УДК 343.9 **DOI: 10.34670/AR.2026.19.30.066**

Уголовно-правовые риски в условиях цифровизации и способа противодействия им

Магомедов Давди Бадавиевич

Кандидат педагогических наук,
доцент кафедры уголовного права и криминологии,
Дагестанский государственный университет,
367000, Российская Федерация, Махачкала, ул. Гаджиева, 43-а;
e-mail: mdb2@mail.ru

Мамайханов Ислам Рашитханович

Магистрант,
Дагестанский государственный университет,
367000, Российская Федерация, Махачкала, ул. Гаджиева, 43-а;
e-mail: ivanm160404@mail.ru

Аннотация

Скорость, с которой преступность осваивает цифровую среду, устойчиво опережает темп уголовного нормотворчества, и этот разрыв порождает особый класс уголовно-правовых рисков – от пробельности закона до конкуренции наспех принятых специальных норм. Возникает противоречие: законодатель вынужден реагировать быстро, но реактивная криминализация привязывает нормы к преходящим техническим формам и плодит коллизии с действующими составами хищения. Цель работы – оценить, насколько уголовно-правовой инструментарий, сформированный в России в 2025 году, отвечает реальной структуре цифровых рисков, и предложить решения, снимающие выявленные противоречия. Применены формально-юридический и сравнительно-правовой методы, системное и телеологическое толкование, обобщение судебной практики; привлечён риск-ориентированный подход. Установлено, что новеллы 2025 года закрыли ряд пробелов: криминализированы дропперство, незаконный оборот SIM-карт и аккаунтов, нанесён удар по инфраструктуре телефонного мошенничества. Вместе с тем они воспроизвели казуистичность и породили конкуренцию с нормами о мошенничестве; при этом снижение числа регистрируемых деяний сопровождалось ростом ущерба. Обоснованы предложения de lege ferenda: функциональное описание цифрового орудия в главе 28, разъяснение Пленума о разграничении смежных составов, обязательная криминологическая экспертиза новелл. Результаты применимы в законопроектной работе и в практике уголовно-правовой квалификации.

Для цитирования в научных исследованиях

Магомедов Д.Б., Мамайханов И.Р. Уголовно-правовые риски в условиях цифровизации и способы противодействия им // Вопросы российского и международного права. 2026. Том 16. № 5А. С. 585-596. DOI: 10.34670/AR.2026.19.30.066

Ключевые слова

Уголовно-правовые риски, цифровизация, киберпреступность, дропперство, конкуренция уголовно-правовых норм, противодействие преступности, статья 187 УК РФ, криминологическая экспертиза.

Введение

Темп, с которым преступность осваивает цифровую среду, давно обогнал законодателя. По данным МВД России, в 2024 году в стране зарегистрировано 765,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий, – на 13,1 % больше, чем годом ранее, а их удельный вес в структуре преступности поднялся до 40 % против примерно 20 % в 2020 году. Рост шёл не первый год. Уголовный закон отвечал с запаздыванием – точечными поправками, описывающими уже устоявшиеся схемы, но не упреждающими их появление. Разрыв между скоростью технологической трансформации и инерцией нормотворчества обозначили ещё в начале десятилетия В. П. Кириленко и Г. В. Алексеев [Кириленко, Алексеев, 2021]. С тех пор он скорее углубился, чем сократился.

Само понятие уголовно-правового риска в цифровом контексте трактуется неединообразно. Под ним понимают то угрозу появления деяний, не охваченных действующими составами, то опасность ошибочной квалификации при переносе традиционных конструкций на новую фактуру, то – в более широком смысле – вероятность того, что уголовно-правовое регулирование окажется либо избыточным, либо запоздалым. Р. В. Шишкин [Шишкин, 2024] сводит риск преимущественно к пробельности закона; Т. И. Матюхина [Мойченко, 2025] смещает акцент на сторону правоприменения, где цифровой след одновременно облегчает доказывание и порождает новые поводы для его фальсификации. Расхождение не терминологическое. От того, что считать источником риска, зависит и выбор средства противодействия – законодательного, правоприменительного либо организационного.

Минувший год принёс необычно плотную серию уголовно-правовых новелл, прямо адресованных цифровой преступности. За несколько месяцев законодатель криминализировал дропперство, незаконный оборот SIM-карт и аккаунтов, перестроил профилактический контур вокруг новой государственной информационной системы. О. С. Капинус [Капинус, 2022] предупреждала, что цифровизация преступности рано или поздно вынудит уголовное право к структурной, а не косметической перестройке. Реформа 2025 года – первая попытка такого рода.

