

Дата поступления рукописи в редакцию: 28.01.2026 г.

DOI: 10.24412/2782-3849-2026-2-251-256

Дата принятия рукописи в печать: 12.03.2026 г.

СТРИЖАНОВ Алексей Вячеславович,
Воронежский институт МВД России,
доцент кафедры огневой подготовки,
кандидат педагогических наук,
e-mail: strizhanov_a_v@mail.ru,

ГУСЕВ Юрий Михайлович,
заместитель начальника кафедры огневой подготовки,
Белгородский юридический институт МВД России
имени И.Д. Путилина,
e-mail: 89803209873@yandex.ru,

КОВАЛЕВА Юлия Александровна,
Белгородский юридический институт МВД России
имени И.Д. Путилина, слушатель,
e-mail: kuulia8678@mail.ru.

КИБЕРПОЛИЦИЯ В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИИ DEEPFAKE: ПРОБЛЕМНЫЕ АСПЕКТЫ И ПУТИ ПРОТИВОДЕЙСТВИЯ

◇ **Аннотация.** Актуальность исследования определена необходимостью анализа специ-
◇ фических черт процесса цифровизации в современном мире, в том числе положительных и
◇ отрицательных черт. В результате исследования были определены проблемные аспекты про-
◇ тиводействия преступности, совершаемой с использованием информационно-коммуникаци-
◇ онных технологий, в том числе путем применения технологии deepfake и социальной инженер-
◇ ии, позволяющей фальсифицировать аудио- и видеофайлы с целью достижения преступно-
◇ го результата.

◇ **Ключевые слова:** технология deepfake, социальная инженерия, технология искусствен-
◇ ного интеллекта, цифровизация общества, киберугрозы, информационно-коммуникационных
◇ технологии, фальсификация, киберполиция.

STRIZHANOV Alexey Vyacheslavovich,
Voronezh Institute of the Ministry of Internal Affairs of Russia,
Associate Professor of the Department of Fire Training,
Candidate of Pedagogical Sciences

GUSEV Yuri Mikhailovich,
Deputy Head of the Department of Fire Training,
Belgorod Law Institute of the Ministry of Internal Affairs
of Russia named after I.D. Putilin

KOVALEVA Yulia Alexandrovna,
Belgorod Law Institute of the Ministry
of Internal Affairs of Russia named after I.D. Putilin,
police student

CYBER POLICE IN THE CONTEXT OF THE DEVELOPMENT OF DEEPFAKE TECHNOLOGY: PROBLEMATIC ASPECTS AND WAYS TO COUNTERACT

◇ **Annotation.** The relevance of the research is determined by the need to analyze the specific
◇ features of the digitalization process in the modern world, including positive and negative features.
◇ As a result of the study, problematic aspects of countering crime committed using information and

communication technologies were identified, including through the use of deepfake technology and social engineering, which makes it possible to falsify audio and video files in order to achieve a criminal result.

Key words: deepfake technology, social engineering, artificial intelligence technology, digitalization of society, cyber threats, information and communication technologies, falsification, cyber police.

Цель исследования – определить наиболее эффективные способы и методы противодействия преступлениям, совершаемым с использованием технологии deepfake и социальной инженерии, в том числе выделить проблемные аспекты, связанные с механизмами превентивной деятельности киберполиции и предложить свои пути комплексного решения.

Задачи исследования – обосновать необходимость противодействия распространению использования информационных технологий, в том числе технологии deepfake в противоправных целях, определить проблемные аспекты противодействия преступности, совершаемой с использованием информационно-коммуникационных технологий, в том числе путем применения технологии deepfake и социальной инженерии.

Методы исследования: метод системного анализа, статистический метод, сравнительно-правовой метод.

На сегодняшний день можно с уверенностью сказать, что Россия является развитой информационной страной, где информация и технологии – одни из важнейших ценностей общества. В эпоху цифровизации люди приобрели действительно большое количество возможностей – практически неограниченного доступа к знаниям, коммуникациям и самореализации в информационной среде. Все это привело к формированию совершенно новой цифровой экономики, инновационным продуктам и услуг, повышению эффективности государственных ресурсов и бизнес-процессов.

