**Дата поступления рукописи в редакцию: 18.08.2026 г.**
**Дата принятия рукописи в печать: 01.10.2026 г.**
DOI: 10.24412/2224-9133-2026-9-190-197

***БОГДАНОВ Дмитрий Евгеньевич,***
*Российский государственный университет правосудия им. В.М. Лебедева, Москва, Россия, д.ю.н., доцент, заведующий кафедрой информационного и интеллектуального права, цифровых технологий и инноватики, e-mail: bogdanov.de@yandex.ru*

***ГОРЕЕВ Денис Эдуардович,***
*Российский государственный университет правосудия им. В.М. Лебедева, Москва, Россия, Магистрант 2 курс программы «Юрист в сфере цифровых и инновационных технологий», e-mail: denisgoreeff@gmail.com*

***ЕГОРОВ Игорь Алексеевич,***
*Российский государственный университет правосудия им. В.М. Лебедева, Москва, Россия, Магистрант 2 курса программы «Юрист в сфере цифровых и инновационных технологий», e-mail: SleepoBeepo@yandex.ru*

# *МОШЕННИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ ОБХОДА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ АВТОРСКИХ ПРАВ: ПЕРЕСЕЧЕНИЕ СОСТАВОВ СТ. 159 УК РФ И СТ. 1299–1300 ГК РФ*

***Аннотация.*** *Статья посвящена анализу соотношения уголовно-правовой нормы о мошенничестве (ст. 159 УК РФ) и гражданско-правового режима технических средств защиты авторских прав (ст. 1299–1300 ГК РФ) в ситуациях, когда обход технической защиты выступает инструментом или способом совершения хищения. На основе доктринального анализа, изучения нормативной базы и судебной практики формулируются критерии разграничения исследуемых составов, предлагается авторская концепция «функционального назначения ТСЗ» для разрешения конкуренции норм, а также рекомендации по совершенствованию уголовного и гражданского законодательства.*

***Ключевые слова:*** *технические средства защиты авторских прав; DRM; мошенничество; ст. 159 УК РФ; ст. 1299 ГК РФ; ст. 1300 ГК РФ; мошенничество в сфере компьютерной информации; обход ТСЗ; конкуренция норм; информация об управлении правами; ДАП ВОИС 1996.*

***BOGDANOV Dmitry Evgenievich,***
*Lebedev Russian State University of Justice, Moscow, Doctor of Law, Associate Professor, Head of the Department of Information and Intellectual Law, Digital Technologies and Innovation*

***GOREEV Denis Eduardovich,***
*Lebedev Russian State University of Justice, Moscow, Russia, Master's degree course 2 of the program "Lawyer in the field of digital and innovative technologies"*

***EGOROV Igor Alekseevich,***
*Lebedev Russian State University of Justice, Moscow, Russia, 2nd year Master of the program "Lawyer in the field of digital and innovative technologies"*

# *FRAUDULENT USE OF CIRCUMVENTION OF TECHNICAL MEANS OF COPYRIGHT PROTECTION: CROSSING THE COMPOSITIONS OF ART. 159 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION AND ST. 1299-1300 CIVIL CODE OF THE RUSSIAN FEDERATION*

***Annotation.*** *The article analyses the relationship between the criminal law provision on fraud (Art. 159 of the Criminal Code of the Russian Federation) and the civil law regime of technical copyright protection measures (Art. 1299–1300 of the Civil Code of the Russian Federation) in situations where circumvention of technical protection measures serves as a tool or method of theft. Based on doctrinal analysis, study of the regulatory framework and judicial practice, criteria for distinguishing the studied elements of offences are formulated, the author's concept of "functional purpose of TPM" is proposed for resolving competition between norms, as well as recommendations for improvement of criminal and civil legislation.*

***Key words:*** *technical copyright protection measures; DRM; fraud; Art. 159 of the CC RF; Art. 1299 of the CC RF; Art. 1300 of the CC RF; computer information fraud; circumvention of TPM; competition of norms; rights management information; WIPO Copyright Treaty 1996.*

1. Введение

Цифровизация экономики и повсеместное распространение стриминговых платформ, SaaS-сервисов, онлайн-кинотеатров и многопользовательских игровых экосистем кардинально изменили модель монетизации исключительных прав. Правообладатель во всё большей степени опирается не только на договорные механизмы, но и на технические средства защиты (далее — ТСЗ), превратившиеся в основной инструмент контроля доступа к охраняемым объектам. Параллельно сформировалась устойчивая практика обхода этих средств с целью получения имущественной выгоды — от кряков программного обеспечения до организованных схем продажи взломанных подписок на медиасервисы [12].

