Дата поступления рукописи в редакцию: 25.08.2026 г.
Дата принятия рукописи в печать: 01.10.2026 г.
DOI: 10.24412/2224-9133-2026-9-198-203

БЫКОВА Елена Анатольевна,
преподаватель кафедры специальных дисциплин Волгодонского филиала Ростовского юридического института МВД России, старший лейтенант полиции,
e-mail: alena-bykova-1987@mail.ru.

МАРКОВСКИЙ Максим Сергеевич,
доцент кафедры уголовного права Уральского юридического института МВД России, полковник полиции,
e-mail: sakh_rider_88@mail.ru.

ТАРАНИН Михаил Александрович,
преподаватель кафедры специальных дисциплин Крымского филиала Краснодарского университета МВД России, майор полиции,
e-mail: v.shanko@mail.ru.

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ: ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ РОЛИ ИИ В МЕХАНИЗМЕ ПРЕСТУПНОГО ДЕЯНИЯ

Аннотация. *В статье исследуется уголовно-правовая роль генеративного искусственного интеллекта в механизме преступного деяния. Обосновывается, что ИИ в действующей модели уголовного права не является субъектом преступления, а в большинстве случаев выступает технологически сложным средством реализации человеческого умысла. Рассматриваются ситуации частичной автономности генерации, проблемы установления умысла, причинной связи и соучастия разработчиков и операторов цифровых систем. Предлагается авторский критерий функционального контроля, включающий цель использования, параметры работы системы, возможность принятия или отклонения результата и его фактическое применение. Формулируются предложения для судебного толкования преступлений, совершенных с использованием генеративного ИИ.*

Ключевые слова: *искусственный интеллект, генеративный искусственный интеллект, уголовная ответственность, субъект преступления, средство совершения преступления, дипфейк, мошенничество, соучастие, умысел, причинная связь, функциональный контроль.*

BYKOVA Elena Anatolyevna,
Senior Police Lieutenant, Lecturer in the Specialized Disciplines Department at the Volgodonsk Branch of the Rostov Law Institute of the Ministry of Internal Affairs of Russia

MARKOVSKY Maxim Sergeevich,
associate professor of the criminal law department of the Ural Law Institute of the Ministry of Internal Affairs of Russia, police colonel

TARANIN Mikhail Aleksandrovich,
Lecturer in the Department of Specialized Disciplines at the Crimean Branch of the Krasnodar University of the Ministry of Internal Affairs of Russia, Police Major

USE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN CRIME: DETERMINING THE ROLE OF AI IN THE MECHANISM OF A CRIMINAL ACT

Annotation. *The article examines the criminal-law role of generative artificial intelligence in the mechanism of crime. It argues that under the current criminal-law model AI cannot be an offender and normally functions as a technologically complex instrument for implementing human intent. Situations involving partly autonomous generation, intent, causation and possible complicity of developers and operators are analyzed. The author proposes a functional-control test based on the purpose of use, system parameters, the ability to accept or reject the output and the actual use of that output. Proposals are formulated for judicial interpretation of crimes committed with generative AI.*

Key words: *artificial intelligence, generative AI, criminal liability, offender, instrument of crime, deepfake, fraud, complicity, intent, causation, functional control.*

Можно с уверенностью утверждать, что генеративный искусственный интеллект за короткий период времени превратился из специализированной технологии в массовый инструмент создания текста, изображения, аудио, видео и программного кода. Если рассматривать развитие технологии генеративного ИИ с точки зрения уголовного права, то для него принципиально не само распространение новой технологии, а изменение масштаба и качества действий, которые с ее помощью способен совершить человек. Генеративная модель позволяет быстро подготовить персонализированное сообщение, воспроизвести голос конкретного лица, создать убедительный видеоряд, адаптировать сценарий обмана под реакцию потерпевшего, автоматизировать коммуникацию с множеством адресатов и существенно снизить стоимость преступной подготовки. Поэтому можно с уверенностью сказать, что общественная опасность деяния тут будет связана, прежде всего, с усилением возможностей субъекта преступления, тогда как вопрос о юридической роли самой системы искусственного интеллекта требует самостоятельного анализа [1; 2].

