ISSN 2949-1150 (online)
2071-8284 (print)

Научная статья
УДК 343.9

Криминологические и уголовно-правовые аспекты дистанционного мошенничества с применением deepfake-технологий и социальной инженерии

Екатерина Сергеевна Палий

Московский университет МВД России имени В. Я. Кикотя
Москва (117437, ул. Академика Волгина, д. 12), Российская Федерация
alibi-2013@mail.ru
https://orcid.org/0009-0006-0590-4561

Аннотация:
Введение. *Статья посвящена актуальной проблеме дистанционного мошенничества в условиях цифровой трансформации общества, с особым упором на использование преступниками искусственного интеллекта (ИИ).*
Методы. *Автором проведен комплексный виктимологический анализ современных мошеннических схем, основанных на технологиях глубокого обучения, генерации текстов, аудио- и видеоподделок (deepfake).*
Результаты. *Подчеркивается, что доступность и развитие технологий ИИ существенно усиливают возможности мошенников по созданию персонализированных атак и автоматизированных схем социальной инженерии. Рассматриваются виктимологические последствия данного феномена, включая рост уязвимости широких слоев населения и снижение эффективности традиционных мер защиты. Исследование опирается на зарубежную научную традицию, отражающую передовые подходы к пониманию социальных и технических аспектов цифровой виктимизации. Выявлены ключевые направления противодействия мошенничеству, включая развитие антифрод-систем, многоуровневую аутентификацию, интеграцию обучающих материалов в популярные онлайн-платформы и совершенствование международного правового регулирования.*
Выводы. *Автор заключает, что для эффективного снижения виктимности в условиях использования ИИ необходимы комплексный подход, объединяющий технологические инновации, повышение цифровой грамотности и развитие правовых механизмов защиты.*

Ключевые слова:
дистанционное мошенничество, искусственный интеллект, виктимологический анализ, цифровая виктимизация, deepfake, социальная инженерия, антифрод-системы, машинное обучение, персонализированные атаки, цифровая безопасность, международное сотрудничество, киберпреступность

Для цитирования:
Палий Е. С. Криминологические и уголовно-правовые аспекты дистанционного мошенничества с применением deepfake-технологий и социальной инженерии // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 149–157.

Статья поступила в редакцию 11.07.2025; одобрена после рецензирования 01.10.2025; принята к публикации 25.12.2025.

Original article

Criminological and criminal-legal aspects of remote fraud involving deepfake technologies and social engineering

Ekaterina S. Paliy

Moscow University of the MIA of Russia named after V. Ya. Kikot
12, Academician Volgina str., Moscow, 117437, Russian Federation
alibi-2013@mail.ru
https://orcid.org/0009-0006-0590-4561

Abstract:
Introduction. *The article is dedicated to the actual problem of remote fraud in the context of digital transformation of society, with a particular focus on the use of artificial intelligence (AI) by criminals.*
Methods. *The author carried out a comprehensive victimological analysis of modern fraud schemes based on deep learning technologies, text generation, and audio and video forgeries (deepfakes).*
Results. *The author emphasises that the accessibility and development of AI technologies significantly increase the possibilities for fraudsters to create personalised attacks and*

Keywords:
remote fraud, artificial intelligence, victimological analysis, digital victimisation, deepfake, social engineering, anti-fraud systems, machine learning, personalised attacks, digital security, international cooperation, cybercrime

automated social engineering schemes. The victimological consequences of such a phenomenon are considered, including the increased vulnerability of broad segments of the population and the reduced effectiveness of traditional protective measures. The research is based on foreign scientific traditions reflecting advanced approaches to understanding the social and technical aspects of digital victimisation. Key areas for counteracting fraud are identified, including the development of anti-fraud systems, multi-level authentication, integration of educational materials into popular online platforms, and improvement of international legal regulation.

Conclusions. *The author concludes that in order to effectively reduce victimisation in the context of AI use, a comprehensive approach integrating technological innovation, increased digital literacy and development of legal protection mechanisms is required.*

For citation:
Paliy E. S. Criminological and criminal-legal aspects of remote fraud involving deepfake technologies and social engineering // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 4 (108). P. 149–157.

