Унификация уголовной ответственности за хищения, совершаемые с использованием компьютерных технологий

Федотова Анастасия Вячеславовна,
кандидат культурологии, доцент кафедры юриспруденции, Мурманский арктический университет, fedotovaav@mauniver.ru

Статья посвящена обоснованию исключения ст.159.6 УК РФ, как избыточной, не соответствующей юридической природе мошенничества, а также порождающей излишнюю конкуренцию со статьей 158 УК РФ и «компьютерной» главой УК РФ. В работе предлагаются ряд изменений в статью 158 УК РФ, которые направленны на разграничение имущественных и компьютерных преступлений и внедрение реальной совокупности, а также на преодоление дисгармонии юридической ответственности за хищения с использованием цифровых технологий, совершенных при квалифицирующих обстоятельствах и при отсутствии квалифицирующих признаков. Для повышения эффективности применения данных изменений предлагается разработать разъяснения судам в форме пленума Верховного суда Российской Федерации.
Ключевые слова: мошенничество, кража, «компьютерная» глава, кибератаки, цифровые технологии.

Стремительное развитие цифровых технологий, динамика внедрения технологических решений на базе искусственного интеллекта и AI-агентов требует от системы права активизации процессов обновления и корректировки норм. Ускоренное технологическое развитие существенным образом преобразует содержание всех отраслей права, в том числе уголовного. Традиционные уголовно-правовые конструкции, сформированные для материальной реальности, теряют свою эффективность в отношении деяний, совершенных средствами цифровизации. В условиях автоматизации процессов большая часть юридически значимых деяний сопровождается техническими средствами и, в ряде случаев, исключает ментальное и физическое их сопровождение со стороны субъекта. В настоящей статье рассматривается устоявшийся институт преступлений против собственности, анализ которого выявляет совокупность концептуальных проблем.

Сегодня фокус внимания закономерно помимо привычной защиты имущества от непосредственно физических посягательств, включает обеспечение сохранности цифровых активов в виртуальном пространстве. Однако, разработанные в период, когда преступления только начали переходить в цифровой формат, они не отвечают динамике технологического развития. Мошеннические схемы и способы хищения денежных средств значительно усложнились, внедряются AI-агенты и иные инструменты на базе искусственного интеллекта и действующие конструкции норм и составов преступлений не отвечают требованиям реальности. Как отмечается в статье о трендах мирового рынка информационной безопасности «развитие комплексных мультиагентных систем повышает сложность инфраструктуры и создает потенциальные бреши» [9]. Увеличивается сложность и масштаб атак, которые в настоящее время могут затрагивать целую экосистему от операторов связи до облачных сервисов, увеличивается число нечеловеческих идентичностей, принадлежащих ботам и службам, а не людям, растет автономность ИИ-систем. Обеспечение безопасности в цифровой среде становится критически важной и требует не только проработку комплекса защиты агентных систем, внедрение генеративных ИИ для осуществления непрерывного управления рисками и иных мер обеспечения кибербезопасности, но и выработку соответствующих правовых механизмов, поскольку такие системы становятся все более доступными злоумышленникам.

Отечественная правоохранительная система сегодня активно противостоит преступлениям, совершаемым с применением информационно-телекоммуникационных систем, о чем свидетельствует статистика. Так, по данным Министерства внутренних дел за 2025 год общее количество киберпреступлений снизилось на 12% [1], число краж на 23,8%, случаев мошенничества – на 9%, а количество фактов неправомерного доступа к компьютерной информации сократилось на 44%. Причиной снижения, как отмечают в ведомстве, стало обновление законодательства в сфере кибермошенничества. Однако, развитие технологий позволяет злоумышленникам быстро адаптироваться к изменениям и находить новые возможности осуществления преступных деяний, о чем свидетельствует небольшой рост указанных преступлений через непродолжительное время. Следовательно, совершенствование законодательства должно быть более гибким, в допустимых границах проактивно, и, что представляется крайне актуальным, должно оперативно корректироваться исходя из правоприменительной практики.

