BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

оригинальная статья

eLibrary EDN: FVGAYI

Криминалистические аспекты распознания дипфейков

Волгин Юрий Геннадьевич
Кемеровский государственный университет, Россия, Кемерово
eLibrary Autor SPIN: 5312-3220
https://orcid.org/0000-0003-3694-8058
volgin384@mail.ru

Аннотация: В данной статье на основе анализа криминогенной обстановки в Российской Федерации делается вывод о существенном изменении способов, которые используются лицами при совершении преступлений. В последние годы значительно возросло число преступлений, совершаемых с использованием средств искусственного интеллекта, в частности такого его продукта, как фальсифицированный контент (дипфейк). В целях проведения детального расследования преступлений, совершаемых с использованием дипфейков, и установления всех обстоятельств необходимо иметь четкое представление о признаках и методах, позволяющих распознавать фальсифицированный контент и представлять такие выводы в доказательственной форме. Цель – установить, какие существуют признаки фальсифицированного контента, созданного с использованием средств искусственного интеллекта. Детальное изучение научных публикаций и практической деятельности экспертных подразделений позволило выделить следующие группы признаков фальсифицированного контента: признаки фальсифицированного графического изображения; признаки фальсифицированного звукового сообщения; признаки фальсифицированного видео. Распознавание указанных групп признаков предполагает проведение компьютерной, фонографической, фототехнической, портретной и видеотехнической экспертиз. В целях распознания отличительных признаков фальсифицированного контента, содержащего голос или изображение конкретных лиц, целесообразно использование возможностей идентификационных экспертиз по динамическим признакам внешности человека и признакам, характеризующим автора сообщений. С учетом наличия разнообразных по своему характеру признаков фальсифицированного контента делается вывод о целесообразности комплексного подхода и назначения комплексных судебных экспертиз.

Ключевые слова: преступление, информационно-телекоммуникационные технологии, искусственный интеллект, дипфейк, фальсифицированный контент, комплексная судебная экспертиза

Цитирование: Волгин Ю. Г. Криминалистические аспекты распознания дипфейков. *Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки*. 2026. Т. 10. № 2. С. 376–383. https://doi.org/10.21603/2542-1840-2026-10-2-376-383

Поступила в редакцию 29.01.2026. Принята после рецензирования 25.02.2026. Принята в печать 04.03.2026.

original article

Criminal Aspects of Identifying Deepfakes

Yurii G. Volgin
Kemerovo State University, Russia, Kemerovo
eLibrary Autor SPIN: 5312-3220
https://orcid.org/0000-0003-3694-8058
volgin384@mail.ru

Abstract: The contemporary criminal landscape in the Russian Federation is undergoing a paradigm shift driven by evolving operational methods. It demonstrates a significant surge in offenses that utilize artificial intelligence and AI-generated synthetic media (deepfakes). Conducting effective investigations into these crimes requires a precise comprehension of the markers and detection methodologies necessary to establish robust evidentiary verification in court. Based on a comprehensive review of scientific literature and expert reports, these forensic markers can be categorized by source into image, audio, and video data. Their identification involves an intersection of specialized forensic disciplines, including computer, phonographic, phototechnical, portrait, and video-technical examinations. Detecting signs of manipulation relies on identifying the dynamic features of a subject's altered physical appearance alongside idiolect anomalies within communications, which can be verified through forensic

identification examinations. An integrated approach and a multidisciplinary, complex forensic examination are required given the multi-layered complexity of synthetic AI-generated falsifications.
Keywords: crime, information and telecommunication technologies, artificial intelligence, deepfake, falsified content, complex forensic examination

Citation: Volgin Yu. G. Criminal Aspects of Identifying Deepfakes. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriia: Gumanitarnye i obshchestvennye nauki*, 2026, 10(2): 376–383. (In Russ.) https://doi.org/10.21603/2542-1840-2026-10-2-376-383

Received 29 Jan 2026. Accepted after review 25 Feb 2026. Accepted for publication 4 Mar 2026.

