

УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.60797/LAW.2026.11.1 EDN: SAKXSC

УГОЛОВНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Научная статья

Довгань Е.А.[1, *]

[1] Волгодонский филиал Ростовского Юридического института МВД России, Волгодонск, Российская Федерация

* Корреспондирующий автор (dovghan_72[at]mail.ru)

Предложена: 18.02.2026; Принята: 06.04.2026; Опубликована: 26.08.2026

Аннотация

Статья посвящена уголовно-правовой квалификации киберпреступлений, совершаемых с применением технологий искусственного интеллекта. Обосновывается, что искусственный интеллект в механизме преступления преимущественно выступает средством его совершения, влияющим на характеристику способа, но не подменяющим его. Проводится разграничение преступлений в сфере компьютерной информации и смежных составов с учетом использования синтетических медиа, автоматизированных атак и технологий социальной инженерии. Формулируется научная новизна, заключающаяся в разработке функционального подхода к оценке роли ИИ в структуре состава преступления и предложении уточнения квалифицирующих признаков без технологической привязки. Обосновываются направления совершенствования судебной практики и уголовного законодательства.

Ключевые слова: киберпреступления, искусственный интеллект, уголовно-правовая квалификация, компьютерная информация, вредоносные программы, deepfake, фишинг, цифровые следы, причинная связь, судебная практика.

THE CRIMINAL CLASSIFICATION OF CYBERCRIMES INVOLVING THE USE OF ARTIFICIAL INTELLIGENCE

Research article

Dovgan E.A.[1, *]

[1] Volgodonsk branch of the Rostov Law Institute of the Ministry of Internal Affairs of Russia, Volgodonsk, Russian Federation

* Corresponding author (dovghan_72[at]mail.ru)

Suggested: 18.02.2026; Accepted: 06.04.2026; Published: 26.08.2026

Abstract

The article is devoted to the criminal law classification of cybercrimes committed using artificial intelligence technologies. It is argued that, within the mechanism of a crime, artificial intelligence primarily acts as a means of committing it, influencing the nature of the method but not replacing it. A distinction is drawn between crimes in the field of computer information and related offences, considering the use of synthetic media, automated attacks and social engineering techniques. The scientific novelty is formulated, consisting in the development of a functional approach to assessing the role of AI in the structure of the offence and a proposal to refine the qualifying characteristics without a technological link. Directions for improving judicial practice and criminal legislation are substantiated.

Keywords: cybercrimes, artificial intelligence, criminal classification, computer information, malware, deepfakes, phishing, digital footprints, causality, case law.

Введение

Распространение генеративных моделей искусственного интеллекта и инструментов синтетических медиа обусловило качественную трансформацию киберпреступности: повышается эффективность социальной инженерии, упрощается имитация личности (голос, изображение, цифровая идентичность), ускоряется разработка и модификация вредоносного кода, автоматизируется подбор уязвимостей и персонализация атак [7]. Алгоритмы машинного обучения позволяют злоумышленникам масштабировать противоправную деятельность при относительно низких транзакционных издержках, формировать фишинговые сообщения с учетом психолингвистического профиля адресата, генерировать дипфейк-контент для обхода биометрических механизмов аутентификации, а также оптимизировать сценарии обхода систем обнаружения вторжений. Такие процессы усиливают нагрузку на уголовно-правовые механизмы противодействия и требуют устойчивой практики квалификации деяний, совершаемых с использованием электронных или информационно-телекоммуникационных сетей [2].

В научной литературе отмечается, что искусственный интеллект становится значимым фактором усложнения как механизма совершения преступлений, так и их уголовно-правовой оценки. При этом сохраняется необходимость применения традиционной конструкции состава преступления, включающей объект, объективную сторону, субъект и субъективную сторону. Вместе с тем возникает потребность уточнения роли ИИ в механизме преступления и его влияния на квалификацию деяния.

Особую актуальность приобретает вопрос: может ли искусственный интеллект рассматриваться как способ совершения преступления либо он выступает исключительно средством? Данный аспект имеет принципиальное значение для корректной уголовно-правовой оценки.

Исследование основано на формально-юридическом, системном и сравнительно-правовом методах. Использованы нормы уголовного законодательства Российской Федерации [1], разъяснения Верховного Суда РФ [2], а также положения научных трудов, включая монографические исследования: Шутова А.А. [13]; Мосечкин И.Н. [14]; Бойко Т.К. [15].