Одной из приоритетных в рассматриваемой сфере представляется задача исключения устаревшей, «искусственной» статьи 159.6 УК РФ, как избыточной. Эта проблема длительное время обсуждается в научных источниках, однако, усложнение технологических решений совершения противоправных деяний актуализирует внимание к изменению уголовного законодательства в этой части [6].

Во-первых, само понятие мошенничества, данное в ст. 159 УК РФ, определяет его как посягательство на чужое имущество «путем обмана или злоупотребления доверием». Следовательно, по своей юридической природе ст. 159.6 УК РФ в принципе не может квалифицироваться как мошенничество, поскольку классическое мошенничество всегда предполагает воздействие на сознание и волю потерпевшего, то есть непосредственный контакт преступника с потер-

певшим. Согласно смыслу статьи 159.6 УК РФ воздействие оказывается на программный код, базу данных, алгоритмы, у которых нет психики, а, значит, их можно взломать, найти уязвимость и спровоцировать системный сбой, нарушить логику работы, но их невозможно обмануть или злоупотребить их доверием. Хабыев Х. также отмечает, что в качестве способа в статье указывается «техническое вмешательство в работу компьютерных систем, не предполагающее обмана человека как такового» [7]. Иными словами, использование вредоносной программы для списания денежных средств со счета потерпевшего без его ведома, является «насилием» над системой, а не обманом человека.

Более того, правоприменительная практика по ст. 159.6 УК РФ постоянно сталкивается с конкуренцией норм. Главным образом, по смыслу она максимально близка к понятию «кража» п.«г» ч.3 ст.158 УК РФ. На это особое внимание обращает Скоморохова М.С., актуализируя сложность в разграничении этих статей, даже несмотря на рекомендации по квалификации, представленные в Постановлении Пленума Верховного суда РФ от 30.11.2017 №48 [4]. На тесную конкуренцию составов мошенничества и кражи указывает и Халиков А.Н. [8] В целом, если рассматривать обе эти статьи Уголовного кодекса, то судебная практика, главным образом, базирующаяся на разъяснениях Пленума Верховного суда РФ № 29 [3] и 48 позволяет выделить ключевые системные проблемы, влияющие на продуктивность их применения. Во-первых, сложность разграничения статей влечет разную меру ответственности за практически аналогичные деяния. Так, если правонарушитель списал средства через онлайн-банк, используя подобранный пароль, данное деяние будет квалифицировано как кража в соответствии с п. «г» ч. 3 ст. 158 УК РФ. Однако, если он совершит аналогичное деяние, но используя вредоносную программу, которая перехватила пароль и обошла защитную систему финансовой организации, это будет квалифицировано как мошенничество по ст. 159.6 УК РФ, тогда как для потерпевшего вред, объект посягательств и умысел будет одинаковыми. Отсюда проистекает вторая проблема – криминологический дисбаланс. Согласно разъяснениям Генеральной прокуратуры п. «г» ч. 3 ст. 158 УК РФ относится к категории тяжких преступлений «независимо от суммы похищенного» [5], тогда как ч. 1 ст. 159.6 УК РФ относится к категории преступлений небольшой тяжести. Таким образом получается, что списание даже маленькой суммы с банковского счета или найденной карты будет считаться тяжким преступлением, автоматически исключающим возможность прекращения дела путём применения сторон и повлечет наказание до 6 лет лишения свободы, тогда как списание кратно большей суммы, но с применением, например, вирусной программы, будет относиться к преступлениям средней тяжести с ответственностью до 2 лет лишения свободы. Иными словами, целенаправленная кибератака, совершенная при квалифицирующих обстоятельствах, влечет за собой более мягкое наказание, чем кража, совершённая при отсутствии квалифицирующих признаков.