Для развитого информационного общества характерно:

1. увеличение роли информации и знаний в обществе;
2. возрастание числа людей, занятых в сфере информационных и коммуникационных технологий;
3. рост доли информационных продуктов и услуг в валовом внутреннем продукте;
4. появление глобального информационного пространства;
5. развитие информационной экономики, электронного правительства, социальных сетей и цифровых рынков. [1]

Такое движение вперед обусловлено постоянно развивающимся обществом и государством в лице государственных органов и различных государственных систем. Развитие информа-

ционного общества характеризуется не только количественными изменениями, но и качественными преобразованиями как в экономике страны, так и в социально-культурной сфере общества. Так, все более доступны стали туры по музеям и галереям, поскольку появилась возможность их виртуального посещения, в том числе различные онлайн-концерты и выступления, появились и онлайн-платформы для распространения культурного контента. Например, Рефик Анадолу – турецкий художник и дизайнер, известный интерактивными инсталляциями и проекциями, использующий виртуальную реальность. Мультимедийный проект «Сколково ARTs» – проект, который воплощает в себе симбиоз искусства и инноваций, проводит интерактивные выставки, на которых посетители могут взаимодействовать с произведениями искусства, используя современные технологии. [2]

Кроме этого, развитие информационных и коммуникационных технологий стимулирует инновации, повышение производительности труда и способствует созданию новых отраслей экономики. Например, телемедицина, электронные медицинские карты и информационные системы здравоохранения улучшают предоставление медицинских услуг, мониторинг состояния пациентов и доступ к медицинской информации. [3]

Электронное правительство, как неотъемлемая часть информационного общества, призвано обеспечить эффективное и прозрачное взаимодействие государства с гражданами. Предоставление государственных услуг упрощает процедуры, сокращает транзакционные издержки и повышает уровень доверия граждан к государству и государственным органам. Ярким примером такого проявления являются всем известные приложения «Госуслуги», «Налоги ФЛ», «Культура» и многие другие.

Однако, несмотря на множество положительных черт цифровизации общества и появления современных информационных технологий, различных автоматизированных систем, отмечаем, что необходимо проанализировать и оборотную сторону данного процесса. Среди негативных черт цифровизации необходимо выделить:

1. Высокие риски для приватизации и защиты персональных данных.

2. Киберугрозы информационной безопасности.
3. Цифровое неравенство.
4. Зависимость от технологий.
5. Снижение эмоциональных связей коммуникаций и взаимодействия.
6. Повышение уровня безработицы.
7. Загрязнение окружающей среды.
8. Утрата культурной идентичности в связи с глобализацией общества.
9. Информационная перегрузка.
10. Посягательства на цифровую свободу и права граждан и многое другое.

Безусловно, приведенный перечень опасностей не является исчерпывающим, однако характеризует большую часть негативных последствий для общества и государства. Важно понимать, что останавливать дальнейшее развитие, исходя из большого количества опасностей, не рационально, поскольку важно формировать специализированные системы, способные противодействовать таким угрозам, чтобы не только сохранить уже существующие успехи в науке и технике, но и продолжить дальнейшее их совершенствование. В связи с этим, с учетом всех возможных угроз, было принято решение о создании самостоятельного структурного подразделения – Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, которое было учреждено в 2022 году Указом Президента Российской Федерации «О внесении изменений в некоторые акты Президента Российской Федерации» и именуемого как киберполиция России. [4]

Согласно Приказу МВД России «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации», данное управление призвано осуществлять противодействие преступлениям в сфере информационно-коммуникационных технологий, обеспечивать и осуществлять предупреждение, выявление, пресечение и раскрытие преступлений, совершаемых с использованием (в сфере) информационно-коммуникационных технологий и выполнять иные задачи. [5]

Перечень полномочий и функций киберполиции довольно обширен, что говорит о ее ключевом значении в обеспечении безопасности информационного пространства.

На сегодняшний день особую опасность как для рядовых пользователей сетью Интернет, так и для огромных корпораций, представляет технология *deepfake*. Данная технология основана на искусственном интеллекте и позволяет создавать реалистичные, но, к сожалению, ложные видеозаписи и аудиозаписи. Технология *deepfake* при-

влекает к себе особое внимание со стороны правоохранителей и специалистов в сфере информационной безопасности, поскольку мошенники очень быстро освоили возможности современной технологии и превратили ее в мощное оружие обмана. Многие специалисты отметили, что число мошенничеств с использованием *deepfake* в 2025 году выросло в 2,3 раза по сравнению с 2024 годом. В 85-90% мошенничеств используется методы социальной инженерии, примерно 3-5% от числа таких случаев преступники используют технологию *deepfake*, что не выделяет данный показатель на общем фоне, однако, совсем недавно он не превышал и десятых долей процента. Поэтому такой рост преступных деяний создает серьезную угрозу для безопасности информационного пространства современного общества. [6]

