Дата поступления рукописи в редакцию: 27.07.2026 г.
Дата принятия рукописи в печать: 01.09.2026 г.
DOI: 10.24412/2224-9133-2026-8-28-35

ТАРАСОВ Александр Анатольевич,
старший преподаватель Департамента уголовного права, процесса и криминалистики Факультета права Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ), ORCID: 0000-0078-9276-5211, e-mail: tarasov.aa@hse.ru

ПРОТИВОДЕЙСТВИЕ ЦИФРОВОМУ МОШЕННИЧЕСТВУ И ВОВЛЕЧЕНИЮ В ТЕРРОРИЗМ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация. *В статье приведены результаты авторского исследования проблем квалификации и предупреждения гибридные преступные схемы, в которых смешиваются методы цифрового мошенничества по ст. 159, 159.3, 159.6 УК РФ и вовлечение граждан в террористическую деятельность по ст. 205.1, 205.2 УК РФ. Сделан вывод, что использование цифровых технологий и психологического манипулирования нивелирует четкие критерии квалификации преступлений. Это влечет за собой конкуренцию уголовно-правовых норм и отсутствие стабильности в судебной практике.*

На основе анализа законодательства и судебных кейсов автор показывает, что у этого явления есть вполне конкретные криминологические причины: анонимность цифровых платформ, использование уязвимостей людей и низкая цифровая грамотность жертв. В работе обосновывается необходимость уточнить диспозиции ст. 159, 205.1, 205.2 УК РФ. Выработаны предложения по совершенствованию законодательства и меры виктимологической профилактики. Полученные результаты способствуют повышению правовой определенности и укреплению национальной безопасности.

Ключевые слова: *кибермошенничество, социальная инженерия, вовлечение в террористическую деятельность, гибридные преступления, конкуренция норм, виктимологическая профилактика.*

TARASOV Aleksandr Anatolyevich,
Senior Lecturer at the Department of Criminal Law, Procedure and Criminology, Faculty of Law, National Research University Higher School of Economics (HSE University)

COUNTERING DIGITAL FRAUD AND INVOLVEMENT IN TERRORISM: CRIMINAL LAW AND CRIMINOLOGICAL ISSUES AND PERSPECTIVES

Annotation. *The article presents the results of the author's research on the issues of qualification and prevention of hybrid crime schemes that combine digital fraud methods under Articles 159, 159.3, and 159.6 of the Criminal Code of the Russian Federation and the involvement of citizens in terrorist activities under Articles 205.1 and 205.2 of the Criminal Code of the Russian Federation. It is concluded that the use of digital technologies and psychological manipulation eliminates clear criteria for the qualification of crimes. This entails a competition of criminal law norms and a lack of stability in judicial practice.*

Based on the analysis of legislation and court cases, the author shows that this phenomenon has specific criminological causes: the anonymity of digital platforms, the exploitation of human vulnerabilities, and the low digital literacy of victims. The paper substantiates the need to clarify the dispositions of Articles 159, 205.1, and 205.2 of the Criminal Code of the Russian Federation. Proposals for improving legislation and victimological prevention measures have been developed. The results obtained contribute to increasing legal certainty and strengthening national security.

Key words: *digital fraud, social engineering, involvement in terrorist activities, hybrid crimes, competition of norms, victimological prevention.*

Стремительная цифровая трансформация общества, когда информационно-коммуникационные технологии встраиваются почти в каждую сферу жизни, а онлайн-сервисов становится все больше, создала для старых схем мошенничества благоприятную почву. Цифровизация общественных отношений обусловила существенное изменение форм и способов совершения преступлений террористической направленности. Информационно-телекоммуникационная среда в современных условиях выступает не только инструментом коммуникации, но и самостоятельной площадкой распространения террористической идеологии, вербовки участников и координации противоправной деятельности [1].

