УДК 004.056:34 **DOI: 10.34670/AR.2026.21.94.053**

Перехват информации: правовые проблемы разграничения с неправомерным доступом

Кальтенбергер Никита Александрович

Аспирант,
Национальный исследовательский университет
«Московский институт электронной техники»,
124498, Российская Федерация, Москва, Зеленоград, пл. Шокина, 1;
e-mail: mnnnp@mail.ru

Аннотация

Данное исследование посвящено сравнительно-правовому анализу уголовно-правовых категорий в области неправомерного доступа к компьютерной информации. В частности, подвергаются исследованию такие категории, как неправомерный доступ и перехват информации. Сложности уголовно-правовой квалификации данных деяний обусловлены тем, что современные технологические приемы и механизмы позволяют перехватывать информацию без взлома или иного прямого неправомерного доступа к системе. Автор предлагает расширить сферу применения статьи 272 Уголовного кодекса Российской Федерации, которая посвящена неправомерному доступу к компьютерной информации, посредством включения категории перехвата в качестве уголовно наказуемого деяния. По мнению автора, это приведет уголовное право в вопросе неправомерного доступа к компьютерной информации к соответствию сложившимся неправомерным правоотношениям, в результате которых злоумышленники иным, не в полной степени урегулированным уголовным правом, способом получают доступ к компьютерной информации, обладая злонамеренным умыслом получить данную информацию в обход действующего законодательства.

Для цитирования в научных исследованиях

Кальтенбергер Н.А. Перехват информации: правовые проблемы разграничения с неправомерным доступом // Вопросы российского и международного права. 2026. Том 16. № 1А. С. 429-438. DOI: 10.34670/AR.2026.21.94.053

Ключевые слова

Перехват информации, неправомерный доступ, уголовно-правовая квалификация, проблемы уголовного права, киберпреступность, компьютерная информация.

Введение

Современная цифровая среда представляет собой неотделимый элемент современного общества поскольку присутствует не только в жизни и деятельности государства, но и обычного человека. Развитие цифровых технологий, которые открывает новые возможности и направления роста для бизнеса и государства порождают за собой ряд всевозможных рисков [Шинкарецкая, 2019, с. 120]. А фактор развития неотъемлемо влечёт необходимость в усовершенствовании нормативно-правового регулирования, в том числе и в области уголовного права.

Как верно отмечают ученые: «действие механизма правового регулирования будет способствовать установлению информационно-правового режима, определяющего … порядок урегулирования споров между субъектами информационных отношений, установление государственного контроля за распределением информационно-коммуникационных технологий и другие» [Теоретико-правовая парадигма..., 2022, с. 10].

Актуальность темы исследования по вопросу неправомерного доступа к компьютерной информации и её неправомерного перехвата основана на увеличение качественного и количественного критерия данных неправомерных и общественно опасных деяний.

Так, согласно официальной статистике министерства внутренних дел Российской Федерации 2024 год ознаменовался увеличением количества киберпреступлений на 13% по сравнению с 2023 годом. Количество тяжких и особо тяжких составов киберпреступлений увеличилось примерно на 8%, по сравнению с предыдущим годом [[МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за 2024 год, www].

Также, анализируя статистику министерства внутренних дел необходимо сделать вывод, что порядка 40% из общего количества преступлений составляют именно киберпреступление, что напрямую подчеркивает роль и актуальность правовой квалификации действий в области информационных технологий [[МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за 2024 год, www].

Из этого следует сделать однозначный вывод, что количественное и качественное увеличение киберпреступлений требует системной и вымеренной правовой квалификации преступлений в области компьютерной безопасности.

Актуальность тематики правового регулирования киберпреступлений по аспекту перехвата информации и неправомерного доступа подтверждается активной заинтересованностью государства в регулировании сферы цифровых технологий. Интерес государства выражается в создании национального проекта цифровая экономика, который включил в себя меры и механизмы по регулированию цифровой среды, а также механизмы обеспечивающие уровень информационной безопасности [Национальная программа «Цифровая экономика Российской Федерации», www].