По данным Судебного департамента при ВС РФ, в 2024 г. судами рассмотрено 34 660 уголовных дел о мошенничестве (ст. 159, 159.1–159.6 УК РФ[2]) в отношении 37 457 лиц, из которых 27 916 признаны виновными (доля осуждённых — 74 %), причём дистанционные и IT-составляющие преступлений демонстрируют устойчивый рост. Статистика МВД России свидетельствует, что в 2024 г. раскрываемость IT-преступлений составила лишь 23,2 %, а мошенничеств — 10,1 %, что указывает на значительный сегмент цифровых хищений, в том числе связанных с нелегальным доступом к цифровым сервисам и контенту.

В этом контексте правоприменитель неизбежно сталкивается с коллизией правовых режимов. Гражданско-правовой деликт, предусмотренный ст. 1299–1300 ГК РФ направлен на защиту исключительного права как режима правомерной монетизации результата интеллектуальной деятельности. Уголовно-правовой состав мошенничества по ст. 159 УК РФ защищает имущественные отношения собственности. Когда обход ТСЗ становится способом хищения, составы данных статей неизбежно пересекаются — причём без достаточной правоприменительной практики и доктринальных исследований для дифференциации составов.

Объект исследования — общественные отношения в сфере охраны исключительных прав и имущественных прав в условиях цифровой экономики. Предмет — нормы ст. 159 УК РФ и ст. 1299–1300 ГК РФ, практика их применения и доктринальные позиции. Цель — разработать критерии разграничения и модель соотношения указанных составов с предложениями по совершенствованию законодательства. Методологическую основу составляют формально-юридический, сравнительно-правовой и системно-структурный методы.

2. Нормативная база и её эволюция

2.1. Статьи 1299–1300 ГК РФ: содержание и место в системе охранительного права

Статья 1299 ГК РФ в действующей редакции устанавливает запрет на обход технических средств защиты авторских прав, под которыми понимаются «любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообла-

дателем». Норма запрещает: (а) непосредственный обход ТСЗ без разрешения правообладателя; (б) изготовление, распространение, сдачу в прокат, импорт любой технологии или технического устройства, предназначенного для обхода; (в) оказание соответствующих услуг. Данный запрет не требует одновременного нарушения исключительного права, вследствие чего ТСЗ охраняется самостоятельно как инструмент реализации правообладателем своих прав.

Статья 1300 ГК РФ распространяет охранительный режим на информацию об управлении правами — сведения об авторе, правообладателе и условиях использования произведения. Эта норма имплементирует обязательства России по ст.12 Договора ВОИС по авторскому праву 1996 г. (ДАП ВОИС) [3].

С точки зрения гражданско-правовой квалификации нарушения ст. 1299–1300 ГК РФ представляют собой специальный деликт в сфере интеллектуальных прав. Ответственность определяется общими правилами гл. 59 ГК РФ о возмещении вреда либо специальной мерой — компенсацией по ст. 1301 ГК РФ в размере от 10 тыс. до 10 млн руб. либо в двукратном размере стоимости контрафактных экземпляров. Ю.С. Данилов в своём диссертационном исследовании обосновывает, что компенсация за нарушение режима ТСЗ должна рассматриваться как самостоятельный механизм защиты имущественных интересов правообладателя.

