Дата поступления рукописи в редакцию: 30.06.2026 г. DOI: 10.24412/2782-3830-2026-7-369-378
Дата принятия рукописи в печать: 13.07.2026 г.

АКАПЬЕВ Виктор Львович,
кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: akapevv@yandex.ru

КОВАЛЕВА Екатерина Геннадьевна,
кандидат технических наук, доцент кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: kovalevazchs@yandex.ru

БОРИСЕНКО Александр Васильевич,
кандидат физико-математических наук, старший преподаватель кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина,
e-mail: borisenko02.94@mail.ru

МАТРОСОВА Лидия Дмитриевна,
кандидат юридических наук, доцент, начальник кафедры информационных технологий в деятельности органов внутренних дел Орловского юридического института МВД России имени В.В. Лукьянова,
e-mail: matrosovald@mail.ru

ПРОБЛЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ И ПРОФИЛАКТИКА МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ДИПФЕЙК-ТЕХНОЛОГИЙ

Аннотация. *Современное общество переживает стремительную цифровую трансформацию, которая затрагивает практически все сферы жизни человека: от бытового общения до финансовых операций и государственного управления. Вместе с очевидными благами технологического прогресса возникают принципиально новые угрозы, среди которых особое место занимает мошенничество с применением методов социальной инженерии и дипфейк-технологий. Указанные явления представляют собой качественно иной уровень преступной деятельности, поскольку злоумышленники используют не грубую силу или технические уязвимости систем, а манипулируют психологией человека, его доверием и неспособностью отличить подлинное от сфабрикованного.*

Ключевые слова: *кибермошенничество, киберпреступления, киберпреступник, фишинг, правовая квалификация.*

AKAPYEV Viktor Lvovich,
Candidate of Pedagogical Sciences, Docent of the Department ICT in Law Enforcement Agencies Belgorod Law Institute The Ministry of Internal Affairs of Russia named after I.D. Putilin

KOVALEVA Ekaterina Gennadievna,
Candidate of Technical Sciences, Associate Professor
of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs
of Russia named after I.D. Putilin

BORISENKO Alexander Vasilyevich,
Candidate of Physico-mathematical Sciences,
Senior lecturer of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs
of Russia named after I.D. Putilin

MATROSOVA Lidiya Dmitrievna,
Candidate of Law Sciences, docent,
Head of the Department of Information Technology
in the Activities of Law Enforcement Agencies Oryol Law Institute
The Ministry of Internal Affairs of Russia named after V.V. Lukyanov

THE PROBLEM OF LEGAL REGULATION AND FRAUD PREVENTION USING SOCIAL ENGINEERING METHODS AND DEEPFAKE TECHNOLOGIES

Annotation. *Modern society is undergoing a rapid digital transformation that affects almost all areas of human life: from everyday communication to financial transactions and public administration. Along with the obvious benefits of technological progress, fundamentally new threats are emerging, among which fraud using social engineering methods and deepfake technologies occupies a special place. These phenomena represent a qualitatively different level of criminal activity, since attackers do not use brute force or technical vulnerabilities of systems, but manipulate a person's psychology, his trust and inability to distinguish the genuine from the fabricated.*

Key words: *cyberbullying, cybercrime, cybercriminal, phishing, legal qualifications.*

Актуальность исследования различных направлений кибермошенничества обусловлена совокупностью факторов, которые в своей взаимосвязи создают серьёзную угрозу как для отдельных граждан, так и для общества в целом. Статистика последних лет свидетельствует о неуклонном росте числа преступлений, совершаемых с использованием технологий искусственного интеллекта и методов психологического воздействия. По данным Министерства внутренних дел Российской Федерации, преступления в сфере информационно-телекоммуникационных технологий ежегодно демонстрируют устойчивый рост, и значительную их долю составляют именно мошеннические схемы, основанные на обмане и введении в заблуждение с помощью цифровых инструментов [1]. Дипфейк-технологии, позволяющие создавать фотореалистичные аудио и видеозаписи с изображением реальных людей, произносящих слова или совершающих действия, которые никогда не имели места, открывают перед преступниками принципиально новые возможности для хищения денежных средств, дискредитации личности и манипулирования общественным мнением.