Основные результаты

Киберпреступления с использованием ИИ целесообразно описывать через функцию ИИ в механизме посягательства: автоматизация подготовки (сбор и агрегация персональных данных из открытых источников, корреляция утечек, подбор уязвимостей), реализация воздействия (генерация контента для обмана, конструирование и модификация вредоносного кода, управление бот-сетями, оптимизация сценариев атак), сокрытие следов (обфускация, полиморфизм, генерация правдоподобных «легенд» общения, имитация нормальной сетевой активности). Такой функциональный подход позволяет избежать избыточной технологической детализации и сосредоточиться на юридически значимых признаках деяния. Отметим, что в уголовно-правовом смысле ИИ, как правило, выступает средством совершения преступления, а не самостоятельным объектом посягательства; что особенно заметно в составах гл. 28 УК РФ — неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ (ст. 273), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274) [1]. При этом технологическая сложность инструмента не трансформирует структуру состава, а влияет на характеристику способа и на оценку степени общественной опасности.

При квалификации по ст. 272 УК РФ необходимо установить неправомерность доступа, наличие режима охраны информации, наступившие последствия (либо реальную угрозу их причинения — в зависимости от конструкции состава) и причинную связь. Пленум № 37 ориентирует суды на конкретизацию используемых устройств и программ, а при необходимости — на привлечение специалистов для оценки технических аспектов [2]. В «ИИ-контексте» автономность инструмента не исключает необходимости доказывать управленческое решение лица о запуске модели, выборе цели, параметров и объекта воздействия. Следовательно, использование ИИ для автоматизированного перебора паролей, сканирования периметра сети или подбора эксплойтов оценивается по общим правилам стадий преступления: при отсутствии фактического доступа — как приготовление или покушение, при преодолении защиты и извлечении сведений — как оконченное деяние. Существенное значение имеет установление осведомленности лица о незаконности доступа и охраняемости информации, что подтверждается совокупностью цифровых следов (лог-файлы, настройки модели, сценарии запуска, переписка о целях атаки).

Квалификация по ст. 273 УК РФ осложняется «двойным назначением» кода, создаваемого или модифицируемого ИИ: многие фрагменты могут быть нейтральными вне конкретного сценария и обладать исследовательской либо тестовой функцией. Решающее значение имеет функциональная пригодность программы к несанкционированному уничтожению, блокированию, модификации, копированию информации либо нейтрализации средств защиты, а также направленность умысла на такое использование. Объективная сторона выражается не в самом факте генерации кода, а в создании, использовании или распространении программы, обладающей вредоносными свойствами и предназначенной для противоправного воздействия. В противном случае криминализация «генерации кода» как таковой нарушала бы принцип вины и законности, поскольку источник кода не равнозначен его преступному применению [6, С. 47–51]. В условиях ИИ-автоматизации особое внимание уделяется установлению роли лица в выборе архитектуры, параметров и источников данных, а также в принятии решения о распространении или внедрении вредоносного функционала.

Использование ИИ для обмана (ИИ-фишинг, голосовая подмена, deepfake-видео) чаще затрагивает отношения собственности либо личные нематериальные блага; в таких случаях основным является состав мошенничества, вымогательства, клеветы и иных преступлений, а цифровой компонент учитывается через квалифицирующие признаки использования электронных или информационно-телекоммуникационных сетей и при характеристике способа [2], [12, С. 38–41]. Deepfake в доктрине обоснованно рассматривается как технологически нейтральный способ совершения различных преступлений, поскольку одна и та же модель синтетической генерации может обслуживать разные объекты посягательства — от имущественных до посягательств на честь и достоинство [6, С. 47–51], [11, С. 387–390]. При этом, необходимо отметить, что повышенная убедительность синтетического контента способна усиливать общественную опасность деяния, что должно учитываться судом при индивидуализации наказания.

Использование искусственного интеллекта в киберпреступлениях требует четкого разграничения его роли в механизме преступления. Представляется обоснованным исходить из того, что ИИ не может одновременно являться и способом, и средством совершения преступления.