Отсюда – задача настоящей работы. Требуется оценить, насколько инструментарий, появившийся в 2025 году, отвечает реальной структуре цифровых рисков, где он создаёт новые коллизии и конкуренцию норм и какие решения de lege ferenda способны снять обнаруженные противоречия. Г. Р. Галеева, С. В. Дубовиченко и А. А. Иванов [Галеева, Дубовиченко, Иванов, 2023] замечают, что цифровизация уголовного права рискует выродиться в простое умножение специальных составов. Проверке этого опасения подчинён дальнейший разбор.

Материалы и методы исследования

Работа опирается на формально-юридический (догматический) метод, дополненный системным и телеологическим толкованием норм, методом юридической квалификации и обобщением судебной практики. Сопоставление редакций Уголовного кодекса до и после

реформы 2025 года потребовало сравнительно-правового приёма в его внутригосударственном, диахронном варианте. Там, где речь шла о переносе регуляторных конструкций из смежных отраслей, привлекался риск-ориентированный подход, описанный применительно к борьбе с киберпреступностью А. Д. Трушаниной [Трушанина, 2025]. Метод этот для уголовного права непривычен.

Нормативную основу составили Уголовный кодекс Российской Федерации в редакции федеральных законов от 24 июня 2025 г. № 176-ФЗ и от 31 июля 2025 г. № 282-ФЗ, Федеральный закон от 1 апреля 2025 г. № 41-ФЗ о государственной информационной системе противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, а также разъяснения Пленума Верховного Суда Российской Федерации по делам о хищениях. Фактологический контур задан официальной статистикой МВД России за 2024–2025 годы. Числовые показатели приводятся по ведомственным публикациям; динамика прослеживается до последних обнародованных данных 2025 года.

Результаты и обсуждение

Цифровая трансформация преступности затрагивает саму морфологию посягательства, проникая глубже отдельных составов. В. А. Тирранен [Тирранен, 2025] описывает её как смену носителя преступной активности: деяние утрачивает привязку к физическому пространству, орудие становится программным, а соучастие – распределённым и анонимным. На этом фоне уголовно-правовые риски удобно разложить на четыре слоя, хотя границы между ними подвижны.

Первый слой – появление деяний, для которых в Кодексе нет адекватной формы. Е. Ю. Антонова [Антонова, 2022] относит сюда целые сегменты теневой цифровой экономики, выросшие быстрее, чем успевала реагировать догматика. Второй – трансформация привычных преступлений: хищение, вымогательство, сбыт запрещённого мигрируют в дистанционный формат, сохраняя объект, но меняя способ до неузнаваемости. Третий слой – риски правоприменения: квалификация по аналогии, трудность установления места совершения деяния, зависимость доказывания от волатильных цифровых следов. Четвёртый, о котором говорят реже, – риск избыточной реакции, когда законодатель, торопясь закрыть пробел, вводит специальную норму там, где хватило бы толкования общей.

Слои эти не равнозначны. Практический вес сместился ко второму и третьему – именно там сосредоточена основная масса регистрируемых деяний, тогда как доктринальная тревога чаще адресуется первому. Перекос объясним. Новое пугает сильнее, чем количественно разросшееся старое.

Чтобы оценить точность реакции, стоит вспомнить, как устроена сама глава 28 УК РФ. Её ядро сложилось из четырёх норм: статья 272 карает неправомерный доступ к охраняемой компьютерной информации, статья 273 – создание и оборот вредоносных программ, статья 274 – нарушение правил эксплуатации средств хранения и обработки данных, а статья 274.1 с 2017 года защищает критическую информационную инфраструктуру. Объект здесь узок и понятен – безопасность обращения с компьютерной информацией. Долгое время глава жила этим скромным набором, лишь точечно достраиваясь. Архитектура была цельной.

Реформа 2025 года поместила в эту главу статьи 274.3, 274.4 и 274.5 – о терминалах пропуска трафика, абонентских номерах и данных авторизации. Формально соседство

объяснимо: все они вращаются вокруг цифровой среды. По существу же охраняемый интерес сместился. Новые составы берегут уже иное – надёжность платёжной и коммуникационной инфраструктуры, через которую проходит чужое преступление; целостность компьютерной информации отходит на второй план. Глава, задуманная как защита данных, обросла разнородными запретами. Объект расплылся.

Статистика последних лет рисует картину менее линейную, чем ожидалось. Пик пришёлся на 2024 год: 765,4 тыс. зарегистрированных деяний, 40 % в структуре преступности, причём около 85 % из них (649,1 тыс.) совершены через интернет, а 346 тыс. – с использованием мобильной связи. Ущерб от дистанционных хищений за январь–ноябрь 2024 года МВД России оценило в 168 млрд руб.