Правовое регулирование в данной области существенно отстаёт от темпов технологического развития. Действующее российское законодательство содержит общие нормы об ответственности за мошенничество, закреплённые в статье 159 Уголовного кодекса Российской Федерации, однако специального механизма противодействия преступлениям, совершаемым с использованием дипфейков и методов социальной инженерии, в отечественном праве до сих пор не сформировано. Это порождает серьёзные затруднения в правоприменительной практике: сложности с квалификацией деяний, проблемы доказывания факта использования синтетических медиаматериалов, высокую латентность таких преступлений. Зарубежный опыт, в частности подходы США, Европейского союза и Китайской Народной Республики, демонстрирует более детальное регулирование данной сферы, что позволяет рассматривать их практику в качестве ориентира для совершенствования российского законодательства.

Современное мошенничество претерпело существенные изменения по сравнению с теми формами, которые были известны правовой

науке и практике ещё несколько десятилетий назад. Если прежде преступники делали ставку преимущественно на физический обман, поддельные документы или непосредственный контакт с жертвой, то сегодня центр тяжести сместился в сторону психологического воздействия, которое осуществляется дистанционно и нередко без каких-либо технически сложных инструментов. Именно здесь на первый план выходит социальная инженерия как самостоятельный метод преступной деятельности, основанный на манипулировании поведением человека через эксплуатацию его психологических особенностей, доверия, страха, любопытства или желания помочь.

Само понятие социальной инженерии пришло в криминологию и правовую науку из области информационной безопасности, где оно изначально обозначало совокупность приёмов, позволяющих получить конфиденциальную информацию не путём взлома технических систем, а путём введения в заблуждение людей, имеющих к ней доступ [1]. Со временем это понятие приобрело более широкое значение и стало применяться для описания любых манипулятивных технологий, с помощью которых злоумышленник добивается от жертвы нужного ему поведения, будь то передача денежных средств, раскрытие паролей, совершение юридически значимых действий или отказ от защиты своих интересов.

В отечественной правовой литературе социальная инженерия как самостоятельное явление долгое время оставалась без должного внимания, поскольку исследователи склонны были рассматривать её лишь как частный случай обмана в рамках состава мошенничества, предусмотренного статьёй 159 Уголовного кодекса Российской Федерации. Между тем такой подход не позволяет в полной мере отразить специфику данного явления, поскольку социальная инженерия представляет собой не просто разновидность обмана, а целую систему последовательных манипулятивных воздействий, которые могут растягиваться во времени, включать несколько этапов подготовки и исполнения, задействовать различные каналы коммуникации и эксплуатировать самые разные психологические механизмы.

Среди наиболее распространённых приёмов социальной инженерии, используемых в мошеннических целях, следует выделить фишинг, то есть рассылку сообщений, имитирующих официальные обращения от банков, государственных органов или иных организаций с целью получения персональных данных или платёжных реквизитов жертвы. Не менее распространён фишинг, при котором преступник звонит жертве по телефону, представляясь сотрудником банка, правоохранительных органов или иной авторитетной структуры, и под различными предлогами убеждает её перевести денежные средства или сообщить конфиденциальную информацию. Помимо этого, широко применяются техники претекстинга, когда злоумышленник заблаговременно создаёт искусственный повод для общения с жертвой, формируя доверительные отношения, которые впоследствии используются для совершения хищения [2].

Принципиальная особенность всех этих методов состоит в том, что жертва в большинстве случаев добровольно совершает действия, выгодные преступнику, будучи убеждена в их законности и необходимости. Именно это обстоятельство существенно осложняет как раскрытие подобных преступлений, так и доказывание вины злоумышленника, поскольку внешне ситуация нередко выглядит как добровольная передача имущества или добровольное совершение иных действий без какого-либо принуждения.

Если социальная инженерия опирается прежде всего на психологические механизмы воздействия на жертву, то дипфейк-технологии представляют собой качественно новый инструментарий, позволяющий создавать фальсифицированный аудиовизуальный контент, практически неотличимый от подлинного. Термин deepfake образован от слов deep learning и fake, что отражает сущность технологии: речь идёт об использовании алгоритмов глубокого машинного обучения для синтеза изображений, голосовых сообщений или видеозаписей, в которых реальный человек произносит слова, которых никогда не говорил, или совершает действия, которых никогда не совершал.

С технической точки зрения создание дипфейков стало возможным благодаря развитию генеративно-состязательных нейронных сетей, представляющих собой особый класс алгоритмов искусственного интеллекта, в которых две взаимосвязанные модели одновременно обучаются друг на друге: одна генерирует фальшивый контент, а другая пытается отличить его от подлинного, что в итоге приводит к созданию материалов высочайшего качества. Ещё несколько лет назад подобные технологии требовали значительных вычислительных ресурсов и специализированных знаний, однако сегодня соответствующее программное обеспечение стало общедоступным, а в ряде случаев создание убедительного дипфейка занимает считанные минуты при использовании обычного смартфона.