Таким образом, для преодоления терминологической путаницы, избыточной конкуренции норм, парадокса тяжести наказания, а также в целях упрощения квалификации представляется целесообразным признать утратившей силу искусственную статью 159.6 УК РФ, а все цифровые и безналичные хищения аккумулировать в ст. 158 УК РФ, сделав более сложную градацию по степени тяжести. Для этого, например, изложить норму в следующей редакции:

- дополнить ч.2 ст.158 УК РФ пунктом «д»:

«д) с банковского счета, а равно в отношении электронных денежных средств или цифровой валюты (при отсутствии признаков преступления, предусмотренного пунктом «д» части третьей настоящей статьи), -»;

- признать утратившим силу пункт «г» ч.3 ст. 158 УК РФ;

- дополнить ч.3 ст.158 УК РФ новым пунктом «д»:

«д) путем ввода, удаления, блокирования, модификации компьютерной информации либо иного несанкционированного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -».

Такие корректировки сбалансируют тяжесть наказания за содеянное, когда кража, совершённая при отсутствии квалифицирующих признаков (подобрал карту, расплатился ею в магазине и пр.) переходит из ч.3 в ч.2 ст. 158 УК РФ (средняя тяжесть), что позволит судам при примирении сторон и полном возмещении ущерба применять ст. 76 УК РФ. А целенаправленные кибератаки, сверхтехнологичные кражи, реализуемые посредством взлома, обхода системы безопасности, фишинга, то есть совершенные при квалифицирующих обстоятельствах, требующих дорогостоящих экспертиз, переходят в ч.3 ст. 158 УК РФ (тяжкие преступления). Что представляется целесообразным, поскольку даже если оно совершается с помощью AI-агентов и не всегда требует от преступника профессиональных навыков, оно напрямую угрожает дигитальной безопасности государства и бизнеса, и может повлечь за собой значительный ущерб. Таким образом, ст.158 УК РФ распределяет тяжесть наказания в зависимости от методов использования цифровых инструментов хищения.

Данные предложения преодолевают и терминологический тупик ст. 159.6 УК РФ и любое скрытое корыстное хищение безналичных или цифровых средств без обмана человека будет признаваться судами как кража, что представляется технически верным.

Более того, эти изменения смогут упорядочить и взаимодействие нормы с главой 28 УК РФ. Текущая практика показывает конкуренцию ст. 159.6 УК РФ с так называемой «компьютерной» главой по принципу «специальная и общая норма», а перенос хищений с использованием цифровых средств в ст.158 УК РФ позволит перевести этот спор в сферу «цели и средства». И если сейчас в случае, например, взлома пароля и несанкционированного доступа в личный кабинет потерпевшего ради хищения денежных средств, суды вменяют наказание только по 159.6 УК РФ, как специальной нормы, то после внедрения изменений потребуется квалификация по совокупности преступлений по п.«д» ч.3 ст. 158 УК РФ и ст. 272 УК РФ. Это представляется более целесообразным, поскольку любой взлом системы – это самостоятельное посягательство на дигитальную безопасность. По предложенному п.«д» ч.3 ст. 158 УК РФ наказание предполагается именно за хищение с использованием технических средств воздействия на компьютерные системы, но не включает сам факт взлома компьютерной защиты. Совокупность статей позволит привлекать к ответственности и за кражу средств, и за вред цифровой системе. Аналогичный подход (совокупность преступлений) станет возможным и по ст. 272.1 УК РФ, где ответственность будет предусмотрена и за факт несанкционированного использования персональных данных или баз данных пользователей, и за кражу, если эти данные были использованы для автоматизированного списания средств.