В настоящее время злоумышленники все активнее используют инструменты искусственного интеллекта и приемы социальной инженерии, то есть подстраивают атаки под конкретного человека и нередко автоматизируют общение с жертвой. Из-за этого мошенничество уже давно не сводится только к экономическому преступлению. Оно превращается в многофункциональный инструмент, который используют, в том числе, для вовлечения в террористическую деятельность. На этом фоне возникают гибридные угрозы национальной безопасности. Для повышения эффективности нейтрализации новых вызовов требуется пересмотр старых подходов к уголовно-правовому противодействию.

Если посмотреть на действующее уголовное законодательство, особенно на статьи 159, 205.1 и 205.2 УК РФ, видно, что в нем есть заметные пробелы и коллизии, когда мошеннические действия одновременно становятся способом вербовки или финансирования терроризма. На практике из-за этого возникают серьезные трудности с разграничением этих составов, и, как следствие, нередко появляются ошибки в квалификации и правовая неопределенность. Особенно остро это чувствуется в ситуациях, когда мошенничество с цифровыми технологиями и социальной инженерией используется как средство достижения террористических целей. Здесь уже нужны четкие критерии, иначе возникают сложности в правильной уголовно-правовой оценке.

Цель исследования состоит в выработке научно обоснованные критерии разграничения мошенничества, совершенного с использованием цифровых технологий и социальной инженерии и направленного на вовлечение в террористическую деятельность, от смежных составов преступлений, а также выявлении криминологические детерминанты этого явления. Для этого проанализировано действующие уголовно-правовые нормы и правоприменительную практику, изучить механизмы социальной инженерии и криминологические характеристики субъектов, а затем сформулировать предложения по совершенствованию уголовного закона и унификации судебной практики. Такой подход, по сути, должен помочь убрать существующую правовую неопределенность и усилить противодействие гибридным преступным схемам.

Научная новизна работы состоит в комплексном анализе гибридных преступных схем, где сочетаются признаки мошенничества и вовлечения в террористическую деятельность, с акцентом на использование цифровых платформ и методов социальной инженерии. В отличие от тех исследований, где эти явления обычно рассматриваются по отдельности, здесь делается попытка показать их связь и предложить общие меры противодействия. В результате должны получиться конкретные рекомендации по унификации судебной практики и совершенствованию профилактических мер, а это уже задает работе и теоретическую, и практическую значимость для уголовного права и криминологии.

Исследователь Е. С. Палий считает, что "дистанционное мошенничество", совершаемое через информационно-коммуникационные технологии, по-прежнему формирует признаки составов преступлений, предусмотренных ст. 159, 159.3 и 159.6 УК РФ. В тоже время указанные противоправные деяния приобрели сегодня новые формы. Так, с появлением искусственного интеллекта злоумышленники получили инструменты, которые позволяют им анализировать большие массивы данных, делать фейковые сообщения и автоматизировать атаки [2, с. 2].

В этой связи, по мнению автора, когда правоприменители пытаются понять, есть ли в том или ином деянии мошенничество, необходимо изучать не только цель и результат хищения. Важны так же и дистанционный формат общения, и автоматизированные операции, и алгоритмы, которые помогают скрыть личность. Границы самого понятия "дистанционное мошенничество" и его соотношение с нормами УК РФ требуют отдельного уточнения терминологии и критериев квалификации. На практике от этого зависит и то, как описывается способ совершения преступления, и то, как выявляется злоупотребление доверием, когда люди вообще не встречаются лично. А значит, нужно менять и доказательственную базу, и то, как ее проверяют.

Развитие искусственного интеллекта дало

мошенникам новые способы обмана, в том числе генерацию персонализированных текстов, аудио и видео. Все это заметно расширило инструменты социальной инженерии, и в исследовании как раз отдельно выделяются дипфейки и машинное обучение как ключевые элементы современной угрозы.

