

Дата поступления рукописи в редакцию: 20.05.2026 г.

DOI: 10.24412/2782-3830-2026-6-322-326

Дата принятия рукописи в печать: 02.07.2026 г.

БУРХАНОВА Софья Давуровна,

документовед группы документационного
обеспечения и осуществления контроля
Восточно-Сибирского института МВД России,
e-mail: honeyymilk@yandex.ru

МИСНИК Ирина Владиславовна,

к.ю.н., доцент, доцент кафедры гражданского,
административного и уголовного судопроизводства
Восточно-Сибирского филиала Российского государственного
университета правосудия имени В.М.Лебедева»,
e-mail: iramis@yandex.ru

ЦИФРОВИЗАЦИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. Статья посвящена анализу цифровизации уголовного судопроизводства в России, которая прошла путь от фрагментарной компьютеризации отдельных задач до попыток системной трансформации процессуальных форм. Автор характеризует современное состояние как «лоскутную цифровизацию», то есть внедрение технологий в отдельные процедуры без изменения общей логики процесса. На досудебной стадии рассматриваются электронный документооборот, методы киберкриминалистики, программные комплексы «Атлант» и «КСБ», а также единая информационно-телекоммуникационная система органов внутренних дел. Отмечается, что механизмы подачи электронных заявлений о преступлениях в настоящее время не соответствуют уголовно-процессуальному законодательству, что требует внесения изменений в статьи 141, 142 и 144 Уголовно-процессуального кодекса Российской Федерации. На судебной стадии анализируется применение видеоконференцсвязи и электронного судопроизводства, а также проблема автоматической компиляции судебных актов, которая снижает качество мотивировочной части и подрывает авторитет судебной власти. Исследуются изменения уголовного законодательства 2025–2026 годов, включая ужесточение ответственности за кибератаки на критическую информационную инфраструктуру по статье 274.1 УК РФ с заменой оценочного понятия вреда на конкретный перечень последствий, введение так называемой «кибер-амнистии», а также новую статью 272.1 УК РФ об обороте персональных данных. Выявляются риски предвзятости алгоритмов искусственного интеллекта на примере американской системы COMPAS, недостаток цифровой компетентности юристов, угрозы неприкосновенности частной жизни. В заключении обосновывается необходимость перехода к стратегическому проектированию цифрового уголовного процесса на основе конституционных принципов состязательности и защиты прав личности.

Ключевые слова: цифровизация, уголовный процесс, информационные технологии, критическая информационная инфраструктура (КИИ), искусственный интеллект (ИИ), электронное правосудие, доказательства, права человека.

BURKHANOVA Sofia Davurovna,

Documentation Specialist,
Documentation Support and Control Group
East Siberian Institute MVD of Russia

MISNIK Irina Vladislavovna,

PhD in Law, Associate Professor,
Associate Professor of the Department of Civil,
Administrative, and Criminal Procedure,
V.M. Lebedev Russian State University of Justice

DIGITIZATION IN CRIMINAL LEGAL PROCEEDINGS

Annotation. This article analyzes the digitalization of criminal proceedings in Russia, which has evolved from fragmented computerization of individual tasks to attempts at systemic transformation of procedural forms. The author characterizes the current state as “patchwork digitalization,” that is, the introduction of technologies into individual procedures without changing the overall logic of the process. At the pre-trial stage, electronic document management, cyberforensics methods, the Atlant and KSB software systems, and the unified information and telecommunications system of internal affairs agencies are being examined. It is noted that the mechanisms for filing electronic crime reports are currently inconsistent with the criminal procedure context, necessitating amendments to Articles 141, 142, and 144 of the Criminal Procedure Code of the Russian Federation. At the trial stage, the use of videoconferencing and electronic legal proceedings is being analyzed, as well as the problem of automatic compilation of judicial decisions, which reduces the quality of reasoning and undermines the authority of the judiciary. This article examines changes to criminal legislation for 2025–2026, including increased penalties for cyberattacks on critical information infrastructure under Article 274.1 of the Russian Criminal Code, replacing the evaluative concept of harm with a specific list of consequences, the introduction of a so-called “cyber amnesty,” and the new Article 272.1 of the Russian Criminal Code on the circulation of personal data. The article identifies the risks of bias in artificial intelligence algorithms, using the example of the American COMPAS system, the lack of digital competence among lawyers, and threats to privacy. The article concludes by substantiating the need for a transition to strategic design of digital criminal proceedings based on constitutional principles of adversarial proceedings and the protection of individual rights.

