ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ПЕРСОНАЛИЗАЦИИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Рашитханов Р.С.[1]

Ключевые слова: *уголовная политика, персонализация преступности, цифровизация преступности, преступность и прогресс.*

Аннотация

Цель работы: *состоит в анализе криминологического и уголовно-правового значения использования технологий искусственного интеллекта при персонализации дистанционного мошенничества, а также в разработке предложений по совершенствованию мер противодействия таким деяниям.*

Метод исследования: *в работе использованы формально-юридический, системно-структурный, сравнительно-правовой и криминологический методы. Нормы уголовного законодательства рассматриваются во взаимосвязи с механизмом преступного поведения и современными способами цифрового воздействия на потерпевшего. Особое внимание уделено анализу доктринальных подходов к мошенничеству, социальной инженерии, искусственному интеллекту как средству совершения преступления и незаконному использованию сведений о лице. Эмпирическую основу составили описанные в открытых источниках случаи применения синтетического голоса, поддельных изображений, генеративных систем и автоматизированной обработки информации в мошеннических схемах.*

Результаты исследования: *обосновано, что применение технологий искусственного интеллекта не меняет юридическую природу мошенничества, однако существенно изменяет условия его подготовки, воспроизводства и сокрытия. Показано, что криминологическое значение имеет не само наличие сведений о потерпевшем, а их последовательное превращение в средство адресного воздействия. Предложено использовать категорию персонализирующих сведений, охватывающую любую информацию, пригодную для построения правдоподобной мошеннической легенды. Сделан вывод о том, что искусственный интеллект снижает издержки персонализации, позволяет соединять массовость и адресность обмана, ускоряет подбор легенды и поддерживает ложную информационную обстановку.*

Практическая ценность: *сформулированы предложения по уточнению квалифицирующих признаков мошенничества, усилению ответственности за незаконный оборот персональных данных, используемых для подготовки корыстных преступлений, и разработке критериев фиксации применения искусственного интеллекта в способе совершения преступления.*

DOI: 10.24412/2226-0692-2026-2-164-172

Введение

Дистанционное мошенничество относится к числу тех форм корыстной преступности, в которых решающее значение имеет не столько доступ преступника к имуществу, сколько способность направить поведение потерпевшего в нужную сторону. Обман здесь выступает способом организации действий потерпевшего, поскольку именно он сообщает реквизиты, подтверждает операцию, переводит денежные средства либо совершает иное действие, создающее имущественный результат для преступника. В этом состоит одна из причин устойчивости мошенничества как преступной практики, поскольку меняются каналы связи, легенды и технические средства, но сохраняется основной механизм, а именно — использование заблуждения и доверия в корыстных целях [1, 2].

При этом уголовно-правовая природа мошенничества не исчерпывается этим. Для квалификации принципиально важно установить, что обман либо злоупотребление доверием выступали способом хищения, то есть были направлены на формирование у потерпевшего такого представления о действительности, которое обусловило последующее распоряжение имуществом. Именно поэтому в доктрине последовательно подчеркивается необходимость разграничения мошенничества и иных форм недобросовестного поведения, прежде всего в сфере гражданско-правовых обязательств [3, 4].

[1] **Рашитханов Руслан Салихович**, заместитель директора Института правового анализа проблем информационной и медиабезопасности Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), руководитель Лаборатории правовых исследований в сфере национальной безопасности РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Россия. E-mail: rsrashithanov@msal.ru

Вместе с тем современная дистанционная форма мошенничества эволюционировала. Ее результативность все чаще определяется тем, насколько точно преступник подбирает адресата, роль, канал связи, эмоциональный тон и последовательность аргументов. Иначе говоря, обман становится персонализированным. Такая персонализация существовала и ранее. Например, преступник мог учитывать возраст, социальное положение, родственные связи, служебное положение, бытовые обстоятельства потерпевшего. Однако до цифровой эпохи она имела ограниченное значение, поскольку требовала времени, наблюдения, личного контакта либо доступа к узкому кругу сведений.

Именно здесь технологии искусственного интеллекта меняют криминологическую ситуацию. Они позволяют резко снизить затраты на поиск, обработку и сопоставление сведений о потенциальном потерпевшем, ускорить подготовку правдоподобной легенды, варьировать речевые модели, имитировать служебный или доверительный стиль общения, а при необходимости даже сопровождать несколько диалогов одновременно. Персонализация в таких условиях перестает быть индивидуальным мастерством мошенника и превращается в воспроизводимую процедуру, пригодную для массового применения. Поэтому исследовательский интерес представляет не сам факт использования ИИ, а его роль в изменении механизма дистанционного мошенничества.

Криминологическое значение персонализации посредством ИИ состоит в том, что она изменяет условия воспроизводства мошенничества. Преступник получает возможность заранее отбирать восприимчивые группы потерпевших, варьировать легенды под их социальные роли и поддерживать множество контактов одновременно. Поэтому исследовательский интерес представляет не техническая новизна ИИ сама по себе, а его роль в перестройке выбора потерпевшего, подготовки легенды, коммуникационного воздействия и сокрытия связи между эпизодами.