Подмена личности теперь стала куда проще: алгоритмы способны синтезировать речь и мимику так, что на первый взгляд это выглядит настоящим. Виктимологи, которые изучают эту историю, прямо говорят о резком скачке в методах социальной инженерии, потому что обычные сигналы, по которым человек раньше мог распознать обман, перестают работать как надо [2, с. 2]. В такой ситуации привычные признаки способа совершения мошенничества уже не дают надежной картины, и процессуальные подходы приходится пересматривать. Сейчас нужен более широкий набор доказательств. Помимо переписки, показаний свидетелей, номеров телефонов и реквизитов счетов, в дело могут идти машинный код, лог-файлы, точки входа и следы взаимодействия нейросетевых моделей. Экспертам для этого нужны очень специфические технические навыки, и это, конечно, добавляет нагрузку на правоохранительную систему [2, с. 7]. При этом виктимологические выводы показывают, что нужны антифрод-системы, многоуровневая аутентификация и повышение цифровой грамотности населения [2, с. 1].

Результаты анализа уголовно-правовой характеристики деяний, связанных с вовлечением в террористическую деятельность (ст. 205.1, 205.2 УК РФ), показывают, что указанные составы нацелены на пресечение вовлечения в террористическую деятельность и публичных призывов к ней. В то же время в условиях цифровой среды с их применением возникает немало трудностей. Серьезным вызовом последних лет стала интеграция инструментов социальной инженерии в схемы ресурсного обеспечения терроризма. Денежные средства граждан, похищаемые под видом перевода на "безопасные счета", транзитом направляются на материально-техническое обеспечение запрещенных военизированных формирований. Правовой статус лица, ставшего жертвой психологического воздействия и лично переведшего денежные средства, зависит от наличия умысла. Отсутствие осознания лицом общественно опасного характера своих действий исключает субъективную сторону преступления, предусмотренного статьей 205.1 УК России. Обманутый гражданин должен рассматриваться в качестве потерпевшего от мошенничества (статья 159 УК России). Напротив, действия организаторов таких мошеннических колл-центров обладают повышенной общественной опасностью. Требуют вменения по совокупности преступлений и привлечению к ответственности за хищение чужого имущества путем обмана и последующее умышленное финансирование террористической деятельности [3, с. 277].

Кроме того, в криминологических исследованиях прямо говорится "о миллионных рассылках электронных писем, тысячах одновременных звонков и многоступенчатых атаках, где боты сначала собирают сведения о пользователе, а потом уже выстраивает для него индивидуальный сценарий вовлечения" [2, с. 4]. Такая автоматизация и персонализация воздействия сильно мешают установить, что конкретное лицо умышленно склоняло или вербовало. Квалификация еще и потому осложняется, что законодатель, когда адаптировал нормы о мошенничестве под дистанционные способы, то есть ст. 159, 159.3 и 159.6 УК РФ, ничего похожего для террористических составов не сделал. И вот правоприменителю приходится доказывать, что автоматическая рассылка сообщений или сценарий, созданный ботом, это именно вовлечение, а не просто распространение информации. При этом четких критериев разграничения действий, совершенных через социальную инженерию, и смежных составов пока явно не хватает, поэтому судебная практика получается неровной и тут уже нужны разъяснения высшей судебной инстанции.

У современной пропаганды идеологии терроризма есть еще одна особенность: она активно использует социальную инженерию, чтобы манипулировать сознанием потенциальных участников. Злоумышленники шлют персонализированные сообщения с учетом психологических особенностей и интересов жертвы, и это, конечно, повышает шансы на вовлечение в террористическую деятельность. Такие схемы зачастую используют модули машинного обучения, анализирующие реакцию потенциальных жертв и конструирующих направляемые им сообщения с учетом выявленных психологических особенностей. При этом преступники воздействуют на потерпевших удаленно, без прямого контакта, по цифровым каналам. Данные особенности требуют уточнения признаков объективной стороны вовлечения, склонения и вербовки для участия в террористической деятельности.

В условиях, когда для генерации фейковых сообщений и автоматизации атак используется искусственный интеллект, привычные ориентиры вроде личного обращения или передачи инструкций не являются очевидными. Поэтому следует закрепить, на законодательном уровне или через судебное толкование, что систематическая рассылка персонализированных призывов через мессенджеры или социальные сети, а также использование чат-ботов для вербовки образуют

объективную сторону преступлений по ст. 205.1 и 205.2 УК РФ.