Затем кривая повела себя неожиданно. По итогам 2025 года число преступлений, совершённых с использованием информационно-телекоммуникационных технологий, снизилось на 11,8 % к предыдущему году; дистанционные кражи просели на 23,6 %, дистанционные мошенничества – на 9 %, а деяния в сфере компьютерной информации – сразу на 42,2 %. Доля цифровых посягательств отступила от сорокапроцентной отметки, оставшись, впрочем, выше трети всего массива. Снижение регистрируемых деяний редко означает снижение реальной угрозы.

Параллельно с падением числа дел рос ущерб. За первые пять месяцев 2025 года он прибавил порядка 23 % и достиг 81 млрд руб. при 308 тыс. зарегистрированных деяний. Расхождение между убывающим количеством и растущим вредом – самый показательный сигнал периода. По всей видимости, оно отражает укрупнение и профессионализацию схем: меньше эпизодов, но каждый дороже. Р. И. Дремлюга и А. И. Коробеев [Дремлюга, Коробеев, 2022] связывают эту тенденцию с платформизацией преступной деятельности, при которой разовый исполнитель замещается устойчивым сервисом, продающим преступление как услугу. Сорокапроцентное падение по компьютерным составам на этом фоне выглядит подозрительно резким – вероятнее, часть деяний переучтена в смежные рубрики, а не исчезла.

Стоит присмотреться и к тому, на кого ложится ущерб. Основную тяжесть дистанционных хищений несут граждане – пенсионеры, доверчиво переводящие сбережения «сотруднику банка», молодёжь, втянутая в фиктивные инвестиции, люди в стрессовой ситуации, на которой играет социальная инженерия. Корпоративные потери крупнее в пересчёте на эпизод, зато массив пострадавших – это рядовые держатели карт. Рост среднего чека хищения при сжатии их числа говорит о смещении преступников к более подготовленным и доходным атакам. Жертву всё чаще выбирают прицельно. За сухими процентами стоит конкретная разорённая семья.

Любые цифры здесь следует читать с поправкой на латентность. Дистанционные посягательства регистрируются заведомо неполно: часть потерпевших не обращается в полицию из-за стыда или неверия в результат, часть эпизодов дробится на множество мелких списаний ниже порога внимания, часть вовсе не осознаётся жертвой как преступление. Оценки скрытой части разнятся, но сходятся в одном – видимая статистика показывает лишь вершину. Поэтому спад регистрации 2025 года допустимо объяснять не только реальным сжатием угрозы, но и тем, что заявлять о хищении люди стали реже либо иначе. Снижение цифры и снижение опасности – не синонимы. Тёмное число остаётся тёмным.

Вывод напрашивается осторожный. Цифры спада 2025 года не следует читать как успех противодействия. Скорее они фиксируют перестройку рынка преступных услуг.

Понять, почему точечные запреты буксуют, помогает взгляд на устройство современной

цифровой преступности. Она давно переросла фигуру одиночки и обрела черты индустрии: одни пишут вредоносный код, другие держат колл-центры социальной инженерии, третьи поставляют SIM-карты и дропперов, четвёртые обналичивают и отмывают добытое. Каждое звено продаётся как самостоятельная услуга и легко замещается при выбытии. Преступный бизнес устроен модульно. Выбивая один модуль отдельной статьёй, правоприменитель сталкивается с тем, что рынок быстро отращивает замену. Поэтому давление приходится распределять по всей цепочке сразу – технически, финансово, организационно, – а уголовная норма работает лишь как один из рычагов. В одиночку статья цепь не рвёт.

Законодательный ответ 2025 года заслуживает отдельного разбора – хотя бы потому, что по плотности новелл он не имеет аналогов в новейшей истории главы о компьютерных преступлениях. Три акта задают его каркас.

Федеральный закон от 24 июня 2025 г. № 176-ФЗ дополнил статью 187 УК РФ частями третьей–шестой, впервые прямо криминализировав дропперство. Состав охватывает передачу электронного средства платежа либо доступа к нему другому лицу для неправомерных операций, равно как и совершение таких операций по чужому указанию из корыстной заинтересованности. Санкция по части четвёртой – штраф от 100 до 300 тыс. руб. либо лишение свободы на срок до трёх лет. Норма вступила в силу 5 июля 2025 года. Прежде фигура дроппера квалифицировалась через пособничество в мошенничестве, что давало защите слишком много пространства; М. А. Ефремова [Ефремова, 2024] относила подобные конструкции к числу наиболее уязвимых средств противодействия. Новая часть закрывает этот зазор.