**The article was submitted July 11, 2025;
pproved after reviewing October 1, 2025;
accepted for publication December 25, 2025.**

Введение

Современное общество переживает стремительную цифровую трансформацию, в ходе которой информационно-коммуникационные технологии становятся все более доступными и многогранными. Интернет, мобильная связь, социальные сети и широкий спектр онлайн-сервисов радикально изменили способы взаимодействия людей, формируя новую среду для экономической, культурной и социальной деятельности. В научном дискурсе под дистанционным мошенничеством понимаются хищения, совершаемые удаленно с использованием информационно-коммуникационных технологий; при этом соответствующие деяния охватываются составами преступлений, предусмотренных ст. 159, 159[3] и 159[6] Уголовного кодекса Российской Федерации[1] (далее – УК РФ). Вместе с тем по мере роста цифровых возможностей растут и угрозы преступного характера, среди которых одно из ведущих мест занимает дистанционное мошенничество. Это явление многократно усложнилось с появлением искусственного интеллекта (далее – ИИ), предоставляющего злоумышленникам инструменты анализа больших массивов данных, генерации фейковых сообщений и автоматизации атак. В результате столкновение с высокотехнологичным мошенничеством перестает быть редким исключением и все чаще превращается в рутинную опасность для массового пользователя сети, тогда как ущерб только в России составляет миллиарды рублей[2]. Цель настоящего исследования заключается в комплексном анализе феномена дистанционного мошенничества в цифровую эпоху (с особым акцентом на использование искусственного интеллекта злоумышленниками), выявлении его социальных, виктимологических и правовых особенностей и определении ключевых направлений противодействия данной угрозе. Для достижения указанной цели были поставлены следующие задачи исследования:

1) сформулировать понятие и границы «дистанционного мошенничества», обосновав легитимность данного термина в научном дискурсе и соотнеся его с соответствующими нормами УК РФ;

2) проанализировать современные схемы и технологии дистанционного мошенничества (включая *deepfake* и другие методы социальной инженерии), выявив их криминологические характеристики;

3) исследовать виктимологические факторы и последствия подобных преступлений, определив наиболее уязвимые категории жертв и используемые злоумышленниками механизмы;

4) предложить перспективные меры профилактики и противодействия высокотехнологичным мошенническим схемам. Важно отметить, что настоящее исследование сфокусировано на виктимологических и криминологических аспектах проблемы (с учетом нормативного фона) и не предусматривает детального уголовно-правового анализа.

Материалы и методы

Методологическую основу работы составляет виктимологический анализ, направленный на выявление и исследование особенностей жертв дистанционного мошенничества в цифровую эпоху с акцентом на использование искусственного интеллекта преступниками. Для раскрытия поставленной задачи был использован широкий круг источников, отражающих современную отечественную и зарубежную научную традицию в области киберпреступности и социальной

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.03.2024) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 1996. № 25. Ст. 2954.

[2] Прокурорами направлены в суды иски о взыскании 1,5 млрд рублей с владельцев банковских карт, куда первично поступали похищенные у людей деньги / Генеральная прокуратура Российской Федерации : [официальный сайт]. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=100723474 (дата обращения: 20.03.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

инженерии. Кроме этого, проведен контент-анализ актуальной зарубежной научной литературы по данной проблеме, что позволило учесть новейшие идеи зарубежных исследователей в отношении рассматриваемого явления. Особое внимание уделено трудам зарубежных авторов, поскольку именно международные исследования в большей степени раскрывают новейшие угрозы и технологические аспекты мошенничества, связанные с искусственным интеллектом [1–4]. Анализируются подходы авторов, раскрывающих виктимологическую специфику онлайн-преступлений, психологию жертв, технологии социальной инженерии [5–7]. Дополнительно были использованы материалы эмпирических исследований и статистических обзоров, посвященных современным схемам мошенничества, а также технические работы по антифрод-системам и машинному обучению[3] [8; 9]. Виктимологический анализ позволяет рассмотреть механизмы воздействия злоумышленников на жертвы, выявить социально-психологические и технические факторы уязвимости, а также предложить возможные направления противодействия [10].