В рамках проведенного авторского исследования выявлены коллизии и пробелы в правоприменении, связанные с отдельными проблемами в разграничении смежных составов при сопряжении (многоэтапная преступная схема, в которой первоначальное деяние служит инструментом для совершения последующего) в рамках единой криминальной схемы мошенничества и террористической деятельности. Когда мошенничество сочетается с вовлечением в террористическую деятельность, правоприменителю приходится разбирать, как разграничить смежные составы. Одно и то же деяние, к примеру, обман ради получения денег и потом использование жертвы для совершения теракта, может идти по совокупности статей 159 и 205.1 УК РФ. И тут возникает вопрос о реальной совокупности преступлений. Нужны четкие критерии, чтобы понять, речь идет об одном сложном преступлении или о двух самостоятельных составах. Пока таких критериев нет, в судебной практике возникают коллизии. Похожие по фактам дела получают разную уголовно-правовую оценку. Ситуация усложняется еще и тем, что мошенничество через цифровые технологии и социальную инженерию оставляет цифровые следы, а для их анализа нужны специальные технические знания. Это нагружает правоохранительные органы и может затягивать расследование [2, с. 7]. В таких условиях особенно трудно установить умысел на вовлечение в террористическую деятельность, потому что злоумышленники способны сокрыть свои подлинные намерения под обычные мошеннические схемы. Если не выработать единый подход к квалификации таких сопряженных деяний, останется риск и необоснованного привлечения к ответственности, и ухода от нее.

Пробелы в правовом регулировании состоят также в отсутствии единой терминологии и общепризнанных мировым сообществом стандартов для квалификации гибридных преступлений, в которых соединяются мошенничество и вовлечение в террористическую деятельность. Существующая правовая неопределенность позволяет преступным группам выбирать для размещения своей инфраструктуры государства с ослабленным правовым режимом противодействия киберпреступности и терроризму. Трансграничный характер таких деяний еще сильнее осложняет ситуацию, поскольку правоохранительным органам приходится сталкиваться с несовершенством международных механизмов экстрадиции и сотрудничества. Анонимизация и облачные сервисы, размещенные в разных юрисдикциях, помогают скрывать личность и местонахождение, так что оперативно остановить такую деятельность почти невозможно. В итоге жертвы, особенно если они находятся в разных странах, фактически остаются без правовой защиты, а преступники продолжают безнаказанно действовать.

Стремительное развитие технологий искусственного интеллекта, особенно появление дипфейков, создает совсем новые угрозы, и действующее уголовное законодательство, если честно, уже не всегда успевает на них нормально реагировать. В научной литературе прямо пишут, что в разных странах пытаются по-разному криминализировать создание и распространение дипфейков, усиливают ответственность за кражу персональных данных, но право все равно часто отстает от технологических изменений, а транснациональный характер таких преступлений мешает и выносить приговоры, и останавливать международные группировки [2, с. 6]. В случае мошенничества, связанного с вовлечением в террористическую деятельность, эта проблема особенно заметна: дипфейки могут использоваться для правдоподобных образов жертв или вербовщиков, да и для дискредитации людей и организаций тоже. Поэтому выглядит вполне обоснованным предложение криминализировать действия, связанные с созданием и распространением контента, сгенерированного искусственным интеллектом, если это делается ради мошенничества или вовлечения в террористическую деятельность. Такую норму можно включить в УК РФ либо как отдельный состав преступления, либо как квалифицирующий признак в уже существующих статьях. Изменение самой природы дистанционного мошенничества на фоне развития ИИ отражается и в практике: расследовать такие дела сложно, потому что нужны очень специфические технические знания, а это серьезно нагружает правоохранительную систему [2]. Из этого, по сути, вытекает необходимость не только вводить криминализацию, но и создавать специализированные подразделения, которые будут заниматься расследованием таких преступлений.

Для более точного противодействия таким деяниям нужно внести изменения в статьи 159, 159.3 и 159.6 УК РФ и прямо указать квалифицирующий признак, когда мошенничество совершается с использованием технологий искусственного интеллекта и методов социальной инженерии. Кроме того, стоит установить более строгую ответственность, если такие действия связаны с финансированием терроризма, потому что общественная опасность тут заметно выше. Если ввести такие признаки, правоприменителю будет проще и точнее квалифицировать деяния, назначать справедливое наказание, а судебная практика в целом станет более единообразной.