2.2. Состав мошенничества по ст. 159 УК РФ: эволюция и структура

Мошенничество как форма хищения характеризуется двумя конститутивными признаками способа совершения: обманом или злоупотреблением доверием. Обман, согласно п. 2 Постановления Пленума ВС РФ от 30 ноября 2017 г. № 48 [7], может состоять в сознательном сообщении заведомо ложных сведений, умолчании об истинных фактах либо умышленных действиях, направленных на введение потерпевшего в заблуждение. Злоупотребление доверием выражается в использовании в корыстных целях доверительных отношений с потерпевшим.

Федеральный закон от 29 ноября 2012 г. № 207-ФЗ дифференцировал состав мошенничества по предметному признаку, выделив специальные разновидности, в том числе ст. 159.6 УК РФ — мошенничество в сфере компьютерной информации, диспозиция которой принципиально отличается: хищение совершается путём ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи информации. Пленум ВС РФ в п. 20 Постановления № 48 раскрывает «вмешательство» как целенаправленное воздействие программных и/или программно-аппаратных средств на серверы, компьютерные устройства или сети, нарушающее установленный процесс обработки информации. При этом мошенничество с компьютерной информацией, совершённое посредством неправомерного доступа по ст. 272 УК РФ или вредоносных программ по ст. 273 УК РФ, требует дополнительной квалификации по совокупности.

2.3. Смежные составы: ст. 146, ст. 272–274.1 УК РФ

Состав преступления по ст. 146 УК РФ охраняет непосредственно исключительные права: предметным условием ч. 2 является крупный ущерб (свыше 100 тыс. руб. исходя из стоимости экземпляров) или деяние в крупном размере. Статьи 272–274.1 УК РФ защищают компьютерную информацию как таковую: ст. 272 — от неправомерного доступа; ст. 273 — от создания и распространения вредоносных программ; ст. 274.1 — от посягательств на критическую информационную инфраструктуру. В редакции ст. 273 УК РФ объективная сторона включает «нейтрализацию средств защиты компьютерной информации». Постановление Пленума ВС РФ № 37 от 15 декабря 2022 г. [8] разъяснило, что под нейтрализацией понимается воздействие на технические, криптографические и иные средства, предназначенные для защиты компьютерной информации, что создаёт прямое пересечение с понятием ТСЗ из ст. 1299 ГК РФ на уровне объективной стороны при различных охраняемых объектах.

3. Технические средства защиты и их обход: гражданско-правовой аспект

3.1. Доктринальное понимание ТСЗ и их виды

В доктрине ТСЗ принято классифицировать на два функциональных класса. Первый — средства контроля доступа (access controls): шифрование, системы аутентификации, программные блокировки, DRM-оболочки (Widevine, PlayReady, FairPlay). Второй — средства защиты использования (copy controls): ограничения на копирование, распечатку, конвертацию форматов, количество воспроизведений. Аналогичное разграничение проводит DMCA США в §1201(a) и §1201(b) [4]. Статьи 6,7 Директивы 2001/29/EC [5] и ст. 7 Директивы2019/790/EU [6] обязали государства-члены ЕС обеспечить правовую охрану обоих типов ТСЗ, однако вопрос их криминализации был оставлен на усмотрение национальных законодателей. Российская ст. 1299 ГК РФ, в отличие от DMCA, не разграничивает оба типа, охватывая их в единой норме.

К видам ТСЗ, актуальным для правоприменительной практики, относятся: (а) DRM-оболочки стриминговых сервисов; (б) привязка к аккаунту как форма лицензионного контроля доступа; (в) динамические коды аутентификации в онлайн-

играх (аналог WoW Warden, значимость которого подтверждена в деле MDY Industries v. Blizzard Entertainment [11]); (г) цифровые водяные знаки, сопряжённые с информацией об управлении правами по ст. 1300 ГК РФ; (д) аппаратные блокировки.