Основная часть

Особую роль выполняет государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Значимость данной государственной системы подчёркивает необходимость не только

фактического предупреждения возможных киберпреступлений но и необходимость правового регулирования которое касается метода и способа совершения данного рода преступлений, в частности неправомерного доступа к компьютерной информации или её перехвата

Актуальность вопроса перехвата компьютерной информации и его разграничения с неправомерным доступом основана на дискуссионности аспекта правовой квалификации в рамках неправомерного доступа к компьютерной информации. Так, многие учёные ведут дискурс по вопросу допустимости применения уголовно-правового режима ответственности за неправомерный доступ информации к перехвату информации. Перехват информации и неправомерный доступ имеют, как множество сходств, так и множество различий. Данный сходства и различия находят своё отражение не только возможной правовой квалификации или догматических подходов учёных, но и в вопросах компьютерно-технического характера. Многие эксперты отмечают сложность разграничения перехвата информации и неправомерного доступа к ней. Данные исследования ставит своей целью найти критерий разграничения перехвата и неправомерного доступа к информации с необходимостью последующей справедливой и соответствующей фактическим отношениям уголовно-правовой квалификации деяния.

Предметом исследования выступают общественные отношения которые складываются в результате неправомерного доступа к информации и её перехвата, которые в дальнейшем подвергаются последующий уголовно-правовой квалификации. Объектом исследования выступает подходы учёных, судебная практика и опыт регулирования общественных отношений в области неправомерного доступа и перехвата информации, который складывается в других правопорядках. Методология исследования основана на системном и формально-юридическом методе с использованием сравнительно правовых конструкций.

Перед тем как перейти к критике и возможно предложением по правовой квалификации неправомерного доступа к информации и перехвата необходимо обозначить общие особенности и черты, которые присущи высокотехнологичный преступности в современных условиях.

В частности, высокотехнологичная преступность выступает набором преступлений, которые реализуются при использовании информационных компьютерных и других высокотехнологичных устройств и механизмов [удрин, Бегтин, Кучерена, Ларина и др., 2016, с. 125-130].

Терминологический дискурс по аспекту определение групп преступлений отражён и в рамках российского юридического сообщества, поскольку группы учёных по-разному определяют данные группы преступлений, в частности указывая на такие категории, как компьютерная преступность [Иванов, Кондрат, 2024, с. 2-9], киберпреступность [Евдокимов, 2021, с. 69-72], или цифровая преступность [Поляков, 2023, с. 117-126].

С позиции прямого толкования действующего законодательства стоит сказать что высокотехнологичные преступность включает в себя ряд следующих преступлений. В частности к ним относятся, неправомерный доступ к компьютерной информации, её незаконное использование или использования и создание вредоносных компьютерных программ, а также нарушение порядка хранения и обработки данной информации, которая включает в себя и неправомерное взаимодействие с информационными системы, которые принадлежат государству. Правоприменитель, в вопросе высокотехнологичных преступлений дифференцируют их в зависимости от использования электронных или информационно-телекоммуникационных сетей [Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37, 2022].

Основная проблематика заключается в том, что не законодатель ни правоприменитель не могут достигнуть полноценного баланса в вопросе правовой квалификации и ежедневно совершенствующихся методов совершения киберпреступлений. Однако такой метод, как перехват информации представляется вполне популярным способом совершения киберпреступлений, как в россии, так и во всём мире.

До этапа реформы уголовного законодательства в нём отсутствовала такая нормативная категория, как компьютерная информация. Ранее неправомерный доступ к компьютерной информации не учитывал понятие таковой информации, положение данной статьи указывали лишь на необходимость носителя данной информации. В свою очередь - это порождало определённый дискурс по вопросу понимание уголовным законодательством сущностные характеристики состава преступления [Федеральный закон от 07.12.2011 № 420-ФЗ, 2011].

Современное нормативное регулирование не содержит единого подхода по вопросу киберпреступлений вследствие этого реформа носит хаотичный характер [Хисамова, 2016, с. 346].