Спустя считаные недели Федеральный закон от 31 июля 2025 г. № 282-ФЗ ввёл сразу несколько новых статей. Статья 274.4 УК РФ установила ответственность за организацию деятельности по передаче абонентских номеров в нарушение требований законодательства, если она продиктована корыстью либо умыслом на иное преступление; статья 274.5 распространила сходную логику на передачу данных для авторизации в интернет-аккаунтах; статья 274.3 ударила по инфраструктуре телефонного мошенничества – незаконному использованию терминалов пропуска трафика и виртуальных АТС, тех самых SIM-боксов. Статья 274.4 заработала с 1 сентября 2025 года, а верхний предел санкции по ней доходит до трёх лет лишения свободы и штрафа до 700 тыс. руб.

Логика этих норм отличается от прежней. Удар наносится не по конечному хищению, а по обеспечивающему звену – по тем, кто поставляет преступникам платёжные и коммуникационные инструменты. Тем же законом перечень отягчающих обстоятельств пополнился совершением преступления с использованием программно-аппаратных средств доступа к информационным ресурсам с ограниченным доступом. Сдвиг от результата к инфраструктуре в доктрине предвидели: Е. И. Сейфетдинова [Сейфетдинова, 2025] увязывала противодействие цифровой преступности с защитой инфраструктурного слоя национальной безопасности, что выходит за пределы наказания за отдельный эпизод. Смещение фокуса методологически оправдано.

И всё же смещение далось ценой системной стройности. Поместив инфраструктурные запреты рядом с неправомерным доступом, законодатель свёл в одной главе деяния с несхожими объектами и разной природой вреда. Продавец SIM-карт компьютерную информацию не трогает; его роль – снабдить посторонних средством анонимной связи. Кассир теневого обнала систему не взламывает; он лишь проводит чужие деньги. Объединять столь разные посягательства под общей рубрикой удобно для учёта, но рискованно для квалификации:

суд вынужден всякий раз заново отыскивать охраняемый интерес. Стройность приносится в жертву скорости.

Третий акт – Федеральный закон от 1 апреля 2025 г. № 41-ФЗ – лежит вне уголовно-правовой плоскости, но без него картина неполна. Он учредил государственную информационную систему противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и возложил на банки, операторов связи и государственный сектор обязанности по выявлению подозрительных операций. С. Я. Лебедев и В. Ф. Джафарли [Лебедев, Джафарли, 2024] описывают формирующееся цифровое уголовное право как замыкающий контур, который без предупредительной и регуляторной обвязки повисает в воздухе. Закон № 41-ФЗ – попытка собрать эту обвязку в единый механизм.

Плотность новелл породила собственную проблему – конкуренцию норм. Часть четвёртая статьи 187 соседствует с мошенничеством с использованием электронных средств платежа (статья 159.3) и мошенничеством в сфере компьютерной информации (статья 159.6), а также с общим составом хищения. Где заканчивается неправомерная операция дроппера и начинается соучастие в мошенничестве – вопрос, на который текст закона прямого ответа не даёт.

Разграничение упирается в субъективную сторону и в момент окончания деяния. Если дроппер охвачен единым умыслом с организатором хищения, логичнее вменять соучастие в мошенничестве; если же его роль ограничена обналичиванием и он безразличен к судьбе конкретной жертвы, на первый план выходит самостоятельный состав по статье 187. Граница тонкая, и практика рискует развести сходные ситуации по разным статьям с несопоставимыми санкциями. Действующие разъяснения – постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (в редакции от 15 декабря 2022 г.) о судебной практике по делам о мошенничестве, присвоении и растрате – приняты до реформы и новой коллизии не касаются. А. С. Перина [Перина, 2023] обращала внимание, что в цифровой среде потерпевший нередко выпадает из поля зрения квалификатора, тогда как его интерес и определяет объект посягательства. Без потерпевшего состав теряет ориентир.

Добавляет неясности и момент окончания. Новые статьи 274.4 и 274.5 сконструированы как формальные составы – деяние окончено с момента организации передачи номеров или данных, безотносительно к тому, состоялось ли потом хищение. Дропперская часть статьи 187 устроена сходно. Отсюда практический парадокс. Пособник будущего мошенничества может оказаться наказан раньше, чем наступит сам ущерб, а порой и строже, чем тот потребовал бы. Привязка наказания к стадии организации, минуя итоговый вред, смещает тяжесть репрессии на подготовительный этап. Стадия ранняя – а спрос с неё взрослый.

Остаётся вопрос о нижней границе наказуемого. Сама по себе передача SIM-карты или учётной записи правомерна и буднична – люди отдают старые номера родственникам, продают аккаунты, делятся доступом к сервисам. Уголовным деяние становится лишь при корыстной заинтересованности либо цели совершить иное преступление; этот субъективный признак и отделяет преступление от безобидной бытовой сделки. Граница хрупкая. Стоит правоприменителю истолковать корысть расширительно, и под подозрение рискует попасть добросовестный продавец подержанного телефона. Диспозиция требует осторожного прочтения, иначе охват нормы расползётся за пределы замысла.