3.2. Состав гражданско-правового деликта

Для целей ст. 1299–1300 ГК РФ объектом деликта служит не исключительное право как таковое, а охранительный режим его реализации. Поэтому нарушение режима ТСЗ самостоятельно, даже без последующего воспроизведения произведения, образует основание для иска. Объективная сторона нарушений ст. 1299 ГК РФ включает любое из следующих действий: непосредственный обход ТСЗ; изготовление средств обхода; распространение, сдача в прокат, импорт таких средств или оказание услуг по обходу. Умысел на последующее незаконное использование произведения не является элементом состава. Субъективная сторона трактуется широко: вина предполагается (ст. 1064 ГК РФ), а нарушитель должен доказать её отсутствие. Особую сложность представляет доказывание факта обхода ТСЗ, требующее специальной технической экспертизы, подтверждающей факт существования действующего ТСЗ в момент предполагаемого обхода, принятые меры обхода и наличие причинно-следственной связи.

4. Мошенничество при обходе ТСЗ: уголовно-правовой аспект

4.1. Модели мошенничества с использованием обхода ТСЗ

На основе анализа правоприменительной практики можно выделить три основные модели преступного поведения, где обход ТСЗ пересекается с составом мошенничества. Модель 1 — получение доступа к платным сервисам в обход оплаты посредством взломанных учётных данных или генераторов ключей. Согласно позиции Пленума ВС РФ № 48, п. 21, если хищение осуществляется «путём использования учётных данных» без воздействия на программное обеспечение серверов, содеянное квалифицируется как кража (ст. 158 УК РФ[2]), а не мошенничество. Ст. 159 УК РФ применима лишь при наличии активного обмана; при техническом вмешательстве в систему защиты возможно применение ст. 159.6 в совокупности со ст. 272 или 273 УК РФ.

Модель 2 — продажа инструментов обхода (кряки, активаторы, «читы» для онлайн-игр) под видом «лицензионных ключей» или «официальных активаций». Здесь формируется полноценный состав мошенничества по ст. 159 УК РФ — обман конечного потребителя: лицо сообщает ложные сведения о природе предлагаемого продукта. Одновременно реализуется объективная сторона ст. 1299 ГК РФ по изготовлению и распространению средств обхода и, вероятно, ст. 273 УК РФ в части распространения вредоносных программ. Пленум ВС РФ № 48, п. 20 прямо предусматривает квалификацию по совокупности ст. 159.6, 272 и 273 УК РФ. Данная модель подтверждается приговором Сургутского городского суда № 1-762/2017 от 12.11.2017 по совокупности ст. 272 и ст. 159 УК РФ [9].

Модель 3 — схемы с поддельными или взломанными лицензиями, аккаунтами, подписками: организация интернет-магазина или сервиса «активации» ПО, предлагающего взломанные ключи активации или массовые аккаунты, полученные путём взлома систем платформ. Ущерб причиняется как конечным пользователям при продаже нефункциональных ключей, так и правообладателям в виде недополученной выручки от подписок. Л.М. Болсуновская в исследовании практики применения ст. 159.6 УК РФ указывает на системные трудности разграничения данного состава с кражей и традиционным мошенничеством [13].

4.2. Конкуренция норм: ст. 159 и ст. 146, 272–274.1 УК РФ

Конкуренция ст. 159 и ст. 146 УК РФ разрешается через различие в непосредственном объекте и наличии хищения. Ст. 146 направлена против незаконного использования объектов авторского права и не требует имущественного завладения. Ст. 159 требует хищения — безвозмездного изъятия и обращения чужого имущества. Е.В. Хромов и В.Ю. Зябликов в монографическом исследовании «Хищение бестелесного имущества» анализируют проблему имущественной оценки нематериальных объектов при хищении в цифровой среде и приходят к выводу о необходимости расширения понятия предмета хищения применительно к правам на цифровой контент [14].

Соотношение ст. 159 и 159.6 УК РФ является центральным с практической точки зрения. Разграничение проводится по способу совершения деяния: ст. 159 предполагает обман или злоупотребление доверием с воздействием на волю потерпевшего; ст. 159.6 — техническое вмешательство с помощью воздействия на информационную систему, минуя волю потерпевшего. Это разграничение подтверждается Постановлением Пленума ВС РФ № 48.