Персонализация мошенничества как криминологический феномен

Персонализацию мошенничества не следует понимать только как технический прием, связанный с цифровыми данными. В более широком смысле она означает приспособление обмана к конкретному потерпевшему, например, к его социальному положению, жизненной ситуации, ожиданиям, страхам, профессиональной роли, семейным связям, привычным формам общения. Речь идет не о простом включении в сообщение имени, адреса или иных сведений, а о построении такой ситуации, в которой ложное сообщение оказывается для потерпевшего внутренне правдоподобным. Персонализация относится не к внешней форме мошенничества, а к самому механизму воздействия, поскольку она повышает вероятность того, что потерпевший не только воспримет сообщение, но и совершит действие, которого пытается добиться преступник.

Такое воздействие не является новым. Как было отмечено выше, мошенники и до появления цифровых технологий стремились знать того, на кого направлено посягательство. В одних случаях эти сведения получались путем наблюдения, через личное окружение, служебные или бытовые связи; в других — выводились из поведения самого потерпевшего в ходе общения. Подбирались роль, тон, момент обращения, круг обстоятельств, на которые следовало сослаться. Иначе говоря, персонализация существовала в мошенничестве всегда, поскольку обман, лишенный учета адресата, менее устойчив.

Однако ранее персонализация редко выступала самостоятельным предметом криминологического рассмотрения. Она растворялась в более общих характеристиках механизма преступного поведения. Например, в обмане, злоупотреблении доверием, подготовке преступления, выборе потерпевшего, виктимологической уязвимости. В этом есть своя логика. Пока персонализированное воздействие зависело от индивидуального опыта мошенника и не могло быть легко воспроизведено в большом числе эпизодов, оно не образовывало отдельного криминогенного фактора. Оно усиливало конкретный обман, но не меняло устройство мошеннической практики в целом. Поэтому значимым является не всякое приспособление обмана к потерпевшему, а только такое, которое приобретает устойчивость, воспроизводимость и способность превращаться в серию посягательств.

Именно это произошло сегодня в цифровой среде. Данные о человеке стали возникать и накапливаться вне его непосредственного общения с преступником. Например, в социальных сетях, объявлениях, сервисах доставки и торговли, банковских и телекоммуникационных системах, корпоративных базах, мессенджерах, открытых реестрах. Часть этих сведений публикуется самим лицом добровольно, часть создается организациями в ходе обычного обслуживания, часть попадает в незаконный оборот в результате утечек данных, неправомерного доступа или целенаправленной незаконной передачи. В результате преступник получает возможность не столько «узнать» потерпевшего в прежнем смысле, сколько собрать о нем достаточный набор признаков для правдоподобного воздействия.

На этом этапе персонализация приобретает новое качество. Она уже не сводится к предварительному знанию отдельных фактов, а строится как последовательная обработка сведений. Для одного лица убедительной оказывается имитация банковской процедуры, для другого — обращение от имени руководителя, для третьего — сообщение о родственнике, для четвертого — ссылка на доставку, медицинскую запись, государственную услугу. Общим

остается приспособление к тому, что потерпевший готов признать вероятным.

В этом смысле персонализация тесно связана с виктимологическим измерением мошенничества. Потерпевший не является причиной преступления, однако его положение, дефицит информации, доверие к определенным социальным ролям, страх негативных последствий, желание быстро устранить угрозу или сохранить значимые отношения используются преступником как условия воздействия.

С указанной позиции персонализация должна быть соотнесена с социальной инженерией, однако не может быть полностью сведена к ней. Социальная инженерия характеризует совокупность приемов психологического и организационно-технического воздействия, направленных на побуждение лица к совершению выгодного преступнику действия [5, 6]. Персонализация же указывает на способ подбора и настройки этих приемов под конкретного потерпевшего или группу потерпевших. Поэтому социальная инженерия отвечает на вопрос о том, какими приемами воздействует преступник, а персонализация на вопрос о том, почему именно эти приемы оказываются пригодными для данного адресата.

Анализ, сведенный к техническому каналу связи, неизбежно обедняет картину. Для понимания дистанционного мошенничества важно установить не только то, каким способом было направлено сообщение, но и почему именно это сообщение, обращенное именно к этому лицу и в данной ситуации, оказалось действенным. Такая постановка вопроса соответствует общей криминологической традиции, в которой преступление рассматривается как поведение, включенное в систему личности, ситуации и социальной среды [7].

Применительно к дистанционному мошенничеству это означает, что персонализация должна рассматриваться как самостоятельный элемент механизма преступления. Она соединяет подготовку и реализацию посягательства. При этом чем точнее подобрана легенда, тем меньше потерпевший воспринимает ситуацию как требующую проверки. Он действует не потому, что полностью лишен критического мышления, а потому, что преступник искусственно сужает пространство выбора. Так, например, он часто создает срочность, имитирует компетентный источник, запрещает советоваться, переводит общение в удобный канал, постепенно ведет к нужному решению.

Искусственный интеллект усиливает именно эту связку. Его значение состоит в том, что он делает персонализацию более дешевой, быстрой и серийной. Тем самым персонализация перестает быть преимущественно индивидуальным приемом и приобретает значение в виде элемента воспроизводимой серии преступлений.