Таким образом, предложенные поправки в УК РФ позволят четко разграничить имущественные и компьютерные преступления и внедрить реальную совокупность, что сделает наказание за сложные кибератаки более справедливыми и дифференцированными. Иными словами, глава 21 (ст. 158) УК РФ будет четко направлена на наказание незаконного обогащения с помощью цифровых технологий, а глава 28 (ст. 272-274) УК РФ направлена на пресечение самого технологического взлома системы, разрушающего его целостность и безопасность данных. Безусловно, что Постановление Пленума ВС РФ дает разъяснение о необходимости применения норм ст.159.6 УК РФ в совокупности с гл.28 УК РФ, дополняя специальный состав, но по ряду примеров наблюдается состояние конкуренции, когда суды признают «компьютерную» составляющую только в качестве мошенничества, исключая применение гл.28 УК РФ и снижая эффективность применения норм. На рассогласованность простых составов, предусмотренных ст. 159.6 У К РФ и ст. 272 У К РФ обращает внимание и Попова Е.М. [2], которая отмечает, что квалификация по совокупности в этом случае «противоречит правилам квалификации преступлений и ставит под вопрос обоснованность и законность выносимых судами приговоров».

Однако, чтобы указанные выше поправки действительно эффективно работали, в целях единообразия применения закона также представляется необходимым разработать разъяснения для судов в форме Постановления Пленума Верховного суда РФ. В нем, во-первых, должны быть обозначены принципы разграничения объекта посягательства. Так, должно быть прописано, что хищение денежных средств, цифровой валюты, совершенное путем вмешательства в функционирование средств хранения, обработки и передачи данных (п. «д» ч. 3 ст. 158 УК РФ), посягает на отношения собственности, а преступления, предусмотренные ст. 272-274 УК РФ, посягают на безопасность цифровой информации (глава 28 УК РФ). И поскольку указанные деяния имеют самостоятельные объекты преступного посягательства их соотношения

строится по принципу «цели и средства», а, следовательно, их составы при наличии соответствующих признаков подлежат квалификации по реальной совокупности преступлений.

Далее важно дать пояснение и по другим «компьютерным» статям. Так, для ст. 272 УК РФ важно предусмотреть реальную совокупность преступлений в случае тайного изъятия денежных средств путем неправомерного доступа к охраняемой законом компьютерной информации, а в случаях если списание средств не состоялось по независящим от злоумышленника обстоятельствам, считать неправомерный доступ оконченным в момент получения доступа к охраняемым данным и квалифицировать деяния по ст. 272 УК РФ, ч.3. ст. 30 и п. «д» ч.3.ст. 158 УК РФ.

Относительно оборота персональных данных важно закрепить, что за сам факт незаконного оборота должен квалифицироваться по ст. 272.1 УК РФ, а факт кражи денежных средств с использованием таких данных подлежит квалификации по п. «д» ч.3.ст. 158 УК РФ.

Разъяснение совокупности с положениями ст. 273 УК РФ должно опираться на то, что создание, распространение и/или использование вредоносных компьютерных программ должно рассматриваться в качестве преступного орудия для совершения высокотехнологичного хищения денежных средств. И поскольку оно создает угрозу неограниченному кругу цифровых систем, ее поглощение нормой о краже недопустимо. Такие преступления также должны рассматриваться только в реальной совокупности.

Если хищение совершило лицо, имеющее правомерный доступ к охраняемой законом информации, например, путем её модификации или удаления, в таком случае судам изначально необходимо проверить были ли нарушены правила работы с информацией. Если деяние повлекло крупный ущерб самой информационно-телекоммуникационной инфраструктуре, уничтожение или блокирование критических систем данных, действия виновного должны квалифицироваться по совокупности ст. 274 и п. «д» ч.3.ст. 158 УК РФ. Но, здесь важно отметить, что если нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации не повлекло последствий, предусмотренных ч.1. ст. 274 УК РФ (крупный ущерб безопасности и работоспособности компьютерной инфраструктуры собственника или оператора компьютерной системы), содеянное не образует совокупности преступлений и должно охватываться составом кражи.