По нашему мнению, актуальность проблемы усилилась в 2026 году, когда был принят Федеральный закон от 26 июля 2026 г. № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации», закрепивший базовые понятия и принципы регулирования больших фундаментальных моделей искусственного интеллекта. Здесь отметим, что основная часть закона вступила в силу 1 сентября 2026 г., тогда как положения об обязанностях разработчиков, маркировке созданных с применением таких моделей материалов и использовании результатов интеллектуальной деятельности начнут действовать лишь с 1 марта 2027 г. В контексте же рассматриваемой нами проблемы, для уголовно-правовой оценки важно, что данный закон формирует специальную технологическую терминологию, но не превращает искусственный интеллект в самостоятельного субъекта юридической, а тем более уголовной ответственности. В мае 2026 г. Верховный Суд Российской Федерации объявил о проведении первого общероссийского обобщения судебной практики по делам, связанным с применением ИИ, включив в предмет анализа квалификацию преступлений с использованием дипфейков и мошеннических схем с чат-ботами, вопросы доказательственного значения созданных ИИ документов и иные проблемы, что подтверждает переход обсуждения из преимущественно теоретической плоскости в сферу практического правоприменения.

Цель нашего исследования состоит в определении уголовно-правовой роли генеративного искусственного интеллекта в механизме преступного деяния и разработке критериев отграничения случаев, когда ИИ является лишь техническим средством реализации человеческого умысла, от ситуаций, в которых особенности автономной генерации влияют на установление вины, причинной связи и пределов ответственности. Методологическую основу исследования составляют формально-юридический, системно-структурный и функциональный методы. Важным является и учет двойственной природы цифровых технологий, поскольку они используются как в преступных целях, так и для охраны правопорядка. Так, В. В. Шанько и И. Ю. Касницкая специально обращаются к применению систем видеонаблюдения и аналитики больших данных в охране общественного порядка [7, с. 226-230], что говорит о юридической оценке, которая должна быть связана не с технологией как таковой, а с целью, способом и конкретными последствиями ее использования.

Как известно действующий УК РФ строится на антропоцентрической модели уголовной ответственности, когда субъектом преступления признается вменяемое физическое лицо, достигшее установленного возраста, а в предусмотренных законом случаях уголовно-правовые последствия связываются с деятельностью организации

через ответственность конкретных физических лиц. Искусственный интеллект же не обладает уголовно-правовой правосубъектностью, не имеет собственной вины в нормативном смысле и не может самостоятельно нести наказание, поэтому употребляемые в публицистике формулы «ИИ совершил преступление» или «нейросеть обманула потерпевшего» юридически неточны, поскольку они описывают технологический механизм, но не заменяют установления лица, которое сформировало преступную цель, инициировало использование системы, выбрало или скорректировало результат, ввело его в оборот и тем самым реализовало соответствующую объективную сторону.

Наиболее распространенной моделью является использование генеративного ИИ как средства совершения преступления, когда пользователь ставит системе задачу, получает результат и сознательно применяет его для достижения заранее определенной противоправной цели. Генерация поддельного голосового сообщения для убеждения потерпевшего перевести деньги, создание фиктивного изображения для вымогательства, автоматическая подготовка фишинговых текстов, создание поддельных документов или адаптация вредоносного кода не изменяют основополагающего правила о том, что уголовно-правовая квалификация определяется признаками конкретного состава преступления, а технология характеризует способ, средство либо обстановку его совершения. Вот почему исследователи дипфейк-преступлений справедливо отмечают, что синтетический контент способен выступать формой сообщения ложных сведений, но не образует сам по себе нового вида хищения [1; 3; 4].

Мы считаем, что особенно важно это положение для разграничения ст. 159 и 159.6 УК РФ, поскольку использование генеративной модели, чат-бота или синтезированного голоса для обмана потерпевшего не означает автоматически совершения мошенничества в сфере компьютерной информации. Ведь если человек под воздействием ложного аудио-, видео- или текстового сообщения сам распоряжается имуществом либо правом на него, при наличии остальных признаков речь идет о классическом мошенничестве. Статья же 159.6 УК РФ требует воздействия на компьютерную информацию либо функционирование средств ее хранения, обработки или передачи как элемента механизма завладения имуществом, поэтому технологическая сложность обмана не должна подменять юридическое содержание способа хищения. И, нельзя не отметить, что такой подход уже получил развитие в современной литературе, где подчеркивается необходимость отделять использование ИИ как средства социальной инженерии от собственно компьютерного воздействия [1; 3].