Key words: digitalization, criminal procedure, information technology, critical information infrastructure (CII), artificial intelligence (AI), e-justice, evidence, human rights.

Цифровизация уголовного судопроизводства в России прошла путь от фрагментарной компьютеризации отдельных задач к попыткам системной трансформации процессуальных форм. Начальный этап цифровизации уголовного процесса характеризовался использованием компьютерных технологий в качестве вспомогательных средств (набор текстов, ведение электронных картотек). Базы данных применялись для хранения информации без изменения процессуальных процедур.

На современном этапе информационные технологии внедряются на всех стадиях уголовного судопроизводства: от регистрации сообщения о преступлении до постановления приговора, а затем и обжалования. В доктрине данное обстоятельство рассматривается как основание для выделения элементов «цифровой процессуальной формы», при этом формирование целостной системы не завершено.

В досудебном производстве цифровизация реализуется в нескольких направлениях. Электронный документооборот замещает бумажные носители, что упрощает хранение материалов уголовного дела, их обработку, передачу между следователями и из органов предварительного расследования в суд. Следствием выступает повышение оперативности процессуальных действий и снижение рисков утраты либо повреждения документов. Наряду с этим в расследовании активно применяются методы киберкриминалистики: анализ цифровых следов, метаданных, данных с видеокамер. Указанные методы приоб-

ретают ключевое значение при расследовании преступлений, совершаемых в условиях высокого уровня цифровизации.

Разрабатываются и модернизируются программные продукты, автоматизирующие процессуальные действия, преимущественно на стадии возбуждения уголовного дела. К их числу относятся: программный комплекс «Атлант» (автоматизация делопроизводства в органах внутренних дел — регистрация заявлений, ведение журналов учёта, формирование статистики); ПК «КСБ» (криминалистическое сопровождение безопасности) — для работы с цифровыми следами и изъятия информации с носителей. Единая информационно-телекоммуникационная система (ЕИТКС) органов внутренних дел обеспечивает сквозной электронный документооборот и межподразделенческое взаимодействие, ускоряя передачу материалов.

В научной литературе отмечается несоответствие механизма подачи заявлений о преступлениях в электронной форме уголовно-процессуальному закону, что требует внесения изменений в ст. 141, 142 и 144 Уголовно-процессуального кодекса Российской Федерации. В частности, необходимо разработать более детальные требования к оформлению электронных заявлений.

На судебных стадиях цифровизация реализуется в нескольких формах. Следует отметить, что дистанционное участие путем использования видеоконференц-связи (ВКС) разрешено уже на досудебной стадии — статья 189.1 УПК РФ. В судебных инстанциях ВКС также применяется,

что способствует процессуальной экономии. В ст. 241.1 УПК РФ закреплена возможность участия подсудимого в судебном заседании с использованием ВКС, за исключением рассмотрения уголовных дел с участием присяжных заседателей. Общей статистики по применению ВКС в уголовных делах в открытом доступе нет. На сайте Судебного департамента при Верховном суде, например, данные разрозненные или отсутствуют.

С 2026 года в рамках сервиса «Правосудие онлайн» и «Подача документов в суд в электронном виде» на Едином портале государственных услуг реализована возможность направления в суды общей юрисдикции и мировым судьям процессуальных документов, предусмотренных Уголовно-процессуальным кодексом РФ (ходатайств, жалоб, возражений, заявлений и др.) [11]. Доступ к сервису предоставляется совершеннолетним гражданам, имеющим подтверждённую учётную запись в ЕСИА и усиленную квалифицированную электронную подпись; допускается подача документов как от своего имени, так и в качестве представителя другого лица. Данный механизм направлен на сокращение сроков документооборота и минимизацию необходимости личного посещения судебных органов.