Введение

Анализ криминогенной ситуации в Российской Федерации позволяет сделать вывод о кардинальном изменении подходов лиц, совершающих преступления, к выбору способов. Так, в последние годы широкое распространение имеют преступления, совершаемые с использованием средств искусственного интеллекта. К сожалению, нынешний подход к статистическому учету не дает возможности оценки детальной картины степени распространенности указанной группы преступлений. Вместе с тем о таковой можно судить по косвенным показателям. Так, за 2024 г. официально зарегистрировано 765365 преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[1]. За 11 месяцев 2025 г. было зарегистрировано 627037 преступлений данного вида[2]. По состоянию на 2017 г. (год, с которого был введен официальный учет преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации) рассматриваемый показатель составлял 90587 преступлений[3]. Число совершаемых преступлений указанного вида за эти годы увеличилось почти в 8,5 раз, а их доля в общей массе зарегистрированных преступлений возросла с 4,00 % до 40,05 %.

А. А. Бессонов также указывает на расширение видов преступлений, которые совершаются с использованием информационных технологий [1, с. 29]. Среди преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, особо следует выделить именно преступления, совершаемые с использованием искусственного интеллекта. В своем исследовании М. А. Иващенко делает вывод о появлении новой формы организованной преступности – совершение преступлений с использованием искусственного интеллекта [2, с. 139].

Объяснение данному феномену приводят в своих публикациях такие авторы, как Н. Ф. Бодров и А. К. Лебедева [3, с. 130], Р. И. Дремлюга [4, с. 161], О. Б. Дронова [5, с. 13], Я. А. Климова [6, с. 82], Е. И. Пырьева и коллеги [7, с. 208]. В качестве объяснений данному феномену они выделяют:

1) повышение эффективности преступного воздействия за счет возможностей анализа средствами искусственного интеллекта больших объемов финансовой и иной информации, изменения значительных массивов информации, а также возможностей по созданию вредоносного кода;

2) минимизируются риски со стороны лиц, использующих данные средства в целях совершения преступлений, чему способствует значительное его удаление от предмета преступного посягательства, а также трудности по выявлению и фиксации следов совершенного преступления;

3) расширяется число лиц, в отношении которых предпринимаются попытки совершить преступление;

4) относительная доступность средств искусственного интеллекта, включая аппаратно-технические.

Отдельно следует указать на крайне низкую раскрываемость преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. За 2024 г. было раскрыто всего 172627 преступлений (22,55 %)[4].

В качестве еще одного аргумента, определяющего необходимость рассмотрения криминалистических аспектов, связанных с раскрытием и расследованием

[1] Состояние преступности в России за январь – декабрь 2024 года. М., 2025. С. 6. URL: https://media.mvd.ru/files/application/9209203 (дата обращения: 12.01.2026).

[2] Состояние преступности в России за январь – ноябрь 2025 года. М., 2026. С. 6. URL: https://media.mvd.ru/files/application/16106985 (дата обращения: 12.01.2026).

[3] Состояние преступности в России за январь – декабрь 2017 года. М., 2018. С. 4. URL: https://media.mvd.ru/files/application/1241295 (дата обращения: 12.01.2026).

[4] Состояние преступности в России за январь – декабрь 2024 года…

преступлений, совершаемых с использованием искусственного интеллекта, следует указать, что, помимо требования ст. 73 Уголовно-процессуального кодекса Российской Федерации (УПК РФ) по выяснению всех обстоятельств совершения преступления, в последнее время появилась точка зрения о целесообразности оценки самого факта использования искусственного интеллекта в преступных целях в качестве обстоятельства, отягчающего наказание, с включением такового в перечень обстоятельств, предусмотренных ч. 1 ст. 63 Уголовного кодекса Российской Федерации (УК РФ).

Так, президент Российской Федерации В. В. Путин в своем поручении от 5 марта 2025 г. указал на необходимость рассмотрения вопроса «о целесообразности признания в качестве обстоятельства, отягчающего ответственность или наказание, использования при совершении правонарушения (преступления) технологий искусственного интеллекта»[5].