Тревожит и другое. Законодатель пошёл по пути дробной казуистики – отдельная статья на SIM-карты, отдельная на аккаунты, отдельная на терминалы трафика. Р. А. Забавко и

Т. И. Забавко [Забавко, Забавко, 2025] предупреждают, что «цифровизация» уголовного закона методологически неверно сводится к перечислению технических средств, поскольку техника устаревает быстрее, чем правится Кодекс. Норма, привязанная к SIM-боксу, рискует устареть вместе с ним. Рамочная конструкция, описывающая функцию вместо устройства, оказалась бы долговечнее.

Что из этого следует для способов противодействия. Уголовно-правовой инструмент 2025 года закрыл несколько зиявших пробелов, но воспроизвёл старую болезнь – реактивность и казуистичность. Лечится она переменой самой техники их конструирования; отказ от новелл проблему не снимет.

В способах противодействия проступают две конкурирующие философии. Первая делает ставку на устрашение: новые статьи, выше санкции, шире составы. Вторая – на предупреждение: техническое блокирование схем, финансовый мониторинг, антифрод-системы, просвещение потенциальных жертв. Реформа 2025 года качнулась к первой, добавив сразу несколько составов, и лишь законом № 41-ФЗ обозначила вторую. Перекос объясним инерцией: расширить Кодекс быстрее и заметнее, чем выстроить профилактику. Но устрашение упирается в предел – нельзя бесконечно повышать сроки там, где исполнитель и так заменим. Запас прочности у репрессии невелик.

Предупредительная философия упирается в трансграничность угрозы. Серверы, платёжные шлюзы и операторы схем рассредоточены по юрисдикциям, и в одиночку национальный закон цепь не разрывает. Отсюда ценность согласованных стандартов – общих определений деяний, ускоренных каналов обмена данными, взаимного признания цифровых доказательств. Полная гармонизация в нынешней международной обстановке труднодостижима, однако частные технические договорённости между правоохранителями возможны и полезны. Изоляция же играет на руку преступнику, которому границы только удобны. Сеть не признаёт границ – противодействие тоже не должно.

Перспективным выглядит перенос риск-ориентированной логики из финансового регулирования в уголовную политику – ради приоритизации правоохранительного ресурса, без криминализации риска как такового. А. Л. Осипенко и В. С. Соловьев [Осипенко, Соловьев, 2021] выстраивают вокруг цифровой преступности развёрнутый предупредительный контур, в котором уголовная репрессия занимает подчинённое место по отношению к ранней профилактике и техническому блокированию схем. Подход созвучен идее замыкающего контура. Карать дешевле, чем предупреждать, но эффект обратный.

Нельзя обойти и человеческое измерение дропперства. Исполнителями нижнего звена чаще становятся подростки, студенты, люди в денежной нужде, откликнувшиеся на объявление о лёгком заработке. Формально они субъекты преступления; по сути – расходный материал в чужой схеме, втянутый обманом и плохо понимающий последствия. Уголовный удар по ним бьёт точно, но мимо организатора, который остаётся в тени и набирает новых. Возникает риск символической репрессии: статистика раскрытий растёт, а корень проблемы цел. Отсюда ценность не только кары, но и девиктимизации – разъяснения, ранней профилактики, перекрытия каналов вербовки. Карать звено проще, чем разрушить цепь.

Цифровая природа деяний обостряет и старый вопрос о месте их совершения. Исполнитель может сидеть в одном регионе, сервер – в другом государстве, жертва – в третьем. Территориальный принцип действия уголовного закона, закреплённый в статьях 11 и 12 УК РФ, рассчитан на деяние с ясной географией. Когда же преступление распылено по сети, установить

место его окончания порой невозможно без запроса в иностранную юрисдикцию. От скорости и доброй воли зарубежного партнёра зависит судьба доказательств. Национальная норма, сколь угодно строгая, упирается в границу. Закон есть – дотянуться трудно.

Трудность с местом дополняется трудностью с лицом. Анонимизирующие сервисы, цепочки прокси, чужие учётные записи и подставные абонентские номера разрывают связь между действием и его автором. Установить, кто сидел за клавиатурой, порой тяжелее, чем доказать сам факт посягательства. А без надёжной атрибуции рушится субъективная сторона: умысел, корысть, цель – всё это надо вменить конкретному человеку, тогда как перед следствием нередко лишь обезличенный сетевой адрес. Здесь и обнаруживается смысл новых инфраструктурных статей. Перекрывая каналы анонимности у их источника, они косвенно облегчают будущую атрибуцию. Запрет на поставку анонимности работает на доказывание.