Еще одно ключевое направление связано с законодательным уточнением, где надо четче раз-

вести мошенничество, сопряженное с вовлечением в террористическую деятельность, и смежные составы преступлений. Тут нужны понятные критерии для оценки действий по вербовке и финансированию терроризма через цифровые каналы, а также ясное понимание, в каких случаях мошенничество надо рассматривать как способ вовлечения в террористическую деятельность, а в каких как самостоятельное преступление. Такие разъяснения помогут убрать существующие коллизии и выровнять судебную практику, а это уже нормальная база для противодействия таким угрозам.

По данным МВД России, с начала 2025 года более 424,9 тысячи преступлений - около 40 процентов от их общего числа - совершено с использованием информационно-коммуникационных технологий.

Основанный на официальную статистику за 2025-2026 гг. криминологический анализ демонстрирует снижение общего числа ИТТ-преступлений на 10–12%. Вместе с тем позитивный эффект от спада является лишь внешним, т.к. криминалитет перешел в латентную стадию, на более точечные, технологичные и психологически выверенные схемы. Мошенничество по статье 159 Уголовного кодекса Российской Федерации по-прежнему остается самой большой категорией хищений, причем больше половины дел приходится на тяжкие и особо тяжкие составы, а средний ущерб на одного потерпевшего уже вырос до 280 000 рублей. Ключевым фактором в тренде 2025–2026 годов является широкое применение генеративного искусственного интеллекта и подложных медиаданных [4]. Финансовые потери граждан РФ огромны. Ущерб от дистанционных хищений приблизился к 200 миллиардам рублей, тогда как потерпевшим возвращено лишь 8,8 миллиарда. Такие данные говорят о наличии системных проблем не только в части профилактики подобных преступлений, но и в возмещении вреда, то есть в защите имущественных прав граждан [5].

Н. В. Гладыч считает, что для современной преступности характерны хищение или подбор цифровых данных платежных карт, генерация поддельных реквизитов, применение вредоносного программного обеспечения, фишинг, социальная инженерия. Киберпространство становится естественной средой и инструментом реализации противоправного деяния, в связи с чем способ совершения преступления прямо соответствует критерию технологической опосредованности [6]. Злоумышленники используют сгенерированные аудиосообщения и видео-дипфейки, чтобы имитировать голоса родственников или руководителей компаний потенциальных жертв. Существующая в настоящее время криминальная схема уже не выглядит как хаотичные звонки подряд. Применяются многоступенчатые цепочки манипуляций. Жертву сначала ведут через взломанный личный кабинет Единого портала госуслуг, потом подключают фейковых сотрудников правоохранительных органов, Банка России и служб безопасности. Преступники почти окончательно ушли из сотовых сетей в защищенные зарубежные мессенджеры Telegram и WhatsApp, потому что отечественные операторы связи системно блокируют подменные номера мошенников. Похищенные средства при этом выводят через иностранные юрисдикции и трансграничные криптомиксеры.

Исследователь Р. С. Рашитханов считает, что «захват и использование личных данных потенциальных жертв (персонификация) - один из эффективных и наиболее распространенных способов совершения преступлений, который известен давно и стал быстро распространяться одновременно с использованием этих данных гражданами в Интернете. Однако если первоначально преступниками применялись обычные методы социальной инженерии (анализ сообществ, личной информации, такой как вуз, место работы и т.д.), то сейчас их интересуют в том числе данные пользовательской активности в Интернете. При этом структура личных данных зачастую крайне разнообразна и включает в себя временами крайне чувствительные для людей данные: о месте жительства человека, членах его семьи, передвижении человека, его покупках, в том числе совершенных в Интернете. Утечка такой очень личной информации делает потенциальных жертв крайне уязвимыми для преступных посягательств» [7].

