Дата поступления рукописи в редакцию: 17.09.2026 г. **DOI: 10.24412/3033-6775-2026-3-117-120**
Дата принятия рукописи в печать: 28.09.2026 г.

МАНСУРОВ Даниэль Рамилевич,
студент, Автономная некоммерческая профессиональная образовательная организация «Башкирский кооперативный техникум»,
e-mail: Daniael.13579@gmail.com

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ

Аннотация. *Статья посвящена анализу правового регулирования противодействия преступлениям, совершаемым с применением цифровых технологий и систем искусственного интеллекта. Установлено, что киберпреступность в 2023–2025 гг. занимала существенную долю в общей структуре зарегистрированной преступности. Рассмотрены действующие нормы российского законодательства и организационные решения государства, включая учреждение специализированного подразделения МВД России и принятие в 2025 году закона о государственной информационной системе противодействия соответствующим правонарушениям. На основании доктринальных источников, статистики и разъяснений Верховного Суда РФ обосновывается вывод о необходимости уточнения понятийного аппарата, внедрения риск-ориентированной модели регулирования и укрепления межведомственного взаимодействия. Сформулированы предложения по корректировке уголовного, административного, информационного и процессуального законодательства.*

Ключевые слова: *цифровые технологии; искусственный интеллект; киберпреступность; электронные доказательства; уголовно-процессуальное доказывание; УБК МВД России; риск-ориентированное регулирование; цифровая безопасность.*

MANSUROV Daniel Ramilevich,
student, Autonomous Non-Commercial Professional Educational Organization «Bashkir Cooperative Technical School»

LEGAL REGULATION OF COUNTERACTION TO CRIME USING DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE: PROBLEMS AND DIRECTIONS FOR IMPROVEMENT

Annotation. *The article analyzes the legal regulation of counteraction to crimes committed using digital technologies and artificial intelligence systems. Cybercrime in 2023–2025 occupied a substantial share of registered crime. The author examines Russian legislation and organizational measures, including the establishment of a specialized unit within the Ministry of Internal Affairs and the adoption in 2025 of a law on a state information system for counteracting such offenses. Based on doctrinal sources, statistics and Supreme Court clarifications, the article substantiates the need to clarify the conceptual apparatus, introduce a risk-based model and strengthen interagency cooperation. Proposals for amending criminal, administrative, informational and procedural legislation are formulated.*

Key words: *digital technologies; artificial intelligence; cybercrime; electronic evidence; criminal procedural proof; Cybercrime Combating Unit of the Ministry of Internal Affairs; risk-based regulation; digital security.*

Введение

Криминальная среда современной России претерпевает трансформацию, обусловленную проникновением цифровых технологий в противоправную деятельность. Посягательства, совершаемые с применением информационно-телекоммуникационных технологий, утратили характер эпизодического явления, а их удельный вес в структуре зарегистрированных деяний неуклонно возрастает. Актуальность исследования обусловлена переходом от единичных

компьютерных посягательств к системному использованию искусственного интеллекта на всех стадиях преступной деятельности, что ставит перед правоприменителем задачи, лишённые устоявшегося нормативного разрешения.

Объектом исследования выступают общественные отношения в сфере правового регулирования противодействия цифровой преступности. Предметом – нормы уголовного, уголовно-процессуального, административного и информационного законодательства Российской Федерации, доктринальные позиции и разъяснения высших судебных инстанций. Цель работы состоит в выявлении проблемных аспектов действующего регулирования и формулировании предложений по его совершенствованию. Задачи исследования включают анализ статистической динамики киберпреступности за 2019–2025 гг., оценку организационных и нормативных мер государства, рассмотрение доктринальной дискуссии о правовой природе электронных доказательств, изучение конкурирующих позиций о допустимости применения искусственного интеллекта в доказывании и формулирование направлений совершенствования законодательства de lege ferenda.

Методологическую основу составляют методы анализа и синтеза, а также формально-юридический, сравнительно-правовой методы и метод анализа судебной практики. Нормативную базу образуют УПК РФ, Федеральный закон от 01.04.2025 № 41-ФЗ, Указ Президента РФ от 10.10.2019 № 490, постановления Пленума Верховного Суда РФ от 26.12.2017 № 57, от 23.04.2019 № 10 и от 15.12.2022 № 37.

Основная часть

Согласно сведениям МВД России, в 2019 году зарегистрировано 294,4 тыс. преступлений с использованием информационно-телекоммуникационных технологий [1]; к 2024 году показатель возрос до 765 тыс., составив около 40% от общего массива правонарушений [2]. В первом полугодии 2025 года удельный вес дистанционных посягательств сохраняет высокий уровень, а преобладающим инструментом выступают мессенджеры [3]. Почти двукратный рост показателя за пять лет при неизменной доле в структуре преступности свидетельствует об устойчивом структурном изменении криминогенной обстановки, требующем системного правового реагирования.