Конкретные предложения сводятся к трём. Во-первых, главу 28 УК РФ стоит снабдить унифицирующим примечанием, которое описывало бы цифровое орудие через выполняемую функцию, минуя его текущее техническое воплощение, – это сняло бы нужду плодить статьи под каждое новое устройство. Во-вторых, назрело разъяснение Пленума Верховного Суда о разграничении части четвёртой статьи 187 и статей 159.3, 159.6, без которого судебная практика разойдётся по регионам. В-третьих, каждую новеллу о цифровых составах разумно проводить через обязательную криминологическую экспертизу, проверяющую, упреждает она угрозу или лишь догоняет её.

Первое из предложений стоит пояснить подробнее. Унифицирующее примечание к главе 28 могло бы определить цифровое орудие через выполняемую им функцию: обеспечение анонимного доступа, проведение или сокрытие операции, маскировку источника связи. От того, реализована ли функция через SIM-бокс, виртуальную АТС или ещё не изобретённое устройство, квалификация при этом не зависела бы. Тогда появление новой технологии не потребовало бы новой статьи: деяние подпадало бы под уже существующую функциональную формулу. Техника описания через назначение, минуя привязку к конкретному железу, давно освоена в смежных отраслях права. Уголовный закон здесь отстаёт без веской причины. Функция долговечнее устройства.

Последнее заслуживает развёртывания. Криминологическая экспертиза новелл – не бюрократическая формальность, а доступный способ разорвать порочный круг «новая схема – запоздалая статья – устаревшая статья». Реформа 2025 года показала, что законодатель умеет действовать быстро; чего ему недостаёт, так это упреждающего взгляда, способного предвидеть следующую итерацию преступной технологии прежде, чем она наберёт массовость. Предсказуемые направления удара известны заранее: биометрия, токенизированные активы, генеративные модели для социальной инженерии. Закон же приходит к ним последним.

Сюда примыкает риск, о котором в спорах о санкциях вспоминают в последнюю очередь, – хрупкость доказательственной базы. Цифровой след недолговечен: логи перетираются, переписка удаляется, криптокошельки меняют адреса за часы. Норма может быть выверена безупречно и всё же остаться мёртвой, если к моменту изъятия фиксировать уже нечего. Скорость реакции правоохранителя весит здесь не меньше, чем точность формулировки состава. Получается, что эффективность свежих статей решается за пределами их текста – технической готовностью собрать и сохранить улики прежде, чем они растворятся. Хорошая норма без быстрой фиксации бесполезна.

Если свести разбор воедино, реформа 2025 года продвинула противодействие цифровой

преступности по двум направлениям – закрыла пробел вокруг дропперства и впервые ударила по инфраструктуре телефонного мошенничества. Достижения реальны, и недооценивать их не стоит.

Уязвимости, однако, лежат глубже отдельных составов. Они коренятся в самой технике нормотворчества – в привязке норм к преходящим техническим формам и в нерешённой конкуренции с давно действующими составами хищения. Пока эта техника не изменится, каждая следующая волна цифровых угроз будет заставать уголовный закон врасплох.

Заключение

Оценивая итог, приходится признать двойственность результата. За один год уголовный закон обзавёлся статьями против дропперов, продавцов SIM-карт и аккаунтов, операторов терминалов трафика, а заодно – государственной информационной системой, замкнувшей предупредительный контур. Скорость беспрецедентна. И всё же набор новелл собран по принципу заплат: каждая закрывает конкретную дыру, ни одна не меняет логики, по которой эти дыры возникают. Привязка к технике обрекает свежие статьи на скорое старение. Конкуренция со статьями 159.3 и 159.6 оставлена практике без ориентира. Реактивность осталась.

На фоне законодательной активности статистика повела себя непривычно. Число дел в 2025 году упало почти на 12 %, тогда как ущерб в первой половине года рос. Спад регистрации – не победа.

Объяснение этому контрасту даёт сам рынок преступных услуг: он укрупняется, и меньшее число эпизодов приносит больший вред. Значит, и противодействие придётся мерить способностью предвидеть очередную схему до того, как она станет массовой; счёт возбуждённых дел тут обманчив. Инструмент для этого один – обязательная криминологическая экспертиза цифровых новелл, переводящая уголовную политику из догоняющего режима в упреждающий. Пока же баланс таков: ущерб от дистанционных хищений только за пять месяцев 2025 года составил 81 млрд руб.