В уголовно-правовом смысле способ преступления представляет собой совокупность действий (бездействия), посредством которых осуществляется посягательство. Искусственный интеллект не формирует такую совокупность действий самостоятельно, а применяется субъектом преступления как инструмент реализации преступного замысла. Следовательно, ИИ следует рассматривать преимущественно как средство совершения преступления, влияющее на характеристики способа, но не заменяющее его.

Данное положение может быть квалифицировано как элемент научной новизны настоящего исследования, поскольку в ряде работ допускается смешение указанных категорий.

Функциональная роль ИИ проявляется в трех основных направлениях:

- автоматизация подготовки преступления (сбор данных, анализ уязвимостей);

- реализация противоправного воздействия (генерация контента, управление атаками);
- сокрытие следов (обфускация, имитация поведения пользователя).

Такой функциональный подход позволяет избежать избыточной технологизации уголовно-правовых норм и сосредоточиться на юридически значимых признаках деяния.

При квалификации преступлений, предусмотренных ст. 272 УК РФ, ключевое значение имеет установление неправомерности доступа, режима охраны информации и причинной связи. Использование ИИ для автоматизированного подбора паролей или эксплуатации уязвимостей не изменяет юридическую природу деяния, а лишь усложняет процесс доказывания.

В рамках ст. 273 УК РФ особое значение приобретает проблема «двойного назначения» программного обеспечения. Как справедливо отмечает И.Н. Мосечкин, уголовная ответственность должна наступать не за сам факт создания программного продукта, а за его противоправную направленность и использование [14].

Аналогичная позиция прослеживается и в исследованиях Т.К. Бойко, подчеркивающей необходимость разграничения легитимных и противоправных форм использования технологий искусственного интеллекта [15].

Использование ИИ в целях обмана (deepfake, голосовая подмена, фишинг) чаще всего образует составы преступлений против собственности или личности. В таких случаях технологии ИИ выступают средством совершения преступления, а квалификация осуществляется по основному составу (например, мошенничество), с учетом способа совершения деяния [2].

Особого внимания требует вопрос конкуренции норм. Если неправомерный доступ к компьютерной информации причиняет самостоятельный вред, возможна совокупность преступлений. В противном случае он рассматривается как способ совершения основного преступления.

Доказывание по делам данной категории осложняется необходимостью анализа цифровых следов, алгоритмических процессов и параметров работы ИИ-систем. Как отмечает А.А. Шутова, развитие технологий требует адаптации доказательственных стандартов без отказа от принципов уголовного права [13].

Обсуждение

Научная дискуссия о роли искусственного интеллекта в уголовном праве свидетельствует о необходимости отказа от технологически ориентированных формулировок в пользу функционального подхода.

Представляется, что закрепление ИИ как самостоятельного квалифицирующего признака нецелесообразно ввиду быстрого устаревания технологий и риска неопределенности правоприменения. Более устойчивым является подход, при котором учитывается не сама технология, а характер причиненного вреда и способ его достижения.

В этой связи предлагается:

- развивать судебные разъяснения по вопросам квалификации преступлений с использованием ИИ;
- уточнить подходы к оценке цифровых доказательств;
- обеспечить единообразие практики применения норм гл. 28 УК РФ.

Заключение

Искусственный интеллект в механизме киберпреступления следует рассматривать преимущественно как средство его совершения, влияющее на способ, но не подменяющее его.

Научная новизна исследования заключается в:

- разграничении категорий «средство» и «способ» применительно к ИИ;
- разработке функционального подхода к оценке роли ИИ;
- обосновании отказа от технологически обусловленных квалифицирующих признаков.

Перспективы развития уголовного законодательства связаны с уточнением критериев квалификации и совершенствованием судебной практики без избыточной криминализации технологической деятельности.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: федер. закон: [от 13 июня 1996 г. № 63-ФЗ (ред. действующая)]. — URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 18.02.2026).

2. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 дек. 2022 г. № 37. — URL: https://rg.ru/documents/2022/12/28/document-postanovlenie-plenuma-verkhovnogo-suda.html (дата обращения: 18.02.2026).

3. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. действующая). — URL: https://priemnaya.duma.gov.ru/ru/info/inf/fz149/ (дата обращения: 18.02.2026).