Для уголовного права дипфейк-технологии представляют особый интерес прежде всего потому, что они позволяют принципиально расширить возможности преступников в части создания иллюзии достоверности обманных сообщений. Если прежде жертва, услышав незнако-

мый голос или увидев незнакомое лицо, могла усомниться в подлинности обращения, то теперь злоумышленники способны воспроизвести голос и внешность конкретного человека, будь то руководитель организации, родственник жертвы или представитель государственного органа, с такой степенью достоверности, что отличить подделку от оригинала становится крайне затруднительно даже при достаточном уровне критического мышления [3].

Именно поэтому в правовой науке всё активнее обсуждается вопрос о том, не следует ли рассматривать использование дипфейк-технологий при совершении мошенничества в качестве самостоятельного квалифицирующего признака, существенно повышающего общественную опасность деяния. Такой подход представляется обоснованным, поскольку применение подобных технологий свидетельствует о заблаговременной подготовке преступления, значительных технических возможностях злоумышленника и целенаправленном стремлении максимально затруднить разоблачение обмана.

Классификация рассматриваемых преступлений имеет не только теоретическое, но и существенное практическое значение, поскольку позволяет систематизировать накопленный опыт правоприменения, выявить пробелы в действующем законодательстве и разработать дифференцированные меры противодействия различным видам преступной деятельности.

По характеру применяемых технологий представляется возможным выделить преступления, совершаемые с применением исключительно методов психологической манипуляции без использования каких-либо технических средств фальсификации, преступления, при совершении которых используются технические средства имитации, в частности поддельные сайты, электронные письма или SMS-сообщения, оформленные в стиле официальных источников, а также преступления, связанные с применением дипфейк-технологий, обеспечивающих синтез поддельного аудиовизуального контента. Последняя категория представляет наибольшую общественную опасность именно в силу труднодостижимой достоверности создаваемых фальсификатов [4].

По субъектному составу жертв преступлений можно разграничить мошенничество, направленное против физических лиц, мошенничество, направленное против организаций и предприятий, и мошенничество, направленное против органов государственной власти или государственных структур. Каждая из этих категорий обладает собственной спецификой с точки зрения применяемых манипулятивных приёмов, поскольку психология принятия решений физическим лицом, действующим в личных интересах, существенно отличается от механизмов корпоративного или государственного управления, где решения принимаются коллегиально или на основании формализованных процедур.

По степени организованности преступной деятельности следует различать единичные преступления, совершаемые одним лицом без предварительного сговора с другими участниками, преступления, совершаемые группой лиц по предварительному сговору с распределением ролей между исполнителями, и преступления, совершаемые в рамках организованной преступной группы, располагающей устойчивой структурой, специализированным оборудованием и, нередко, международными связями. Именно последняя форма организации преступной деятельности характерна для крупнейших мошеннических схем с применением дипфейков, поскольку создание качественного синтезированного контента требует технических специалистов, а организация массовых атак на жертв предполагает наличие разветвлённой инфраструктуры.

По цели преступного посягательства выделяется мошенничество, направленное на хищение денежных средств, мошенничество, направленное на получение конфиденциальных данных с целью их последующего использования или продажи, мошенничество, связанное с принуждением жертвы к совершению юридически значимых действий в интересах злоумышленника, а также мошенничество, преследующее цель дискредитации конкретного лица или организации путём распространения синтезированного компрометирующего контента.

Приведённая классификация не является исчерпывающей, поскольку технологии как социальной инженерии, так и создания дипфейков продолжают стремительно развиваться, порождая всё новые разновидности преступной деятельности, которые правоприменительная практика и правовая наука вынуждены осмыслять уже после того, как они получили широкое распространение. Это обстоятельство наглядно свидетельствует о необходимости опережающего развития уголовно-правовой доктрины и законодательства в данной сфере, а не реакции на уже сложившиеся угрозы постфактум.

Стремительное развитие цифровых технологий породило принципиально новые формы преступности, которые отличаются высокой степенью латентности, транснациональным характером и исключительной сложностью с точки зрения правовой квалификации и доказывания. Среди наиболее острых проблем, с которыми сталкивается современная правоохранительная система в этой сфере, особого внимания заслуживают две взаимосвязанные, но при этом самостоятельные проблемы: недостаточность право-

вого регулирования и отставание законодательной базы от темпов технологического развития, а также крайне низкий уровень цифровой грамотности населения в сочетании с отсутствием эффективных механизмов верификации цифровой информации.