Результаты

Расширение цифрового пространства усилило возможности для дистанционных атак, особенно учитывая, что многие социальные и экономические процессы переходят в онлайн-формат [11]. Банковский сектор, электронная коммерция, государственные услуги, образование и даже медицина все более тесно интегрируются с интернетом, предоставляя пользователям существенные удобства и ускоряя многие жизненно важные процессы. Однако вместе с тем повышается уязвимость, связанная с хранением и передачей личных данных, а также с доверительными механизмами идентификации и авторизации[4]. Если в первые годы эры интернета преобладали относительно примитивные мошеннические схемы, то с течением времени злоумышленники освоили социальную инженерию и начали использовать более изощренные методы. Особую значимость приобретают технологии искусственного интеллекта, которые позволяют автоматизировать действия, раньше выполнявшиеся вручную, и генерировать убедительные подделки – от фишинговых писем до синтетических медиафайлов, известных как *deepfake*. Исследователи подчеркивают, что данная тенденция ведет к существенному изменению парадигмы безопасности: если раньше для распознавания обмана достаточно было базовых навыков цифровой гигиены, то сегодня даже опытным пользователям бывает сложно отличить искусственно сгенерированные сообщения от реальных [12]. «Мошенники предпринимают определенные действия, чтобы получить доступ к банковской карте потенциальной жертвы: используют списки рассылки от имени банка, содержащие веб-адреса нужных страниц, копии официальных сайтов, предлагающих ввести реквизиты банковской карты для дальнейшего ее использования. Довольно часто встречаются ситуации, когда жертве звонит мошенник, представляющийся сотрудником банка, и просит сообщить конфиденциальные сведения о карте или данные для входа в онлайн-банк, для того чтобы пресечь подозрительную транзакцию, совершаемую с использованием банковской карты или счета абонента. В таких случаях потерпевший, находясь в состоянии испуга, предоставляет необходимую злоумышленнику информацию» [13].

Рост использования ИИ в криминальной сфере неразрывно связан с широкой доступностью высокопроизводительных вычислительных ресурсов и алгоритмов машинного обучения с открытым исходным кодом. В прошлом сложные нейронные сети требовали дорогого оборудования и штата высококвалифицированных специалистов, однако демократизация технологий, включая появление облачных платформ и готовых к использованию библиотек, значительно снизили порог входа для злоумышленников. Теперь разработка вредоносных программ, способных анализировать большие объемы украденных баз данных, становится значительно проще. Кроме того, инструменты ИИ позволяют оптимизировать сценарии мошеннических атак, подбирая конкретную «приманку» в соответствии с профилем потенциальной жертвы. Это может выражаться, например, в таргетированных фишинговых письмах, ориентированных на индивидуальные интересы пользователя, его социальный статус, сферу деятельности или даже психотип [5]. С точки зрения виктимологии, подобная персонализация, проводимая машинным алгоритмом, повышает эффективность обмана, ведь человек, получая письмо с темами, которые ему действительно интересны, менее склонен критически относиться к содержанию. Существует и другой аспект: искусственный интеллект способен генерировать правдоподобные

[3] Обзор операций, совершенных без согласия клиентов – 2020 // Банк России : [официальный сайт]. URL: https://www.cbr.ru/collection/collection/file/32190/review_of_transactions_2020.pdf (дата обращения: 20.03.2025).

[4] Online Holiday Shopping Scams // Cybersecurity and Infrastructure Security Agency (CISA) : (website). URL: https://www.cisa.gov/news-events/alerts/2020/11/24/online-holiday-shopping-scams (дата обращения: 20.03.2025).

тексты и даже вести переписку, имитируя стиль живого человека, что еще более затрудняет распознавание мошеннической схемы.

Если традиционное мошенничество требует определенного человеческого ресурса, времени и навыков, то с внедрением ИИ и автоматизации злоумышленники могут обрабатывать огромное количество потенциальных жертв. Речь идет о миллионных рассылках электронных писем, тысячах одновременных телефонных звонков, а также многоступенчатых атаках, где бот на одном этапе собирает информацию о пользователе, а на другом этапе уже генерирует индивидуальный сценарий вовлечения. Подобные схемы часто используют модули машинного обучения, которые анализируют реакции жертв и адаптируют сообщения, повышая вероятность успеха [14]. Одновременно расширяются и формы мошенничества. Если раньше злоумышленники в основном подделывали сайты банков и делали фишинговые письма, то теперь появляются инвестиционные платформы, полностью созданные фейковыми алгоритмами, или мобильные приложения, якобы предлагающие консультации на базе искусственного интеллекта, но фактически ворующие данные пользователей. В контексте этой эволюции традиционные меры кибербезопасности, основанные на статических сигнатурах и опознавании типовых шаблонов, могут быть недостаточны, поскольку ИИ на стороне преступников умеет генерировать все новые варианты вредоносных сценариев без явных повторений, которые можно было бы заранее занести в антивирусные базы [6].