Реакция государства охватывает организационное и нормативное направления. В структуре МВД России сформировано специализированное подразделение по противодействию противоправному применению информационно-телекоммуникационных технологий (УБК МВД России), а в апреле 2025 года принят Федеральный закон № 41-ФЗ [2], предусмотревший правовую основу для государственной информационной системы в данной сфере. Вместе с тем действующие акты – УК РФ, УПК РФ, Федеральный закон об информации – охватывают отдельные сегменты цифрового пространства, не образуя целостного механизма: организационная реформа опередила нормативную, что порождает разрыв между институциональными возможностями и правовыми основаниями их реализации.

Понятийная неопределённость остаётся острой проблемой доктрины: законодательство не закрепляет дефиниций категорий «электронные доказательства», «электронный документ», «электронный носитель», что, по наблюдению Ю. И. Андреевой, влечёт коллизии в правоприменении [4, с. 147]. На процессуальные сложности верификации цифровых данных указывает В. В. Долгаев [5, с. 177]. Разъяснения Верховного Суда РФ частично компенсируют пробел: Пленум в постановлении от 26.12.2017 № 57 определил электронный документ как созданный в электронной форме и подписанный электронной подписью [6], однако оставил за рамками регулирования переписку в мессенджерах, метаданные и журналы серверных операций.

В доктрине не сложилось единой позиции о том, подлежат ли электронные доказательства выделению в самостоятельную категорию либо квалифицируются как иные документы по ст. 84 УПК РФ [7]. Судебная практика частично восполняет спор: Пленум Верховного Суда РФ в постановлении от 23.04.2019 № 10 признал скриншоты допустимыми доказательствами при указании адреса источника и времени получения [8, абз. 2 п. 55] – логика, заслуживающая распространения на уголовный процесс. Постановление Пленума от 15.12.2022 № 37 [9] подтверждает самостоятельное процессуальное значение электронных носителей информации, что говорит о движении практики к признанию электронных доказательств

автономной категорией без законодательного закрепления такой позиции.

Дискуссионным остаётся вопрос о допустимости использования искусственного интеллекта в доказывании. Согласно Национальной стратегии развития искусственного интеллекта до 2030 года, под ним понимается совокупность программных средств, воспроизводящих когнитивные функции человека [10]. В. А. Биляев, Н. В. Сошина и А. С. Климовский констатируют принципиальную неразрешимость вопроса о субъектности ИИ в процессуальных решениях [11, с. 594]: такие решения должны приниматься человеком на основе внутреннего убеждения. С. Б. Россинский предлагает не исключать ИИ из процесса, а квалифицировать его результаты как «иные документы» по ст. 84 УПК РФ либо, при наличии специальных знаний в модели, как заключение эксперта по аналогии со ст. 80 УПК РФ [12]. Обе позиции сходятся в требовании обязательной верификации выводов ИИ человеком, расходясь лишь в способе процессуального оформления; второй подход представляется более практичным, поскольку не требует создания новых институтов.

Реактивная модель противодействия цифровой преступности исчерпала потенциал: необходим переход к риск-ориентированному регулированию – рамочному акту, выстраивающему иерархию категорий от электронных данных до статуса систем искусственного интеллекта с унифицированными стандартами работы с цифровыми следами. Квалифицирующие признаки, связанные с ИИ и дипфейками, целесообразно вводить точечно – только там, где технологии объективно повышают общественную опасность деяния, избегая избыточной криминализации. Процессуальная составляющая не менее значима, чем материально-правовая: без механизма, обеспечивающего достоверность цифровых доказательств и соблюдение права на неприкосновенность частной жизни, эффективное противодействие технологическим вызовам недостижимо.

Заключение

Проведённый анализ показывает, что действующее регулирование характеризуется опережением организационных мер над нормативными: институциональные решения не подкреплены систематизацией понятийного аппарата на уровне закона. Полагаем обоснованным закрепление в федеральном законе дефиниций электронных доказательств, документа и носителя с распространением на уголовный процесс подхода Пленума Верховного Суда РФ – обязательной фиксации источника и времени получения сведений. Применительно к ИИ в доказывании предпочтителен процессуально-инструментальный подход с квалификацией результатов как «иных документов» или заключения эксперта при обязательной верификации человеком. Квалифицирующие признаки, связанные с ИИ и дипфейками, целесообразно вводить лишь при объективном повышении общественной опасности деяния. Дальнейшая систематизация законодательства должна строиться на риск-ориентированной модели, обеспечивающей баланс между эффективностью противодействия цифровой преступности и защитой конституционных прав граждан.

Список литературы:

[1] Состояние преступности в России за январь-декабрь 2019 года // МВД ФКУ «ГИАЦ». URL: https://opis-cdn.tinkoffjournal.ru/mercury/sostoyanie_prestupnosti_yanvary-dekabry_2019.pdf (дата обращения: 15.04.2026).