Первая из обозначенных проблем носит системный характер и проявляется сразу в нескольких измерениях. Большинство государств располагает уголовным законодательством, которое формировалось в эпоху, когда дипфейк-технологии не существовали как таковые, а социальная инженерия в её нынешнем виде не рассматривалась как самостоятельный инструмент совершения преступлений [5]. В результате правоприменители вынуждены применять к качественно новым деяниям нормы, которые изначально создавались для регулирования совершенно иных общественных отношений, что неизбежно порождает трудности с квалификацией и ведёт к тому, что значительная часть преступлений либо остаётся безнаказанной, либо получает заниженную юридическую оценку. Показательно, что создание заведомо ложного аудиовизуального контента с целью обмана конкретного лица во многих правовых системах не образует самостоятельного состава преступления и квалифицируется лишь в той мере, в какой за ним последовало имущественное хищение или иной очевидный вред. Такой подход не учитывает ни специфику инструмента, ни масштаб потенциального ущерба для репутации, психологического состояния и личной безопасности жертвы, а главное, не создаёт никаких превентивных механизмов. Отдельную сложность представляет транснациональный характер подобных преступлений: техническая инфраструктура, исполнители и жертвы нередко находятся в разных государствах, что делает расследование и уголовное преследование крайне затруднительными даже при наличии политической воли к сотрудничеству [6]. Механизмы международного взаимодействия правоохранительных органов в целом не успевают за скоростью, с которой преступные группы адаптируют свои методы к новым условиям, а взаимное признание доказательств, полученных в рамках цифровых расследований, по-прежнему сопряжено с многочисленными правовыми и процессуальными препятствиями. Технические возможности для атрибуции конкретных действий конкретным лицам существуют, однако перевод этих данных в юридически значимые доказательства требует специализированной экспертизы, которой большинство следственных органов пока не располагает в достаточной мере.

Вторая проблема в определённом смысле является зеркальным отражением первой и касается не институциональной, а человеческой стороны вопроса. Социальная инженерия как метод воздействия на жертву эксплуатирует не технические уязвимости систем, а психологические особенности человеческого восприятия и поведения: склонность доверять авторитетным источникам, реагировать на срочность и эмоциональное давление, не подвергать критическому анализу информацию, поступающую по привычным каналам. Дипфейк-технологии в этом контексте выступают усилителем существующих уязвимостей, поскольку позволяют имитировать знакомых людей, авторитетных фигур или официальные источники с таким уровнем правдоподобия, который делает распознавание подделки практически невозможным для неподготовленного человека. Исследования в области когнитивной психологии устойчиво подтверждают, что даже люди с высоким уровнем общего интеллекта и образования оказываются уязвимы перед хорошо выстроенными манипулятивными сценариями, поскольку защита от подобных воздействий требует специфических знаний и навыков, а не просто общей критичности мышления. При этом цифровая грамотность населения в большинстве стран остаётся на крайне низком уровне применительно именно к вопросам распознавания синтетического контента и верификации цифровой информации. Люди в целом осведомлены о том, что мошенничество в интернете существует, однако конкретные механизмы проверки подлинности голосовых сообщений, видеозвонков или фотографий остаются за пределами массового знания. Парадоксально, что технические инструменты детекции дипфейков развиваются параллельно с самими технологиями генерации, однако доступность и удобство использования этих инструментов для рядового пользователя остаются крайне низкими, а их интеграция в повседневные коммуникационные платформы носит фрагментарный характер [7]. Сами же технологии синтеза аудиовизуального контента распространяются преимущественно коммерческими структурами и независимыми исследовательскими командами, которые как правило преследуют совершенно законные цели в сфере развлечений, образования или доступности контента, однако те же самые инструменты с лёгкостью переориентируются на совершение преступлений, и никакой системы контроля за их использованием на сегодняшний день не существует. Вопрос о том, в какой мере разработчики подобных технологий несут ответственность за их преступное применение третьими лицами, остаётся дискуссионным как в правовой, так и в этической плоскости, и его решение потребует широкого международного диалога с участием государств, технологических компаний и гражданского общества.

Таким образом, совокупность перечисленных проблем формирует картину системного вызова, с которым правоохранительная система и общество в целом пока не в состоянии справиться в полной мере. Эффективное противодействие мошенничеству с применением социальной инженерии и дипфейк-технологий требует одновременных усилий в нескольких направлениях: законодательного совершенствования, развития технической экспертизы, укрепления международного сотрудничества и повышения цифровой грамотности населения, причём все эти направления в равной степени необходимы и ни одно из них не может подменить остальные.