Однако в последующем были внесены сущностные изменения, которые унифицировали и систематизировали понятийно-правовой аппарат в области киберпреступлений [Федеральный закон от 11.07.2011 № 200-ФЗ, 2011].

Стоит отметить, что компьютерная информация, к которой отсылает статья 272 уголовного кодекса Российской Федерации, напрямую связаны с цифровой информацией иными схожими категориями информации. Необходимо принять за основу нормативную категорию компьютерной информации, толкуя в расширительном понимании, поскольку современные тенденции цифровых направлений задают новые векторы для развития различающихся между собой видов информации, но в сущности схожих.

Допустимо прийти к выводу что компьютерная информация является в реальности одним из видов цифровой информации, поскольку нормативное регулирование указывают, что компьютерная информация наличествует исключительно в рамках компьютерной системы, которая является лишь частью общего информационно-цифрового пространства.

Современное нормативное определение компьютерной информации включает в себя не только данные которые могут быть в форме электрических сигналов вне зависимости от средств и методов их существования, но и включает в себя любую информацию, которая может быть записано на цифровой носитель [Кургузкина, Ратникова, 2016, с. 79].

В свою очередь достаточно сложно охарактеризовать единую группу преступлений, которые совершаются при помощи или в рамках информационно-цифровых систем , поскольку они не носят однородный характер. Однако, учёные пытаются вывести общую категорию всех разновидностей киберпреступлений: «виновные общественно опасные деяния, причиняющие ущерб общественным отношениям, связанным с безопасностью охраняемой законом информации, соблюдением установленного законом порядка оборота и использования информационно-телекоммуникационных технологий» [Хисамова, 2017, с. 28].

Один из подходов предполагает исключение особой главы уголовного кодекса, которые регулируют особенности преступления в сфере компьютерной информации, предлагая заимствовать опыт зарубежных правопорядков и сделать неправомерные деяния связанные с компьютерной информацией и её использованием подвидами уже существующих составов преступлений [Трофимцева, Илюшин, Линьков, 2015, с. 3-11].

Противоположного взгляда придерживаются учёные, которые считают что категория преступлений в информационной сфере включает в себя намного больше количество видов и

потенциальных категорий преступлений, что позволяет предусмотреть нормативное регулирование с учётом развития цифровых технологий [Савченко, 2016, с. 156].

Стоит отметить, что современные реалии информационно-цифрового пространства предполагают что существует различные методы несанкционированного доступа к информации, например такие как утечка информации при помощи различных технических средств: средства регистрации информации, средства перехвата информации, средства приёма и съёма информации а также иные методы и способы, которые нарушают безопасность информации [5 Савченко, 2016, с. 156].

В виду постоянно развивающиеся системы преступлений в области информационно-цифровых технологий возникают определённые несоответствия действующего законодательства применительно к современным реалиям. Как отмечают учёные одной из проблем является отсутствие прямого разграничения в уголовном кодексе таких категорий, как перехват информации и неправомерный доступ к ней: «под электромагнитный перехват может попасть цифровая информация, которая циркулирует в пространстве, а для совершения неправомерного доступа необходимо нарушить систему защиты информации информационно-телекоммуникационных устройств» [Бегишев, 2010, с. 255].

Автор предлагает внести изменения в примечание к комментируемой статье, закрепив понятие перехвата компьютерной информации. С одной стороны данный подход, по уточнению в отельных вопросах киберпреступлений представляется оправданным, поскольку с одной стороны, дает возможность правопорядку оценить степень угрозы и соразмерность наказания, а также критерии квалификации для нового вида или способа киберпреступления.

С другой стороны возникает проблема, когда законодатель не успевает регулировать вновь осложняющиеся правоотношения, на время, упуская из своего «вида» потенциально опасные деяния, в связи с чем возникают вопросы квалификации определенных действий, в том числе и в сфере киберпреступлений.

Анализируя опыт страны снг стоит отметить что республика армения криминализировала несанкционированный перехват компьютерной информации, в качестве одного из уголовных преступлений, которые связаны с неправомерным использованием компьютерной информации, повлёкшее значительный ущерб [Уголовный кодекс Республики Армения, www].

В методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации генпрокуратура указывает на особенность диспозиции статьи 272 ук рф, в которой уточняется, что неправомерный доступ, который повлек копирование компьютерной информации, является уголовным деянием. Давая расширительное толкование категории копирования, указывается на воспроизведение информации на носителе в материальной форме при помощи перехвата данной информации.

Однако, стоит подвергнуть критике предлагаемое расширительное толкование категории копирования, поскольку осуществление копирования при помощи перехвата выходит за рамки комментируемой статьи. Перехват напрямую не упомянут в качестве одного из предполагаемых способов или методов совершения противоправного деяния в области неправомерного доступа к компьютерной информации. Исходя из этого расширительное толкование выходит за рамки запятая в попытке установить соответствие действующего законодательства с современным компьютерно-информационным реалиям в области совершения таковых преступлений.

Стоит отметить, что в правоприменительной практике находится примеры признания неправомерного перехвата в качестве одного из способов неправомерного доступа к

компьютерной информации. Так, в одном из дел суд квалифицировал действия лица неправомерными поскольку эксперты установили что перечень используемого программного обеспечения которое данное лицо применило в рамках получения доступа к компьютерной информации предполагала возможность перехвата трафика для его последующего анализа и неправомерного использования [Определение Первого кассационного суда общей юрисдикции от 21.04.2020 № 77-530/2020, 2020].

В связи с использованием данного программного обеспечения которое позволило лицо осуществить свой преступный замысел суд квалифицировал действия данного лица как неправомерный доступ к информации в рамках уголовного деяния.

В другом деле, которая рассматривала вопрос о признании кредитного договора недействительным суд сделала отсылку к уголовному делу по статье о неправомерном доступе компьютерной информации. В деле у неправомерном доступе компьютерной информации указывалось, что для перехвата информации использовалась электронная sim-карта, которая позволяла получить доступ к личному кабинету, как на государственных услугах, так и в приложении банка. Тем самым, подключение к телефону потерпевшего иного устройства при помощи которого удалось не только осуществить вход в личные кабинеты с целью неправомерного получения кредита и денежных средств, но и перехватить соответствующую информацию для осуществления неправомерного деяния в совокупности послужило технической возможности для неправомерного доступа к его информации [Апелляционное определение Пермского краевого суда от 22.01.2025 № 33-820/2025, 2025].

Одним из наиболее показательных дел является дело о хищении денег при помощи доступа к счетам лиц. Так, один из преступников использовал интернет бот внедрив в него программное обеспечение, которое позволяло анализировать и собирать данные лиц при помощи перехвата информации. Углубляясь в технические подробности стоит отметить важный аспект, поскольку лица сами вводили в браузерах или приложениях номера карт и иные цифровые идентификаторы, которые позволяли получить доступ к личным кабинетам. Рассуждая на тему неправомерного доступа к компьютерной информации её перехвата при исключительно нормативном толковании положений уголовного кодекса неправомерном доступе к компьютерной информации возможно свести перехват к того рода деянию, которое не предполагает уголовную ответственность. В свою очередь из материалов дела и актов суда допустимо предположить что перехват информации используется исключительно в противоправных целях для завладевания данными потерпевших с целью хищения денежных средств. Исходя из этого суд верно перехват информации с помощью специального программного обеспечения является одним из элементов всей цепочки преступных деяний с целью хищения денежных средств при неправомерном доступе к компьютерной информации [Постановление Московского городского суда от 10.05.2017 № 4у-1093/2017, 2017].

В судебной практике существует один из подходов, который предполагает распознавание перехвата информации в качестве метода или способы неправомерного доступа к компьютерной информации при помощи специальной экспертизы. Так, в одном из дел эксперты установили что на жёстких дисках содержались программы и файлы которые позволяли копировать данные для входа в различные системы при помощи перехвата информации в рамках функционирования программ. Целью использования программ перехватчиков являлось получение доступа к ряду личных кабинетов, а также внедрение собственного вредоносного обеспечения, которое позволяло бы осуществлять удалённый доступ за компьютером потерпевшего [Апелляционное определение Московского городского суда от 22.12.2016 по делу

№ 10-18451/2016, 2016].