Для усиления эффекта злоумышленники используют современные технологии: "Подобные схемы часто используют модули машинного обучения, которые анализируют реакции жертв и адаптируют сообщения, повышая вероятность успеха" [2]. Анализ больших массивов утекших персональных данных помогает разделять пользователей по возрасту, полу, интересам и психологическим особенностям. В итоге вербовка превращается в очень точную социальную инженерию.

Если смотреть на разграничение уголовной ответственности, то классическое хакерство по статьям 272–274.1 Уголовного кодекса Российской Федерации в общей массе играет скорее вспомогательную роль, как инструмент подготовки. При этом ключевой риск для потерпевшего связан с хищением денежных средств. Разница между составами состоит в участие самой жертвы. Так, при мошенничестве по статье 159 потерпевший под психологическим давлением сам совершает операцию, берет кредиты или передает злоумышленникам СМС-коды. При краже с банковского счета, по пункту «г» части 3 ста-

тьи 158 Уголовного кодекса, активы похищаются тайно, без ведома владельца, используя вредоносное программное обеспечение или дубликаты SIM-карт.

Виктимологический анализ жертв вовлечения в террористическую деятельность через мошенничество показывает целый набор уязвимостей, которыми злоумышленники пользуются очень активно. Среди ключевых факторов тут недостаточная цифровая грамотность, социальная изоляция и психологическая нестабильность. Все это вместе заметно снижает способность человека критически оценивать информацию, которая к нему приходит. В исследованиях отмечается, что пожилые люди традиционно считаются одной из самых уязвимых групп из-за меньшего опыта цифровой гигиены и повышенной доверчивости к звонкам от официальных структур [2, с. 5]. Вместе с тем в 2025-2026 гг. появилась тенденция снижения до 40% доли потерпевших пенсионного возраста. Основной группой пострадавших, составляющих в настоящее время более 45%, стали экономически активные граждане от 22 до 45 лет. Представителей данной категории мошенники чаще всего вовлекают в деятельность фейковых инвестиционных платформ.

В качестве еще одной уязвимой категорией эксперты называют несовершеннолетних, вовлекаемых в совершение наиболее опасных видов преступлений. Среди них выделяются терроризм, экстремизм и кибермошенничество, используемое для финансирования террористической деятельности. Данные преступления характеризуются переходом их организационных и подготовительных стадий в киберсферу, в рамках которой происходит вербовка потенциальных исполнителей террористических атак, диверсий и экстремистских акций [8].

Для всех групп жертв характерен общий один и тот же триггер. Потерпевшим навязывают ощущение, что надо срочно что-то делать прямо сейчас. После перевода денег 75% граждан сами удаляют переписку, потому что паникуют или стыдятся, и тем самым уничтожают доказательства. А больше 60% в первые двое суток идут с претензиями в банк, а не в полицию, и упускают возможность оперативно действовать "по горячим следам"[4].

Действенная профилактика без существенного повышения цифровой грамотности населения просто не работает, и тут речь идет о навыке критически воспринимать информацию, особенно когда нужно распознать манипуляцию и социальную инженерию. Исследователи считают, что "одних памяток и брошюр уже мало, поэтому в научной литературе предлагают встраивать обучающие модули прямо в те платформы, которыми люди пользуются каждый день: социальные сети, онлайн-банкинг, государственные порталы. Если система замечает подозрительную активность, она должна не только блокировать ее, но и объяснять пользователю, где именно риск, чтобы человек учился распознавать фейки" [2, с. 7]. Такие меры, в том числе с элементами геймификации, помогают вырабатывать привычку перепроверять информацию и осознанно противостоять попыткам вовлечения в террористическую деятельность через манипулятивные приемы.

Для реального противодействия нужен еще и рабочий механизм межведомственного и международного обмена информацией о новых видах мошенничества с использованием ИИ, плюс координация между правоохранительными органами, финансовыми организациями и интернет-провайдерами. В научной литературе отмечается, что виктимологическая составляющая показывает простую вещь: если нет согласованных правовых норм и координации на международном уровне, жертвы высокотехнологичной атаки вряд ли получат нормальное возмещение ущерба или помощь в привлечении преступников к ответственности [2]. Такое взаимодействие позволит быстрее реагировать на трансграничные угрозы, обмениваться данными о новых схемах финансирования терроризма и вербовки, а еще вместе разрабатывать алгоритмы для блокировки подозрительных транзакций и контента.