Современное состояние правового регулирования в сфере противодействия мошенничеству с применением социальной инженерии и дипфейк-технологий характеризуется очевидным отставанием нормативной базы от темпов технологического развития, и это отставание уже сегодня порождает конкретные правоприменительные трудности, которые не позволяют эффективно привлекать виновных к ответственности и в полной мере защищать интересы пострадавших. Тем не менее именно осознание этих трудностей создаёт необходимую основу для содержательного разговора о перспективах развития законодательства и правоохранительной практики, поскольку любое реформирование должно начинаться с точной диагностики существующих проблем, а не с абстрактных деклараций о необходимости перемен.

Одной из наиболее острых проблем, требующих первоочередного решения, является отсутствие в уголовном законодательстве большинства государств специальных составов, охватывающих мошеннические действия, совершённые с применением дипфейк-технологий. Действующие нормы об ответственности за мошенничество были созданы в принципиально иных технологических условиях и рассчитаны на традиционные способы введения в заблуждение, тогда как использование синтетических медиаматериалов для имитации личности конкретного человека представляет собой качественно новый способ обмана, который не всегда укладывается в существующие правовые конструкции [8]. Решение этой проблемы видится в разработке и принятии специализированных норм, прямо предусматривающих ответственность за создание и распространение дипфейк-контента в мошеннических целях с установлением квалифицирующих признаков, отражающих повышенную общественную опасность таких деяний, в частности совершение их в отношении неопределённого круга лиц, с использованием автоматизированных систем распространения или с причинением ущерба в крупном и особо крупном размере. Наряду с этим необходимо законодательно закрепить само понятие дипфейк-технологий применительно к уголовно-правовой и административно-правовой сферам, поскольку отсутствие легального определения создаёт серьёзные препятствия как для правоприменителей, так и для судов при квалификации соответствующих деяний [9].

Не менее значимой проблемой остаётся недостаточная техническая оснащённость правоохранительных органов, которые зачастую не располагают ни соответствующим программным обеспечением, ни специалистами, способными проводить экспертизу синтетических медиаматериалов на уровне, достаточном для формирования доказательной базы по уголовным делам. Эта проблема имеет несколько измерений: кадровое, финансовое и организационное, и каждое из них требует самостоятельного решения. В кадровом отношении необходимо формирование устойчивой системы подготовки специалистов в области цифровой криминалистики, включающей как базовое профессиональное образование, так и систематическое повышение квалификации действующих сотрудников, причём эта система должна быть достаточно гибкой, чтобы своевременно реагировать на появление новых инструментов и методов генерации синтетического контента. В финансовом и организационном отношении перспективным направлением представляется создание специализированных межведомственных центров по противодействию цифровому мошенничеству, которые концентрировали бы экспертные ресурсы и обеспечивали бы методологическую поддержку территориальных подразделений, работающих с конкретными уголовными делами. Подобные центры могли бы также выполнять функцию мониторинга технологических тенденций и заблаговременно готовить методические рекомендации по выявлению новых видов дипфейк-мошенничества ещё до того, как они получат широкое распространение.

Проблема юрисдикционных коллизий и транснационального характера значительной части преступлений рассматриваемой категории требует решения на уровне международного права, и в этом отношении определённые перспективы уже обозначились в международной повестке, хотя их реализация остаётся делом отдалённого будущего. Существующие механизмы международного сотрудничества по уголовным делам, прежде всего институт взаимной правовой помощи, создавались применительно к принципиально иным преступлениям и отличаются такой процессуальной громоздкостью, которая делает их практически непригодными для расследования быстротечных дистанционных мошенничеств, совершаемых с использованием инфраструктуры, разбросанной по десят-

кам государств. Перспективный путь здесь состоит в разработке специальных международных соглашений об оперативном обмене данными и ускоренных процедурах правовой помощи применительно к киберпреступлениям, включая дипфейк-мошенничество, по образцу Будапештской конвенции о киберпреступности, однако с существенно более детальной регламентацией порядка взаимодействия применительно к современным технологическим реалиям. Параллельно следует развивать неформальные каналы оперативного взаимодействия между профильными подразделениями правоохранительных органов различных государств, которые позволяли бы обмениваться оперативно значимой информацией в режиме реального времени без необходимости прохождения длительных дипломатических процедур.

