

УДК 343.1**Информационные технологии и специальные компетенции
следователя при производстве процессуальных действий****Храпенкова Евгения Юрьевна**

Аспирант,
Красноярский государственный аграрный университет,
660049, Российская Федерация, Красноярск, просп. Мира, 90;
e-mail: Sosna_evgeniya@mail.ru

Бертовский Лев Владимирович

Доктор юридических наук,
Красноярский государственный аграрный университет,
660049, Красноярский край, город Красноярск, просп. Мира, 90;
e-mail: bg11980@yandex.ru

Аннотация

В статье рассматриваются проблемы и перспективы применения информационных технологий в деятельности следователя при осуществлении процессуальных действий. Анализируются правовые пробелы в Уголовно-процессуальном кодексе Российской Федерации, касающиеся цифровых доказательств, а также недостаточная регламентация процедур изъятия, хранения и аутентификации электронной информации. Сделан вывод о необходимости институциональной трансформации следственной практики в условиях цифровизации уголовного судопроизводства.

Для цитирования в научных исследованиях

Храпенкова Е.Ю., Бертовский Л.В. Информационные технологии и специальные компетенции следователя при производстве процессуальных действий // Вопросы российского и международного права. 2025. Том 15. № 2А. С. 516-525.

Ключевые слова

Информационные технологии, следователь, цифровые доказательства, уголовный процесс, специальные компетенции, криминалистика, законодательство, УПК РФ.

Введение

Растущая цифровизация общественной и частной жизни напрямую повлияла на системы уголовного правосудия, требуя глубокой трансформации процессуальных механизмов и методов расследования. В Российской Федерации эта трансформация выявила серьезные несоответствия между существующими нормами уголовного судопроизводства и оперативными реалиями, с которыми сталкиваются следователи, работающие в технологически насыщенной среде. Поскольку цифровые следы становятся ключевыми элементами в раскрытии преступной деятельности, роль следователя должна выйти за рамки юридических знаний и включить ряд специализированных цифровых компетенций. Уголовно-процессуальный кодекс Российской Федерации (УПК РФ) обеспечивает правовую основу для следственных действий, включая обыск, выемку и сбор доказательств [Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ, [www](http://www.legislation.gov.ru)]. Однако многие его положения, в частности статьи 82, 182 и 183 УПК РФ, по-прежнему основаны на предположениях о материальных, вещественных доказательствах. Эти статьи не содержат достаточных указаний по работе с цифровыми носителями, зашифрованными файлами или данными, хранящимися на иностранных серверах. Например, статья 82 УПК РФ регулирует хранение и копирование вещественных доказательств, но не требует криминалистического сохранения метаданных или хэш-аутентификации, которые имеют решающее значение для поддержания целостности электронных доказательств [там же].

Основная часть

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет общие принципы управления информацией и доступа к ней [Федеральный закон от 27.07.2006 № 149-ФЗ, [www](http://www.legislation.gov.ru)], но не устраняет процессуальный разрыв в отношении цифровых доказательств в уголовных расследованиях. Как отмечали в своем анализе профессор Сергей Васильевич Зуев и Анатолий Игоревич Зазулин, интеграции следователя, обладающих знаниями в сфере информационных технологий, в среду уголовного судопроизводства, эта нормативная фрагментация оставляет следователей без единой методологии работы с цифровыми доказательствами, что подрывает как законность, так и эффективность [Зуев, Зазулин, 2024].

С практической точки зрения использование информационных технологий в следственных действиях требует расширения квалификации следователя. По словам В.С. Качур, цифровые технологии являются не вспомогательными инструментами, а важнейшими компонентами современной процессуальной работы. Теперь от следователей ожидают выполнения задач, связанных с облачными сервисами, криминалистикой мобильных устройств и анализом цифровых коммуникаций в рамках рутинных процедур [Качур, 2019]. Это ожидание подразумевает профессиональный стандарт, который нынешняя система институционального обучения часто не обеспечивает.

Риски, связанные с недостаточной цифровой компетентностью, не являются теоретическими. Как утверждает Н.Ю. Волосова в своем исследовании этических последствий искусственного интеллекта в уголовном судопроизводстве, некритическое использование цифровых инструментов без юридического и технического понимания ставит под угрозу процессуальную легитимность всего расследования [Волосова, 2023]. Поэтому следователи

должны понимать как техническое функционирование таких инструментов, так и их процессуальные ограничения, гарантируя, что ни один элемент процесса сбора доказательств не подрывает права подозреваемых или целостность судебного надзора.