4.3. Судебная практика и типичные квалификационные проблемы

Апелляционным постановлением Свердловского областного суда от 7 мая 2024 г. № 22-3412/2024 (дело № 1-131/2021) была полностью отменена квалификация по ст. 272 УК РФ и наполовину сокращено наказание по ст. 273 УК РФ за использование программы-патчера для нейтрализации защиты «1С: Предприятие 8.3». Суд апелляционной инстанции, руководствуясь

Постановлением Пленума ВС РФ № 37 от 15 декабря 2022 г., указал, что программный код охраняется нормами авторского права (ст. 146 УК РФ, ст. 1299–1300 ГК РФ), а не ст. 272 УК РФ, предназначенной для защиты информации с установленным специальным режимом доступа (персональные данные, коммерческая тайна и т.д.), и что суд первой инстанции смешал объективную сторону двух различных составов [10].

В деле MDY Industries, LLC v. Blizzard Entertainment, Inc., 629 F.3d 928 (9th Cir. 2010), имеющем ориентирующее значение для российской доктрины, Девятый окружной апелляционный суд США при квалификации обхода антибот-системы WoW Warden решал аналогичную проблему функционального назначения ТСЗ — является ли Warden средством контроля доступа по §1201(a) DMCA или средством защиты прав по §1201(b). Суд разграничил эти категории, констатировав, что разработчик бота MDY не нарушил §1201(a), поскольку Warden использовался не как барьер доступа к произведению, а как средство поддержания условий предоставления лицензии, что имеет прямое аналитическое значение при разграничении российских составов.

5. Пересечение и разграничение составов: ст. 159 УК РФ и ст. 1299–1300 ГК РФ

5.1. Критерии разграничения

Первый критерий — непосредственный объект охраны. Ст. 1299–1300 ГК РФ защищают исключительное право и режим его реализации — отношения по управлению доступом к произведению; объектом является правовой статус результата интеллектуальной деятельности, обеспечивающий его правомерный оборот. Ст. 159 УК РФ охраняет имущественные отношения собственности, а предметом преступления выступает имущество либо право на имущество.

Второй критерий — характер посягательства. Нарушение ст. 1299 ГК РФ есть посягательство на охранительный режим («разрушение барьера») вне зависимости от имущественного результата. Мошенничество по ст. 159 УК РФ — посягательство на имущество через обман: элемент хищения (безвозмездное изъятие, корыстная цель, причинение ущерба) обязателен. Третий критерий — наличие обмана как способа: обман предполагает введение в заблуждение конкретного субъекта, под воздействием которого он передаёт имущество или право. Технический обход ТСЗ направлен на информационную систему, а не на психику лица, и сам по себе не является обманом в смысле ст. 159 УК РФ.

Четвёртый критерий — функциональная роль ТСЗ в структуре деяния: (а) ТСЗ как самостоятельный объект посягательства (деликт по ст. 1299–1300 ГК РФ без последующей корыстной эксплуатации); (б) ТСЗ как инструментальный элемент способа хищения (обход ТСЗ как подготовительная стадия или способ мошенничества/кражи); (в) ТСЗ как элемент состава ст. 273 УК РФ, если применяемые средства обхода признаются вредоносными программами. На необходимость чёткого разграничения данных ролей указывает Постановление Пленума ВС РФ № 37.

5.2. Концепция «функционального назначения ТСЗ»

Предлагается следующая доктринальная конструкция для квалификации. Если в конкретном деянии ТСЗ функционально выполняет роль барьера доступа к платной услуге, а обход этого барьера составляет способ безвозмездного завладения правом на эту услугу — ТСЗ есть элемент «имущественной конструкции» обмана; квалификация идёт по ст. 159 (или ст. 159.6) УК РФ. Если же ТСЗ функционально является барьером правомерного использования произведения как объекта авторского права — его обход прежде всего нарушает режим исключительного права, и применяются нормы ст. 1299 ГК РФ и ст. 146 УК РФ (при соответствующем ущербе). Тем самым ключевым является выявление того, что именно «защищает» конкретное ТСЗ: имущественный интерес платформы по получению оплаты за доступ или исключительное право автора на использование произведения. В большинстве практических ситуаций оба аспекта присутствуют одновременно, что предопределяет совокупную квалификацию.

