Секция «Юриспруденция: актуальные вопросы правотворчества и правоприменения (СИУ РАНХиГС)»

# Виктимологический аспект мошенничества с использованием технологий deepfake и искусственного интеллекта

***Бажина Ксения Максимовна***
*Студент (бакалавр)*
Казанский инновационный университет имени В.Г. Тимирясова (ИЭУП), Юридический факультет, Кафедра уголовного права и процесса, Казань, Россия
*E-mail: bazhinakm@ieml.ru*

Цифровая трансформация общества, несущая огромные возможности для всех видов жизни общества, и дает неограниченные возможности для развития, порождает новые вызовы для системы правового регулирования общества. Одним из наиболее опасных феноменов последних лет стало использование технологий искусственного интеллекта (далее – ИИ) и так называемых deepfake для совершения большого количества преступлений, чаще – для мошеннических действий. Доступность нейросетей и их стремительное развитие существенно расширили арсенал средств социальной инженерии, используемой для противоправных действий, позволяя злоумышленникам создавать новые меры с помощью новых механизмов.

Как справедливо отмечается исследователями в области киберпреступлений, в настоящее время в России наблюдается резкий скачок хищений с использованием искусственного интеллекта (далее – ИИ). С начала 2020 года рост дошел до троекратной разницы и в таких условиях изучение виктимологической стороны преступления приобретает особое значение, поскольку именно человеческий фактор остается наиболее уязвимым звеном в системе противодействия подобных преступлений.

Чтобы как можно подробнее рассмотреть виктимологию данных преступных деяний, необходимо разобраться с технологическим базисом, а именно с пояснением используемых методов.

Дипфейк представляет собой один из продуктов технологий искусственного интеллекта для создания реалистичных изображений и фонограмм, видеофонограмм, проверка подлинности которых на современном этапе может быть затруднительна. Генеративная природа этих технологий позволяет создавать контент, который с высокой точностью позволяет пользователям создавать внешность, голос, мимику и жестикуляцию конкретного человека.

С криминалистической точки зрения deepfake – технологии классифицируются по признаку отношения к биометрической информации, поскольку основной массив сгенерированной информации нейросети направлен на подмену именно биометрических данных – различных лиц, синтез реальных голосов и создание видеозаписей с их участием.

С использованием deepfake есть несколько крупных мошеннических схем, позволяющим использовать ИИ и социальную инженерию, например, имитация руководства или просьб близкий лиц. Это использование синтезированных голоса и изображений для обращения к жертве от имени руководителя существующей организации или обращение просьб родственников или друзей о срочном переводе денежных средств. В России такая практика встречается довольно часто и отследить мошенника становится крайне тяжело из-за ряда технологических причин.

Существует несколько факторов, влияющих на уязвимость населения к таким видам мошенничеств. Они заключаются в том, что объектами манипуляций с ИИ становятся не столько техническая защищенность потенциальной жертвы, сколько ее когнитивные установки и доверие к видео- и аудиоинформации.

1. Возрастной фактор. Лица пенсионного возраста составляют наиболее уязвимую группу населения. Данный факт подтверждается тем, что пожилые люди в силу недостаточного уровня цифровой грамотности и сформированных установок в отношении к представителям власти и должностных лиц чаще других становятся жертвами мошеннических схем.

2. Профессиональный фактор. Лица, занимающие руководящие должности в коммерческих организациях и наделенные правом распоряжаться денежными средствами. Такие лица тоже попадают в группу высокого риска из-за особых рабочих установок и трудовых обязанностей. Атаки на менеджмент отличаются особо крупным размером хищения и убытков, так как речь идет о прибыли компании.

3. Психологический фактор. Исследователи выделяют ряд психологических характеристик, которые могут так или иначе способствовать виктимизации – доверчивость, склонность к подчинению авторитетам, если мы говорим о преступлениях с использованием применения должностных лиц, недостаточная критичность при оценке информации, высокая тревожность. Преступники целенаправленно используют эти человеческие качества для применения эмоционального давления.

4. Ложное чувство безопасности. Парадоксальным образом рост осведомленности населения о существовании подобных схем мошенничества может создавать дополнительные риски. Это означает, что даже критически настроенные лица могут оказаться уязвимыми перед высококачественной подделкой и человеческим фактором, если их защитный механизм основывается только на визуальном анализе.

27 января 2026 года депутаты Государственной Думы Российской Федерации предложили установить уголовную ответственность за создание deepfake путем автоматизированной обработки персональных данных. Изменения будут касаться статьи 272.1 Уголовного кодекса Российской Федерации. В статью будут добавлены положения о запрете на автоматизированную обработку персональных данных и будет направлен непосредственно на борьбу с преступлениями с использованием ИИ. Такое предложение связано с тем, что в 2026 году специалисты выявили новый всплеск мошенничества с использованием нейросетей.

## Источники и литература

1) Бодров Н.Ф., Лебедева А.К. Понятие дипфейка (deepfake) в российском праве, его классификация и проблемы правового регулирования. // Юридический вестник Дагестанского государственного университета, 2023 г. URL: https://cyberleninka.ru/article/n/ponyatie-dipfeyka-deepfake-v-rossiyskom-prave-ego-klassifikatsiya-i-problemy-pravovogo-regulirovaniya (дата обращения 01.04.2026 г.)

2) Малышева Ю.Ю. Мошеннические проявления фейков и дипфейков: проблемы противодействия // Российско-азиатский правовой журнал, 2025 г. URL: https://cyberleninka.ru/article/n/moshennicheskie-proyavleniya-feykov-i-dipfeykov-problemy-protivodeystviya (дата обращения 01.04.2026г.)

3) Пикалов П.А. Кибермошенничество с использованием искусственного интеллекта. // Актуальные вопросы борьбы с преступлениями. 2024 г. URL: https://cyberleninka.ru/article/n/kibermoshennichestvo-s-ispolzovaniem-iskusstvennogo-intellekta (дата обращения 01.04.2026 г.)