Одной из главных проблем является отсутствие обязательных протоколов цифровой судебной экспертизы. Хотя такие стандарты, как ГОСТ Р 58296-2018, содержат руководящие принципы криптографической защиты и анализа цифровых доказательств [ГОСТ Р 58296-2018 «Информационные технологии. Криптографическая защита информации. Методики проведения экспертизы информационных систем», www], они остаются необязательными в рамках уголовного судопроизводства. Следовательно, допустимость таких доказательств часто зависит от дискреционных решений отдельных следователей или региональной практики, а не от единых правовых стандартов.

Процедурные формальности, связанные с обыском и изъятием, особенно уязвимы при применении к цифровым доказательствам. Поскольку УПК РФ не регламентирует извлечение информации из зашифрованных устройств или удаленных хранилищ, следователи могут полагаться на импровизированные методы или непроверенные программные решения. Это вносит существенную неопределенность в процессуальный статус доказательств. Более того, как указано в постановлении Правительства № 2040 о создании федеральной информационной системы «Правосудие», цифровые коммуникационные платформы все чаще используются в уголовном судопроизводстве [Постановление Правительства РФ от 03.12.2020 № 2040, www], однако они работают без единых протоколов аутентификации и защиты от подмены личности.

В практике российского уголовного судопроизводства на протяжении последних лет поднимается вопрос о допустимости применения психофизиологических исследований с использованием полиграфа в качестве доказательств. Верховный Суд Российской Федерации в своих правовых позициях указывает на то, что результаты тестирования с применением полиграфа не соответствуют требованиям, предъявляемым к доказательствам в уголовном процессе. Согласно действующему уголовно-процессуальному законодательству, доказательствами признаются полученные в установленном законом порядке сведения, имеющие значение для уголовного дела и подвергшиеся проверке. Между тем полиграф не обеспечивает объективных и воспроизводимых результатов, его данные подвержены влиянию внешних и субъективных факторов, а методика не обладает достаточной научной верифицированностью. В постановлениях Пленума Верховного Суда РФ и в позиции судов кассационной инстанции подчеркивается, что заключения по итогам тестирования на полиграфе не могут рассматриваться в качестве экспертных заключений, поскольку не соответствуют критериям научности, воспроизводимости и допустимости доказательственной информации в рамках статьи 74 УПК РФ.

Данную правовую позицию иллюстрирует один из наиболее резонансных судебных процессов последних лет – уголовное дело в отношении бывшего губернатора Хабаровского края Сергея Ивановича Фургала, осужденного в 2023 году к 22 годам лишения свободы по обвинению в организации убийств предпринимателей в 2004–2005 годах. В ходе предварительного расследования по инициативе следователя по особо важным делам Юрия Буртового было назначено комплексное психолого-лингвистическое исследование с применением компьютерных программ LVA (Layered Voice Analysis, Израиль) и FaceReader (Нидерланды), анализирующих голос и мимику обвиняемого. В результате анализа были выявлены сотни так называемых «индикаторов неискренности», которые легли в основу экспертного заключения. Однако данная практика вызвала масштабную критику со стороны

научного и экспертного сообщества. Заведующая кафедрой судебных экспертиз и криминалистики РГУП Т.В. Моисеева отметила, что используемые методики не имеют нормативного закрепления в российской системе судебных экспертиз и не прошли достаточной научной апробации. Адвокаты Фургала и ряд юристов подчеркнули, что подобные эксперименты с применением иностранных технологий не могут быть признаны допустимыми доказательствами, поскольку они не отвечают требованиям ни Закона о государственной судебно-экспертной деятельности, ни положениям УПК РФ, ни научному консенсусу о допустимости таких методов в уголовном процессе.

Таким образом, пример дела Фургала С.И. подтверждает правомерность критики в адрес практики использования полиграфа и других аналогичных методов в качестве доказательств. В отсутствие научной верификации, утвержденной методологии и единых стандартов оценки любые данные, полученные с применением полиграфа или визуально-эмоционального анализа, могут быть рассмотрены только как ориентировочная информация, но не как надлежащее доказательство в уголовном процессе.