4. Российская Федерация. Законы. О персональных данных: федер. закон: [от 27 июля 2006 г. № 152-ФЗ (ред. действующая)]. — URL: https://priemnaya.duma.gov.ru/ru/info/inf/fz/ (дата обращения: 18.02.2026).

5. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон: [от 26 июля 2017 г. № 187-ФЗ (ред. действующая)]. — URL: https://publication.pravo.gov.ru/document/view/0001201707260023 (дата обращения: 18.02.2026).

6. Светанков Д.Ю. Социально-правовая обусловленность формирования механизма уголовно-правового противодействия преступлениям, совершенным с использованием технологии deepfake / Д.Ю. Светанков // Российский следователь. — 2025. — № 6. — С. 47–51. — DOI: 10.18572/1812-3783-2025-6-47-51. — URL: https://lawinfo.ru/en/articles/10579/ (дата обращения: 18.02.2026).

7. The impact of Large Language Models on Law Enforcement: Tech Watch Flash Report / Europol Innovation Lab. — 2023. — DOI: 10.2813/255453.

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). — URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 18.02.2026).

9. Artificial Intelligence Risk Management Framework (AI RMF 1.0) / National Institute of Standards and Technology. — 2023. — DOI: 10.6028/NIST.AI.100-1.

10. Information technology — Artificial intelligence — Guidance on risk management: ISO/IEC 23894:2023. — Geneva: International Organization for Standardization, 2023. — URL: https://www.iso.org/standard/77304.html (accessed: 18.02.2026).

11. Морозов В.И. Уголовно-правовая оценка использования «дипфейка» при совершении преступлений / В.И. Морозов, С.Г. Лосев // Право в эпоху искусственного интеллекта: перспективные вызовы и современные задачи: сб. науч. ст. по материалам VI Сибирских правовых чтений (Тюмень, 17–19 октября 2024 г.). — Тюмень: ТюмГУ-Press, 2024. — С. 387–390. — URL: https://elib.utmn.ru/jspui/handle/ru-tsu/36994 (дата обращения: 18.02.2026).

12. Кудашкин Д.А. Кибербезопасность и правовая защита информации от угроз искусственного интеллекта / Д.А. Кудашкин // Юрист. — 2025. — № 3. — С. 38–41. — DOI: 10.18572/1812-3929-2025-3-38-41. — URL: https://lawinfo.ru/articles/9724/ (дата обращения: 18.02.2026).

13. Шутова А.А. Уголовно-правовая охрана создания и применения технологий искусственного интеллекта в здравоохранении / А.А. Шутова. — Москва: Проспект, 2025. — 127 с.

14. Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования / И.Н. Мосечкин. — Киров: Вятский государственный университет, 2020. — 111 с.

15. Бойко Т.К. Искусственный интеллект как объект уголовно-правового исследования / Т.К. Бойко. — Тула: Тульский институт (филиал) ВГУЮ, 2024. — 95 с.

Список литературы на английском языке / References in English

1. Rossiiskaya Federatsiya. Zakoni. Ugolovnii kodeks Rossiiskoi Federatsii [Russian Federation. Laws. Criminal Code of the Russian Federation]: Federal Law: [of June 13, 1996, No. 63-FZ]. — URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed: 18.02.2026). [in Russian]

2. O nekotoryh voprosah sudebnoj praktiki po ugolovnym delam o prestupleniyah v sfere komp'yuternoj informacii, a takzhe inyh prestupleniyah, sovershennyh s ispol'zovaniem elektronnyh ili informacionno-telekommunikacionnyh setej, vklyuchaya set' «Internet» [On Certain Issues of Judicial Practice in Criminal Cases Concerning Crimes in the Sphere of Computer Information, as well as Other Crimes Committed Using Electronic or Information and Telecommunications Networks, Including the Internet]: Resolution of the Plenum of the Supreme Court of the Russian Federation of December 15, 2022, No. 37. — URL: https://rg.ru/documents/2022/12/28/document-postanovlenie-plenuma-verkhovnogo-suda.html (accessed: 18.02.2026). [in Russian]

3. Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii [Russian Federation. Laws. On Information, Information Technology, and Information Protection]: Federal Law: [of July 27, 2006, No. 149-FZ (current version)]. — URL: https://priemnaya.duma.gov.ru/ru/info/inf/fz149/ (accessed: 18.02.2026). [in Russian]