Подводя итог можно сделать вывод о том, что до текущего момента остается актуальным вопрос о применении статей уголовного кодекса в сфере дистанционных хищений. Многие ученые указывают на системный кризис квалификации таких преступлений. С ускоряющимся усложнением цифровой среды эта ситуация будет нарастать, поэтому представляется целесообразным скорректировать действующее законодательство. Одной из причин такого кризиса является ст. 159.6 УК РФ, порождающая непреодолимые доктринальные противоречия, вынуждающие правоприменителя «лавировать» при попытках квалифицировать противоправные деяния. Имея статус специальной нормы, она необоснованно блокирует применение статей гл.28 УК РФ, оставляя «за скобками» самостоятельные посягательства на цифровую безопасность и декриминализируя высокотехнологичные способы взлома. В целях упрощения следственно-судебной практики, выравнивание дисбаланса и обеспечения справедливости наказания в настоящей статье предложены изменения в действующее уголовное законодательство. Их суть состоит в трех ключевых моментах. Во-первых, представляется необходимым исключение ст. 159.6 УК РФ, как «искусственной» нормы, размывающей родовые признаки мошенничества. Во-вторых, важно объединить все цифровые хищения в рамках ст. 158 УК РФ («Кража»). Для этого перенести ответственность за хищения безналичных денег, электронных средств, цифровых валют в единый материальный состав (п. «д» ч.2. ст. 158 УК РФ), а хищения, совершенные при квалифицирующих обстоятельствах (путем программно-технических манипуляций и несанкционированного вмешательства в работу компьютерных систем, удаления, блокировки, модификации данных), перевести в п. «д» ч.3 ст. 158 УК РФ. В-третьих, признание утратившей силу ст. 159.6 УК РФ разрушит искусственную конкуренцию «общей и специальной нормы», а в совокупности с принятием поправок в ст. 158 УК РФ, позволит перевести отношения имущественных и компьютерных преступлений в логичную систему «цели и средства» и обяжет суды применять реальную совокупность преступлений. Вместе с рекомендациями для Постановления Пленума ВС РФ предлагаемые изменения позволят четко разграничить материальный и технологический ущербы, преодолеют путаницу в квалификации и обеспечат справедливую дифференциацию уголовной ответственности, когда лицо, просто нашедшее кару и профессиональный кибер-преступник понесут принципиально разное, соразмерное содеянному наказание.

Литература

1. МВД сообщило о снижении числа киберпреступлений в РФ в 2025 году на 12% // Интерфакс. – 18.02.2026 [Электронный ресурс]. URL: https://www.interfax.ru/digital/1073418 (дата обращения: 08.10.2026)
2. Попова, Е.М. Квалификация хищений с использованием информационно-телекоммуникационных технологий: проблемы теории и практики применения ст. 159.6 УК РФ / Е.М. Попова // Полицейская и следственная деятельность. – 2026. – № 2. [Электронный ресурс]. URL: https://nbpublish.com/library_read_article.php?id=79149 (дата обращения: 05.10.2026)
3. 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» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/405863329/ (дата обращения: 15.10.2026)
4. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 28.09.2026)
5. Прокуратура Московского района города Калининграда разъясняет: «Об ответственности за кражу с банковского счета» // Прокуратура Калининградской области [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/proc_39/activity/legal-education/explain/criminal_law/e372159/ (дата обращения: 04.10.2026)
6. Смоляков, А. Н. Хищение безналичных, электронных денежных средств и цифровой валюты: вопросы юридической техники и дифференциации ответственности : диссертация кандидата юридических наук : 5.1.4 / Смоляков Александр Николаевич. – Санкт-Петербург, 2023. – 250 с.
7. Хабыев, Х. Проблемы квалификации мошенничества в сфере компьютерной информации (статья 159.6 УК РФ) / Х.Хабыев // Актуальные исследования. 2026. №25 (311). Ч.III. С. 14-16. [Электронный ресурс]. URL: https://apni.ru/article/15558-problemy-kvalifikacii-moshennichestva-v-sfere-kompyuternoj-informacii-statya-1596-uk-rf (дата обращения: 01.10.2026)
8. Халиков, А. Н. Проблема квалификации дистанционных хищений как отдельного состава преступления / А. Н. Халиков // Евразийская адвокатура. – 2025. – № 4. – С. 117.
9. 2026 Trends in Information Security [Электронный ресурс]. URL: https://pages.marketintelligence.spglobal.com/15701-MS-2512-GL-TMT-DR-451R-NA-2026-Trends-in-Tech_04A---Information-Security.html (дата обращения: 05.10.2026).