Вопрос об ответственности технологических платформ за распространение дипфейк-контента, используемого в мошеннических целях, на сегодняшний день решён крайне неудовлетворительно в большинстве правовых систем, и существующая модель, основанная преимущественно на добровольных инициативах самих платформ, доказала свою недостаточность. Перспективная модель регулирования в этой сфере предполагает введение обязательных требований к платформам по внедрению и применению технических средств обнаружения синтетического контента, установлению чётких процедур реагирования на жалобы пользователей относительно дипфейк-материалов и созданию механизмов взаимодействия с правоохранительными органами при расследовании конкретных преступлений. При этом требования должны быть дифференцированы с учётом размера платформы и масштабов её аудитории, что позволит избежать непропорционального бремени для небольших игроков рынка и сосредоточить регуляторное давление там, где оно наиболее востребовано. Одновременно следует рассмотреть возможность введения режима солидарной ответственности платформ в тех случаях, когда они после получения обоснованного уведомления о мошеннической кампании не принимали своевременных мер по её пресечению, поскольку только реальная правовая ответственность способна создать у платформ достаточные стимулы к активной борьбе с дипфейк-мошенничеством [10].

Проблема недостаточной цифровой грамотности населения и, как следствие, высокой уязвимости граждан перед методами социальной инженерии, усиленными дипфейк-технологиями, решается преимущественно через систему образования и просветительские программы, однако нынешнее состояние этих инструментов явно не соответствует остроте угрозы. Перспективное направление здесь состоит в последовательной интеграции навыков критической оценки цифрового контента в образовательные программы всех уровней, начиная со среднего образования, с акцентом не на теоретические знания о существовании дипфейков, а на практические умения распознавать манипулятивные схемы и верифицировать информацию через независимые источники. Для уже сформировавшихся взрослых аудиторий, особенно для пожилых людей и других демографических групп с повышенной уязвимостью, необходимы специализированные публичные просветительские кампании, реализуемые через каналы коммуникации, которыми эти группы реально пользуются, что требует отказа от универсальных подходов в пользу таргетированных программ. Банки и финансовые организации, которые являются частыми мишенями дипфейк-мошенников и одновременно располагают каналами прямой коммуникации с клиентами, могли бы взять на себя активную роль в распространении практических инструкций по распознаванию попыток манипуляции, превратив это в элемент стандартного информационного сопровождения финансовых услуг.

Техническое направление противодействия дипфейк-мошенничеству в долгосрочной перспективе связано с развитием и масштабным внедрением технологий верификации подлинности медиаконтента, прежде всего систем цифровых подписей для аудио- и видеозаписей, которые позволяли бы однозначно устанавливать их происхождение и целостность [11]. Стандарты цифровой атрибуции контента, разрабатываемые рядом технологических консорциумов, представляют собой перспективную основу для формирования общей инфраструктуры верификации, однако их практическая ценность напрямую зависит от широты охвата: стандарт работает только тогда, когда его применяет достаточно большое число участников рынка, чтобы неатрибутированный контент воспринимался как потенциально ненадёжный. Задача государства в этом контексте состоит в создании нормативных стимулов или обязательных требований к внедрению таких стандартов производителями устройств записи, поставщиками программного обеспечения и медиаплатформами, с тем чтобы техническая инфраструктура верификации получила достаточно широкое распространение для реального снижения рисков дипфейк-мошенничества.

Рассматривая дальнейшие перспективы развития описанных угроз, необходимо исходить из того, что технологии генерации синтетического контента будут продолжать совершенствоваться и становиться доступнее, а значит, ни одно из предложенных решений не может претендовать

на окончательность. Правовое регулирование и правоохранительная практика обречены на постоянное обновление в ответ на технологические изменения, и признание этого факта само по себе является методологически важным: вместо поиска универсального решения следует выстраивать адаптивные механизмы, способные реагировать на появление новых угроз без необходимости каждый раз запускать полноценный законодательный цикл. Перспективным инструментом здесь могут служить так называемые технологически нейтральные нормы, формулируемые на уровне принципов и общих критериев, а не конкретных технических описаний, поскольку такие нормы не устаревают вместе с технологиями, которые они регулируют.