4. Rossiiskaya Federatsiya. Zakoni. O personalnikh dannikh [Russian Federation. Laws. On personal data]: Federal Law: [of July 27, 2006, No. 152-FZ (current version)]. — URL: https://priemnaya.duma.gov.ru/ru/info/inf/fz/ (accessed: 18.02.2026). [in Russian]

5. Rossiiskaya Federatsiya. Zakoni. O bezopasnosti kriticheskoi informatsionnoi infrastrukturi Rossiiskoi Federatsii [Russian Federation. Laws. On the Security of Critical Information Infrastructure of the Russian Federation]: Federal Law: [of July 26, 2017 No. 187-FZ (current version)]. — URL: https://publication.pravo.gov.ru/document/view/0001201707260023 (accessed: 18.02.2026). [in Russian]

6. Svetankov D.Yu. Social'no-pravovaya obuslovlennost' formirovaniya mekhanizma ugolovno-pravovogo protivodejstviya prestupleniyam, sovershennym s ispol'zovaniem tekhnologii deepfake [Social and legal conditions for the formation of a mechanism for criminal-legal counteraction to crimes committed using deepfake technology] / D.Yu. Svetankov // Rossijskij sledovatel' [Russian investigator]. — 2025. — № 6. — P. 47–51. — DOI: 10.18572/1812-3783-2025-6-47-51. — URL: https://lawinfo.ru/en/articles/10579/ (accessed: 18.02.2026). [in Russian]

7. The impact of Large Language Models on Law Enforcement: Tech Watch Flash Report / Europol Innovation Lab. — 2023. — DOI: 10.2813/255453.

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). — URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed: 18.02.2026).

9. Artificial Intelligence Risk Management Framework (AI RMF 1.0) / National Institute of Standards and Technology. — 2023. — DOI: 10.6028/NIST.AI.100-1.

10. Information technology — Artificial intelligence — Guidance on risk management: ISO/IEC 23894:2023. — Geneva: International Organization for Standardization, 2023. — URL: https://www.iso.org/standard/77304.html (accessed: 18.02.2026).

11. Morozov V.I. Ugolovno-pravovaya ocenka ispol'zovaniya «dipfejka» pri sovershenii prestuplenij [Criminal-legal assessment of the use of "deepfake" in the commission of crimes] / V.I. Morozov, S.G. Losev // Pravo v epohu iskusstvennogo intellekta: perspektivnye vyzovy i sovremennye zadachi [Law in the era of artificial intelligence: promising challenges and modern tasks]: collection of scientific articles based on the materials of the VI Siberian Legal Readings (Tyumen, October 17–19, 2024). — Tyumen: Tyumen State University-Press, 2024. — P. 387–390. — URL: https://elib.utmn.ru/jspui/handle/ru-tsu/36994 (accessed: 18.02.2026). [in Russian]

12. Kudashkin D.A. kiberbezopasnost' i pravovaya zashchita informacii ot ugroz iskusstvennogo intellekta [Cybersecurity and Legal Protection of Information from Artificial Intelligence Threats] / D.A. Kudashkin // Jurist [Lawyer]. — 2025. — № 3. — P. 38–41. — DOI: 10.18572/1812-3929-2025-3-38-41. — URL: https://lawinfo.ru/articles/9724/ (accessed: 18.02.2026). [in Russian]

13. Shutova A.A. Ugolovno-pravovaya ohrana sozdaniya i primeneniya tekhnologij iskusstvennogo intellekta v zdravoohranenii [Criminal-legal protection of the creation and application of artificial intelligence technologies in healthcare] / A.A. Shutova. — Moscow: Prospect, 2025. — 127 p. [in Russian]

14. Mosechkin I.N. Iskusstvennyj intellekt v ugolovnom prave: perspektivy sovershenstvovaniya ohrany i regulirovaniya [Artificial intelligence in criminal law: prospects for improving protection and regulation] / I.N. Mosechkin. — Kirov: Vyatka State University, 2020. — 111 p. [in Russian]

15. Boyko T.K. Iskusstvennyj intellekt kak ob"ekt ugolovno-pravovogo issledovaniya [Artificial intelligence as an object of criminal-law research] / T.K. Boyko. — Tula: Tula Institute (branch) of VSUYU, 2024. — 95 p. [in Russian]