На виктимологической структуре цифрового мошенничества влияние искусственного интеллекта сказывается очень заметно. Во-первых, искусственный интеллект позволяет преступникам анализировать громадные объемы утекших персональных данных – пароли, номера телефонов, профили в социальных сетях, предпочтения в покупках. Такие данные нередко продаются в так называемом даркнете (теневом сегменте интернета). Объединив несколько источников, нейронная сеть способна выделить закономерности и сегментировать пользователей по критериям возраста, пола, финансовых возможностей, интересов и даже психологических особенностей. Подобная дифференциация превращает «вспомогательную» деятельность мошенников в целое искусство высокоточной социальной инженерии. Каждый потенциальный пользователь может получать специфическое письмо или сообщение, рассчитанное именно на его слабые места и интересы [7]. Во-вторых, широкий доступ к технологиям генерации текста и медиа (включая *deepfake*) повышает уровень доверия жертвы, когда она слышит или видит, казалось бы, знакомого человека, просящего о денежном переводе, либо слышит голос «реального» сотрудника банка. Подмена личности становится проще, ведь алгоритмы могут синтезировать речь и мимику, неотличимые с первого взгляда от настоящих. Виктимологи, исследующие этот феномен, говорят о качественном скачке в методах социальной инженерии, поскольку традиционные сигналы, по которым человек мог разоблачить обман, становятся ненадежными [15]. Даже видеосвязь уже не гарантирует подлинности собеседника.

Особенно остро проблема проявляется в банковской и финансовой сферах. По данным ряда аналитических докладов, крупные международные банки периодически сталкиваются с тем, что их клиенты становятся жертвами звонков мошенников, которые подделывают не только номер банка, но и голос. Такие сценарии, подкрепленные собранными нейросетью данными о конкретном клиенте, выглядят крайне правдоподобно. Людям сообщают, что их счет якобы взломан, и для его защиты нужно срочно перевести деньги на «резервный» или «страховой» счет, после чего у человека исчезают накопления. С точки зрения классической криминологии, такое поведение со стороны жертвы может показаться нелогичным, ведь люди должны понимать, что настоящий банк не попросит перевести деньги на незнакомый счет. Однако технология синтеза речи, вызов с подмененного номера, обилие персонализированной информации и создание эффекта срочности формируют у жертвы сильнейшее стрессовое состояние. Подобная эмоциональная перегрузка снижает уровень критического мышления и повышает восприимчивость к обману [6]. Ключевую роль играет и фактор авторитета, когда пользователь убежден, что контактирует с официальным представителем организации.

Не меньшее беспокойство вызывает эволюция так называемого *romance scam* (мошенничества, основанного на имитации романтических отношений) и прочих мошеннических схем в социальных сетях. Здесь искусственный интеллект может использоваться для ведения долгосрочной переписки, имитируя стиль и манеру общения, характерные для определенных культурных групп. Некоторые исследования показывают, что преступники создают ботов, способных выдавать себя за реального пользователя и постепенно выстраивать эмоциональную привязанность жертвы, пробуждая у нее доверие и желание помочь. Сгенерированные фотографии и видеоролики добавляют убедительности, поскольку современные генеративные алгоритмы (GAN) в состоянии создавать правдоподобные лица, которые не принадлежат ни одному реальному

ISSN 2949-1150 (online)
2071-8284 (print)

человеку. По мере укрепления отношений мошенник-бот просит деньги на «срочные нужды», «лечение», «билет для встречи» и т. п. Печальные примеры подобных ситуаций известны во многих странах мира, а пострадавшие часто вынуждены замалчивать свою историю из чувства стыда (как отмечалось ранее [9]). Виктимологическая природа таких преступлений весьма сложна, т. к. жертва становится заложником собственного эмоционального вклада, а преступник действует через тщательно подготовленные манипуляции, усиленные технологическими средствами.

С точки зрения социальной динамики нельзя упускать из виду возрастное и культурное многообразие жертв [9]. Пожилые люди традиционно рассматриваются исследователями как одна из наиболее уязвимых групп, поскольку у них нередко меньше навыков цифровой гигиены и они могут более доверчиво относиться к звонкам «от банка» или других официальных структур [16]. Однако в современных условиях и молодежь, а также люди среднего возраста не застрахованы от обмана, особенно если атака носит хорошо продуманный характер и подстраивается под индивидуальные особенности. Это делает проблему дистанционного мошенничества с использованием ИИ еще более актуальной и универсальной, разрушая миф о том, что достаточный уровень образования или технических знаний является абсолютной гарантией защиты. Парадокс в том, что высокотехнологичные пользователи могут испытывать излишнюю самоуверенность и пренебрегать элементарными правилами осторожности [17]. Кроме того, ИИ-системы, обучающиеся на огромном массиве данных, способны обнаруживать уязвимые места даже у подготовленных пользователей, анализируя временные паттерны их активности и подбирая момент, когда они наиболее склонны к ошибкам [18].