Важнейшей перспективой совершенствования системы противодействия рассматриваемым угрозам остаётся развитие государственно-частного партнёрства в этой сфере, которое сегодня носит преимущественно декларативный характер, но может быть преобразовано в реально работающий механизм при наличии политической воли и чёткой институциональной рамки. Технологические компании располагают данными, экспертизой и техническими возможностями, которых нет у государства, тогда как государство обладает регуляторными, принудительными и координационными полномочиями, недоступными для частного сектора, и только устойчивое взаимодействие этих двух сторон способно обеспечить уровень противодействия, соразмерный масштабу угрозы. Конкретными формами такого партнёрства могут служить совместные аналитические центры, механизмы оперативного обмена данными об угрозах, совместно финансируемые исследовательские программы в области детекции дипфейков и согласованные стандарты технической экспертизы, используемой в уголовном судопроизводстве. Именно комплексный подход, объединяющий законодательное совершенствование, техническое развитие, международное сотрудничество, образовательные программы и государственно-частное партнёрство, способен создать ту систему противодействия мошенничеству с применением социальной инженерии и дипфейк-технологий, которая будет адекватна не только сегодняшним, но и завтрашним угрозам.

Подводя итог проведенному исследованию, мы можем сказать, что мошенничество с применением социальной инженерии и дипфейк-технологий представляет собой одну из наиболее сложных и стремительно развивающихся угроз современности, поскольку сочетает в себе психологическое воздействие на жертву с техническими возможностями создания практически неотличимого от подлинного аудиовизуального контента. Действующее законодательство большинства государств, в том числе российское, формировалось в принципиально иных условиях и не содержит норм, способных в полной мере охватить специфику подобных деяний, что ведёт к систематическому занижению их юридической оценки и фактической безнаказанности значительной части преступников. Зарубежный опыт показывает разнообразие подходов к решению этой проблемы: США идут по пути фрагментарного штатового регулирования, Европейский союз выстраивает системную рамку через общее цифровое право, а Китай применяет жёсткий административно-технический надзор с обязательной маркировкой синтетического контента, однако ни одна из этих моделей не может считаться исчерпывающим ответом на угрозу.

Также необходимо сделать ряд выводов, которые в дальнейшем могут способствовать дальнейшему научному изучению поставленной темы, к таким выводам стоит отнести:

1) Современное мошенничество претерпело существенные изменения по сравнению с теми формами, которые были известны правовой науке и практике ещё несколько десятилетий назад. Если прежде преступники делали ставку преимущественно на физический обман, поддельные документы или непосредственный контакт с жертвой, то сегодня центр тяжести сместился в сторону психологического воздействия, которое осуществляется дистанционно и нередко без каких-либо технически сложных инструментов. Именно здесь на первый план выходит социальная инженерия как самостоятельный метод преступной деятельности, основанный на манипулировании поведением человека через эксплуатацию его психологических особенностей, доверия, страха, любопытства или желания помочь.
2) Технологии как социальной инженерии, так и создания дипфейков продолжают стремительно развиваться, порождая всё новые разновидности преступной деятельности, которые правоприменительная практика и правовая наука вынуждены осмыслять уже после того, как они получили широкое распространение. Это обстоятельство наглядно свидетельствует о необходимости опережающего развития уголовно-правовой доктрины и законодательства в данной сфере, а не реакции на уже сложившиеся угрозы постфактум.
3) Эффективное противодействие мошенничеству с применением социальной инженерии и дипфейк-технологий требует одно-

временных усилий в нескольких направлениях: законодательного совершенствования, развития технической экспертизы, укрепления международного сотрудничества и повышения цифровой грамотности населения, причём все эти направления в равной степени необходимы и ни одно из них не может подменить остальные.

4) Важнейшей перспективой совершенствования системы противодействия рассматриваемым угрозам остаётся развитие государственно-частного партнёрства в этой сфере, которое сегодня носит преимущественно декларативный характер, но может быть преобразовано в реально работающий механизм при наличии политической воли и чёткой институциональной рамки. Технологические компании располагают данными, экспертизой и техническими возможностями, которых нет у государства, тогда как государство обладает регуляторными, принудительными и координационными полномочиями, недоступными для частного сектора, и только устойчивое взаимодействие этих двух сторон способно обеспечить уровень противодействия, соразмерный масштабу угрозы. Конкретными формами такого партнёрства могут служить совместные аналитические центры, механизмы оперативного обмена данными об угрозах, совместно финансируемые исследовательские программы в области детекции дипфейков и согласованные стандарты технической экспертизы, используемой в уголовном судопроизводстве. Именно комплексный подход, объединяющий законодательное совершенствование, техническое развитие, международное сотрудничество, образовательные программы и государственно-частное партнёрство, способен создать ту систему противодействия мошенничеству с применением социальной инженерии и дипфейк-технологий, которая будет адекватна не только сегодняшним, но и завтрашним угрозам.

5) Современное состояние правового регулирования в сфере противодействия мошенничеству с применением социальной инженерии и дипфейк-технологий характеризуется очевидным отставанием нормативной базы от темпов технологического развития, и это отставание уже сегодня порождает конкретные правоприменительные трудности, которые не позволяют эффективно привлекать виновных к ответственности и в полной мере защищать интересы пострадавших.