Очень важной частью системы превенции остаются виктимологические меры, которые направлены на выявление и защиту самых уязвимых категорий граждан от мошенничества, связанного с вовлечением в террористическую деятельность. Криминологический анализ показывает, что практически любой пользователь, независимо от уровня технической подготовки, может попасть в зону риска, так что нужна адресная работа с фокус-группами повышенной уязвимости. Такая работа должна включать не только информационную поддержку, но и психологическую помощь, правовое консультирование для тех, кто уже столкнулся с попытками манипуляции, а еще создание специализированных горячих линий и онлайн-сервисов, где можно быстро получить помощь.

Таким образом, проведенное исследование показало, что современные формы мошенничества, которые идут через цифровые технологии и методы социальной инженерии и при этом еще завязаны на вовлечение в террористическую деятельность, складываются в довольно сложный гибридный состав преступления. Вследствие использования разнотипных подходов к пересекающимся нормам статей 159, 205.1 и 205.2 УК РФ у правоприменителей возникают разночтения в уголовно-правовых оценках содеянного. На этом фоне существует потребность в четких, непроти-

воречивых критериях, по которым можно различать эти составы преступлений.

В ходе анализа действующего законодательства и сложившейся практики также выявлены основные пробелы и коллизии, которые возникают, когда мошеннические действия одновременно используются как способ вовлечения лица в террористическую деятельность. Действующие нормы не до конца учитывают специфику использования цифровых платформ и социальной инженерии как инструмента вербовки. Из-за этого возникает правовая неопределенность, когда одно и то же деяние оценивается по-разному, в зависимости от усмотрения правоприменителя. По мнению автора, данную проблему следует решать через унификацию подходов к квалификации и устранение конкуренции норм.

Криминологический анализ позволил установить, что ключевыми детерминантами этого феномена выступают целенаправленная эксплуатация уязвимостей жертв с помощью методов социальной инженерии и использование анонимности, которую дают цифровые платформы. Вербовщики за счет этого довольно ловко маскируют свои настоящие преступные цели, выдавая их за благотворительность, инвестиции или какие-то иные легитимные действия. Выявленные виктимологические особенности, в частности, доверчивость и недостаточная цифровая грамотность отдельных категорий граждан, прямо указывают на острую необходимость в специальных профилактических мерах. Такие меры должны повышать критическое мышление и формировать устойчивые навыки безопасного поведения в цифровой среде у потенциальных жертв.

Чтобы противодействие рассматриваемым гибридным угрозам стало более результативным, сформированы авторские предложения по совершенствованию уголовного законодательства и системы профилактики. В частности, была обоснована необходимость уточнения диспозиций статей 159, 205.1 и 205.2 УК РФ для снятия выявленной правовой неопределенности. Кроме того, разработаны предложения в комплекс криминологических мер с учетом специфики использования цифровых технологий и социальной инженерии. Реализация предложенных законодательных инициатив и профилактических программ, по мнению автора, будет способствовать усилению борьбы с этими преступлениями и укреплению национальной безопасности.

Список литературы:

[1] Семенов, А. У. Информационный терроризм: криминологические и уголовно-правовые проблемы предупреждения в информационно-телекоммуникационной среде / А. У. Семенов. – Текст : электронный // Молодой ученый. – 2026. – № 24 (627). – С. 474–476. – URL: moluch.ru (дата обращения: 26.08.2026).

[2] Палий, Е. С. Криминологические и уголовно-правовые аспекты дистанционного мошенничества с применением deepfake-технологий и социальной инженерии / Е. С. Палий. – Текст : электронный // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 4 (108). – С. 149–157. – URL: cyberleninka.ru (дата обращения: 26.08.2026).