Искусственный интеллект в механизме персонализации дистанционного мошенничества

До появления технологий искусственного интеллекта дистанционное мошенничество уже обладало признаками массовости, но эта массовость нередко достигалась ценой упрощения воздействия. Один и тот же текст, один и тот же сценарий телефонного разговора, одинаковая легенда, рассчитанная на неопределенный круг лиц, позволяли охватить значительное число потенциальных потерпевших, но снижали убедительность обращения. Персонализация, напротив, повышала действенность обмана, однако требовала временных и ресурсных затрат. Поэтому между массовостью и адресностью долгое время сохранялось известное противоречие.

В российском стратегическом регулировании искусственный интеллект определяется как комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. К технологиям ИИ отнесены компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальная поддержка принятия решений и перспективные методы ИИ. Для рассматриваемой темы особенно значимы большие генеративные модели, способные создавать мультимодальные данные, включая тексты, изображения и видеоматериалы.

Искусственный интеллект ослабляет это противоречие. Его значение состоит не в том, что он заменяет преступника, а в том, что он уменьшает трудоемкость тех операций, которые раньше ограничивали персонализированное мошенничество. Сведения о человеке могут быть быстрее собраны, сопоставлены, очищены от лишнего, разложены по признакам, имеющим значение для преступного посягательства: возраст, профессия, семейное положение, потребительские привычки, финансовое поведение, стиль публичного общения, круг организаций и сервисов, с которыми лицо, вероятно, взаимодействует. Даже если такие сведения неполны, их оказывается достаточно для построения вероятностного образа потерпевшего и выбора той легенды, которая будет выглядеть для него наиболее естественной и подходящей.

Материалы исследователей киберугроз показывают, что в теневой среде уже формируется спрос на инструменты автоматизированной подготовки мошеннической коммуникации. В 2023 г. исследователи Netenrich сообщили о продвижении на даркнет-форумах и в Telegram-каналах сервиса FraudGPT, который позиционировался как инструмент подготовки целевых мошеннических писем, мошеннических сообщений и мошеннических страниц[2]. В том

[2] Krishnan R. FraudGPT: The Villain Avatar of ChatGPT // Netenrich. 2023. 25 July. URL: https://netenrich.com/blog/fraudgpt-the-villain-avatar-of-chatgpt (дата обращения: 01.06.2026).

DOI: 10.24412/2226-0692-2026-2-164-172

же ряду упоминается WormGPT — генеративный ИИ-сервис, который, по данным исследователей и журналистских материалов, продвигался в теневой среде как инструмент для подготовки фишинговых сообщений и сценариев деловой компрометации электронной переписки[3].

Для рассматриваемой темы существенно то, что подобные инструменты обслуживают именно коммуникативный участок мошеннической схемы. Например, подготовку адресного текста, делового тона, срочности, имитации распоряжения и внешней правдоподобности источника. Иначе говоря, преступная коммуникация начинает предлагаться как услуга, доступная лицам, не обладающим выраженными речевыми, психологическими или техническими навыками. При этом сведения о таких сервисах требуют осторожной оценки, поскольку часть объявлений в теневой среде может быть рекламным преувеличением или способом обмана самих злоумышленников. Однако сам факт появления и обсуждения подобных инструментов показывает формирование спроса на автоматизированное производство адресных мошеннических легенд[4].

В механизме персонализированного мошенничества ИИ действует одновременно на информационном и коммуникативном уровнях. На информационном уровне он ускоряет сопоставление разрозненных сведений, позволяет выделять группы потенциальных потерпевших и формировать вероятностное представление об их уязвимости. На коммуникативном уровне он помогает переводить это представление в речевую форму. В частности, он помогает подбирать роль источника, тон обращения, последовательность аргументов, варианты ответа на сомнение, отказ или попытку проверки.

Персонализация в такой форме не сводится к тому, что в сообщении названы имя, банк, место работы или иные узнаваемые сведения. Эти элементы важны, но они выполняют вспомогательную функцию и создают впечатление осведомленности. Главным является построение ситуации, в которой потерпевший воспринимает требуемое от него действие как логичное, срочное и безопасное.

Если речь идет о банковской легенде, то акцент делается на угрозе потери денег и необходимости их немедленной защиты. Если используется образ руководителя или коллеги, воздействие опирается на служебную дисциплину, страх нарушить поручение, нежелание поставить под сомнение распоряжение вышестоящего лица. Если используется семейная ситуация, то главным становится тревога за близкого и готовность действовать без проверки. ИИ усиливает этот механизм тем, что позволяет быстрее подбирать нужную форму обращения и менять ее по ходу диалога.

Особенно существенно то, что ИИ меняет характер самой коммуникации. В традиционной телефонной или текстовой схеме преступник действовал по заранее подготовленному сценарию и был ограничен собственными навыками речи, памятью, реакцией, умением отвечать на возражения. При использовании ИИ сценарий становится более гибким, поскольку заранее подготавливаются разные ветви разговора, формулируются ответы на типичные сомнения, меняется эмоциональная насыщенность сообщения, подбираются разные стили речи. Потерпевший сталкивается не с известным шаблоном, а с сообщением, которое внешне учитывает его реакцию. Тем самым возрастает опасность длительного удержания лица в ситуации заблуждения.