Электронное судопроизводство — это ведение дела в специализированной программной среде. Считается, что так правосудие становится прозрачнее и доступнее. Судебные акты тоже оформляют в цифре. На практике бывает по-разному: иногда приговор просто механически копируют из обвинительного заключения, а иногда дело ведут в электронном виде от возбуждения уголовного дела до исполнения приговора.

Проблема такой «компиляции», на которую справедливо указывает Р.Г. Бикмиев [3], в том, что страдает описательно-мотивировочная часть. А значит, падает и авторитет судебной власти. На это стоит обратить внимание и продумать меры, чтобы правоприменители не просто копировали текст, а давали развёрнутую аргументацию.

Таким образом, сегодняшнее состояние можно назвать «лоскутной цифровизацией». Технологии встраивают в отдельные процедуры, но общая логика процесса не меняется. Из-за этого часто всё сводится к формальностям и возникают новые риски [12].

Государство отвечает на цифровые вызовы жёстко — ужесточает уголовную ответственность в сфере информационной безопасности. Это, в свою очередь, меняет контекст всего уголовного судопроизводства. Например, в январе 2026 года Госдума РФ приняла в первом чтении законопроект, который уточняет состав преступления по статье 274.1 УК РФ.

Ключевое изменение — замена оценочного понятия «причинение вреда» на исчерпывающий перечень последствий: уничтожение, блокирование, модификацию или копирование информации в КИИ. Это направлено на унификацию судебной практики и более эффективное противодействие кибератакам на жизненно важные объекты энергетики, транспорта, здравоохранения и финансов. Законопроект также вводит «кибер-амнистию» для сотрудников, нарушивших правила эксплуатации КИИ, но способствовавших раскрытию преступления, что создает новый процессуальный стимул для сотрудничества со следствием.

Параллельно ФСБ России разработала пакет нормативных актов, вступающих в силу в 2026 году, которые устанавливают для субъектов КИИ режим непрерывного взаимодействия с государственной системой обнаружения атак (ГосСОПКА). Новые правила предписывают в срок до 3 часов информировать о компьютерных инцидентах на значимых объектах КИИ, а также предоставлять планы реагирования и отчитываться о принимаемых мерах. Это трансформирует роль следователя и дознавателя в делах о преступлениях против КИИ, требуя от них работы с массивом технических данных и оперативных отчетов, поступающих в режиме реального времени.

С декабря 2024 года введена в действие ст. 272.1 УК РФ. Изначально направленная против создателей Telegram-ботов для «пробива» информации, статья получила чрезвычайно широкое применение. К уголовной ответственности по ст. 272.1 УК РФ привлекаются, в частности, рядовые сотрудники салонов связи. Основание — передача через мессенджеры даже небольших массивов персональных данных. По оценкам экспертов, данная норма сконструирована как абстрактные формулировки позволяют правоприменителю квалифицировать как уголовно наказуемое деяние практически любое нарушение в сфере персональных данных. Отсутствие чётких критериев разграничения между административным правонарушением и уголовным преступлением в сфере оборота персональных данных ведёт к неоднозначности правоприменения. Для субъектов предпринимательской деятельности это сопряжено с дополнительными рисками. Для судебной системы — с увеличением количества уголовных дел.

Цифровизация юридической деятельности зачастую ограничивается переносом существующих бюрократических процедур в электронную среду без их содержательной оптимизации. Один из распространённых случаев — автоматическое копирование текста обвинительного заключения

в приговор. Данная практика исключает необходимость самостоятельного анализа доказательств судом, что противоречит принципам справедливого судопроизводства. Р.Г. Бикмиев отмечает необходимость корректировки такого подхода [3].

Введение в Уголовный кодекс Российской Федерации статей 272.1 и 274.1 наделяет следственные органы расширенными полномочиями по собиранию цифровых доказательств. Отсутствие надлежащих процессуальных фильтров создаёт предпосылки для нарушения прав личности и ослабления принципа состязательности сторон. Допускается формирование цифровых досье на граждан, что ставит под угрозу неприкосновенность частной жизни и конфиденциальность персональных данных.