В своей диссертации «Проблемы теории и практики выявления и расследования преступного нарушения правил экономической деятельности» профессор, доктор юридических наук Лев Владимирович Бертовский обосновывает необходимость выделения в криминалистике самостоятельного объекта – преступного нарушения правил экономической деятельности, охватывающего как правомерную, так и запрещенную хозяйственную деятельность, сопровождающуюся нарушением нормативных предписаний. Автор предлагает собственное определение этой категории преступлений и строит теоретическую модель, объединяющую уголовно-правовые, криминалистические и процессуальные аспекты. Он указывает на то, что данная группа преступлений обладает высоким уровнем латентности, а действующие методы выявления и расследования не обеспечивают их эффективного преследования. Особое внимание уделяется разработке криминалистической характеристики таких преступлений, включающей типичные способы совершения, следообразующие обстоятельства, личности правонарушителей, а также применяемые способы инсценировки и методы сокрытия. В диссертации вводятся и раскрываются новые научные понятия – «криминальный продукт» (материальный результат преступной экономической деятельности) и «криминалистическая инсценировка» как дезинформационная система, направленная на введение следствия в заблуждение. Автор разрабатывает методику выявления и фиксации таких объектов, предлагает типовую информационную модель расследования дел данной категории и дает рекомендации по тактике следственных действий. Значительная часть исследования посвящена вопросам сравнительного криминалистического анализа и построения общих методик расследования, применимых к различным видам экономических преступлений. Работа профессора Л.В. Бертовского представляет собой комплексное исследование, направленное на совершенствование как теоретической базы криминалистики, так и практики выявления, фиксации и доказывания преступлений, связанных с нарушением установленных правил экономической деятельности.

Еще один уровень сложности возникает, когда следователи используют искусственный интеллект при анализе допросов или поведенческом профилировании. А.А. Емелина, пишущая о будущем искусственного интеллекта в уголовном судопроизводстве, подчеркивает, что, хотя такие технологии могут повысить эффективность процесса, они остаются нерегулируемыми с точки зрения допустимости и требуют тщательной этической и методологической калибровки [Емелина, 2024]. Отсутствие законодательной ясности относительно того, являются ли выводы,

полученные с помощью искусственного интеллекта, вспомогательной информацией или фактическими доказательствами, налагает на следователя тяжелое бремя по интерпретации и применению таких инструментов законным образом.

Принцип процессуальной прозрачности также требует переосмысления в контексте цифровых расследований. Профессоры Л.А. Шестакова и М.Е. Кочнев отмечают, что использование цифровых технологий без надлежащей доказательной документации часто приводит к нарушениям прав обвиняемых и подрывает доказательную ценность критически важных данных [Шестакова, Кочнев, 2024]. Поэтому следователи должны гарантировать, что сбор, передача и хранение цифровой информации регистрируются таким образом, чтобы обеспечить прослеживаемость и внешнюю проверку.

Институциональные последствия значительны. Следователи должны действовать как юристы-практики и технические операторы одновременно, понимая цифровые протоколы связи, инструменты судебной визуализации и децентрализованные информационные системы [Приказ Следственного комитета РФ от 19.12.2022 № 91, [www](#)]. Однако, как показывает практика, такие приказы не обеспечивают достаточного исполнения и оставляют место для непоследовательного толкования и неравномерной реализации.

Подводя итог, можно сказать, что использование информационных технологий в процессуальных действиях является не вопросом удобства, а структурной необходимостью. Правовая система должна развиваться, чтобы предоставлять точные указания по работе с цифровыми доказательствами, а следователи должны быть оснащены междисциплинарными компетенциями, которые соответствуют этой новой реальности. Без такой трансформации процессуальные действия с использованием цифровых следов будут по-прежнему юридически хрупкими и технически неадекватными, что снизит как эффективность расследования, так и процессуальную справедливость.

Взаимодействие процессуальной системы с цифровой реальностью не просто подразумевает использование передовых инструментов, но и фундаментально меняет структуру и логику следственной деятельности. Следователь больше не ограничен традиционными правовыми категориями доказательств и должен работать в преходящей, нематериальной области, где данные не статичны, а динамичны, часто децентрализованы и уязвимы для несанкционированного изменения. Поскольку цифровые следы становятся все более распространенными в качестве источников доказательств, их надлежащее получение, интерпретация и документирование требуют обновленных процессуальных гарантий и пересмотренной институциональной стратегии. Ключевым препятствием остается отсутствие обязательных процессуальных норм, касающихся аутентификации и сохранения электронных данных. Хотя существующее законодательство допускает копирование и хранение цифровых материалов во время следственных действий [Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ, [www](#)], оно не предписывает конкретных методов сохранения их доказательной ценности, таких как криминалистическая визуализация или применение хэш-алгоритмов для обеспечения целостности данных. Хотя существуют национальные стандарты криптографической защиты и цифровой экспертизы [ГОСТ Р 58296-2018, [www](#)], они не интегрированы в процессуальное право, оставляя следователей без последовательного или обязательного протокола. В результате допустимость цифровых доказательств часто зависит от того, обладает ли отдельный следователь достаточными техническими знаниями и удовлетворяет ли документация общим требованиям надежности и проверяемости.