Группа депутатов Государственной Думы, в которую входят С. М. Миронов, Я. В. Лантратова, О. А. Нилов, Н. В. Новичков, А. А. Кузнецов, М. Г. Делягин, Д. Г. Гусев и А. С. Аксененко, в апреле 2025 г. внесла на рассмотрение законопроект о дополнении соответствующим положением ст. 63 УК РФ[6]. Несмотря на отклонение данного законопроекта профильным Комитетом по государственному строительству и законодательству по формальным основаниям, данный вопрос остается открытым.

О необходимости включения использования искусственного интеллекта при совершении преступлений в перечень обстоятельств, отягчающих ответственность, рассуждают и такие специалисты уголовного права, как И. С. Алихаджиева [8, с. 168], Э. Р. Гафурова [9, с. 208], Е. В. Зотина [10, с. 80].

В целях распознавания фальсифицированного контента при расследовании преступлений, совершаемых с использованием дипфейков, важно иметь детальное представление об их криминалистически значимых признаках, а также сформулировать предложения по формированию методических основ проведения экспертных исследований.

Методы и материалы

При проведении исследования были использованы сравнительный и системный анализ научных публикаций по проблемам противодействия преступлениям, совершаемым с использованием средств искусственного интеллекта, а также практики проведения экспертных исследований сотрудниками Экспертно-криминалистического центра Главного управления МВД по Кемеровской области – Кузбассу и Кемеровской лаборатории судебных экспертиз Министерства юстиции Российской Федерации.

Применялся также классификационный метод логики, что дало возможность выделить группы признаков, позволяющих распознавать фальсифицированный контент.

Многомерный подход, заключающийся в осуществлении исследования по нескольким взаимосвязанным направлениям, позволил сформировать целостное представление о свойствах такого сложного объекта, как дипфейк.

Результаты

Основные направления использования средств искусственного интеллекта в преступных целях рассматриваются такими исследователями, как А. А. Бессонов [1, с. 28–29], Р. И. Дремлюга [4, с. 161], В. Б. Батоев и А. В. Руденко [11, с. 91], Ю. А. Даниленко [12, с. 237], П. А. Пикалов [13, с. 57], Я. А. Климова [14, с. 32–33; 15, с. 137], С. В. Лемайкина [16, с. 120; 17, с. 144–145], Г. В. Макович [18, с. 72]. Анализ работ указанных авторов позволяет выделить следующие основные направления: мошенничество (кибермошенничество) и вымогательство; посягательство на национальную безопасность государства; кибератаки на информационные ресурсы; создание и изменение сексуального контента, а также сексуальная эксплуатация детей.

В качестве непосредственных способов использования средств искусственного интеллекта в преступных целях выделяют: создание (генерация) фальсифицированного контента; автоматизация кибератак на пароли и системы безопасности; использование искусственного интеллекта в качестве инструмента социальной инженерии; разработка сценариев будущих преступлений.

Среди указанных способов использования искусственного интеллекта при совершении преступлений следует выделить генерацию фальсифицированного контента – создание так называемых дипфейков. Изначально технология создания дипфейков была ориентирована на использование в развлекательных целях. Их и сейчас применяют в архитектуре, киноиндустрии, искусстве, образовании, рекламе и маркетинговых исследованиях [19, с. 114]. Не обошли своим вниманием предоставляемые технологией дипфейков возможности также и лица, совершающие преступления.

[5] Перечень поручений Президента РФ по итогам совещания с членами Правительства 5 марта 2025 г. URL: http://www.kremlin.ru/acts/assignments/orders/76615 (дата обращения: 06.01.2026).

[6] О внесении изменения в статью 63 Уголовного кодекса РФ. Законопроект № 885494-8. URL: https://sozd.duma.gov.ru/bill/885494-8 (дата обращения: 06.01.2026).

https://doi.org/10.21603/2542-1840-2026-10-2-376-383

Стоит заметить, что в настоящее время термин *дипфейк* не имеет общепринятого определения. И. А. Воронин и Д. П. Гавра разделяют точки зрения на понятие *дипфейк* на три группы: техноцентричный подход, нормативный подход и синтетический подход [20, с. 31–35]. Однако, по нашему мнению, в рамках рассматриваемой проблемы следует за основу принять дефиницию, которую сформулировали Н. Ф. Бодров и А. К. Лебедева. Ими предлагается под дипфеком понимать «цифровой продукт в виде текста, графики, звука или их сочетания, сгенерированный полностью или частично при помощи нейросетевых технологий, для цели введения в заблуждение или преодоления пользователем систем контроля и управления доступом» [21, с. 178].