Вторая модель нам представляется немного сложнее, к примеру, пользователь задает незаконную цель, но делегирует системе значительную часть выбора конкретного способа, содержания и адресатов воздействия, а программа уже автоматически формирует множество вариантов сообщений, отбирает наиболее убедительные, адаптирует их с учетом ответов пользователей и продолжает коммуникацию без постоянного ручного управления. Но и здесь искусственный интеллект по-прежнему не становится субъектом преступления, однако возрастает значение пределов человеческого контроля, в связи с чем представляется, что ключевым должен быть критерий целевого запуска, то есть если лицо сознательно создает или настраивает систему для достижения преступного результата, понимает типичный механизм ее работы и принимает генерируемые ею варианты как допустимые средства реализации замысла, то случайная непредсказуемость отдельных фраз или последовательности действий не исключает умысла, субъект как бы контролирует не каждую операцию, а преступную функцию системы в целом.

Третья рассматриваемая нами модель связана с генерацией результата, который выходит за пределы поставленной пользователем задачи, поскольку современные модели ИИ имеют вероятностный характер и способны выдавать содержание, которое прямо не задавалось запросом, хотя сам по себе факт технической возможности предвидеть ошибочную или нежелательную генерацию не означает уголовно-правовой вины пользователя. К примеру, если лицо использует ИИ для правомерной цели и не осознает, что результат содержит, например, клеветнические сведения, незаконно раскрываемую тайну или инструкции, создающие реальную опасность причинения вреда, ответственность не может строиться на объективном вменении. Иная же ситуация возникает, когда сознательное распространение или использование результата способно образовать самостоятельное умышленное действие, и тогда момент возникновения умысла переносится с этапа генерации на этап последующего распоряжения полученным материалом.

Для решения подобных ситуаций нами предлагается использовать критерий функционального контроля, включающий в себя четыре взаимосвязанных элемента, таких как постановка цели, определение существенных параметров работы системы, возможность принятия либо отклонения результата и фактическое использование результата в объективной стороне преступления. И чем полнее совокупность этих элементов сосредоточена у конкретного лица, тем меньше оснований объяснять причиненный вред «автономностью» алгоритма, поскольку если пользователь заказы-

вает синтез голоса руководителя, выбирает подходящую запись и направляет ее бухгалтеру с требованием перевода денег, его контроль очевиден. Если же разработчик создает универсальную модель общего назначения и не участвует в конкретном преступном использовании, одна лишь техническая возможность злоупотребления не образует соучастия. И вот между этими полюсами и находятся случаи предоставления специально настроенного сервиса, когда вопрос ответственности должен решаться с учетом осведомленности о преступной цели и реального содействия ее достижению.

Такая конструкция на наш взгляд особенно важна для института соучастия, когда разработчик, оператор платформы, владелец вычислительной инфраструктуры или автор программного модуля не становится пособником любого преступления, совершенного конечным пользователем, поскольку для пособничества необходимо умышленное содействие конкретному преступлению либо преступной деятельности в пределах требований соответствующего состава. Общая осведомленность о том, что технологией потенциально можно злоупотребить, на наш взгляд недостаточна, напротив, сознательное создание инструмента под конкретную мошенническую схему, настройка обхода механизмов безопасности, обучение модели на материалах потерпевшего и последующее сопровождение преступного использования при доказанном общем умысле способны образовать интеллектуальное или физическое пособничество. То есть мы видим, что генеративная технология усложняет доказывание, но не отменяет традиционное требование умышленной совместности.

Использование ИИ для масштабирования преступления так же довольно интересно, поскольку один человек способен поддерживать сотни параллельных диалогов, автоматически переводить сообщения, менять легенду, имитировать разные социальные роли и создавать уникальные медиаматериалы для каждого адресата. В результате технология повышает не только вероятность успеха, но и число потенциальных потерпевших, хотя автоматически признавать само использование ИИ квалифицирующим признаком любого состава не стоит. Универсальная формула «с использованием искусственного интеллекта» здесь была бы чрезмерно широкой, так как ИИ может применяться как для создания высокореалистичного дипфейка, так и для незначительной редакции текста, перевода или технической обработки изображения. Поэтому уголовный закон должен дифференцировать ответственность по реальному увеличению общественной опасности, а не по наличию модного технологического инструмента.

В связи с чем, более обоснованным нам представляется функциональный подход к оценке повышенной опасности, когда существенное значение могут иметь достоверная имитация личности другого человека, автоматизированное воздействие на неопределенно широкий круг лиц, использование ИИ для преодоления средств защиты, персонализированное воздействие на заведомо уязвимого потерпевшего либо создание контента, объективно затрудняющего установление его искусственного происхождения. В отдельных же составах эти обстоятельства могут учитываться через уже существующие признаки — группу лиц, крупный или особо крупный размер, использование служебного положения, тяжкие последствия. То есть становится очевидным, что только после накопления устойчивой практики возможно обсуждать специальные квалифицирующие признаки для тех составов, где применение генеративного ИИ действительно изменяет характер посягательства, а не просто облегчает подготовительную работу [4; 5].

