжение; незаконный доступ; незаконный контроль системы; а также ответственность за предоставление «инструментов» для таких действий [10]. Интересен пример законодательства Южной Кореи, отличавшийся установлением ответственности за нарушение норм об установлении секретного делопроизводства для информации о защите передаваемой и обрабатываемой конфиденциальной информации в сети. Например, ст. 48 Закона об информационно-коммуникационных сетях (Information and Communications Network Act, Article 48) [11].

Защита прав потерпевших по делам о неправомерном доступе к компьютерной информации требует не только высокой правовой подготовки, но и понимания технических аспектов инцидента. В каждом случае необходимо установить способ несанкционированного доступа, его механизм и наступившие последствия. Существенную роль здесь играют специалисты в области ИТ и цифровой криминалистики, чьи заключения позволяют обосновать позицию потерпевшей стороны.

Ключевые процессуальные механизмы защиты связаны с обращением в правоохранительные органы и своевременной фиксацией события преступления. Эффективность правовой защиты во многом зависит от качества доказательственной базы: журналов доступа, сведений о вредоносном ПО, сетевых логов, данных с носителей и иных цифровых следов, подтверждающих противоправные действия. Достоверность и полнота собранных материалов непосредственно влияют на перспективы дальнейшего судебного разбирательства [12].

Противодействие неправомерному доступу должно опираться как на действующее законодательство, так и на современные практики информационной безопасности. В условиях ускоренной цифровизации необходима многоуровневая защита, охватывающая и частных пользователей, и организации. Пользователям следует соблюдать базовые правила цифровой гигиены: критически оценивать интернет-контент, не переходить по подозрительным ссылкам, избегать фишинговых ресур-

сов и не использовать небезопасные публичные Wi-Fi-сети, способные создать условия для перехвата данных [13].

Существенно снижает риски применение сложных уникальных паролей и двухфакторной аутентификации, особенно в отношении онлайн-сервисов с персональными и финансовыми данными. Для организаций важны регламентированная парольная политика, регулярная смена учетных данных сотрудников и приведение внутренних стандартов к актуальным требованиям кибербезопасности [14].

Отдельное внимание должно уделяться безопасному использованию физических носителей. Подключение неизвестных или временно полученных USB-устройств может привести к заражению систем и компрометации информации, масштаб которой нередко невозможно определить немедленно. Поэтому обучение пользователей правилам работы с носителями является обязательным элементом профилактики.

Не менее значима физическая защита ИТ-инфраструктуры: ограничение доступа к оборудованию и данным, применение замков, систем видеонаблюдения, проведение регулярной инвентаризации, а также внедрение четких процедур контроля доступа. Эти меры уменьшают вероятность несанкционированного вмешательства на уровне инфраструктуры.

Организациям целесообразно системно развивать программы обучения персонала по вопросам киберугроз и способов реагирования. Осведомленность сотрудников о типичных схемах атак, социальной инженерии и признаках инцидентов позволяет снижать число ошибок, вызванных человеческим фактором. В корпоративной среде должна формироваться культура оперативного уведомления о подозрительных действиях и попытках мошенничества, что обеспечивает своевременное реагирование.

В целом обеспечение безопасности возможно только при согласованных действиях государства, бизнеса и граждан. Неправомерный доступ к компьютерной информации представляет собой не только правовую, но и социально-технологическую проблему, требующую сочетания юридических, организационных и технических решений.

В заключение следует отметить, что данная категория преступлений остается одной из наиболее актуальных для современного общества. По мере развития цифровых технологий их формы становятся более сложными и вариативными. Эффективное противодействие возможно лишь при комплексном подходе, объединяющем совершенствование законодательства, качественное правоприменение и повседневные практики кибербезопасности. Осознание ответственности каждым участником цифровых отношений является необходимым условием формирования устойчивой и справедливой системы защиты от киберугроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025, с изм. и доп., вступ. в силу с 20.01.2026) // СПС КонсультантПлюс.

2. Прокуратура информирует // Ординский муниципальный округ: сайт. URL: https://orda-adm.ru/obshhestvo-1/bezopasnost-1/prokuratura_informirujet/24174/?ysclid=mkqeew9u4w53605301 (дата обращения: 23.01.2026).

3. 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 Российской Федерации от 15.12.2022 № 37 // СПС КонсультантПлюс.

4. Приговор от 05.07.2023 по делу № 1–226/2023 Пролетарского районного суда г. Тулы (Тульская область) // Судебные решения РФ: сайт. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/software/%D0%94%D0%B5%D0%BB%D0%BE%201–2262023%20 (%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F%20273%20%D0%A3%D0%9A%20%D0%A0%D0%A4) %20 (%D0%92%D0%B5%D0%B1-.pdf (дата обращения: 23.01.2026).

5. Приговор от 17.01.2024 по делу № 1–439/2023 Ленинского районного суда г. Владимира (Владимирская область) // Судебные и нормативные акты РФ: сайт. URL: https://sudact.ru/regular/doc/m9BSsgO0B7dw/?ysclid=mkqf21on52812404202 (дата обращения: 23.01.2026).

6. Неправомерный доступ к охраняемой законом компьютерной информации: судебная практика // Главный радиочастотный центр: сайт. URL: https://4people.grfc.ru/analytics-and-legislation/analysis-practice-ru/nepravomernyy-dostup-k-ohranyaemoy-zakonom-kompyuternoy-informacii-sudebnaya-praktika/ (дата обращения: 23.01.2026).

7. Japanese Law Translation. URL: https://www.japaneselawtranslation.go.jp/en/laws/view/3933/ja (дата обращения: 27.03.2026).

8. Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act-Rev/50A/Published?DocDate=20070731&ProvIds=P1II- (дата обращения: 27.03.2026).

9. UNODC (United Nations Office on Drugs and Crime). The Information Technology Act, 2000: Chapter XI, Sections 65–66. URL: https://www.unodc.org/cld/en/legislation/ind/the_information_technology_act_2000/chapter_xi/sections_6566/sections_65–66.html (дата обращения: 27.03.2026).

10. UNODC (United Nations Office on Drugs and Crime). Criminal Law of the People's Republic of China: Part Two, Chapter VI, Article 285. URL: https://www.unodc.org/cld/en/legislation/chn/criminal_law_of_the_peoples_republic_of_china/part_two-_chapter_vi/article_285/article_285.html? (дата обращения: 27.03.2026).

11. Case Note. 정보통신망이용촉진및정보보호등에관한법률제49조 (비밀등의보호). URL: https://casenote. kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D_%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84_%EB%B0%8F_%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8_%EB%93%B1%EC%97%90_%EA%B4%80%ED%95%9C_%EB%B2%95%EB%A5%A0/%EC%A0%9C49%EC%A1%B0 (дата обращения: 27.03.2026).

12. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // СПС КонсультантПлюс.

13. Уголовно-правовые риски в условиях цифровизации: способы противодействия // СПС Гарант.

14. Прокуратура Комсомольского района разъясняет: «Как обезопасить себя от преступлений в сфере информационных технологий или киберпреступности?» // Администрация Комсомольского муниципального района: сайт. URL: https://adminkoms37.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_455.html (дата обращения: 23.01.2026).