Поддельный контент (дипфейк), как указывает С. В. Лемайкина, создается с целями последующего использования в качестве: дезинформации и распространения фальсифицированных новостей; фальсифицированных аккаунтов известных личностей; фальсифицированной порнографии [16, с. 120; 17, с. 144–145].

Изучение практики деятельности сотрудников Экспертно-криминалистического центра Главного управления МВД по Кемеровской области – Кузбассу позволило установить, что помимо создания фальсифицированных аккаунтов известных личностей, генерируются также и аккаунты несуществующих (вымышленных) лиц.

После создания фальсифицированный контент для реализации преступного замысла целенаправленно доводится до аудитории. А. Л. Осипенко, положив в основу анализа публикации зарубежных и отечественных специалистов, выделяет следующие каналы донесения до адресатов фальсифицированного контента (содержания дипфейков): традиционные средства массовой информации; устные коммуникации; социальные сети; мессенджеры и чаты; интернет-сайты и блоги; электронная почта [22, с. 17–18].

Детальное изучение научных публикаций, авторами которых являются В. Б. Батоев, А. В. Руденко [11, с. 91], Я. А. Климова [14, с. 33–34], Ю. С. Гречкина, И. К. Карабинцева [19, с. 115–117], А. М. Андриянов, О. В. Баюк [23, с. 170], И. Н. Поздняк [24, с. 75], а также практики деятельности Экспертно-криминалистического центра Главного управления МВД по Кемеровской области – Кузбассу и Кемеровской лаборатории судебных экспертиз Министерства юстиции РФ позволяет выделить следующие группы признаков фальсифицированного контента, созданного с использованием средств искусственного интеллекта: признаки фальсифицированного графического изображения; фальсифицированного звукового сообщения; фальсифицированного видео. Аналогичную точку зрения в выделении видов дипфейков выражают также Н. Ф. Бодров и А. К. Лебедева. Вместе с тем данные ученые обозначают и виды, являющиеся сочетанием вышеуказанных [21].

Признаками фальсифицированного графического изображения, как указывают М. В. Бабичева и И. А. Третьяков, являются различные аномалии и артефакты [25, с. 95]. К таковым следует отнести:

- муар, который представляет собой волнообразный узор, возникающий из-за наложения одного пиксельного изображения на другое;
- излишнюю пикселизацию, при которой группы отдельных пикселей, формирующих изображение, заменяются одноцветными пикселями;
- нечеткое или смазанное изображение;
- механический и неестественный характер лица или лиц;
- различие в освещенности и тенях отдельных элементов изображений;
- нарушение детализации отдельных элементов изображений.

Признаками, указывающими на наличие фальсифицированного звукового сообщения или звуковой дорожки, могут быть: дрожание речи; внезапное изменение тембра речи; отсутствие пауз, вызванных необходимостью перевести дыхание.

Признаки фальсифицированного видео:

- неестественные движения как лиц, так и иных элементов вещной обстановки, формирующих видеоизображение;
- неестественная мимика (лицевые экспрессии) человека;
- отсутствие синхронизации между речью и движениями губ, запаздывание речи;
- полное отсутствие моргания или же видеоизображение человека, при котором частота моргания намного реже чем в реальной жизни;
- диспропорции во внешности, прическе и голосе, которые возникают при изменении речевых параметров технологии синтеза речи;
- понижение качества видео как попытка скрыть факт использования дипфейка.

Распознание дипфейка, по утверждениям специалистов, возможно благодаря выявлению наличия указанных признаков и осуществляется двумя путями: посредством использования программных средств либо посредством проведения судебных экспертиз.