Применение искусственного интеллекта в юридической практике сопряжено с рисками. Анализ зарубежного опыта, в частности системы COMPAS (США), свидетельствует о подверженности алгоритмов предвзятости вследствие нерепрезентативных обучающих выборок и недостаточной прозрачности. Доверие к результатам таких систем без критической проверки вступает в противоречие с принципом персональной ответственности судей и следователей, что снижает качество правосудия.

Недостаточная цифровая компетентность правоприменителей ведёт либо к игнорированию цифровых доказательств, либо к их некритическому восприятию. Указанное обстоятельство негативно отражается на качестве правосудия и создаёт риски для объективного рассмотрения дел.

Для эффективного внедрения цифровых технологий требуется комплексная правовая модель, охватывающая все аспекты электронного уголовного дела. Возможные решения видятся в принятии цифрового процессуального кодекса либо отдельного федерального закона. В таком акте необходимо регламентировать идентификацию участников с использованием квалифицированной электронной подписи, порядок обжалования электронных судебных решений, требования к кибербезопасности процесса. Искусственный интеллект должен использоваться только как вспомогательный инструмент: анализ больших массивов данных, выявление закономерностей. Принятие процессуальных решений, затрагивающих права и свободы граждан, остаётся прерогативой человека. Алгоритмы ИИ подлежат обязательной сертификации на предмет предвзятости и потенциальных ошибок.

Защита прав личности — приоритетная задача. Необходимо законодательно определить критерии допустимости цифровых доказательств, расширить право на участие IT-специалистов со

стороны защиты, установить строгий судебный порядок санкционирования скрытых электронно-цифровых следов [13]. Для преодоления цифрового разрыва требуется масштабная переподготовка юридических кадров, разработка специализированных образовательных программ по цифровой криминалистике и киберправу. Без этих мер технологическая модернизация остаётся декларативной.

Цифровизация уголовного судопроизводства России находится на переломном этапе. Пройден путь от механизации рутинных операций до признания цифровой информации объектом уголовно-правовой защиты и процессуального доказывания. Однако реактивное ужесточение уголовного закона и фрагментарное внедрение технологий опережают формирование сбалансированной процессуальной доктрины.

Задача состоит в том, чтобы цифровизация служила не только целям эффективности и безопасности государства, но и укрепляла гарантии прав личности, состязательность, справедливость суда. Необходим переход от лоскутной оптимизации к стратегическому проектированию цифрового уголовного процесса на основе конституционных принципов. Технологии не должны полностью заменять человека. Требуется гибридная система, в которой технологии усиливают аналитические возможности юриста, а правовая культура и процессуальные гарантии предотвращают технологические ошибки и авторитарные риски. Следующий шаг — широкое профессиональное и общественное обсуждение этико-правовых рамок цифровизации, результаты которого должны лечь в основу системной законодательной реформы.

Список литературы:

- [1] Гусева И., Ионова А. Цифровизация уголовного процесса в современных условиях // Цифровые технологии и право. 2025. № 1(2). С. 89–92.
- [2] Клименкова Е. М., Зиновьева Д. В. Использование современных технологий в уголовном процессе: возможности и риски // Молодой ученый. 2025. № 22 (573). С. 418–420.
- [3] Бикмиев Р. Г. Цифровизация судебных решений: перспективы и риски // Наука для практиков. 2026.
- [4] Арзуманян А. Э. Системы искусственного интеллекта в уголовном процессе США: опыт применения и правовое регулирование // Полицейская деятельность. 2026. № 1. С. 1–15.
- [5] Моругина Н. А. Цифровая трансформация уголовного судопроизводства России и зарубежных стран: монография. – М.: Норма, 2026. – 208 с.

[6] Госдума ужесточила ответственность за кибератаки на КИИ // ВКирове.ру. 2026. 27 января.