5.3. Конкуренция уголовно-правовой и гражданско-правовой ответственности

Ситуация 1: нарушение ст. 1299–1300 ГК РФ занимает самостоятельное значение. Если лицо обходит ТСЗ без корыстного умысла, уголовная ответственность по ст. 159 УК РФ исключена, а гражданско-правовая ответственность применяется самостоятельно. Даже при наличии последующего безвозмездного доступа к контенту без корыстной цели хищения ст. 159 неприменима — возможна лишь квалификация по ст. 146 УК РФ при условии крупного ущерба или по ст. 165 УК РФ (причинение имущественного ущерба без признаков хищения). Ситуация 2: действия по обходу ТСЗ «растворяются» в составе ст. 159 УК РФ, когда обход ТСЗ и использование произведения образуют единый умысел, направленный на извлечение имущественной выгоды путём обмана. Нормы ст. 159 УК РФ в рамках уголовного преследования поглощают норму ст. 1299 ГК РФ, однако самостоятельное гражданско-правовое требование по ст. 1299–1300 ГК РФ может быть заявлено в рамках гражданского иска в уголовном деле.

6. Зарубежный и международный контекст

DMCA 1998 г. установил автономный запретительный режим в §1201, отделив нарушение режима ТСЗ от нарушения авторского права:

обход ТСЗ является самостоятельным деликтом вне зависимости от факта нарушения исключительного права. §1204 DMCA криминализирует обход ТСЗ при наличии «коммерческой выгоды или частного финансового умысла», устанавливая санкцию до 5 лет лишения свободы и штраф до 500 000 долл. США за первое нарушение. Такая формулировка позволяет охватить случаи, когда обход ТСЗ направлен на извлечение имущественной выгоды, не требуя доказывания «обмана» как конститутивного элемента. Американское право тем самым решает проблему, актуальную и для России: не пытается квалифицировать мошеннический обход ТСЗ через общий состав, а создаёт специальную криминализированную норму с имущественным квалифицирующим признаком.

Договор ВОИС по авторскому праву 1996 г. (ст. 11, 12) установил международный стандарт охраны ТСЗ, которому должны следовать государства-участники, в том числе Россия. Директива 2001/29/ЕС (ст. 6, 7) и Директива 2019/790/EU (ст. 7) обязали государства-члены ЕС обеспечить правовую охрану обоих типов ТСЗ, оставив вопрос криминализации на усмотрение национальных законодателей. Германия и Франция ввели специальные уголовные составы за обход ТСЗ; другие государства ограничились гражданско-правовой ответственностью. Директива 2019/790 дополнительно устанавливает, что исключения из авторского права не должны использоваться в качестве обоснования обхода ТСЗ.

7. Заключение и предложения

Предлагается изложить ст. 1299 ГК РФ с разграничением двух типов ТСЗ: (а) технических мер контроля доступа к произведению; (б) технических мер защиты прав на произведение, — с различным регулированием допустимых исключений для каждого типа (по аналогии с §1201(a) и §1201(b) DMCA). Ст. 1300 ГК РФ следует дополнить указанием на самостоятельное основание компенсации за использование произведения с заведомо изменённой информацией об управлении правами.

В части уголовного законодательства целесообразно рассмотреть дополнение ст. 146 УК РФ квалифицированным составом, предусматривающим ответственность за нарушение авторских прав, сопряжённое с систематическим обходом ТСЗ в коммерческих целях. Альтернативный вариант — введение в гл. 28 УК РФ отдельной нормы об ответственности за обход ТСЗ с коммерческим умыслом (аналог §1204 DMCA), криминализирующей именно имущественно направленный обход без необходимости доказывания «обмана». Одновременно представляется необходимым уточнить диспозицию ст. 159.6 УК РФ применительно к цифровым услугам, урегулировав вопрос о том, является ли обход системы аутентификации сервиса «вмешательством» по смыслу данной нормы или же такие действия квалифицируются исключительно как кража по ст. 158 УК РФ.