Так, уже сейчас для распознания дипфейков используются различные программные средства. В публикациях В. Б. Батоева, А. В. Руденко [11, с. 92], Л. С. Макаровой и коллег [26, с. 24] упоминаются следующие разработки ведущих зарубежных IT-компаний: Microsoft Video AI Authenticator, Intel FakeCatcher, Sentinel AI, Sensity AI, Deepware Scanner,

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

WeVerify Deepfake Detection Tool. Приводятся ими также примеры отечественных IT-решений, позволяющих распознавать дипфейки, а именно: ИС «Вепрь», ПО «Зефир», технические решения ПАО «Сбербанк», Deep-Fake-детектор.

Необходимо указать на то, что программный способ позволяет решать задачи оперативного распознания и профилактики.

Для формирования методических основ проведения экспертных исследований при расследовании преступлений, совершаемых с использованием фальсифицированного контента, необходим несколько иной взгляд на признаки дипфейков.

По нашему глубокому убеждению, признаки, по которым распознаются дипфейки, следует разделять с использованием многомерного подхода по следующим основаниям: по характеру контента (виду информации, имеющей признаки фальсификации); по характеру причин, определяющих появление признаков, по которым возможно распознание фальсифицированного контента.

Предлагаемый нами подход позволяет:

1) определить конкретный вид судебной экспертизы, при проведении которой будет сделан вывод о наличии признаков, указывающих на фальсификацию контента;

2) сформировать методические рекомендации по проведению экспертного исследования цифрового фальсифицированного контента.

Ранее нами были выделены такие виды фальсифицированного контента, как аудио (звуковое сообщение), графическое изображение и видео. Именно они представляют собой соответствующие объекты экспертного исследования. Так, исследование фальсифицированного аудио требует проведения фонографической экспертизы, исследование графического изображения – фототехнической или портретной, исследование видео – видеотехнической.

Вместе с тем Н. Ф. Бодров и А. К. Лебедева выделяют такие разновидности фальсифицированного контента, как сочетание звука и графики; сочетание текста, графики и звука [21]. Отмеченные обстоятельства, несомненно, требуют комплексной оценки разнородной информации, т. е. назначения и проведения комплексных экспертиз.

Также необходимо рассмотреть, что является причинами возникновения отличительных признаков дипфейков. К таковым следует отнести: техническое несовершенство средства искусственного интеллекта, использованного при создании контента; наличие отличительных признаков, присущих лицу, чей образ фальсифицируется (например, динамические признаки внешности, авторская лексика).

Именно различие признаков, характеризующих «оригинал» (лицо, чей исходный «образ» был использован в качестве основы генерации фальсифицированного контента), может служить основой распознания дипфейка.

В этом отношении весьма интересна позиция Г. В. Маковича, по мнению которого могут быть применены идиолектные маркеры речи, являющиеся индивидуальными языковыми особенностями, используемыми «для авторской атрибуции синтетических материалов» [18, с. 72]. Н. Ф. Бодров и А. К. Лебедева вносят предложение по проведению автороведческой экспертизы для распознания авторства речевого содержания контента [27, с. 137]. Также авторы ведут речь о необходимости комплексного подхода для распознания синтезированного аудиального контента [Там же, с. 138]. Нами полностью разделяется точка зрения И. Н. Позняка, указывающего на целесообразность применения комплексного подхода при распознании дипфейков с привлечением экспертов из различных отраслей знаний, компетентных в проведении портретных, компьютерно-технических и фоноскопических видов экспертиз, а также специалистов из других областей [24, с. 75].

Важным представляется не только характеристика признаков, по которым осуществляется распознание дипфейков, но и методы решения данной задачи. К таким методам С. В. Лемайкина относит анализ качества изображений; статистический анализ; выявление артефактов, специфичных для фальсифицированного контента; выявление временных или пространственных несоответствий [16, с. 121–122]. Данные методы выработаны различными отраслями научных знаний.

Заключение

На основании проведенного исследования установлено, что указанные признаки дипфейков могут быть использованы для распознания таковых при проведении судебных экспертиз. Также в качестве рекомендации следует указать на целесообразность комплексного характера таких экспертиз, который требует собственно назначение комплексных экспертиз; привлечение для проведения экспертиз специалистов различных отраслей науки и техники; применение методов проведения исследований, заимствованных из смежных с криминалистикой, прежде всего технических, наук.