Исходя из сложившейся судебной практики стоит не согласиться с позицией ученых, которые квалифицируют деяния связанные с перехватом информации с банковских карт, при помощи специальных устройств и программного обеспечения в рамках уголовного состава преступления, предусмотренного ст. 158 ук рф [Долгих, 2025].

Стоит отметить что аналогичного подхода о перехвате информации, как методе получения скопированной информации в рамках неправомерного доступа придерживается и ряд авторитетных учёных в области уголовного права, однако общей проблемой является не раскрытие категории перехвата информации в качестве одного из возможных способов неправомерного доступа к ней. Также следует поднять правовой вопрос о криминализации исключительно перехвата информации. Является ли преступлением перехват информации без последующего её неправомерного использования или хранения. Возможно ли случайно в отсутствии умысла перехватить информацию. Данные правовые вопросы требуют отдельного философско-правового исследования в области уголовного права, поскольку большинство проблемных аспектов разграничения неправомерного доступа к компьютерной информации её перехвата было раскрыто в данном исследовании [Комментарий к Уголовному кодексу Российской Федерации, 2017].

Заключение

В качестве промежуточного вывода стоит отметить что правоприменительные органы расширительно толкуют понятие неправомерного доступа к компьютерной информации, вследствие чего удаётся идентифицировать перехват информации и квалифицировать его в качестве неправомерного деяния, такого как неправомерного доступа к компьютерной информации. Узкая и исключительно нормативное толкование нормы он неправомерном доступе компьютерной информации позволило бы избежать уголовной ответственности тем лицам которые использовали устройство или приложение а также иные способы для перехвата информации с целью её дальнейшего преступного использования. В этом смысле правоприменитель пусть и в определённой степени выходят за рамки существующего законодательства, но в рамках судебного правотворчества создаёт справедливые прецеденты для привлечения лиц перехватывающих информацию уголовной ответственности.

Библиография

1. Апелляционное определение Московского городского суда от 22.12.2016 по делу № 10-18451/2016. Доступ из СПС «КонсультантПлюс».
2. Апелляционное определение Пермского краевого суда от 22.01.2025 № 33-820/2025 по делу № 2-3634/2024. Доступ из СПС «КонсультантПлюс».
3. Бегишев И.Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект // Информация и безопасность. 2010. № 2. С. 255-258.
4. Долгих Т.Н. Ответственность за хищение денежных средств с банковского счета // СПС КонсультантПлюс. 2025.
5. Евдокимов К.Н. К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. 2021. № 10. С. 69-72.
6. Иванов И.И., Кондрат И.Н. Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий // Мировой судья. 2024. № 12. С. 2-9.
7. Ищейнов В.Я. Системы и сети передачи информации и угрозы ее конфиденциальности // Делопроизводство. 2022. № 4. С. 97-102.

8. Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / А.В. Бриллиантов, А.В. Галахова, В.А. Давыдов и др.; отв. ред. В.М. Лебедев. М.: Юрайт, 2017. Т. 3: Особенная часть. Раздел IX. 298 с.
9. Кудрин А.Л., Бегтин И.В., Кучерена А.Г., Ларина Е.С. и др. Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса // Индекс безопасности. 2016. Т. 22. № 1 (116). С. 121-136.
10. Кургузкина Е.Б., Ратникова Н.Д. Место совершения компьютерных преступлений // Вестник Воронежского института ФСИН России. 2016. № 1. С. 79-87.
11. МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за 2024 год. URL: https://мвд.рф/reports/item/62137988/ (
12. Национальная программа «Цифровая экономика Российской Федерации». URL: https://digital.gov.ru/ru/activity/directions/858/
13. Определение Первого кассационного суда общей юрисдикции от 21.04.2020 № 77-530/2020. Доступ из СПС «КонсультантПлюс».
14. Поляков В.В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности // Российский юридический журнал. 2023. № 1. С. 117-126.
15. Постановление Московского городского суда от 10.05.2017 № 4у-1093/2017. Доступ из СПС «КонсультантПлюс».
16. 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. № 294. 28.12.2022.
17. Савченко О.А. Совершенствование уголовно-правового законодательства в сфере компьютерной информации на современном этапе развития информационных технологий // Законность и правопорядок в современном обществе. 2016. № 29. С. 156-161.
18. Теоретико-правовая парадигма существования кибернетической (информационной) цивилизации: монография / под ред. С.А. Комарова. М.: Изд-во МАТГиП, 2022. 320 с.
19. Трофимцева С.Ю., Илюшин Д.А., Линьков А.В. Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ // Информационное противодействие угрозам терроризма. 2015. № 24. С. 3-11.
20. Уголовный кодекс Республики Армения. Ст. 254, ч. 3, п. 3. URL: http://www.parliament.am/legislation.php?ID=1349&lang=rus&sel=show#24 .
21. Федеральный закон от 11.07.2011 № 200-ФЗ (ред. от 30.12.2021) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об информации, информационных технологиях и о защите информации"». Доступ из СПС «КонсультантПлюс».
22. Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001201112080002 .
23. Хализов С.В. Виды преступлений в сфере цифровой информации // Современное право. 2024. № 7. С. 77-83.
24. Хисамова З.И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф. (30 сентября 2016 г.). Краснодар: Краснодарский университет МВД России, 2016. С. 346-350.
25. Хисамова З.И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. М.: Юрлитинформ, 2017. 160 с.
26. Шинкарецкая Г.Г. Цифровизация - глобальный тренд мировой экономики // Образование и право. 2019. № 8. С. 119-123.

Information Interception: Legal Problems of Distinguishing from Unauthorized Access

Nikita A. Kal'tenberger

Postgraduate Student,
National Research University "Moscow Institute of Electronic Technology",
124498, 1, Shokin Square, Zelenograd, Moscow, Russian Federation;
e-mail: mnnnp@mail.ru

Abstract

This study is devoted to a comparative legal analysis of criminal law categories in the field of unauthorized access to computer information. In particular, categories such as unauthorized access and information interception are subjected to research. The difficulties of criminal legal qualification of these acts are due to the fact that modern technological techniques and mechanisms make it possible to intercept information without hacking or other direct unauthorized access to the system. The author proposes to expand the scope of Article 272 of the Criminal Code of the Russian Federation, which is dedicated to unauthorized access to computer information, by including the category of interception as a criminally punishable act. According to the author, this will bring criminal law in the matter of unauthorized access to computer information into conformity with the established illegal legal relations, as a result of which attackers gain access to computer information in another way not fully regulated by criminal law, having malicious intent to obtain this information in circumvention of current legislation.

For citation

Kal'tenberger N.A. (2026) Perekhvat informatsii: pravovyye problemy razgranicheniya s nepravomernym dostupom [Information Interception: Legal Problems of Distinguishing from Unauthorized Access]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (1A), pp. 429-438. DOI: 10.34670/AR.2026.21.94.053

Keywords

Information interception, unauthorized access, criminal legal qualification, problems of criminal law, cybercrime, computer information.