[3] Тарасов, А. А. Цифровые и квазифинансовые каналы содействия терроризму: государственно-правовое регулирование и проблемы квалификации преступлений / А. А. Тарасов. – Текст : электронный // Право и управление. – 2026. – № 7. – С. 224–229. – URL: https://law.law-books.ru/article/tsifrovye-i-kvazifinansovye-kanaly-sodeystviya-terrorizmu-gosudarstvenno-pravovoe/ (дата обращения: 26.08.2026).

[4] Мошенничество и киберпреступность в 2025 — начале 2026 года. – Текст : электронный // Ассоциация юристов России : [официальный сайт]. – 2026. – URL: alrf.ru (дата обращения: 26.08.2026).

[5] Фесько, Д. Как защитить права человека в цифровой среде? / Д. Фесько. – Текст : электронный // Интернет-портал «Российской газеты». – 2025. – 30 октября. – URL: rg.ru (дата обращения: 26.08.2026).

[6] Гладыч, Н. В. Система финансовых преступлений, совершаемых в киберпространстве / Н. В. Гладыч. – Текст : непосредственный // Юстиция. – 2025. – № 3. – С. 112–124. – (Доступ из справочно-правовой системы «КонсультантПлюс»).

[7] Рашитханов, Р. С. Трансформация преступности под влиянием искусственного интеллекта: к постановке проблемы / Р. С. Рашитханов. – Текст : непосредственный // Актуальные проблемы российского права. – 2026. – № 1. – С. 45–58. – (Доступ из справочно-правовой системы «КонсультантПлюс»).

[8] Коваленко, В. И. Вовлечение несовершеннолетних в противоправную деятельность с использованием информационно-телекоммуникационных технологий: правовые и криминологические аспекты противодействия / В. И. Коваленко. – Текст : электронный // ЮристъПравоведъ. – 2025. – № 3 (114). – С. 139–145. – URL: cyberleninka.ru (дата обращения: 26.08.2026).

References:

[1] Semenov, A.U. Information terrorism: criminological and criminal law problems of prevention in the information and telecommunication environment/A.U. Semenov. - Text: electronic // Young scientist. – 2026. – № 24 (627). - S. 474-476. - URL: moluch.ru (access date: 26.08.2026).

[2] Paliy, E. S. Criminological and criminal law

aspects of remote fraud using deepfake technologies and social engineering/E. S. Paliy. - Text: electronic // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2025. – № 4 (108). - S. 149-157. - URL: cyberleninka.ru (access date: 26.08.2026).

[3] Tarasov, A. A. Digital and quasi-financial channels for promoting terrorism: state-legal regulation and problems of qualification of crimes/A. A. Tarasov. - Text: electronic // Law and management. – 2026. – № 7. - S. 224-229. – URL: https: //law.law-books.ru/article/tsifrovye-i-kvazifinanso vye-kanaly-sodeystviya-terrorizmu-gosudarstvenno-pravovoe/ (дата обращения: 26.08.2026).

[4] Fraud and cybercrime in 2025 - early 2026. - Text: electronic // Association of Lawyers of Russia: [official website]. – 2026. - URL: alrf.ru (access date: 26.08.2026).

[5] Fesko, D. How to protect human rights in a digital environment ?/D. Fesko. - Text: electronic // Internet portal "Rossiyskaya Gazeta." – 2025. - October 30. - URL: rg.ru (access date: 26.08.2026).

[6] Gladych, N.V. The system of financial crimes committed in cyberspace/N.V. Gladych. - Text: direct // Justice. – 2025. – № 3. - S. 112-124. - (Access from ConsultantPlus Legal Reference System).

[7] Rashitkhanov, R. S. Transformation of crime under the influence of artificial intelligence: to the formulation of the problem/R. S. Rashitkhanov. - Text: immediate // Actual problems of Russian law. – 2026. – № 1. - S. 45-58. - (Access from ConsultantPlus Legal Reference System).

[8] Kovalenko, V.I. Involvement of minors in illegal activities using information and telecommunication technologies: legal and criminological aspects of counteraction/V.I. Kovalenko. - Text: electronic // Lawyer-Lawyer. – 2025. – № 3 (114). - S. 139-145. - URL: cyberleninka.ru (access date: 26.08.2026).