Конфликт интересов: Автор заявил об отсутствии потенциальных конфликтов интересов в отношении исследования, авторства и / или публикации данной статьи.

Conflict of interests: The author declared no potential conflict of interests regarding the research, authorship, and / or publication of this article.

 https://doi.org/10.21603/2542-1840-2026-10-2-376-383

Литература / References

1. Бессонов А. А. Киберпреступность: тенденции и перспективы. *Расследование преступлений: проблемы и пути их решения*. 2024. № 3. С. 23–30. [Bessonov A. A. Cybercrime: Trends and prospects. *Investigation of crimes: problems and solution*, 2024, (3): 23–30. (In Russ.)] https://doi.org/10.54217/2411-1627.2024.45.3.002
2. Иващенко М. А. Новые технологии и их влияние на трансформацию организованной преступности в России. *Расследование преступлений: проблемы и пути их решения*. 2020. № 4. С. 136–140. [Ivashchenko M. A. New technologies and their impact on the transformation of organized crime in Russia. *Investigation of crimes: problems and solution*, 2020, (4): 136–140. (In Russ.)] https://elibrary.ru/kqoypr
3. Бодров Н. Ф., Лебедева А. К. Судебно-экспертное противодействие дипфейк-дезинформации. *Союз криминалистов и криминологов*. 2024. № 4. С. 129–142. [Bodrov N. F., Lebedeva A. K. Forensic countering of deepfake disinformation. *Union of Criminalists and Criminologists*, 2024, (4): 129–142. (In Russ.)] https://doi.org/10.31085/2310-8681-2024-4-216-129-142
4. Дремлюга Р. И. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика. *Азиатско-Тихоокеанский регион: экономика, политика, право*. 2021. Т. 23. № 3. С. 153–165. [Dremliuga R. I. Application of artificial intelligence for criminal purposes from criminal law perspective. *Pacific RIM: Economics, Politics, Law*, 2021, 23(3): 153–165. (In Russ.)] https://doi.org/10.24866/1813-3274/2021-3/153-165
5. Дронова О. Б. Криминалистические аспекты преступности в цифровом обществе: современные проблемы и перспективы развития. *На страже закона*. 2024. № 4. С. 11–16. [Dronova O. B. Forensic aspects of combating crime in digital society: Modern problems and development prospects. *Law enforcement*, 2024, (4): 11–16. (In Russ.)] https://elibrary.ru/roodvv
6. Климова Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий. *Вестник Волгоградской академии МВД России*. 2023. № 1. С. 81–87. [Klimova Ya. A. Artificial intelligence and digital evidences while investigating crimes committed through the use of modern information and communication technologies. *Vestnik Volgogradskoi akademii MVD Rossii*, 2023, (1): 81–87. (In Russ.)] https://doi.org/10.25724/VAMVD.A079
7. Пырьева Е. И., Попова Н. В., Лихачева Е. А. Наиболее значимые элементы криминалистической характеристики хищений, совершаемых с применением методов социальной инженерии и информационно-телекоммуникационных технологий. *Вестник Воронежского института ФСИН России*. 2025. № 2. С. 208–215. [Pyryeva E. I., Popova N. V., Likhacheva E. A. The most significant elements of the criminalistic characteristics of thefts committed using methods of social engineering and information and telecommunication technologies. *Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service*, 2025, (2): 208–215. (In Russ.)] https://elibrary.ru/dllcas
8. Алихаджиева И. С. Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8). *Известия Юго-Западного государственного университета. Серия: История и право*. 2025. Т. 15. № 2. С. 154–171. [Alikhadzhieva I. S. Prospects for establishing criminal liability for crimes involving the use of identity substitution technologies (Draft Law № 718538-8). *Proceedings of Southwest State University. Series: History and law*, 2025, 15(2): 154–171. (In Russ.)] https://doi.org/10.21869/2223-1501-2025-15-2-154-171
9. Гафурова Э. Р. Совершение преступлений с использованием искусственного интеллекта как новая форма организованной преступности. *Правовые взгляды Анатолия Федоровича Кони и их влияние на развитие судебной системы*: Междунар. науч.-практ. конф. (Ижевск, 27–28 марта 2024 г.) Ижевск: ВГУЮ, 2024. С. 206–209. [Gafurova E. R. Committing crimes using artificial intelligence as a new form of organized crime. *Anatoly F. Koni' views on law and their influence on the development of the judicial system*: Proc. Intern. Sci.-Prac. Conf., Izhevsk, 27–28 Mar 2024. Izhevsk: ARSUJ, 2024, 206–209. (In Russ.)] https://elibrary.ru/hufyoe
10. 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. С. 72–82. [Zotina E. V. Criminal aspect of public telecommunications networks crime and social engineering prevention. *Bulletin of the Kazan Law Institute of MIA of Russia*, 2024, 15(3): 72–82. (In Russ.)] https://doi.org/10.37973/VESTNIKKUI-2024-57-8
11. Батоев В. Б., Руденко А. В. О детекции дипфейков, используемых в преступной деятельности. *Юристъ-Правоведъ*. 2025. № 1. С. 87–94. [Batoev V. B., Rudenko A. V. On the identification of deepfakes used in criminal activity. *Jurist-Pravoved*, 2025, (1): 87–94. (In Russ.)] https://elibrary.ru/dzydcd