Еще одна важная деталь, формирующая современную структуру дистанционного мошенничества, – международный характер атак. Системы искусственного интеллекта могут быть развернуты в облачных центрах обработки данных, расположенных в юрисдикциях с низким уровнем правового контроля, а сами преступные группировки часто действуют по всему миру, подчиняя себе целые нелегальные колл-центры [12]. Трансграничный характер операций затрудняет преследование преступников, ведь правоохранительным органам приходится сталкиваться с несовершенством международных механизмов экстрадиции и сотрудничества. Более того, ИИ может маскировать источники трафика, использовать прокси-серверы и сети анонимизации, усложняя процедуру поиска реального организатора атак. В виктимологическом плане это означает, что риск стать жертвой имеется у пользователей из разных стран, при этом многие могут испытывать трудности с обращением в правоохранительные органы другого государства, не зная языка, процедур, имеющихся возможностей компенсации и защиты [15]. Таким образом, цифровая среда выступает своего рода глобальным «мегаполисом», где преступность не знает национальных границ, а системы ИИ еще более стирают оставшиеся барьеры.

Значительный интерес для исследователей представляет вопрос о том, каким образом искусственный интеллект может использоваться не только при исполнении мошеннических атак, но и при их подготовке. Проанализировав большое количество уязвимостей, утекших баз данных пользователей, паттернов поведения в сети, ИИ способен выдавать прогнозы о том, какая мошенническая схема принесет наибольшую выгоду. К примеру, в момент пандемии COVID-19 резко возросло число фейковых предложений медицинских товаров (тестов, лекарств, защитных масок), а затем стали появляться фиктивные схемы с «вакцинами» [10]. Злоумышленники использовали алгоритмы машинного обучения, чтобы мониторить рост поисковых запросов о коронавирусе, отслеживать содержание сообщений в соцсетях и подбирать релевантный контент для фишинга. Таким образом, преступники оперативно реагировали на тревоги и потребности людей, предлагая «решения», которые на деле были лишь мошенническими приманками. В контексте подобных ситуаций классическая киберзащита оказывалась неэффективной, поскольку специфические сигнатуры таких угроз не были заранее известны, и вредоносные сайты или письма оставались вне поля зрения антивирусных компаний в течение критически важного времени.

Отдельно нужно упомянуть *deepfake* – технологию, базирующуюся на генеративно-состязательных сетях (GAN). Первоначально этот термин ассоциировался в основном с созданием порнографических видео, где лица знаменитостей накладывались на реальных актеров, однако со временем сфера применения расширилась [3]. Теперь мошенники используют *deepfake*, чтобы, к примеру, сфабриковать аудио- или видеозаписи от имени представителей крупных компаний, политиков, общественных деятелей, выдавать себя за руководителя для подчиненных и давать «официальные» указания совершить финансовые переводы. Ситуации, когда бухгалтер или менеджер получает видеообращение босса с требованием срочно перевести деньги на другой счет, уже не являются сюжетами из научной фантастики. Атакуемая сторона может

не догадаться перепроверять личность, ведь она видит «живое» видео и слышит голос, в точности повторяющие мимику и интонации реального человека. На этот счет зафиксированы некоторые резонансные случаи в Европе и США, когда компании теряли крупные суммы, не распознав подделку [2]. Виктимологическая составляющая здесь особенно сложна, поскольку жертва действует из лучших побуждений, выполняя распоряжение начальника и не подозревая, что видео или аудио сгенерированы искусственно. В дальнейшем доказать факт обмана может быть крайне трудно, что подрывает доверие даже внутри коллектива и заставляет пересматривать привычные методы коммуникации.

Расширение возможностей мошенников в сфере *deepfake* и генеративного ИИ актуализирует вопрос о том, как сами люди будут реагировать на подобные новые вызовы и какие механизмы могут снижать риск виктимизации. Технологические компании, банки, государственные органы и правозащитные организации уже предпринимают усилия для создания антифейковых решений, позволяющих выявлять следы синтеза в аудио- и видеофайлах [4]. Разрабатываются алгоритмы распознавания аномалий в моргании, микродвижениях мышц лица, артефактах на фоне видеозаписи. Существуют программы, способные автоматически определять несоответствия в характеристиках звука, указывающие на машинную генерацию. Однако подобные инструменты требуют больших вычислительных ресурсов и часто отстают от прогресса генеративных технологий. Чем совершеннее становились нейросети для создания подделок, тем более изощренными приходилось делать системы их выявления. Возникает гонка вооружений, в которой преступники, обладая достаточными ресурсами и мотивацией, стремятся обходить новые фильтры и совершенствовать маскировку [1]. С другой стороны, обучать массового пользователя методам распознавания *deepfake* непросто, особенно если речь идет об аудиозвонках, где у человека нет возможности проводить детальный технологический анализ. В итоге реальной практикой борьбы становится многофакторная проверка личности: не верить голосу или видеозаписи на сто процентов, а перепроверять запрос, используя иные каналы связи, задавать контрольные вопросы, сверяться с внутренними корпоративными процедурами. Виктимологи подчеркивают, что распространение таких правил в корпоративной и повседневной среде может сократить число жертв, но требует изменения поведенческих привычек и отказа от безусловного доверия новым технологиям.