В этом отношении полезны положения исследований человеческо-машинной коммуникации. А.Л. Гузман и С. Льюис обращают внимание на то, что искусственный интеллект в коммуникации не может рассматриваться только как нейтральный канал передачи информации, поскольку он участвует в формировании сообщения и влияет на то, как человек воспринимает источник общения [8]. Сходная мысль проводится в исследованиях, где подчеркивается, что интеллектуальный агент может модифицировать, дополнять или генерировать сообщения для достижения коммуникативной цели [9].

Для уголовно-правовой оценки данный вывод требует существенного уточнения, ведь ИИ не должен рассматриваться как самостоятельный носитель вины или субъект преступления. В российской доктрине обоснованно подчеркивается, что применительно к преступному поведению человека ИИ выступает прежде всего как техническое средство, используемое для достижения результата, заданного лицом, контролирующим соответствующую систему [10]. Поэтому в контексте дистанционного мошенничества вопрос должен ставиться не об условной вине ИИ, а о том, какую функцию он выполнил в ходе преступления.

При этом не следует преувеличивать самостоятельность ИИ. В мошеннической схеме он обычно не действует автономно в юридическом смысле. Решение о выборе цели, запуске воздействия, изменении легенды и получении имущественного результата остается за человеком. Однако преступник получает возможность распределить между собой и техническим средством разные функции. Человек задает цель, выбирает общий сценарий, контролирует результат и принимает решения в нестандартных ситуациях. ИИ выполняет подготовительную и коммуникативную работу, то есть ускоряет обработку сведений, предлагает речевые конструкции, подстраивает стиль, помогает удерживать несколько контактов одновременно. Опасность возникает именно из этого соединения.

---

[3] Burgess M. Criminals Have Created Their Own ChatGPT Clones // Wired. 2023. 7 August. URL: https://www.wired.com/story/chatgpt-scams-fraudgpt-wormgpt-crime (дата обращения: 01.06.2026).

[4] Kaspersky Digital Footprint Intelligence. Shadowy innovation: how cybercriminals experiment with AI on the dark web // Kaspersky. 2024. URL: https://dfi.kaspersky.com/blog/ai-in-darknet (дата обращения: 01.06.2026).

Реальные эпизоды показывают, что ИИ-персонализация уже вышла за пределы обычного фишингового письма. Одним из наиболее известных примеров является дело Arup. В рамках этого дела, в 2024 г. сотрудник гонконгского подразделения компании был подключен в видеоконференцию, участники которой выглядели и звучали как руководители организации, после этого были осуществлены переводы на сумму около 25 млн долларов США[5]. В данном случае преступное воздействие строилось на служебной роли потерпевшего, поскольку он воспринимал происходящее как внутреннее корпоративное распоряжение, исходящее от узнаваемых лиц.

Близкую логику демонстрирует попытка атаки на компанию WPP. По данным The Guardian, злоумышленники использовали находящееся в открытом доступе изображение руководителя компании для создания WhatsApp-аккаунта, организовали встречу в Microsoft Teams в рамках которой была осуществлена попытка мошенничества[6]. Атака была пресечена, однако сама схема показательна, поскольку персонализация достигалась не одним техническим приемом, а соединением нескольких признаков достоверности — фотографии, корпоративного канала, знакомого имени, голоса, объединенных дипфейком в рамках конференции.

Похожие выводы содержатся в материалах Europol[7]. В оценке угроз организованной преступности за 2025 г. отмечается, что голосовое клонирование и видео-дипфейки в режиме реального времени расширяют возможности мошенников, поскольку они позволяют имитировать руководителей, должностных лиц, родственников и иных людей, которым потерпевший склонен доверять. Такие технологии используются не изолированно, а вместе с фишингом, поддельными аккаунтами и автоматизированной рассылкой. В результате преступные группы получают возможность быстрее готовить убедительные обращения, обращаться к большему числу лиц и труднее выявляться правоохранительными органами. Для рассматриваемой темы это важно потому, что ИИ-персонализация становится частью более широкой трансформации организованной цифровой преступности, ведь обман сохраняет прежнюю корыстную цель, но становится более гибким, масштабируемым и внешне правдоподобным.

Жизненный цикл персонализирующих сведений в механизме дистанционного мошенничества

Данные о человеке в рамках рассматриваемой проблематики имеют значение не сами по себе. Они становятся значимыми лишь тогда, когда включаются в механизм преступного поведения. Поэтому в рассматриваемом контексте точнее говорить не просто о персональных данных, а о персонализирующих сведениях — то есть о любой информации, которая может быть использована преступником в целях персонализации.

Такие сведения могут быть различными по происхождению и правовому режиму. Например, одни из них лицо сообщает о себе добровольно: в социальных сетях, объявлениях, профессиональных сообществах, публичных переписках. Другие возникают в ходе обычного участия человека в цифровом обороте: при использовании банковских, телекоммуникационных, торговых, транспортных, медицинских, образовательных и государственных сервисов. Третьи попадают к преступникам в результате утечек, незаконной передачи, неправомерного доступа либо незаконного оборота баз. Для мошенника принципиально не то, каким языком эти сведения описываются в законодательстве о данных, а то, какую роль они могут сыграть в конструировании доверия.