Но, проблема не исчерпывается только мошенничеством, синтетические изображения и аудиозаписи могут использоваться для клеветы, вымогательства, нарушения неприкосновенности частной жизни, незаконного распространения сведений ограниченного доступа, ложных сообщений об опасности, фальсификации цифровых доказательств и иных деяний. При этом один и тот же файл способен последовательно участвовать в нескольких преступлениях, сначала создаваться путем незаконного использования персональных данных, затем применяться как средство угрозы, а после распространяться публично. Квалификация же должна отражать реальные самостоятельные объекты посягательства и не сводить многоэпизодное поведение к абстрактному «преступлению с использованием ИИ», поскольку именно отсутствие единого универсального объекта подтверждает, что генеративный ИИ в современной системе уголовного права разумнее рассматривать прежде всего как технологически сложное средство, а не как основание для формирования самостоятельного родового состава.

Для умышленных преступлений несомненно особое значение имеет доказывание того, что пользователь понимал свойства синтетического материала и желал использовать их для конкретного противоправного результата, так как не всякий факт применения нейросети свидетельствует о таком понимании. Следствие должно устанавливать содержание запросов, историю генераций, последующие команды, выбор из нескольких вариантов, ручное редактирование, экспорт файла, способ его распространения и связь с иными действиями обвиняемого. Мы считаем, что в доказательственном отношении полезно различать

технический след создания контента и уголовно-правовой вывод об умысле, поскольку первый показывает происхождение материала, второй формируется только из совокупности обстоятельств. И, несомненно, будущие требования закона № 243-ФЗ о маркировке материалов, созданных с использованием больших фундаментальных моделей, будут способны облегчить идентификацию синтетического происхождения, хотя соответствующие положения и начнут действовать лишь с 1 марта 2027 г. и сами по себе не решают вопрос об авторстве преступного замысла.

Хочется обратить внимание на тот факт, что разъяснения Верховного Суда Российской Федерации по итогам начатого в 2026 году обобщения могли бы закрепить несколько базовых ориентиров. Во-первых, использование генеративного ИИ не изменяет правила определения субъекта преступления, когда ответственность несет физическое лицо, действия которого отвечают признакам состава. Во-вторых, создание синтетического контента должно оцениваться с учетом его фактической функции, так как само наличие дипфейка не предопределяет квалификацию. В-третьих, разработчик или оператор универсальной системы не признается соучастником без доказательств умышленного содействия преступлению. В-четвертых, при частичной автономности алгоритма необходимо устанавливать цель запуска, параметры контроля, возможность отклонения результата и последующее сознательное использование. В-пятых, документы и медиаматериалы, созданные ИИ, требуют проверки происхождения и целостности, но вопрос об их доказательственном значении не может решаться только по признаку искусственного происхождения.

Так же по нашему мнению отдельно следует разграничивать использование общедоступной модели и создание специализированной системы, ориентированной на противоправные задачи. В первом случае разработчик предоставляет универсальный инструмент, пригодный для множества правомерных целей, и причинная связь между разработкой и последующим преступлением опосредована самостоятельным решением пользователя. А во втором случае программная архитектура, набор данных, ограничения и интерфейс могут изначально быть подчинены узкой противоправной функции, например массовому созданию поддельных идентичностей или автоматизированному формированию сообщений для обмана. Поэтому уголовно-правовое значение имеет не техническая специализация сама по себе, а доказанная направленность умысла создателя и его вклад в конкретную преступную деятельность, что позволяет избежать как безосновательной ответственности разработчиков технологий общего назначения, так и искусственного исключения соучастия там, где программный продукт сознательно создается как элемент преступной инфраструктуры.

Использование генеративного ИИ способно влиять и на стадии преступления, когда подготовка промптов, сбор образцов голоса, обучение персонализированной модели или создание синтетического изображения могут представлять собой правомерные действия, приготовление либо уже входить в объективную сторону конкретного состава, что зависит от конструкции соответствующей нормы. К примеру, создание ложного видеоролика для будущего мошенничества само по себе обычно еще не означает оконченного хищения, если воздействие на потерпевшего не началось, но при наличии условий может оцениваться в рамках приготовления. И, напротив, для преступлений с формальным составом изготовление или распространение определенного материала способно иметь самостоятельное юридическое значение, поэтому стадия определяется не технической завершенностью цифрового продукта, а моментом начала выполнения объективной стороны конкретного преступления. То есть можно сказать, что это правило особенно важно для предотвращения ошибочной квалификации, когда факт готовности дипфейка механически отождествляется с оконченным преступлением.