Проблема использования искусственного интеллекта в мошенничестве упирается и в этический аспект. Вопросы, связанные с разработкой и внедрением алгоритмов ИИ, становятся предметом международных дискуссий. С одной стороны, ИИ несет огромный положительный потенциал, применяясь в медицине, логистике, образовании, автоматизации монотонных задач, аналитике больших данных. С другой стороны, те же самые инструменты, попадая в руки злоумышленников, создают беспрецедентные возможности для обмана людей, кражи их денег и личных данных [15]. Очевидно, что запретить или существенно ограничить развитие ИИ в целом невозможно, равно как и удержать инновации внутри строго контролируемых лабораторий. Поэтому правовое сообщество и эксперты в области технологий стремятся найти компромисс между прогрессом и безопасностью. Одним из вариантов считают стимулирование ответственного проектирования ИИ – так называемый “*Responsible* AI” – где разработчики обязуются внедрять механизмы аутентификации, отслеживания происхождения данных и предотвращения злоупотреблений [19]. Однако криминальные элементы не станут придерживаться принципов этики, поэтому основная надежда остается на совершенствование систем обнаружения мошенничества и повышение цифровой грамотности пользователей.

Особое место во всех этих процессах занимает государство и его регулирующие органы. В разных странах предпринимаются попытки криминализировать те или иные аспекты создания и распространения *deepfake*, а также усилить ответственность за кражу персональных данных. Тем не менее правовое регулирование часто не поспевает за технологическими инновациями, а транснациональный характер преступлений затрудняет вынесение приговоров и пресечение деятельности международных группировок. Еще одна проблема – отсутствие единой терминологии и правовых стандартов, что создает лазейки для злоумышленников, способных действовать из юрисдикций с более слабыми законами. Вопрос о разработке глобальных соглашений по противодействию киберпреступности под эгидой ООН или иных международных организаций не раз поднимался, но до окончательного консенсуса еще далеко. Виктимологическая составляющая указывает, что без согласованности правовых норм и координации усилий на международном уровне жертвы, столкнувшиеся с высокотехнологичной атакой, вряд ли получат адекватное возмещение ущерба или помощь в привлечении преступников к ответственности [7]. Это порождает ощущение безнаказанности у мошенников, побуждая их к дальнейшему использованию ИИ и расширению масштабов операций.

ISSN 2949-1150 (online)
2071-8284 (print)

С точки зрения формирования культуры цифровой безопасности, эксперты сходятся во мнении, что ведущую роль должны играть просветительские кампании, информационная поддержка и разработка удобных инструментов самозащиты. Если пользователь не будет понимать принципы работы дистанционного мошенничества или возможности ИИ по созданию правдоподобных подделок, то его шансы вовремя распознать угрозу существенно снижаются [5]. Однако классические материалы вроде памяток и брошюр уже не справляются с поставленной задачей. Необходимо интегрировать модули обучения в сами платформы, которые люди используют ежедневно: социальные сети, онлайн-банкинг, государственные порталы. При выявлении подозрительной активности система должна не просто блокировать ее, но и объяснять пользователю потенциальные риски, обучая его алгоритмам выявления фейков. Механизмы геймификации (*gamification*) также могут помочь, если, например, перед подтверждением перевода деньги сервис предлагает небольшой тест-квест, помогающий отсеять мошеннические сценарии. В числе приоритетных направлений профилактики – внедрение многофакторной аутентификации, требование подтверждать операции не только кодами и паролями, но и биометрическими или другими независимыми методами верификации. Правда, биометрию тоже можно обмануть с помощью *deepfake*, если система несовершенна, поэтому одной лишь технологии часто недостаточно.