Библиография

1. Антонова Е. Ю. Новые формы преступной деятельности в условиях цифровизации // Ученые записки юридического факультета. 2022. № 1. С. 18–23.
2. Галеева Г. Р., Дубовиченко С. В., Иванов А. А. Цифровизация уголовного права // Вестник Волжского университета им. В.Н. Татищева. 2023. Т. 2, № 4 (106). С. 70–81.
3. Дремлюга Р. И., Коробеев А. И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности // Всероссийский криминологический журнал. 2022. Т. 16, № 1. С. 47–56.
4. Ефремова М. А. Уголовно-правовые средства противодействия преступности в условиях цифровизации // Вестник Южно-Уральского государственного университета. Серия: Право. 2024. Т. 24, № 2. С. 21–26.
5. Забавко Р. А., Забавко Т. И. Теоретико-методологические подходы к «цифровизации» уголовного закона // Академический юридический журнал. 2025. Т. 26, № 3 (101). С. 501–510.
6. Капинус О. С. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13, № 1.
7. Кириленко В. П., Алексеев Г. В. Киберпреступность и цифровая трансформация // Теоретическая и прикладная юриспруденция. 2021. № 1. С. 39–53.
8. Лебедев С. Я., Джафарли В. Ф. о. Цифровое уголовное право: перспективы формирования и развития (часть 2) // Гуманитарные, социально-экономические и общественные науки. 2024. № 12. С. 166–170.
9. Мойченко А. Б. Интеграция спутникового и наземного мониторинга с промышленными датчиками для оперативного выявления нарушений природопользования на трубопроводной инфраструктуре // Вопросы природопользования. 2025. Т. 4, № 6. С. 50–59.
10. Осипенко А. Л., Соловьев В. С. Основные направления развития криминологической науки и практики

предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 681–691.
11. Перина А. С. Уголовно-правовые инструменты охраны личности в условиях цифровизации // Виктимология. 2023. Т. 10, № 2. С. 193–203.
12. Сейфетдинова Е. И. Уголовно-правовое противодействие цифровой преступности в целях обеспечения национальной безопасности Российской Федерации // Евразийский юридический журнал. 2025. № 2 (201). С. 314–315.
13. Тирранен В. А. Цифровая трансформация современной преступности // Уголовное право: стратегия развития в XXI веке. 2025. № 4. С. 5–11.
14. Трушанина А. Д. Трансформация риск-ориентированного подхода для борьбы с кибер-преступностью в условиях цифровизации // Вестник евразийской науки. 2025. Т. 17, № S1.
15. Шишкин Р. В. Уголовно-правовые риски в условиях цифровой трансформации и противодействие им // Право и государство: теория и практика. 2024. № 9 (237). С. 503–506.

Criminal Law Risks in the Context of Digitalization and Methods of Counteracting Them

Davdi B. Magomedov

PhD in Pedagogy,
Associate Professor of the Department of Criminal Law and Criminology,
Dagestan State University,
367000, 43-a, Gadzhieva str., Makhachkala, Russian Federation;
e-mail: mdb2@mail.ru

Islam R. Mamaikhanov

Master's Student,
Dagestan State University,
367000, 43-a, Gadzhieva str., Makhachkala, Russian Federation;
e-mail: ivanm160404@mail.ru

Abstract

The speed with which crime masters the digital environment steadily outpaces the rate of criminal rulemaking, and this gap generates a special class of criminal law risks – from gaps in the law to the competition of hastily adopted special norms. A contradiction arises: the legislator is forced to react quickly, but reactive criminalization ties norms to transient technical forms and creates collisions with the existing elements of theft. The objective of the work is to assess the extent to which the criminal law instruments formed in Russia in 2025 correspond to the real structure of digital risks, and to propose solutions that remove the identified contradictions. Formal-legal and comparative-legal methods, systemic and teleological interpretation, generalization of judicial practice have been applied; a risk-oriented approach has been employed. It has been established that the novelties of 2025 closed a number of gaps: drop activity, illegal trafficking of SIM cards and accounts have been criminalized, and a blow has been dealt to the infrastructure of telephone fraud. At the same time, they reproduced casuistry and generated competition with the norms on fraud; meanwhile, the decrease in the number of registered acts was accompanied by an increase in damage. Proposals de lege ferenda have been substantiated: a functional description of a digital instrument

in Chapter 28, a clarification of the Plenum on the delimitation of related elements, and mandatory criminological expertise of novelties. The results are applicable in legislative drafting work and in the practice of criminal law qualification.

For citation

Magomedov D.B., Mamaikhanov I.R. (2026) Ugolovno-pravovye riski v usloviyakh tsifrovizatsii i sposoby protivodeystviya im [Criminal Law Risks in the Context of Digitalization and Methods of Counteracting Them]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (5A), pp. 585-596. DOI: 10.34670/AR.2026.19.30.066

Keywords

Criminal law risks, digitalization, cybercrime, drop activity, competition of criminal law norms, crime counteraction, Article 187 of the Criminal Code of the Russian Federation, criminological expertise.