Таким образом, мы видим, что генеративный искусственный интеллект не образует нового субъекта преступления и не требует отказа от базовых конструкций российского уголовного права, основная задача которого состоит в адаптации этих конструкций к ситуации распределенного технологического действия, когда человек контролирует преступную функцию системы, но не каждую промежуточную операцию. И наиболее продуктивным по нашему мнению является критерий функционального контроля, основанный на цели, параметрах использования, возможности выбора результата и его фактическом включении в объективную сторону преступления, поскольку он позволяет отделить умышленное использование ИИ как средства преступления от правомерного применения технологии с непредвиденным результатом, а также ограничить необоснованное расширение ответственности разработчиков и операторов. Вот почему дальнейшее совершенствование должно идти прежде всего по линии судебного толкования и накопления практики, а не путем создания универсального состава «преступления с использованием искусственного интеллекта».

Список литературы:

[1] Майстренко Г. А. Мошенничество с ис-

пользованием дипфейк-технологий и искусственного интеллекта: проблемы уголовно-правовой квалификации и направления совершенствования законодательства // Право и управление. 2026. № 8. С. 242-250. DOI: 10.24412/2224-9133-2026-8-242-250..

[2] Кочетов В. А., Гридин А. С. Искусственный интеллект как катализатор киберпреступности: вызовы для уголовного права и правоприменения // Финансовая безопасность: новые горизонты. Материалы научной конференции. М.: НИЯУ МИФИ, 2025. С. 643-647.

[3] Долгиева М. М. Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. 2024. Т. 19. № 11. С. 106-113. DOI: 10.17803/1994-1471.2024.168.11.106-113..

[4] 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.

[5] Ситник В. Н. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // Уральский журнал правовых исследований. 2026. № 1. С. 119-126. DOI: 10.33693/2541-8025-2026-22-1-119-126..

[6] Ефремова М. А., Русскевич Е. А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 97-105.

[7] Шанько В. В., Касницкая И. Ю. Применение систем видеонаблюдения и аналитики больших данных в охране общественного порядка // Право и управление. 2026. № 4. С. 226-230.

[8] Зотина Е. В. Уголовно-правовой аспект предупреждения мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 3 (57). С. 72-82. DOI: 10.37973/VESTNIKKUI-2024-57-8..

[9] Бодров Н. Ф., Лебедева А. К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11.

References:

[1] Maistrenko G. A. Fraud using deepfake technologies and artificial intelligence: problems of criminal legal qualification and directions for improving legislation // Law and management. 2026. № 8. S. 242-250. DOI: 10.24412/2224-9133-2026-8-242-250..

[2] Kochetov V. A., Gridin A. S. Artificial intelligence as a catalyst for cybercrime: challenges for criminal law and law enforcement // Financial security: new horizons. Scientific conference materials. M.: NRNU MEPHI, 2025. S. 643-647.

[3] Dolgieva M. M. Qualification of deepfake fraud and human cyber theft // Actual problems of Russian law. 2024. VOL. 19. № 11. S. 106-113. DOI: 10.17803/1994-1471.2024.168.11.106-113..

[4] Paliy E. S. Criminological and criminal legal aspects of remote fraud using deepfake technologies and social engineering // Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia. 2025. № 4 (108). S. 149-157.

[5] Sitnik V.N. Prospects for criminalizing crimes committed using deepfake technology // Ural Journal of Legal Research. 2026. № 1. S. 119-126. DOI: 10.33693/2541-8025-2026-22-1-119-126..

[6] Efremova M.A., Russkevich E.A. Deepfake (deepfake) and the criminal law // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. VOL. 15. № 2 (56). S. 97-105.

[7] Shanko V. V., Kasnitskaya I. Yu. Application of video surveillance systems and big data analytics in the protection of public order // Law and management. 2026. № 4. S. 226-230.

[8] Zotina E. V. Criminal law aspect of fraud prevention using information and telecommunication technologies and social engineering techniques // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. VOL. 15. № 3 (57). S. 72-82. DOI: 10.37973/VESTNIKKUI-2024-57-8..

[9] Bodrov N.F., Lebedeva A.K. The concept of deepfake in Russian law, classification of deepfakes and issues of their legal regulation // Legal research. 2023. № 11.