Анализируя представленные статистические сведения, можно отметить, что рост фактов использования такой технологии позволяет сделать вывод о совершенствовании преступных методов и большей доступности инструментов для создания подделок. Особую тревогу вызывает сочетание *deepfake* – технологии с приемами социальной инженерии. Злоумышленники, обладая огромным спектром возможностей имитации голоса, внешности реальных людей, получают мощный инструмент не только для обмана, но и для манипулирования людьми. В 2025 году участились случаи, когда мошенники используют такую технологию для компрометации деловой репутации и шантажа. Как отмечает пресс-служба МВД России, в ноябре 2025 года была зафиксирована новая схема мошенничества, связанная с незаконным получением страховых выплат: злоумышленники подделывают фотографии с мест якобы произошедшего дорожно-транспортного происшествия для последующего предоставления их в страховые компании. Помимо фотографий, искусственный интеллект способен подделать голос знакомых людей, видеосообщения в социальных сетях. [7]

В глобальном смысле, с помощью технологии *deepfake* возможно создавать и подделывать выступления политиков, представителей государственных органов, руководителей компаний и организаций – различных влиятельных личностей, что, безусловно, может привести к серьезным последствиям для бизнеса, политики, да и общества и государства в целом.

Поэтому, одной из функциональных обязанностей современной киберполиции является борьба с распространением противоправного контента и создания ложных голосовых и аудиозаписей, используемых как для общения в различных мессенджерах, так и в деятельности раз-

личных организаций и предприятий. Бесспорно, повышенный интерес к их использованию вызван довольно обширным перечнем возможностей:

- простотой и доступностью технологий для различных категорий населения, что говорит о безграничном использовании технологии людьми различного уровня образования. Данный фактор оказывает значительное влияние на распространение deepfake-технологии, поскольку простота использования и применения для различных целей человеком с любым уровнем умственного развития – одно из преимуществ данной системы, в отличие от сложнейших кибератак, создания вредоносных программ и много другого, для чего необходимо не только образование, но и навыки работы с компьютером и программами.
- методы обработки и изменения видео и аудио файлов – не является подпольной системой, все больше приложений и программных обеспечений находятся в свободном доступе для пользования людьми, что обусловлено сильнейшим коммерческим стимулом.
- использование технологий изменения аудио и видео файлов для огромных рекламных проектов, массовых рассылок потребителям, позволяющих снизить затраты на рекламные кампании крупных организаций и предприятий и другое.

Использование deepfake-технологий правонарушителями с целью получения материальной выгоды является нарушением имущественных и личных прав граждан, однако профильного законодательства, регулирующего данную область, в России нет.

В Уголовном кодексе РФ отражены лишь отдельные статьи особенной части в области мошенничества в сфере компьютерной информации. Это говорит об отсутствии в нормативно-правовых актах какого-либо упоминания о рассматриваемой технологии. Однако, анализируя различные мнения в научной и учебной литературе относительно сущности deepfake-технологии и особенностей квалификации преступлений при ее использовании, мы выделили различные мнения специалистов, которые разделили на две группы:

1. необходимы кардинальные изменения уголовного законодательства путем введения отдельных статей, отражающих незаконное использование deepfake-технологии для получения прибыли или иной материальной выгоды, услуг, либо внесение изменений в отдельные уже существующие нормы Уголовного кодекса РФ путем дополнения квалифицирующим признаком «использование

технологии deepfake», что ужесточит наказание за подобные деяния. В дополнение можно отметить, что некоторые правоведы склоняются к внесению изменений в ст. 63 Уголовного кодекса РФ путем дополнения перечня обстоятельств,отягчающих наказания, пунктом – «использование информационных технологий, таких как искусственный интеллект, при совершении преступлений против собственности». [8, С.109]

Таким образом, относительно первого мнения, отмечено явное стремление к ужесточению наказания и усиления уголовной ответственности за преступления, совершаемые с использованием информационных технологий, в том числе технологии deepfake и социальной инженерии.