Процессуальная уязвимость возрастает в контексте удаленных следственных действий, которые быстро становятся нормой из-за развития официальных цифровых платформ. Несмотря на введение федеральной системы судебной информации [Постановление Правительства РФ от 03.12.2020 № 2040, [www](#)], многие процессуальные сценарии остаются лишь слабо регулируемы. Например, хотя видеодопрос разрешен, действующая правовая база не дает четких инструкций по обеспечению проверки личности участника, безопасной передаче аудиовизуального контента или поддержанию цепочки процессуального контроля во время удаленного взаимодействия. Эта непоследовательность ставит под угрозу надежность результатов и увеличивает риск процессуальных проблем на более поздних этапах.

Юридический формализм в цифровых контекстах оказывается недостаточным, когда технологические условия кардинально меняют метод и среду действия. Поиск и изъятие данных, хранящихся в распределенных сетях или зашифрованных форматах, не могут проводиться в соответствии с теми же процедурами, которые применяются к физическим помещениям или объектам. Следователям часто приходится проводить быструю техническую оценку сложных систем без какой-либо предварительной подготовки, полагаясь либо на внешних специалистов, либо на недостаточные общие знания. Такая зависимость от неформального принятия решений приводит к процессуальному неравенству и увеличивает вероятность нарушения прав. Действующие правовые нормы не обязывают присутствовать судебных экспертов во время изъятия электронной информации, а также не требуют технических протоколов для записи таких операций [Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ, [www](#); Приказ Следственного комитета РФ от 19.12.2022 № 91, [www](#)].

Усугубляет проблему отсутствие законодательного определения таких категорий, как цифровой след, метаданные или виртуальная инфраструктура, несмотря на их частую процессуальную значимость. Отсутствие таких определений препятствует формированию устойчивой практики толкования в следственных органах, судах и экспертных учреждениях. Без общего юридического языка и методологии цифровые доказательства подвержены фрагментации, противоречивым оценкам и непоследовательному применению процессуальных гарантий. Следователи сталкиваются со значительными трудностями при внедрении данных с онлайн-платформ, облачных хранилищ или служб обмена сообщениями в уголовное судопроизводство. Действующие нормы не в полной мере регулируют способы, с помощью которых эти данные могут быть запрошены, извлечены и аутентифицированы. Институциональный ответ должен начинаться с профессиональной реформы. Роль следователя требует перестройки не только с точки зрения квалификации, но и с точки зрения процессуальной ответственности. Техническая компетентность больше не может рассматриваться как вспомогательный актив; она должна быть интегрирована в необходимое ядро следственной подготовки. Выполнение процессуальных действий в цифровой среде – это не просто юридический процесс, это также технический акт, требующий знания архитектуры системы, судебно-медицинского программного обеспечения и конкретных уязвимостей, связанных с цифровой средой. Без этого процессуальные результаты становятся произвольными и уязвимыми для юридической недействительности.

Внедрение алгоритмических систем в следственную работу еще больше усложняет нормативную среду. Инструменты искусственного интеллекта для поведенческого анализа, семантического сравнения текстов или распознавания личности все чаще используются на предварительных этапах расследования. Однако в настоящее время ни одна процессуальная

норма не определяет их правовой статус и не устанавливает критерии приемлемости их результатов [Федеральный закон от 27.07.2006 № 149-ФЗ, [www](#); Емелина, 2024; Волосова, 2023]. Это ставит следователей в шаткое положение, когда они могут использовать такие системы для принятия решений, но не могут четко установить доказательную обоснованность этих результатов в суде. Такая ситуация создает не только процессуальную неопределенность, но и стратегический риск, поскольку результаты дела могут зависеть от нерегулируемых и непрозрачных технологических процессов. Этические и правовые проблемы также возникают в связи со сбором данных с цифровых платформ. Растущая зависимость от социальных сетей, служб личных сообщений и удаленных баз данных требует строгого соблюдения как национальных законов об информации, так и международных стандартов конфиденциальности и пропорциональности [Федеральный закон от 27.07.2006 № 149-ФЗ, [www](#)]. Следователи должны гарантировать, что их действия оправданы, необходимы и соразмерны тяжести предполагаемого преступления. Однако такую пропорциональность трудно оценить в отсутствие точных процессуальных правил, регулирующих доступ к цифровой информации и объем допустимого вторжения в частную цифровую среду.