В этом смысле персонализирующие сведения являются своеобразным промежуточным звеном между социальной жизнью потерпевшего и преступным воздействием. Сведения о банке, месте работы, должности, родственниках, недавней покупке, поездке, заболевании, кредите или служебной переписке еще не образуют обман. Но они позволяют преступнику приблизить ложную ситуацию к обычному жизненному опыту человека. Потерпевший верит не потому, что сообщение безупречно, а потому, что оно попадает в знакомый ему порядок вещей, поскольку совпадение ложной легенды с ожидаемой социальной реальностью и образует внутреннюю силу персонализированного обмана.

Искусственный интеллект усиливает не один изолированный этап, а сам переход от сведений о лице к воздействию на его поведение. Эмпирическую основу для такого вывода дают исследования целевого фишинга. T. Xu, K. Singh и P. Rajivan показали, что высокая доступность информации о цели позволяет формировать контекстно значимые легенды и имитации, а адресаты в таких условиях оказываются существенно более уязвимыми к целевому мошенническому воздействию [11].

Следовательно, персонализация начинается с отбора тех признаков, которые позволяют предположить, какая ложь будет для данного лица убедительной. Здесь важен не полный психологический портрет потерпевшего, а достаточная для преступника

[5] Milmo D. UK engineering firm Arup falls victim to £20m deepfake scam // The Guardian. 2024. 17 May. URL: https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video (дата обращения: 01.06.2026).

[6] Robins-Early N. CEO of world's biggest ad firm targeted by deepfake scam // The Guardian. 2024. 10 May. URL: https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam (дата обращения: 01.06.2026).

[7] Europol. The Changing DNA of Serious and Organised Crime: EU Serious and Organised Crime Threat Assessment 2025. Hague: Europol, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf (дата обращения: 01.06.2026); Europol warns of AI-driven crime threats // Reuters. 2025. 18 March. URL: https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/ (дата обращения: 01.06.2026).

DOI: 10.24412/2226-0692-2026-2-164-172

гипотеза. Исследования целевого фишинга показывают, что в отличие от массового фишинга такие атаки строятся на предварительном сборе сведений о цели и конструировании сообщения под профиль адресата, именно поэтому они труднее распознаются обычными антифишинговыми средствами [12].

Подобная логика проявляется и в посягательствах, в рамках которых используются подделки голоса с помощью ИИ. В 2025 г. Reuters сообщал о расследовании в Италии, где мошенники, используя имитацию голоса министра обороны Гвидо Крозетто, обращались к известным предпринимателям с просьбой о срочной финансовой помощи якобы для освобождения похищенных журналистов. Денежные средства перевел бывший владелец футбольного клуба «Интер» Массимо Моратти. Тем не менее благодаря работе правоохранительных органов впоследствии почти 1 млн евро был обнаружен и заморожен[8]. В этом случае персонализация строилась на предварительном выборе круга адресатов, высокой социальной значимости имитируемого лица и легенде, рассчитанной на срочность, доверие к официальному источнику и готовность к крупному платежу.

Потерпевший сталкивается не просто с незнакомцем, а с фигурой, от которой он привык ожидать указания, предупреждения, помощи или санкции. В этом проявляется связь персонализации с классическими механизмами социального влияния.

Отсюда следует, что жизненный цикл персонализирующих данных должен пониматься не как техническая последовательность операций с информацией, а как путь превращения сведений о человеке в преступное воздействие.

Жизненный цикл персонализирующих сведений в механизме дистанционного мошенничества может быть представлен следующим образом:

- возникновение сведений о лице;
- отрыв этих сведений от первоначального социального, служебного или потребительского контекста;
- их сбор, покупка, извлечение либо незаконное получение;
- сопоставление разрозненных данных и формирование вероятностного профиля потерпевшего;
- выделение уязвимости;
- превращение профиля в легенду;
- выбор канала и формы обращения;
- поддерживаемая ИИ коммуникация;
- имущественно значимое действие потерпевшего;
- получение и сокрытие результата;
- повторное использование профиля либо передача сведений в дальнейший преступный оборот.

Такая последовательность показывает, что значимым является не само наличие сведений о потерпевшем, а их перевод в управляемое поведенческое воздействие. ИИ ускоряет именно этот перевод, поскольку разрозненные сведения быстрее становятся профилем, профиль превращается в легенду, легенда предъявляется потерпевшему в убедительной форме, а коммуникация доводится до имущественно значимого действия.

Такое понимание позволяет иначе поставить вопрос о противодействии. Борьба с дистанционным мошенничеством не может начинаться только в момент звонка или перевода денежных средств. К этому моменту значительная часть преступной работы уже выполнена. Необходимо воздействовать на более ранние звенья. Например, на избыточный сбор и слабую защиту данных, незаконный оборот баз, автоматизированное извлечение сведений, массовое профилирование, подготовку однотипных, но внешне адресных легенд, использование синтетического голоса и изображения, повторное вовлечение потерпевших. Иначе правоприменение будет видеть лишь последний акт, тогда как криминогенный механизм останется сохраненным.