Список литературы:

[1] Антонян Е.А. Блокчейн - технологии в противодействии кибертерроризму / Е.А. Антонян, И.И. Аминов // Актуальные проблемы российского права. - 2019. - № 6 (103). - С. 170 - 175.

[2] Барсуков М.В. Влияние цифровой трансформации на уровень риска финансового мошенничества / М.В. Барсуков // Фундаментальные исследования. - 2022. - № 11. - С. 18 - 23.

[3] Данилова Е.П. Финансовое мошенничество в современном мире / Е.П. Данилова, Е.М. Портняга // SiberianSocium. - 2023. - Том 7. - № 2 (24). - С. 67- 97.

[4] Вестов Ф.А. Возможности цифровых технологий по противодействию мошенничеству / Ф.А. Вестов, А.Р. Абдрашитов // Научный - практический журнал Базис. - 2024. - № 2 (16). - С. 25- 28.

[5] Вестов Ф.А. Проблемы противодействия киберпреступности, как основа повышения эффективности экономики / Ф.А. Вестов, П.П. Шмелев // Эксперт: теория и практика. - 2021. - № 2 (11). - С. 73- 76.

[6] Лопатина Т.М. Проблемы уголовно- правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3-4 (45). С. 98 – 95.

[7] Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть [Текст] / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 2016. – 866 с.

[8] Кулешова Н.Н., Христофорова Е.И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2018. № 14 (26). С. 41-46.

[9] Куликов А.В., Гуц Е.А. Мошенничество в сфере компьютерной информации // Известия тульского государственного университета. экономические и юридические науки. 2020. № 1. С. 81 - 88.

[10] Курс мировой и российской криминологии в 2 т. Т. II. Особенная часть: учебник для вузов / В. В. Лунеев. – М.: Издательство Юрайт, 2015. – 872 с. – Серия: Магистр.

[11] Основы информационных технологий и кибербезопасности в деятельности органов внутренних дел Российской Федерации : Учебно-методическое пособие / В. Л. Акапьев, Е. Г. Ковалева, А. В. Борисенко [и др.]. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2026. – 88 с.

References:

[1] Antonyan E.A. Blockchain technologies in countering cyberterrorism / E.A. Antonyan, I.I. Aminov // Actual problems of Russian law. - 2019. - № 6 (103). - Pp. 170-175.

[2] Barsukov M.V. The impact of digital transformation on the level of risk of financial fraud / M.V. Barsukov // Fundamental Research. - 2022. - No. 11. - Pp. 18-23.

[3] Danilova E.P. Financial fraud in the modern world / E.P. Danilova, E.M. Portnyaga // SiberianSocium. - 2023. - Volume 7. - № 2 (24). - Pp. 67-97.

[4] Vestov F.A. Possibilities of digital technologies to counter fraud / F.A. Vestov, A.R. Abdrashitov // Scientific and practical journal Basis. - 2024. - № 2 (16). - Pp. 25-28.

[5] Vestov F.A. Problems of countering cybercrime as a basis for improving economic efficiency / F.A. Vestov, P.P. Shmelev // Expert: theory and practice. - 2021. - № 2 (11). - Pp. 73-76.

[6] Lopatina T.M. Problems of criminal law protection of computer information spheres: a modern view on fraud // Law and security. 2013. No.3-4 (45). Pp. 98-95.

[7] Lyapunov Yu.I., Pushkin A.V. Crimes in the field of computer information. Criminal law. The special part [Text] / Edited by N.I. Vetrov, Yu.I. Lyapunov, Moscow, 2016, 866 p.

[8] Kuleshova N.N., Khristoforova E.I. Features of fraud qualification in the field of computer information // Issues of science and education. 2018. No. 14 (26). Pp. 41-46.

[9] Kulikov A.V., Guts E.A. Fraud in the field of computer information // Proceedings of Tula State University. Economic and legal sciences. 2020. No. 1. Pp. 81-88.

[10] Course of World and Russian criminology in 2 volumes. Vol. II. Special part: textbook for universities / V. V. Luneev. Moscow: Yurait Publishing House, 2015. – 872 p. – Series: Master.

[11] Fundamentals of information technology and cybersecurity in the activities of the internal affairs bodies of the Russian Federation : An educational and methodological manual / V.L. Akapyev, E. G. Kovaleva, A.V. Borisenko [et al.]. - Belgorod : Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, 2026. – 88 p.