References

1. Appellate ruling of the Moscow City Court dated December 22, 2016, in case No. 10-18451/2016. Accessed from the ConsultantPlus SPS.
2. Appellate ruling of the Perm Krai Court dated January 22, 2025, No. 33-820/2025, in case No. 2-3634/2024. Accessed from the ConsultantPlus SPS.
3. Begishev, I.R. "Manufacture, sale, and acquisition of special technical means designed to violate digital information security systems: legal aspects" // Information and Security. 2010. No. 2. pp. 255-258.
4. Dolgikh, T.N. "Liability for theft of funds from a bank account" // ConsultantPlus SPS. 2025.
5. Evdokimov K.N. On the Issue of Improving the System of Combating Technetronic Crime in the Russian Federation // Russian Investigator. 2021. No. 10. pp. 69-72.
6. Ivanov I.I., Kondrat I.N. Features of Preventing Crimes Committed with the Use of Modern Information and Telecommunication Technologies // Magistrate. 2024. No. 12. pp. 2-9.
7. Ishcheynov V.Ya. Information Transmission Systems and Networks and Threats to Its Confidentiality // Case Management. 2022. No. 4. pp. 97-102.
8. Commentary on the Criminal Code of the Russian Federation: in 4 volumes (article by article) / A.V. Brilliantov, A.V. Galakhova, V.A. Davydov, et al.; ed. by V.M. Lebedev. Moscow: Yurait, 2017. Vol. 3: Special Part. Section IX. 298 p.
9. Kudrin A.L., Begtin I.V., Kucherena A.G., Larina E.S., et al. High-Tech Crime: New Challenges for Society, State, and Business // Security Index. 2016. Vol. 22. No. 1 (116). Pp. 121-136.
10. Kurguzkina E.B., Ratnikova N.D. Location of Computer Crimes // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2016. No. 1. Pp. 79-87.
11. The Ministry of Internal Affairs of Russia publishes statistical information on the state of crime in the Russian Federation for 2024. URL: https://мвд.рф/reports/item/62137988/
12. National Program "Digital Economy of the Russian Federation". URL: https://digital.gov.ru/ru/activity/directions/858/
13. Ruling of the First Cassation Court of General Jurisdiction dated April 21, 2020 No. 77-530/2020. Accessed from the SPS "ConsultantPlus".
14. Polyakov V.V. Group Form of Committing Crimes as One of the Features of High-Tech Crime // Russian Law Journal. 2023. No. 1. pp. 117-126.

15. Resolution of the Moscow City Court dated May 10, 2017 No. 4y-1093/2017. Accessed from the SPS "ConsultantPlus".
16. Resolution of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37 "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 Telecommunications Networks, Including the Internet" // Rossiyskaya Gazeta. No. 294. 28.12.2022.
17. Savchenko O.A. Improving Criminal Legislation in the Sphere of Computer Information at the Current Stage of Information Technology Development // Law and Order in Modern Society. 2016. No. 29. pp. 156-161.
18. Theoretical and Legal Paradigm of the Existence of a Cybernetic (Information) Civilization: Monograph / ed. by S.A. Komarov. Moscow: Publishing House of MATGiP, 2022. 320 p.
19. Trofimtseva S. Yu., Ilyushin D. A., Linkov A. V. The object of computer crimes in Russian and European criminal law: a comparative analysis // Information counteraction to terrorist threats. 2015. No. 24. pp. 3-11.
20. Criminal Code of the Republic of Armenia. Art. 254, Part 3, Clause 3. URL: http://www.parliament.am/legislation.php?ID=1349&lang=rus&sel=show#24 .
21. Federal Law of 11.07.2011 No. 200-FZ (as amended on 30.12.2021) "On Amendments to Certain Legislative Acts of the Russian Federation in Connection with the Adoption of the Federal Law "On Information, Information Technologies and the Protection of Information"". Access from the SPS "ConsultantPlus".
22. Federal Law of 07.12.2011 No. 420-FZ "On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation" // Official Internet Portal of Legal Information. URL: http://publication.pravo.gov.ru/document/0001201112080002 .
23. Khalizov S.V. Types of Crimes in the Sphere of Digital Information // Modern Law. 2024. No. 7. pp. 77-83.
24. Khisamova Z.I. On the Design of Criminal Legislation Providing for Liability for Crimes Committed with the Use of Information and Telecommunication Technologies // Criminal Policy and Culture of Combating Crime: Proc. of the Int. scientific-practical. conf. (September 30, 2016). Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia, 2016. pp. 346-350.
25. Khisamova Z.I. Criminal Liability for Crimes Committed in the Financial Sphere Using Information and Telecommunication Technologies. Moscow: Yurlitinform, 2017. 160 p.
26. Shinkaretskaya G.G. Digitalization - a Global Trend in the World Economy // Education and Law. 2019. No. 8. pp. 119-123.