Обсуждение

Изменение природы дистанционного мошенничества на фоне развития ИИ отражается и на особенностях правоприменительной практики. Если раньше доказательства мошенничества заключались в переписке, показаниях свидетелей, номерах телефонов, реквизитах счетов, то теперь экспертам может понадобиться анализ машинного кода, лог-файлов, точек входа, взаимодействия нескольких нейросетей [2]. Расследование таких случаев требует уникальных технических компетенций, что создает дополнительную нагрузку на правоохранительную систему. В большинстве стран сотрудники полиции, прокуроры, судьи и адвокаты не обладают в достаточной степени знаниями в области больших данных и методов машинного обучения. Это ведет к затягиванию расследований и, возможно, к ошибочным приговорам. Одновременно возникает опасность перегрузки судов, т. к. число дел, связанных с кибермошенничеством, растет. Виктимологическая перспектива требует учета интересов жертв, которые нуждаются в быстром восстановлении справедливости и компенсации ущерба, однако при сложных технологических схемах расследование может длиться годами. Более того, есть риск, что преступник не будет найден, поскольку действовал из-за рубежа или маскировал свою личность с помощью продвинутых инструментов анонимизации [2]. Столкнувшись с подобной безнаказанностью, жертвы теряют веру в возможность правовой защиты, что усугубляет проблему латентности преступлений: люди перестают сообщать о произошедшем, считая, что это бесполезно.

Однако не следует думать, что ИИ однозначно является оружием лишь в руках преступников. Технологические компании и правоохранительные органы могут использовать искусственный интеллект для предотвращения атак, распознавания автоматизированных паттернов мошенничества и выявления аномальной активности на счетах. Существуют продвинутые антифрод-платформы, которые на основе машинного обучения анализируют миллионы транзакций в реальном времени, стараясь моментально определить вероятность мошенничества[5]. Существуют особенности проведения оперативно розыскных мероприятий (далее – ОРМ). В частности, «большое значение для успешного раскрытия и расследования дистанционных мошенничеств имеет и качество изучения и анализа первичных сведений, а не исключительно скорость их получения. Таким образом, извлечение первичных сведений о дистанционном мошенничестве зависит от реализации ОРМ и неотложных следственных действий по нахождению компьютерной техники, банковских карт, мобильных и иных телефонов. Такие оперативно-розыскные методы нахождения, как опрос, наблюдение, оперативное внедрение могут успешно применяться с этой целью» [20]. Автор указывает на механизм следообразования дистанционного мошенничества: «Учитывая его специфику, преобладают информационные или цифровые следы. При этом большое значение имеет то, что они образуются не только в определенном месте (где находится мошенник, например), а на всем маршруте прохождения информационного взаимодействия (сигнала), за счет чего правоохранительные органы могут их обнаружить и зафиксировать. Вместе с тем работать с этими следами довольно сложно и не вызывает сомнения обязательность специальной подготовки субъектов. Оперативное получение данных

[5] URL: https://www.cbr.ru/collection/collection/file/32190/review_of_transactions_2020.pdf (дата обращения: 20.03.2025).

о движении денежных средств в рамках расследуемого преступления, наименьший временной интервал между поступлением сведений о совершенном мошенничестве и направлением в работу технических средств, применяемых мошенниками, выполнение ОРМ по месту присутствия подозреваемого являются ведущими положениями успешного расследования дистанционных мошенничеств» [11]. Системы могут учитывать геолокацию, временной промежуток, историю предыдущих переводов, скорость ввода данных, чтобы составить профиль риска конкретной операции. Если система определяет высокий риск, она блокирует транзакцию или запрашивает у клиента дополнительную проверку. Подобные решения снижают уровень посредственных мошенничеств, где преступники не используют сложных схем персонализации. Тем не менее противодействие более продвинутым атакам, основанным на *deepfake* и таргетированном подходе, требует еще большего уровня технологического совершенства. Тогда возникает необходимость обмена информацией между банками, интернет-провайдерами, правоохранительными органами, что нередко упирается в вопросы конфиденциальности и конкуренции.

Заключение

Исходя из вышеизложенного, можно прийти к выводу, что в цифровую эпоху дистанционное мошенничество переживает глубокую трансформацию, поскольку злоумышленники начали активно использовать искусственный интеллект и смежные технологии для создания более изощренных, масштабных и труднораспознаваемых схем. Традиционные механизмы защиты, включая антивирусные программы и простые памятки о фишинге, уже не могут в полной мере противостоять высокотехнологичным атакам, где машинное обучение обеспечивает криминалистическую точность при выборе жертв и генерации контента. Виктимологические особенности данной угрозы выражаются в том, что практически каждый пользователь, независимо от уровня его технической компетенции, оказывается в зоне риска. Разрешить проблему невозможно, используя лишь репрессивные меры. Она не имеет простых решений, поскольку искусственный интеллект – это универсальный инструмент, способный служить как прогрессу, так и преступлению. Труднее всего будет выработать столь необходимые культурные и поведенческие изменения, формирующие у пользователей устойчивые привычки самопроверки, критического мышления и ответственности за собственные действия в сети. Роль виктимологии здесь неоценима, поскольку она позволяет фокусироваться на фигуре жертвы, анализировать причины ее уязвимости и разрабатывать меры снижения риска. В конечном итоге чем лучше общество понимает психологические и технологические аспекты высокотехнологичных мошеннических схем, тем успешнее может выстраивать многоуровневую защиту, делая цифровое пространство более безопасным и надежным для всех.