[2] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий: Федеральный закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) // Официальный интернет-портал правовой информации. (дата обращения: 15.04.2026).

[3] МВД России публикует статистическую информацию о состоянии преступности в РФ за первое полугодие 2025 года // Пресс-центр МВД России. URL: https://mvdmedia.ru (дата обращения: 15.04.2026).

[4] Андреева Ю. И. Электронные доказательства в уголовном процессе // Закон и право. 2025. № 8. С. 147–152.

[5] Долгаев В. В. Роль электронных доказательств в уголовном судопроизводстве // Государственная служба и кадры. 2025. № 1. С. 177–181.

[6] О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде: постановление Пленума Верховного Суда РФ от 26.12.2017 № 57.

[7] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №

174-ФЗ (ред. от 08.03.2026) // Официальный интернет-портал правовой информации.

[8] О применении части четвёртой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 23.04.2019 № 10.

[9] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37.

[10] О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) // СПС «КонсультантПлюс».

[11] Биляев В. А., Сошина Н. В., Климовский А. С. О перспективе применения искусственного интеллекта в доказывании по уголовным делам // Право и государство: теория и практика. 2025. № 6. С. 592–594.

[12] Россинский С. Б. Искусственный интеллект как субъект и инструмент в уголовном процессе: доктринальный подход // Lawinfo.ru. 2026.

References:

[1] Crime Situation in Russia, January–December 2019 // Ministry of Internal Affairs (MVD), Main Information and Analytical Center (GIATS). URL: https://opis-cdn.tinkoffjournal.ru/mercury/sostoyanie_prestupnosti_yanvary-dekabry_2019.pdf (accessed: April 15, 2026).

[2] On the Creation of a State Information System for Countering Offenses Committed Using Information and Communication Technologies: Federal Law No. 41-FZ dated April 1, 2025 (as amended on July 31, 2025) // Official Internet Portal of Legal Information. (accessed: April 15, 2026).

[3] Ministry of Internal Affairs of Russia Publishes Statistical Data on the Crime Situation in the Russian Federation for the First Half of 2025 // Press Center of the Ministry of Internal Affairs of Russia. URL: https://mvdmedia.ru (accessed: April 15, 2026).

[4] Andreeva Yu. I. Electronic Evidence in Criminal Proceedings // Law and Right. 2025. No. 8. P. 147–152.

[5] Dolgaev V. V. The Role of Electronic Evidence in Criminal Proceedings // Civil Service and Personnel. 2025. No. 1. P. 177–181. [6] On Certain Issues Regarding the Application of Legislation Governing the Use of Electronic Documents: Resolution of the Plenum of the Supreme Court of the Russian Federation No. 57 dated December 26, 2017.

[7] Criminal Procedure Code of the Russian Federation No. 174-FZ dated December 18, 2001 (as amended on March 8, 2026) // Official Internet Portal of Legal Information.

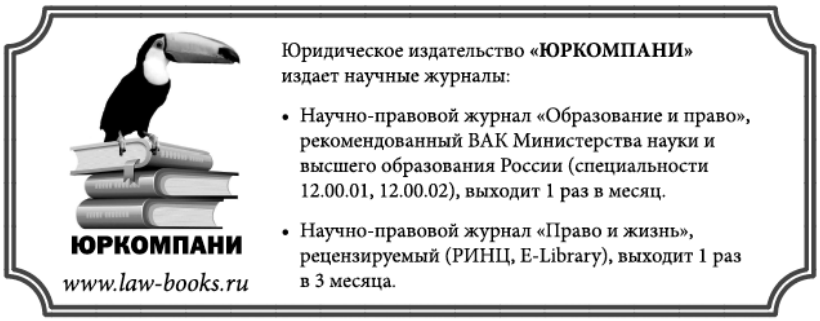
[8] On the Application of Part Four of the Civil Code of the Russian Federation: Resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 dated April 23, 2019.

[9] On Certain Issues of Judicial Practice in Criminal Cases Involving Crimes in the Sphere of Computer Information: Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 dated December 15, 2022.

[10] On the Development of Artificial Intelligence in the Russian Federation: Decree of the President of the Russian Federation No. 490 dated October 10, 2019 (as amended on February 15, 2024) // ConsultantPlus Legal Reference System.

[11] Bilyaev V. A., Soshina N. V., Klimovsky A. S. On the Prospects of Using Artificial Intelligence in the Evidentiary Process in Criminal Cases // Law and State: Theory and Practice. 2025. No. 6. Pp. 592–594.

[12] Rossinsky S. B. Artificial Intelligence as a Subject and Tool in Criminal Proceedings: A Doctrinal Approach // Lawinfo.ru. 2026.



Юридическое издательство **«ЮРКОМПАНИ»** издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.