12. Даниленко Ю. А. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика. *Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки*. 2023. Т. 9. № 4. С. 232–240. [Danilenko Yu. A. The use of artificial intelligence for criminal purposes: Criminal and legal characteristics. *Scientific Notes of V. I. Vernadsky Crimean Federal University. Juridical science*, 2023, 9(4): 232–240. (In Russ.)] https://elibrary.ru/nxvlsm
13. Пикалов П. А. Кибермошенничество с использованием искусственного интеллекта. *Актуальные вопросы борьбы с преступлениями*. 2024. № 2. С. 56–59. [Pikalov P. A. Cyber fraud using artificial intelligence. *Current Issues in Crime Control*, 2024, (2): 56–59. (In Russ.)] https://elibrary.ru/dqklru
14. Климова Я. А. Криминалистический анализ преступлений, совершенных с использованием дипфейк-технологии. *Вестник Калининградского филиала Санкт-Петербургского университета МВД России*. 2024. № 2. С. 29–35. [Klimova Ya. A. Forensic analysis of crimes committed using deepfake technology. *Bulletin of the Kaliningrad Branch of the Saint-Petersburg University of the Ministry of Internal Affairs of Russia*, 2024, (2): 29–35. (In Russ.)] https://elibrary.ru/dwwtgc
15. Климова Я. А. Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия. *Актуальные проблемы российского права*. 2025. Т. 20. № 10. С. 133–143. [Klimova Ya. A. Core principles of a special forensic methodology for investigating crimes committed using deepfake technology: From theory to cyber-investigation practice. *Actual Problems of Russian Law*, 2025, 20(10): 133–143. (In Russ.)] https://doi.org/10.17803/1994-1471.2025.179.10.133-143
16. Лемайкина С. В. Методы обнаружения фальсификации информационного контента. *Философия права*. 2023. № 3. С. 119–124. [Lemaikina S. V. Methods for detecting falsification of information content. *Philosophy of Law*, 2023, (3): 119–124. (In Russ.)] https://elibrary.ru/ejqkqb
17. Лемайкина С. В. Проблемы противодействия использования дипфейков в преступных целях. *Юристъ-Правовед*. 2023. № 2. С. 143–148. [Lemaikina S. V. Problems of combating the use of deepfakes for criminal purposes. *Jurist-Pravoved*, 2023, (2): 143–148. (In Russ.)] https://elibrary.ru/yjcpim
18. Макович Г. В. Идиолектные маркеры в дипфейках как метод идентификации субъекта контента в юридической практике. *Вестник филологических наук*. 2025. Т. 5. № 6. С. 71–75. [Makovich G. V. Idiolect markers in deepfakes as a method of identifying the subject of content in legal practice. *Philological Sciences Bulletin*, 2025, 5(6): 71–75. (In Russ.)] https://elibrary.ru/lbzjcm
19. Гречкина Ю. С., Карабинцева И. К. О некоторых признаках обнаружения дипфейков. *Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова*. 2025. № 2. С. 113–118. [Grechkina Yu. S., Karabintseva I. K. About some sings of deepfake detection. *Vestnik of the Far Eastern Law Institute of the Ministry of the Internal Affairs of the Russian Federation named after I. F. Shilov*, 2025, (2): 113–118. (In Russ.)] https://elibrary.ru/tgvfbb
20. Воронин И. А., Гавра Д. П. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы. *Российская школа связей с общественностью*. 2024. № 33. С. 28–47. [Voronin I. A., Gavra D. P. Deepfakes: Modern understanding, approaches to definition, characteristics, problems and prospects. *Russian School of Public Relations*, 2024, (33): 28–47. (In Russ.)] https://doi.org/10.24412/2949-2513-2023-33-28-47
21. Бодров Н. Ф., Лебедева А. К. Понятие дипфейка (deepfake) в российском праве, его классификация и проблемы правового регулирования. *Юридический вестник Дагестанского государственного университета*. 2023. Т. 48. № 4. С. 173–181. [Bodrov N. F., Lebedeva A. K. The concept of deepfake in Russian law, its classification and problems of legal regulation. *Law Herald of Dagestan State University*, 2023, 48(4): 173–181. (In Russ.)] https://doi.org/10.21779/2224-0241-2023-48-4-173-181
22. Осипенко А. Л. Дезинформация в криминальной деятельности и противодействие ей в условиях цифровизации. *Общество и право*. 2025. № 1. С. 14–23. [Osipenko A. L. Disinformation in criminal activity and counteraction to it in the context of digitalization. *Society and Law*, 2025, (1): 14–23. (In Russ.)] https://elibrary.ru/hrpsma
23. Андриянов А. М., Баюк О. В. Дипфейк как угроза информационной безопасности России и инструмент манипуляции и обмана. *Научно-технический вестник Поволжья*. 2025. № 1. С. 169–172. [Andriyanov A. M., Bayuk O. V. Deepfake as a threat to Russia's information security and a manipulation and deception tool. *Scientific and Technical Volga Region Bulletin*, 2025, (1): 169–172. (In Russ.)] https://elibrary.ru/iaemqz
24. Поздняк И. Н. Цифровые угрозы в современном мире: технология deepfake. *Судебная экспертиза Белоруси*. 2024. № 2. С. 72–77. [Pozdnjak I. N. Digital threats in the modern world: Deepfake technology. *Forensic Examination of Belarus*, 2024, (2): 72–77. (In Russ.)] https://elibrary.ru/sfiiub