2. другая группа специалистов не видит необходимости введения отдельных норм или внесения изменений в существующие нормы уголовного законодательства РФ относительно использования рассматриваемой технологии, поскольку deepfake-технология в совокупности с социальной инженерией является лишь одним из способов совершения противоправного деяния, т.е. злоумышленники применяют противоправный контент или ложные аудио- и видео-файлы с целью обмана или злоупотребления доверием, под воздействием которых владелец имущества или иное лицо предадут это имущество или право на него либо не будут препятствовать изъятию. Фактически для реализации данной формы хищения (мошенничества) используются любые способы, чтобы ввести лицо в заблуждение, в том числе и различные информационные технологии, которые также выступают способом достижения противоправной цели злоумышленника. В таком случае, выделение в качестве квалифицирующего признака, в том числе дополнения перечня обстоятельств, отягчающих наказания, не является необходимой мерой, поскольку является одним из способов обмана лица. Однако, данный факт не свидетельствует об отсутствии необходимости противодействия распространению использования информационных технологий, в том числе технологии deepfake в противоправных целях.

По нашему мнению, представленные точки зрения имеют место в существующей цифровой реальности, поскольку механизм противодействия лишь формируется и до сих пор ведутся исследования в отношении максимально эффективной стратегии борьбы с мошенничеством в информационном пространстве. Например, в 2024 году состоялась попытка внесения в Госу-

дарственную Думу законопроекта №718538-8, который вводил ряд дополнительных квалифицирующих признаков «совершение с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, либо их биометрических персональных данных» в следующие статьи Уголовного кодекса РФ: ст. 1281, ст. 158, ст. 1596, ст. 163, ст. 165. Данный законопроект и был направлен на введение и закрепление в нормативно-правовых документах использования в противоправных целях фальсификации изображений или голоса потерпевших, т.е. рассматриваемой нами технологии deepfake. Однако данный законопроект не был принят по различным причинам, в том числе из-за довольно размытой и неопределенной используемой формулировки, которая может привести к неоднозначному толкованию положения. [9]

Помимо законодательных методов регулирования, действует киберполиция, обладающая особым перечнем полномочий, направленных на использование комплекса методов с целью выявления deepfake в информационной сети. Например, назначение и проведение экспертизы deepfake и синтетического медиа, которая позволяет установить подлинность видеофайла, имеются ли в нем признаки синтеза или модификации, а также содержит ли изображение признаки использования графических редакторов или технологий синтеза изменений внешности и облика человека или иных объектов, какие конкретно фрагменты имеют признаки манипуляций, и каким конкретно манипуляциям был подвержен аудио- или видеофайл. [10] Имеет место проведение и таких судебных экспертиз, как фonoскопическая, которая позволяет анализировать спектральные характеристики звука, выявлять признаки цифровой склейки или монтажа, а также изменения интонаций, фоновых звуков, тембра и многих других специфических особенностей речи.

А.Г. Исакова и А.В. Осин отмечают, что в обнаружении deepfake используется технология искусственного интеллекта, которая способна обнаружить малейшие погрешности изображения и выявить технические изменения, а также иные произведенные манипуляции. Для этого используются различные способы аутентификации, направленные на анализ цифровых подписей, водяных знаков, проверку метаданных и цифровых характеристик. [11, С. 239]

Таким образом, использование технологии deepfake в противоправных целях является серьезной угрозой как для пользователей, так и для различных организаций и предприятий. Дальнейшее развитие их использования может спровоцировать воздействие и на различные сферы

общества, так и на государство в целом. Отсутствие законодательного регулирования такой технологии не говорит об отсутствии противодействия. В качестве основных мер борьбы с действиями противоправного характера с использованием технологии deepfake и социальной инженерии являются: законодательное регулирование противодействия путем наделения функциональными возможностями соответствующие подразделения правоохранительных органов; формирование современных методик расследования преступлений, совершенных с помощью такой технологии; применение современных технических средств и возможностей научного познания (различные экспертизы); формирование новых структурных подразделений в составе органов внутренних дел, таких как «киберполиция», важнейшей функцией которой является расследование, раскрытие преступлений, совершенных с использованием информационно-коммуникационных технологий, в том числе их предупреждение, а также активная профилактическая деятельность и многое другое.

В большинстве своем особое внимание уделяется именно профилактической деятельности, которая напрямую связана с населением, а именно, с донесением информации о наиболее частых способах совершения мошенничества, путем публикации в средствах массовой информации и личных бесед участковых, сотрудников патрульно-постовых служб с категориями населения, в отношении которых противоправные посяательства совершаются чаще всего.

Достигнутые результаты данного исследования позволяют установить особенности использования искусственного интеллекта, в особенности технологии deepfake в совокупности с социальной инженерии, в противоправных целях, а также механизмы противодействия киберполиции развитию киберпреступности.