Действующее Постановление Пленума ВС РФ № 14 от 26 апреля 2007 г. не учитывает ни эволюции цифрового рынка, ни появившейся ст. 159.6 УК РФ, ни Постановления Пленума № 37 от 2022 г. В этой связи представляется целесообразным принять новое постановление Пленума (или существенно обновить имеющееся), включив разъяснения о соотношении ст. 146 с нормами гл. 21 и гл. 28 УК РФ применительно к цифровой среде, дать определение ТСЗ для целей уголовного права и разъяснить порядок исчисления ущерба при обходе ТСЗ, в том числе применительно к упущенной выгоде от несостоявшихся подписок.

Научная новизна работы состоит в разработке концепции «функционального назначения ТСЗ» как критерия разграничения уголовно-правовых и гражданско-правовых составов; в системном анализе трёхуровневой нормативной конструкции (ст. 1299–1300 ГК РФ / ст. 146 УК РФ / ст. 159, 159.6, 272–273 УК РФ) применительно к актуальным моделям цифрового мошенничества; в обосновании предложений по автономной криминализации коммерчески мотивированного обхода ТСЗ и разграничению двух типов технических мер в ст. 1299 ГК РФ.

**Список литературы:**

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954.

[2] Гражданский кодекс Российской Федерации (часть четвёртая): Федеральный закон от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 52 (ч. I). — Ст. 5496.

[3] Договор ВОИС по авторскому праву: принят Дипломатической конференцией ВОИС 20 декабря 1996 г. (ДАП ВОИС / WCT). Статьи 11, 12 // Собрание законодательства Российской Федерации. — 2009. — № 28. — Ст. 3494.

[4] Digital Millennium Copyright Act: Pub. L. No. 105-304, 112 Stat. 2860 (1998). 17 U.S.C. §§ 1201, 1202, 1204. URL: https://www.law.cornell.edu/uscode/text/17/1204 (дата обращения: 04.05.2026).

[5] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society // EUR-Lex. 2001. URL: https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng (дата обращения: 07.05. 2026).

[6] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/

EC and 2001/29/EC // EUR-Lex. 2019. URL: https://eur-lex.europa.eu/legal-content/EN-EL/ALL/?uri=CELEX:32019L0790&from=EN (дата обращения: 07.05.2026).

[7] Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" // Бюллетень Верховного Суда Российской Федерации. — 2018. — № 2.

[8] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 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" // Бюллетень Верховного Суда Российской Федерации. № 3. 2023.

[9] Приговор Сургутского городского суда Ханты-Мансийского автономного округа - Югры от 12 ноября 2017 г. по делу № 1-762/2017 / СудАкт. 2017. URL: https://sudact.ru/regular/doc/SWC7elmLAaQR/?ysclid=mp9wplkrep472294251 (дата обращения: 13.05.2026).

[10] Апелляционное постановление Свердловского областного суда по делу № 22-3412/2024. Официальный сайт Свердловского областного суда. 2024. URL: https://oblsud--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=13830932&case_uid=034c7ce5-7b66-4462-b1c2-014e31310972&delo_id=4&new=4.

[11] MDY Industries, LLC v. Blizzard Entertainment, Inc. and Vivendi Games, Inc. 629 F.3d 928 (9th Cir. 2010) // Lexology. 2019. URL: https://www.lexology.com/library/detail.aspx?g=1c7db854-ac6b-4a30-943d-918b95fb5696 (дата обращения: 08.05.2026).

[12] Данилов Ю. С. Защита имущественных интересов правообладателей при нарушении исключительных и иных имущественных прав на объекты авторского права и смежных прав. М., 2019. 177 с. URL: https://dis.rgiis.ru/files/dis/d40100102/Danilov/dissertaciyayu_s_danilova.pdf (дата обращения: 01.05.2026).

[13] Болсуновская Л. М. Мошенничество в сфере компьютерной информации: анализ судебной практики // Уголовное право. 2016. № 2. С.12-16.