Unification of Criminal Liability for Theft Committed Through the Use of Computer Technologies

Fedotova A.V.

Murmansk Arctic University

The article provides a rationale for the repeal of Article 159.6 of the Criminal Code of the Russian Federation as redundant, inconsistent with the legal nature of fraud, and creating unnecessary statutory conflict with Article 158 of the Criminal Code of the Russian Federation and the «computer crimes» chapter of the Criminal Code of the Russian Federation. The author proposes a series of amendments to Article 158 of the Criminal Code of the Russian Federation aimed at differentiating between property and computer-related offenses, ensuring the application of real joinder of offenses (multiple offenses), and overcoming the disparity in criminal liability for theft involving digital technologies committed under aggravating and non-aggravating circumstances. To enhance the effectiveness of these amendments, it is proposed to develop judicial guidance in the form of a Resolution of the Plenum of the Supreme Court of the Russian Federation.

Keywords: fraud, theft, «computer crimes» chapter, cyberattacks, digital technologies.

References

1. The Ministry of Internal Affairs reported a decrease in the number of cybercrimes in the Russian Federation in 2025 by 12% // Interfax. – 02/18/2026 [Electronic

resource]. URL: https://www.interfax.ru/digital/1073418 (date of request: 08.10.2026)
2. Popova, E.M. Qualification of theft using information and telecommunication technologies: problems of theory and practice of application of art. 159.6 of the Criminal Code of the Russian Federation / E.M. Popova // Police and investigative activities. – 2026. – No. 2. [Electronic resource]. URL: https://nbpublish.com/library_read_article.php?id=79149 (date of request: 05.10.2026)
3. Resolution of the Plenum of the Supreme Court of the Russian Federation dated December 15, 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" [Electronic resource]. URL: https://www.garant.ru/products/ipo/prime/doc/405863329 / (date of request: 10/15/2026)
4. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 11/30/2017 No. 48 (as amended on 12/15/2022) "On judicial practice in cases of fraud, embezzlement and embezzlement." [electronic resource]. URL: https://www.consultant.ru/document/cons_doc_LAW_283918 / (date of access: 09/28/2026)
5. The Prosecutor's Office of the Moscow district of Kaliningrad explains: "On responsibility for theft from a bank account" // Prosecutor's Office of the Kaliningrad region [Electronic resource]. URL: https://epp.genproc.gov.ru/ru/proc_39/activity/legal-education/explain/criminal_law/e372159 / (date of request: 04.10.2026)
6. Smolyakov, A. N. Theft of non–cash, electronic money and digital currency: issues of legal technique and differentiation of responsibility : dissertation of Candidate of Law sciences : 5.1.4 / Smolyakov Alexander Nikolaevich. - St. Petersburg, 2023. – 250 p.
7. Khabyev, H. Problems of fraud qualification in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation) / H.Khabyev // Current research. 2026. No. 25 (311). Part III. pp. 14-16. [electronic resource]. URL: https://apni.ru/article/15558-problemy-kvalifikacii-moshennichestva-v-sfere-kompyuternoj-informacii-statya-1596-uk-rf (date of request: 01.10.2026)
8. Khalikov, A. N. The problem of qualification of remote theft as a separate crime / A. N. Khalikov // Eurasian Advocacy. – 2025. – No. 4. – p. 117.
9. 2026 Trends in Information Security [Electronic resource]. URL: https://pages.marketintelligence.spglobal.com/15701-MS-2512-GL-TMT-DR-451R-NA-2026-Trends-in-Tech_04A---Information-Security.html (date of request: 05.10.2026).