По нашему мнению, необходимо обратить внимание именно на законодательное регулирование использования технологий искусственного интеллекта, в том числе deepfake, поскольку в структуре квалификации преступления имеет решающее значение способ его совершения.

Список литературы:

[1] Шашлова, С. А. Информационное общество и его основные черты / С. А. Шашлова. — Текст : непосредственный // Молодой ученый. — 2022. — № 17 (412). — С. 276-278. — URL: <https://moluch.ru/archive/412/90772> (Дата обращения: 07.12.2025).

[2] Портал Путилово [Сайт] // URL: <https://sdk-putilovo.ru/news-paznoe/item/198-iskusstvo-i-kultura-v-epokhu-tsifrovoykh-media> (Дата обращения: 07.12.2025).

[3] Наука Экспертиза [Сайт] // URL: <https://digitalocean.ru/n/chto-takoe-ikt> (Дата обращения: 07.12.2025).

[4] О внесении изменений в некоторые акты Президента Российской Федерации: Указ Президента РФ от 30 сентября 2022 № 688 // Доступ из справ.-прав. системы Консультант Плюс.

[5] Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: Приказ МВД России от 29 декабря 2022 № 1110 // Доступ из справ.-прав. системы Консультант Плюс.

[6] Forbes [Сайт] // URL: <https://www.forbes.ru/tekhnologii/539953-eksperty-soobsili-o-rezkom-roste-cisla-mosennicestv-s-ispol-zovaniem-dipfejkov> (Дата обращения: 07.12.2025).

[7] TADVISER // URL: <https://www.tadviser.ru/index.php/> (Дата обращения: 10.12.2025).

[8] Долгиева, М.М. Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. — 2024. — Т. 19. — № 11. — С. 106-113.

[9] Система обеспечения законодательной деятельности [Сайт] // URL: <https://sozd.duma.gov.ru/bill/718538-8> (Дата обращения: 07.01.2026).

[10] Судебный эксперт [Сайт] // URL: <https://sudexpa.ru/expertises/ekspertiza-dipfeikov-deepfake-i-sinteticheskogo-media/> (Дата обращения: 07.01.2026).

[11] Исакова, А.Г. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «Дипфейк» // А.Г. Исакова, А.В. Осин // Международный научный журнал Вестник науки. – 2024. – №1(70). – С.235-241.

References:

[1] Shashlova, S. A. Information Society and its main features/S. A. Shashlova. - Text: direct/Young

scientist. — 2022. — № 17 (412). - S. 276-278. - URL: <https://moluch.ru/archive/412/90772> (Accessed: 07.12.2025).

[2] Putilovo Portal [Site]//URL: <https://sdk-putilovo.ru/news-paznoe/item/198-iskusstvo-i-kultura-v-epokhu-tsifrovyykh-media> (Accessed: 07.12.2025).

[3] Science Expertise [Site]//URL: <https://digitalocean.ru/n/chto-takoe-ikt> (Accessed: 07.12.2025).

[4] On amendments to certain acts of the President of the Russian Federation: Decree of the President of the Russian Federation of September 30, 2022 No. 688//Access from reference. systems Consultant Plus.

[5] On approval of the Regulation on the Office for the Organization of Combating the Illegal Use of Information and Communication Technologies of the Ministry of Internal Affairs of the Russian Federation: Order of the Ministry of Internal Affairs of Russia dated December 29, 2022 No. 1110//Access from reference. systems Consultant Plus.

[6] Forbes [Сайт] // URL: <https://www.forbes.ru/tekhnologii/539953-eksperty-soobsili-o-rezkom-roste-cisla-mosennicestv-s-ispol-zovaniem-dipfejkov> (Дата обращения: 07.12.2025).

[7] TADVISER//URL: <https://www.tadviser.ru/index.php/> (Accessed: 10.12.2025).

[8] Dolgieva, M.M. Qualification of deepfake fraud and human cyber theft//Actual problems of Russian law. — 2024. — Т. 19. — № 11. - S. 106-113.

[9] Legislative Support System [Site]//URL: <https://sozd.duma.gov.ru/bill/718538-8> (Accessed: 07.01.2026).

[10] Adjudicator [Site]//URL: <https://sudexpa.ru/expertises/ekspertiza-dipfeikov-deepfake-i-sinteticheskogo-media/> (Accessed: 07.01.2026).

[11] Isakova, A.G. The use of artificial intelligence in the investigation of crimes using the Deepfake technology//A.G. Isakova, A.V. Osin//International Scientific Journal Bulletin of Science. – 2024. – №1(70). - S.235-241.