References

1. Antonova, E. Yu. (2022). Novye formy prestupnoy deyatelnosti v usloviyakh tsifrovizatsii [New forms of criminal activity in the conditions of digitalization]. Uchenye zapiski yuridicheskogo fakulteta, 1, 18-23.
2. Dremlyuga, R. I., & Korobeev, A. I. (2022). Ugolovno-pravovaya politika v sfere protivodeystviya platformizatsii prestupnoy deyatelnosti [Criminal law policy in the sphere of countering the platformization of criminal activity]. Vserossiyskiy kriminologicheskiy zhurnal, 16(1), 47-56.
3. Efremova, M. A. (2024). Ugolovno-pravovye sredstva protivodeystviya prestupnosti v usloviyakh tsifrovizatsii [Criminal law means of countering crime in the conditions of digitalization]. Bulletin of the South Ural State University. Series: Law, 24(2), 21-26.
4. Galeeva, G. R., Dubovichenko, S. V., & Ivanov, A. A. (2023). Tsifrovizatsiya ugolovnogo prava [Digitalization of criminal law]. Vestnik Volzhskogo universiteta im. V.N. Tatishcheva, 2(4), 70-81.
5. Kapinus, O. S. (2022). Tsifrovizatsiya prestupnosti i ugolovnoe pravo [Digitalization of crime and criminal law]. Baikal Research Journal, 13(1).
6. Kirilenko, V. P., & Alekseev, G. V. (2021). Kiberprestupnost i tsifrovaya transformatsiya [Cybercrime and digital transformation]. Teoreticheskaya i prikladnaya yurisprudentsiya, 1, 39-53.
7. Lebedev, S. Ya., & Dzhafarli, V. F. o. (2024). Tsifrovoe ugolovnoe pravo: perspektivy formirovaniya i razvitiya (chast 2) [Digital criminal law: prospects for formation and development (part 2)]. Gumanitarnye, sotsialno-ekonomicheskie i obshchestvennye nauki, 12, 166-170.
8. Moychenko, A. B. (2025). Integratsiya sputnikovogo i nazemnogo monitoringa s promyshlennymi datchikami dlya operativnogo vyyavleniya narusheniy prirodopolzovaniya na truboprovodnoy infrastrukture [Integration of satellite and ground monitoring with industrial sensors for rapid detection of environmental violations on pipeline infrastructure]. Voprosy prirodopolzovaniya, 4(6), 50-59.
9. Osipenko, A. L., & Solovyev, V. S. (2021). Osnovnye napravleniya razvitiya kriminologicheskoy nauki i praktiki preduprezhdeniya prestupleniy v usloviyakh tsifrovizatsii obshchestva [Main directions of the development of criminological science and the practice of crime prevention in the conditions of digitalization of society]. Vserossiyskiy kriminologicheskiy zhurnal, 15(6), 681-691.
10. Perina, A. S. (2023). Ugolovno-pravovye instrumenty okhrany lichnosti v usloviyakh tsifrovizatsii [Criminal law instruments for the protection of the individual in the conditions of digitalization]. Viktimologiya, 10(2), 193-203.
11. Seyfetdinova, E. I. (2025). Ugolovno-pravovoe protivodeystvie tsifrovoy prestupnosti v tselyakh obespecheniya natsionalnoy bezopasnosti Rossiyskoy Federatsii [Criminal law counteraction to digital crime for ensuring the national security of the Russian Federation]. Evraziyskiy yuridicheskiy zhurnal, 2(201), 314-315.
12. Shishkin, R. V. (2024). Ugolovno-pravovye riski v usloviyakh tsifrovoy transformatsii i protivodeystvie im [Criminal law risks in the conditions of digital transformation and countering them]. Pravo i gosudarstvo: teoriya i praktika, 9(237), 503-506.
13. Tirranen, V. A. (2025). Tsifrovaya transformatsiya sovremennoy prestupnosti [Digital transformation of modern crime]. Ugolovnoe pravo: strategiya razvitiya v XXI veke, 4, 5-11.
14. Trushanina, A. D. (2025). Transformatsiya risk-orientirovannogo podkhoda dlya borby s kiber-prestupnostyu v usloviyakh tsifrovizatsii [Transformation of the risk-oriented approach to combating cybercrime in the conditions of digitalization]. Vestnik evraziyskoy nauki, 17(S1).

15. Zabavko, R. A., & Zabavko, T. I. (2025). Teoretiko-metodologicheskie podkhody k "tsifrovizatsii" ugolovnogo zakona [Theoretical and methodological approaches to the "digitalization" of criminal law]. Akademicheskiy yuridicheskiy zhurnal, 26(3), 501-510.