Заключение

Усилия по решению обозначенных выше проблем должны включать скоординированную законодательную реформу. Процессуальное право должно включать конкретные положения о цифровых доказательствах: включая их изъятие, судебно-медицинское сохранение, аутентификацию и представление в суде. Технические стандарты не могут оставаться в области рекомендаций – они должны стать обязательными процессуальными инструментами, признанными и требуемыми для всех следователей, работающих с цифровыми данными. Кроме того, юридическое образование и профессиональная подготовка должны отражать этот сдвиг. Без оснащения следователей необходимыми междисциплинарными навыками процессуальное право останется оторванным от оперативных требований современного уголовного расследования.

Эволюция следственной практики больше не является вопросом институциональной модернизации, – это конституционный императив. Достоверность процессуальных результатов, права обвиняемых и авторитет судебных постановлений зависят от способности следователей выполнять действия, которые не только юридически обоснованы, но и технологически компетентны. Пока правовая система не примирит свою нормативную структуру с реалиями цифровой преступности и доказательств, процессуальное правосудие останется уязвимым к техническому устареванию и нормативной недостаточности. Таким образом, трансформация роли следователя является не факультативным нововведением, а основополагающим условием легитимности современного уголовного процесса.

Библиография

1. Бертовский Л.В. Проблемы теории и практики выявления и расследования преступного нарушения правил экономической деятельности: дис. ... д-ра юрид. наук. М.: Моск. гос. юрид. акад., 2005. 577 с.
2. Верховный Суд Российской Федерации. Определение Судебной коллегии по уголовным делам от 2 февраля 2023 г. № 19-УД22-34-А3 // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 16.04.2025).
3. Волосова Н.Ю. Перспективы использования искусственного интеллекта в уголовном судопроизводстве и формирование новой этики правосудия // Международная ассоциация содействия правосудию. 2023. URL: <https://www.iauaj.net/node/3360> (дата обращения: 02.04.2025).

4. ГОСТ Р 58296-2018 «Информационные технологии. Криптографическая защита информации. Методики проведения экспертизы информационных систем» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 01.04.2025).
5. Емелина А.А. Перспективы использования искусственного интеллекта в уголовном процессе // Law Afterknown: право за гранью обыденного: материалы III Международного молодежного юридического форума (Тюмень, 16–18 мая 2024 г.) Тюмень: ТюмГУ-Press, 2024. С. 222–228.
6. Зуев С.В., Зазулин А.И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 48–54.
7. Качур В.С. Информационные технологии в следственной деятельности // Вестник Тверского государственного университета. Серия: Право. 2019. № 4. С. 123–130. URL: <https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-sledstvennoy-deyatelnosti> (дата обращения: 02.04.2025).
8. Коммерсантъ. «Суд поддакивает машине»: дело Сергея Фургала пополнилось заключением по мимике и голосу // Коммерсантъ. 2021. № 133. URL: <https://www.kommersant.ru/doc/4829033> (дата обращения: 10.04.2025).
9. О федеральной государственной информационной системе «Правосудие»: постановление Правительства РФ от 03.12.2020 № 2040 // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 01.04.2025).
10. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (ред. от 04.07.2023) // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 01.04.2025).
11. Об утверждении Инструкции по организации видеозаписи следственных действий: приказ Следственного комитета РФ от 19.12.2022 № 91 // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 01.04.2025).
12. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 12.10.2023) // СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 01.04.2025).
13. Шестакова Л.А., Кочнев М.Е. Проблемы и перспективы использования цифровых технологий в уголовном судопроизводстве РФ // Юридический аналитический журнал. 2024. Т. 19. № 1. С. 15–25.