Список источников

1. *Jagielski M., Carlini N., Berthelot D., Kurakin A., Papernot N.* High Accuracy and High Fidelity Extraction of Neural Networks / Proceedings of the 29th USENIX Security Symposium (USENIX Security '20). 2020. P. 1345–1362. https://doi.org/10.48550/arXiv.1909.01838

2. *Chawki M.* Navigating legal challenges of deepfakes in the American context: a call to action // Cogent Engineering. 2024. Vol. 11. No. 1. P. 2320971. https://doi.org/10.1080/23311916.2024.2320971

3. *Tolosana R., Fierrez J., Vera-Rodriguez R., Morales A.* DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. 2020. 23 p. https://doi.org/10.48550/arXiv.2001.00179

4. *Verdoliva L.* Media Forensics and DeepFakes: An Overview // IEEE Journal of Selected Topics in Signal Processing. 2020. Vol. 14. Is. 5. P. 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

5. *Hadnagy C.* Social Engineering: The Science of Human Hacking. 2nd ed. USA, Indianapolis : John Wiley & Sons, Inc., 2020. 322 p.

6. *Stajano F., Wilson P.* Understanding Scam Victims: Seven Principles for Systems Security // Communications of the ACM. 2019. Vol. 62, Is. 3. P. 70–75.

7. *Wall D. S.* How Big Data Feeds Big Crime // Current History. 2018. Vol. 795. No. 117. P. 29–34. https://doi.org/10.1525/curh.2018.117.795.29

8. *Макаров В. В., Блатова Т. А., Ворошилова Е. Ю.* Ускоренное развитие информационных технологий в период пандемии // Экономика и качество систем связи. 2021. № 2 (20). С. 12–19.

9. *Палий Е. С.* Виктимологическая характеристика лиц пенсионного возраста: постановка проблемы // Судебная экспертиза и исследования. 2025. № 1. С. 115–123.

10. *Еськова Л. К., Рябчиков В. В.* Новые преступные способы мошенничества в период пандемии коронавирусной инфекции // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 68–70. https://doi.org/10.23672/c3413-0996-0433-v

11. *Иванцов С. В.* Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: вопросы предупреждения // Криминологический журнал. 2019. № 2. С. 35–39.

12. *McGuire M., Dowling S.* Cyber Crime: A Review of the Evidence : Research Report 75 : Summary of key findings and implications. London : Home Office Research Report, 2013. 29 p.

13. *Яковлева Л. В.* Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. № 4 (54). С. 77–80.

ISSN 2949-1150 (online)
2071-8284 (print)

14. *Brenig C., Accorsi R., Müller G.* Economic Analysis of Cryptocurrency Backed Money Laundering / European Journal of Information Systems. ECIS 2015 Completed Research Papers. Paper 20. 2015. https://doi.org/10.18151/7217279

15. *Gercke M.* Understanding Cybercrime: Phenomena, Challenges and Legal Response. Switzerland, Geneva : ITU: International Telecommunication Union, 2012. 356 p.

16. *Cross C., Lee M.* Exploring Fear of Crime for Those Targeted by Romance Fraud // Victims & Offenders. 2022. Vol. 17. No. 5. P. 735–755. https://doi.org/10.1080/15564886.2021.2018080

17. *Baym N. K.* Personal Connections in the Digital Age. 2nd ed. UK, Cambridge : Polity, 2015. 240 p.

18. *Leukfeldt E. R., Roks R.* Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes // Deviant Behavior. 2021. Vol. 42. No. 11. P. 1458–1469. https://doi.org/10.1080/01639625.2020.1755587

19. *Floridi L.* What Is Data Ethics? // Philosophical Transactions A. 2016. Vol. 374 (2083). https://doi.org/1098/rsta.2016.0112

20. *Лустин В. И.* Дистанционные мошенничества // Закон и власть. 2023. № 5. С. 67–74.