Перед рассмотрением предложений по совершенствованию мер противодействия использованию ИИ в качестве инструмента персонализации мошенничества, отдельно следует разграничить рассматриваемые ситуации со ст. 159.6 УК РФ. ИИ-персонализация дистанционного мошенничества в большинстве случаев не образует мошенничество в сфере компьютерной информации, поскольку преступный результат достигается не путем вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, а посредством введения потерпевшего в заблуждение и побуждения его к самостоятельному имущественно значимому действию. Поэтому основной нормой для оценки таких действий остается ст. 159 УК РФ. Статья 159.6 УК РФ может применяться лишь тогда, когда в содеянном имеются признаки специального способа, предусмотренного этой нормой, то есть воздействие на компьютерную информацию или соответствующие средства ее обработки.

Предложения по совершенствованию противодействия персонализации дистанционного мошенничества посредством ИИ

Совершенствование уголовно-правового противодействия дистанционному мошенничеству, совершаемому с использованием технологий искусственного интеллекта, должно исходить из функциональной роли соответствующей технологии в механизме обмана. Для уголовного закона недостаточно указать на сам факт применения искусственного интеллекта. Такая формула была бы чрезмерно широкой и могла бы охватывать случаи, когда программа использовалась для перевода текста, исправления

[8] Italian police freeze cash from AI-voice scam that targeted business leaders // Reuters. 2025. 12 February. URL: https://www.reuters.com/technology/artificial-intelligence/italian-police-freeze-cash-ai-voice-scam-that-targeted-business-leaders-2025-02-12/ (дата обращения: 01.06.2026).

сообщения или иной нейтральной операции, не связанной с введением потерпевшего в заблуждение.

Квалифицирующее значение должно иметь применение технологии, которое участвует в создании ложной информационной обстановки и влияет на решение потерпевшего о распоряжении имуществом. В мошеннической схеме может имитироваться конкретное лицо, организация или орган публичной власти. Вместе с тем не меньшую опасность представляет имитация события, документа, распоряжения, банковской операции, проверки, угрозы утраты денежных средств, происшествия с родственником или иного обстоятельства, которое потерпевший воспринимает как действительное и значимое для принятия решения.

Поэтому законодательная формула должна охватывать не отдельный технический прием, а результат его применения. Речь должна идти о создании, изменении, воспроизведении, распространении заведомо недостоверных сведений либо об автоматизированном подборе содержания обращения к потерпевшему, если такие действия находились в причинной связи с его заблуждением.

В связи с этим представляется возможным дополнить ч. 3 ст. 159 УК РФ новым квалифицирующим признаком. В части третьей статьи 159 слова «в крупном размере» целесообразно заменить словами «в крупном размере, а равно с использованием технологий искусственного интеллекта или иных программных средств автоматизированной обработки информации для создания, изменения, воспроизведения или распространения заведомо недостоверных сведений либо для подбора содержания обращения к потерпевшему, если указанные действия были направлены на формирование у потерпевшего ложного представления о лице, организации, органе публичной власти, событии, документе, распоряжении, операции, угрозе наступления неблагоприятных последствий либо ином обстоятельстве, имеющем значение для распоряжения имуществом или приобретения права на имущество, и находились в причинной связи с введением потерпевшего в заблуждение».

Такая редакция позволяет охватить разные способы обмана, обусловленного ИИ. Она применима к синтетическому голосу, поддельному изображению, измененному видео, сгенерированному документу, ложному уведомлению, автоматизированно подобранному сообщению и иному цифровому материалу. При этом она не превращает любое применение искусственного интеллекта в квалифицирующий признак. Уголовно правовое значение получает только такое использование технологии, которое воздействует на представления потерпевшего об обстоятельствах и способствует совершению имущественно значимого действия.

Для повышения определенности возможно дополнить примечания к ст. 159 УК РФ новым пунктом. Примечания к статье 159 целесообразно дополнить пунктом 3 в следующей редакции:

«*3. Для целей настоящей статьи под использованием технологий искусственного интеллекта или иных программных средств автоматизированной обработки информации понимается применение программ для электронных вычислительных машин, обеспечивающих автоматизированный анализ, отбор, сопоставление, создание, изменение, воспроизведение или распространение сведений, текстов, изображений, звуковых, визуальных или иных цифровых материалов, если такое применение использовалось для введения потерпевшего в заблуждение*».

Отдельного внимания требует незаконный оборот компьютерной информации, содержащей персональные данные. В механизме персонализированного дистанционного мошенничества такие сведения имеют подготовительное значение. Они используются для выбора потерпевшего, определения вероятной линии воздействия, подбора обращения, создания ложной информационной обстановки и последующего сокрытия связи между эпизодами.

В связи с этим часть третью статьи 272.1 УК РФ целесообразно после пункта «г» дополнить пунктом «д» с соответствующим изменением пунктуации в пункте «г»:

«*д) в целях подготовки, облегчения совершения или сокрытия хищения чужого имущества, вымогательства либо иного преступления корыстной направленности, в том числе путем использования компьютерной информации, содержащей персональные данные, для создания, изменения, подбора или распространения сообщений либо иных информационных материалов, предназначенных для введения потерпевшего в заблуждение*».

Такое дополнение позволит точнее связать незаконное получение и оборот персональных данных с их последующим преступным использованием. Данные в такой схеме выступают не пассивным объектом хранения или передачи. Они становятся средством подготовки обмана и построения информационной ситуации, в которой потерпевший совершает действие в интересах виновного.