[14] Хромов Е. В., Зябликов В. Ю. Хищение бестелесного имущества // Новые технологии. 2024. URL: https://newtech.legal/cabinet/catalog/ugolovnoe-pravo/6176/7718/?ysclid=mp9x3vb3rl313798955 (дата обращения: 14.05.2026).

**References:**

[1] Criminal Code of the Russian Federation: Federal Law of June 13, 1996 No. 63-FZ // Collection of Legislation of the Russian Federation. — 1996. — № 25. - Art. 2954.

[2] Civil Code of the Russian Federation (part four): Federal Law of December 18, 2006 No. 230-FZ // Collection of Legislation of the Russian Federation. — 2006. - No. 52 (part I). - Art. 5496.

[3] WIPO Copyright Treaty: adopted by the WIPO Diplomatic Conference on 20 December 1996 (WIPO ADR/WCT). Articles 11, 12 // Collection of legislation of the Russian Federation. — 2009. — № 28. - Art. 3494.

[4] Digital Millennium Copyright Act: Pub. L. No. 105-304, 112 Stat. 2860 (1998). 17 U.S.C. §§ 1201, 1202, 1204. URL: https://www.law.cornell.edu/uscode/text/17/1204 (accessed on: 04.05.2026).

[5] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society // EUR-Lex. 2001. URL: https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng (accessed on: 07.05. 2026).

[6] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC // EUR-Lex. 2019. URL: https://eur-lex.europa.eu/legal-content/EN-EL/ALL/?uri=CELEX: 32019L0790&from = EN (Accessed: 07.05.2026).

[7] Resolution of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017 No. 48 (ed. 15.12.2022) "On judicial practice in cases of fraud, embezzlement and embezzlement" // Bulletin of the Supreme Court of the Russian Federation. — 2018. — № 2.

[8] 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 of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet" // Bulletin of the Supreme Court of the Russian Federation. № 3. 2023.

[9] Verdict of the Surgut City Court of the Khanty-Mansiysk Autonomous Okrug - Ugra dated November 12, 2017 in case No. 1-762/2017 / CourtAct. 2017. URL: https://sudact.ru/regular/doc/SWC7elmLAaQR/?ysclid=mp9wplkrep472294251 (accessed on: 13.05.2026).

[10] Appeal ruling of the Sverdlovsk Regional Court in case No. 22-3412/2024. Official website of the Sverdlovsk Regional Court. 2024. URL: https://oblsud--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=13830932&case_uid=034c7ce5-7b66-4462-b1c2-014e31310972&delo_id=4&new=4.

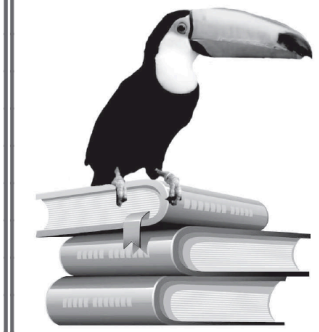
[11] MDY Industries, LLC v. Blizzard

Entertainment, Inc. and Vivendi Games, Inc. 629 F.3d 928 (9th Cir. 2010) // Lexology. 2019. URL: https://www.lexology.com/library/detail.aspx?g=1c7db854-ac6b-4a30-943d-918b95fb5696 (accessed on: 08.05.2026).

[12] Danilov Yu. S. Protection of property interests of copyright holders in case of violation of exclusive and other property rights to objects of copyright and related rights. M., 2019. 177 c. URL: https://dis.rgiis.ru/files/dis/d40100102/Danilov/dissertaciyayu_s_danilova.pdf (дата обращения: 01.05.2026).

[13] Bolsunovskaya L. M. Computer information fraud: analysis of judicial practice // Criminal law. 2016. № 2. S.12-16.

[14] Khromov E.V., Zyablikov V. Yu. Theft of disembodied property // New technologies. 2024. URL: https://newtech.legal/cabinet/catalog/ugolovnoe-pravo/6176/7718/? ysclid = mp9x3vb3rl313798955 (Accessed: 14.05.2026).




Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников, учебных и методических пособий, монографий, научных статей.

Профессионально.

В максимально короткие сроки.

Размещаем в РИНЦ, E-Library.