25. Бабичева М. В., Третьяков И. А. Автоматизация процедуры распознавания фальшивых изображений посредством нейронных сетей. *Проблемы искусственного интеллекта*. 2025. № 1. С. 94–105. [Babicheva M. V., Tretiakov I. A. Avtomatoin is a procedure for deepfake image detection using neural networks. *Problems of Artificial Intelligence*, 2025, (1): 94–105. (In Russ.)] https://doi.org/10.24412/2413-7383-94-105
26. Макарова Л. С., Баташев Ю. В., Солодовников А. Г., Померанцев И. В. Дипфейк как феномен современного информационного пространства. *Челябинский гуманитарий*. 2024. № 3. С. 24–35. [Makarova L. S., Batashev Yu. V., Solodovnikov A. G., Pomerantsev I. V. Deepfake as a phenomenon of the modern information space. *Chelyabinskij gumanitarij*, 2024, (3): 24–35. (In Russ.)] https://doi.org/10.47475/1999-5407-2024-68-3-24-35
27. Бодров Н. Ф., Лебедева А. К. Судебно-экспертное противодействие дипфейк-дезинформации. *Союз криминалистов и криминологов*. 2024. № 4. С. 129–142. [Bodrov N. F., Lebedeva A. K. Forensic countering of deepfake disinformation. *Union of Criminalists and Criminologists*, 2024, (4): 129–142. (In Russ.)] https://doi.org/10.31085/2310-8681-2024-4-216-129-142