Кроме того, представляется обоснованным дополнить ч. 1 ст. 63 УК РФ новым отягчающим обстоятельством. Поскольку действующая редакция ст. 63 УК РФ уже содержит пункт «ф», новый пункт может быть обозначен буквой «х»:

«*х) совершение умышленного преступления с использованием заведомо для виновного незаконно полученных персональных данных, биометрических персональных данных либо иных охраняемых законом сведений о потерпевшем, если такие сведения использовались для выбора потерпевшего, создания у него ложного представления о лице, событии, документе, распоряжении, операции, угрозе наступления неблагоприятных последствий либо ином обстоятельстве, имеющем значение для совершения преступления, или для сокрытия преступления*».

Данная формула имеет межсоставное значение. Она может применяться не только к мошен-

DOI: 10.24412/2226-0692-2026-2-164-172

ничеству, но и к вымогательству, угрозам, преступлениям против частной жизни, преступлениям против собственности и иным умышленным посягательствам, в которых сведения о потерпевшем используются как средство преступного воздействия. При этом необходимо учитывать общее правило ч. 2 ст. 63 УК РФ. Если соответствующий признак уже предусмотрен статьей Особенной части УК РФ, он не должен повторно учитываться при назначении наказания.

Уголовно-правовые изменения должны сопровождаться разработкой межведомственных методических рекомендаций по выявлению, фиксации и доказыванию использования технологий искусственного интеллекта в способе совершения дистанционного мошенничества. В материалах дела должно устанавливаться, какие сведения о потерпевшем были использованы, каким способом они могли быть получены, какие информационные материалы были созданы или изменены с применением программных средств, какие обстоятельства были представлены потерпевшему как действительные, каким образом они повлияли на его решение, имелись ли признаки автоматизированного подбора содержания обращения, повторялась ли аналогичная информационная конструкция в отношении иных потерпевших, связаны ли эпизоды общими учетными записями, устройствами, каналами связи, платежными маршрутами или иными цифровыми следами.

Такой подход позволяет избежать декларативного упоминания искусственного интеллекта в уголовном деле. Доказыванию должно подлежать не абстрактное использование технологии, а ее конкретная функция в механизме преступления. Значение имеют источник сведений о потерпевшем, содержание созданной информационной обстановки, способ ее предъявления потерпевшему и причинная связь между этой обстановкой и преступлением.

Заключение

Искусственный интеллект не изменяет юридическую природу мошенничества, оно по-прежнему основано на обмане или злоупотреблении доверием и направлено на побуждение потерпевшего к имущественно значимому действию. Однако ИИ меняет условия подготовки и реализации этого обмана. Его криминологическое значение состоит в том, что он снижает издержки персонализации, ускоряет обработку сведений о потерпевшем и позволяет сохранять адресность воздействия при массовом характере преступной практики.

Персонализация мошенничества существовала и ранее, но до цифровой среды оставалась преимущественно трудоемким индивидуальным приемом. Цифровая среда и незаконный оборот персональных сведений изменили это соотношение, ведь то, что ранее требовало личного наблюдения или доступа к узкому кругу информации, теперь может быть получено, сопоставлено и использовано при подготовке массового, но внешне адресного воздействия. Поэтому самостоятельное криминологическое значение приобретает не сам факт наличия данных у преступника, а их перевод в управляемое заблуждение потерпевшего.

Главный эффект ИИ-персонализации состоит в соединении массовости и адресности. Преступная схема может сохранять внутреннее единство, но внешне проявляться по-разному. Общими остаются не слова и не конкретная легенда, а логика воздействия.

Из этого следует, что противодействие таким преступлениям должно быть направлено не только на финальный акт. Необходимо разрывать всю цепочку. Меры противодействия должны исходить именно из этой логики, поскольку ИИ опасен не как модный технологический термин, а как средство, делающее традиционный механизм мошеннического обмана более точным, дешевым, гибким и воспроизводимым.

Литература

1. Клепицкий И.А. Мошенничество: проблемы юридической техники и квалификации // Уголовное право. 2015. № 5. С. 48—62.
2. Кочои С.М. Мошенничество: теория и практика квалификации // Актуальные проблемы российского права. 2020. Т. 15. № 9. С. 59—66.
3. Хилюта В.В. Мошенничество и неисполнение гражданско-правовых обязательств: критерии разграничения // Юридический мир. 2020. № 2. С. 70—77.
4. Безверхов А.Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. 2015. № 5. С. 8—14.
5. Старостенко Н.И. Понятие и виды методов социальной инженерии, используемых при совершении хищений с применением информационно-телекоммуникационных технологий // Вестник Нижегородской академии МВД России. 2023. № 1. С. 181—188.
6. Головин А.Ю. Социальная инженерия в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 4. С. 71—78.
7. Антонян Ю.М., Эминов В.Е. Личность преступника: криминолого-психологическое исследование. М. : Норма, Инфра-М, 2010. 366 с.
8. Guzman A.L., Lewis S.C. Artificial intelligence and communication: A Human-Machine Communication research agenda // New Media & Society. 2020. Vol. 22, № 1. P. 70–86.
9. Hancock J.T., Naaman M., Levy K. AI-Mediated Communication: Definition, Research Agenda, and Ethical Considerations // Journal of Computer-Mediated Communication. 2020. Vol. 25, № 1. P. 89–100.