[7] Электронный уголовный процесс: учебник для вузов / ответственные редакторы С. В. Зуев, Н. А. Моругина. – М. : Юрайт, 2026. – 404 с.

[8] Новые правила кибербезопасности для КИИ от ФСБ на 2026 год: обзор изменений // ICT-Online. 2026. 27 января.

[9] ФСБ разработала проект по непрерывному регулированию кибератак // Коммерсантъ. 2025. 18 ноября.

[10] Применение технологий в уголовном процессе: проблемы и перспективы // Научный лидер. 2024. № 21(171).

[11] Официальный сайт Госуслуг. Подача процессуальных документов в суд в рамках уголовного судопроизводства : [Электронный ресурс]. – URL: <https://www.gosuslugi.ru> (дата обращения: 16.04.2026). – Текст : электронный.

[12] Моругина, Н. А. Цифровая трансформация уголовного судопроизводства России и зарубежных стран : монография / Н. А. Моругина. — Москва : Норма, 2026. — 208 с. — DOI 10.12737/2223615. - ISBN 978-5-00156-461-4. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2223615> (дата обращения: 16.04.2026).

[13] Смахтин, Е. В. Соккрытие электронно-цифровых следов как способ противодействия расследованию преступлений / Е. В. Смахтин, М. М. Льянов // Технологии XXI века в юриспруденции : Материалы Пятой международной научно-практической конференции, Екатеринбург, 19 мая 2023 года. – Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб», 2023. – С. 195-203 (дата обращения: 12.05.2026).

References:

[1] Guseva I., Ionova A. Digitalization of Criminal Procedure in Modern Conditions // Digital Technologies and Law. 2025. No. 1 (2). pp. 89–92.

[2] Klimenkova E. M., Zinovieva D. V. Use of Modern Technologies in Criminal Procedure: Opportunities and Risks // Young Scientist. 2025. No. 22 (573). pp. 418–420.

[3] Bikmiev R. G. Digitalization of Court Decisions: Prospects and Risks // Science for Practitioners. 2026.

[4] Arzumanyan A. E. Artificial Intelligence Systems in US Criminal Procedure: Experience of Application and Legal Regulation // Police Activity. 2026. No. 1. pp. 1–15.

[5] Morugina, N. A. Digital Transformation of Criminal Procedure in Russia and Foreign Countries: Monograph. Moscow: Norma, 2026. 208 p.

[6] The State Duma has tightened penalties for cyberattacks on critical information infrastructure // VKirov.ru. January 27, 2026.

[7] Electronic Criminal Procedure: Textbook for Universities / Editors-in-Chief S. V. Zuev, N. A. Morugina. Moscow: Yurait, 2026. 404 p.

[8] New Cybersecurity Rules for Critical Information Infrastructure from the FSB for 2026: An Overview of Changes // ICT-Online. January 27, 2026.

[9] The FSB has developed a project for the continuous regulation of cyberattacks // Kommersant. November 18, 2025.

[10] Application of technologies in criminal proceedings: problems and prospects // Scientific leader. 2024. No. 21(171).

[11] Official website of State Services. Filing procedural documents with the court in criminal proceedings: [Electronic resource]. – URL: <https://www.gosuslugi.ru> (date of access: 16.04.2026). – Text: electronic.

[12] Morugina, N. A. Digital transformation of criminal proceedings in Russia and foreign countries: monograph / N. A. Morugina. - Moscow: Norma, 2026. - 208 p. - DOI 10.12737/2223615. - ISBN 978-5-00156-461-4. - Text: electronic. - URL: <https://znanium.ru/catalog/product/2223615> (date of access: 04/16/2026).

[13] Smakhtin, E. V. Concealing electronic digital traces as a way to counteract the investigation of crimes / E. V. Smakhtin, M. M. Lyanov // Technologies of the 21st century in jurisprudence: Proceedings of the Fifth international scientific and practical conference, Yekaterinburg, May 19, 2023. - Yekaterinburg: ANO "Center for Assistance to the Development of Forensic Science" CrimLib, 2023. - P. 195-203 (date of access: 12.05.2026).