10. Степанова А.В. Взаимосвязь искусственного интеллекта как средства совершения преступления и иных субъективных признаков состава преступления // Образование и право. 2021. № 5. С. 349—355.
11. Xu T., Singh K., Rajivan P. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks // Applied Ergonomics. 2023. Vol. 108. Article 103908.
12. Allodi L., Chotza T., Panina E., Zannone N. The Need for New Antiphishing Measures Against Spear-Phishing Attacks // IEEE Security & Privacy. 2020. Vol. 18. No. 2. P. 23–34.

CRIMINAL LAW

ARTIFICIAL INTELLIGENCE AS A TOOL FOR PERSONALIZATION OF REMOTE FRAUD

Rashitkhanov R.S.[9]

Keywords: *fraud, criminal policy, personalization of crime.*

Abstract

Objective: *This study aims to analyze the criminological and criminal-law implications of using artificial intelligence technologies for the personalization of remote fraud, as well as to develop proposals for improving countermeasures against such acts.*

Methodology: *The research employs formal-legal, systemic-structural, comparative-legal, and criminological methods. The provisions of criminal law are examined in conjunction with the mechanism of criminal conduct and modern methods of digital influence on the victim. Particular attention is paid to doctrinal approaches to fraud, social engineering, artificial intelligence as a means of committing a crime, and the unlawful use of personal information. The empirical basis consists of cases described in open sources involving synthetic voice, fake images, generative systems, and automated information processing in fraudulent schemes.*

Results of the study: *it is substantiated that the use of artificial intelligence technologies does not change the legal nature of fraud, but significantly changes the conditions for its preparation, reproduction and concealment. It is shown that the criminological significance is not the very presence of information about the victim, but its consistent transformation into a means of targeted influence plausible fraudulent legend. It is concluded that artificial intelligence reduces the costs of personalization, allows you to combine the mass and targeted nature of deception, accelerates the selection of a legend and maintains a false information environment.*

Practical value: *proposals are formulated to clarify the qualifying signs of fraud, to increase responsibility for the illegal circulation of personal data used for the preparation of mercenary crimes, and to develop criteria for fixing the use of artificial intelligence in the method of committing a crime.*

References

1. Klepitskii I.A. Moshennichestvo: problemy iuridicheskoi tekhniki i kvalifikatsii // Ugolovnoe pravo. 2015. No. 5. S. 48–62.
2. Kochoi S.M. Moshennichestvo: teoriia i praktika kvalifikatsii // Aktual'nye problemy rossiiskogo prava. 2020. T. 15. No. 9. S. 59–66.
3. Khiliuta V.V. Moshennichestvo i neispolnenie grazhdansko-pravovykh obiazatel'stv: kriterii razgranicheniia // Iuridicheskii mir. 2020. No. 2. S. 70–77.
4. Bezverkhov A.G. Moshennichestvo i ego vidy: voprosy zakonodatel'noi reglamentatsii i kvalifikatsii // Ugolovnoe pravo. 2015. No. 5. S. 8–14.
5. Starostenko N.I. Poniatie i vidy metodov sotsial'noi inzhenerii, ispol'zuemykh pri sovershenii khishchenii s primeneniem informatsionno-telekommunikatsionnykh tekhnologii // Vestnik Nizhegorodskoi akademii MVD Rossii. 2023. No. 1. S. 181–188.
6. Golovin A.Iu. Sotsial'naia inzheneriia v mekhanizme prestupnoi deiatel'nosti v sfere informatsionno-telekommunikatsionnykh tekhnologii // Izvestiia Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i iuridicheskie nauki. 2021. No. 4. S. 71–78.
7. Antonian Iu.M., Eminov V.E. Lichnost' prestupnika: kriminologo-psikhologicheskoe issledovanie. M. : Norma, Infra-M, 2010. 366 s.
8. Guzman A.L., Lewis S.C. Artificial intelligence and communication: A Human-Machine Communication research agenda // New Media & Society. 2020. Vol. 22. No. 1. P. 70–86.
9. Hancock J.T., Naaman M., Levy K. AI-Mediated Communication: Definition, Research Agenda, and Ethical Considerations // Journal of Computer-Mediated Communication. 2020. Vol. 25. No. 1. P. 89–100.
10. Stepanova A.V. Vzaimosviaz' iskusstvennogo intellekta kak sredstva sovershenia prestupleniia i inykh sub"ektivnykh priznakov sostava prestupleniia // Obrazovanie i pravo. 2021. No. 5. S. 349–355.
11. Xu T., Singh K., Rajivan P. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks // Applied Ergonomics. 2023. Vol. 108. Article 103908.
12. Allodi L., Chotza T., Panina E., Zannone N. The Need for New Antiphishing Measures Against Spear-Phishing Attacks // IEEE Security & Privacy. 2020. Vol. 18. No. 2. P. 23–34.

[9] **Ruslan S. Rashitkhanov**, Deputy Director of the Institute of Legal Analysis of Information and Media Security Problems of the Kutafin Moscow State Law University (MSAL), Head of the Laboratory of Legal Studies in the Field of National Security of the Gubkin Russian State University of Oil and Gas, Moscow, Russia. E-mail: rsrashithanov@msal.ru

DOI: 10.24412/2226-0692-2026-2-164-172