Information technologies and special competencies of the investigator in the production of procedural actions

Evgeniya Yu. Khrapenkova

Postgraduate Student,
Krasnoyarsk State Agrarian University,
660049, 90 Mira ave., Krasnoyarsk, Russian Federation;
e-mail: Sosna_evgeniya@mail.ru

Lev V. Bertovskii

Doctor of Law,
Krasnoyarsk State Agrarian University,
660049, 90 Mira ave., Krasnoyarsk, Russian Federation;
e-mail: bg11980@yandex.ru

Abstract

The article explores the challenges and prospects of using information technologies by investigators in the execution of procedural actions. It examines the legal gaps in the Criminal Procedure Code of the Russian Federation concerning digital evidence, as well as the insufficient regulation of procedures for the seizure, storage, and authentication of electronic information. The article concludes that institutional transformation of investigative practice is essential in the context of criminal justice digitalization.

For citation

Khrapenkova E.Yu., Bertovskii L.V. (2025) Informatsionnye tekhnologii i spetsial'nye kompetentsii sledovatelya pri proizvodstve protsessual'nykh deistvii [Information technologies and special competencies of the investigator in the production of procedural actions]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (2A), pp. 516-525.

Keywords

Information technologies, investigator, digital evidence, criminal procedure, special competencies, criminalistics, legislation, CPC RF.

References

1. Bertovskii L.V. (2005) Problemy teorii i praktiki vyyavleniia i rassledovaniia prestupnogo narusheniia pravil ekonomicheskoi deiatel'nosti: dis. ... d-ra iurid. nauk [Problems of Theory and Practice of Detection and Investigation of Criminal Violations of Economic Activity Rules: Dr. jurid. sci. diss.]. Moscow: Moscow State Legal Academia.
2. Emelina A.A. (2024) Perspektivy ispol'zovaniia iskusstvennogo intellekta v ugovnom protsesse [Prospects for Using Artificial Intelligence in Criminal Proceedings]. In: Law Afterknown: pravo za gran'iu obydenno: materialy III Mezhdunarodnogo molodezhnogo iuridicheskogo foruma (Tyumen', 16–18 maia 2024 g.) [Law Afterknown: Law Beyond the Ordinary: Proceedings of the III International Youth Legal Forum (Tyumen, May 16–18, 2024)]. Tyumen: TiumGU-Press Publ., pp. 222-228.
3. Federal'nyi zakon ot 27.07.2006 № 149-FZ (red. ot 04.07.2023) «Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii» [Federal Law No. 149-FZ of July 27, 2006 (as amended on July 4, 2023) "On Information, Information Technologies and Information Protection"]. SPS «KonsultantPlus» [SPS Consultant]. Available at: <https://www.consultant.ru> [Accessed: 01.04.2025].
4. GOST R 58296-2018 «Informatsionnye tekhnologii. Kriptograficheskaia zashchita informatsii. Metodiki provedeniia ekspertizy informatsionnykh sistem» [GOST R 58296-2018 "Information Technology. Cryptographic Information Protection. Methods for Conducting Information Systems Expertise"]. SPS «KonsultantPlus» [SPS Consultant]. Available at: <https://www.consultant.ru> [Accessed: 01.04.2025].
5. Kommersant". (2021) «Sud poddakivaet mashine»: delo Sergeia Furgala popolnilos' zakliucheniem po mimike i golosu ["The Court Nods Along with the Machine": The Case of Sergei Furgal Supplemented with a Conclusion on Facial Expressions and Voice]. Kommersant" [Kommersant], 133. Available at: <https://www.kommersant.ru/doc/4829033> [Accessed: 10.04.2025].
6. Kachur V.S. (2019) Informatsionnye tekhnologii v sledstvennoi deiatel'nosti [Information Technologies in Investigative Activities]. Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Pravo [Bulletin of Tver State University. Series: Law], 4, pp. 123–130. Available at: <https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-sledstvennoy-deyatelnosti> [Accessed: 02.04.2025].
7. Postanovlenie Pravitel'stva RF ot 03.12.2020 № 2040 «O federal'noi gosudarstvennoi informatsionnoi sisteme "Pravosudie"» [Decree of the Government of the Russian Federation No. 2040 of December 3, 2020 "On the Federal State Information System 'Justice'"]. SPS «KonsultantPlus» [SPS Consultant]. URL: <https://www.consultant.ru> [Accessed: 01.04.2025].
8. Prikaz Sledstvennogo komiteta RF ot 19.12.2022 № 91 «Ob utverzhdenii Instruktsii po organizatsii videozapisi sledstvennykh deistvii» [Order of the Investigative Committee of the Russian Federation No. 91 of December 19, 2022 "On Approval of the Instruction on Organizing Video Recording of Investigative Actions"]. SPS «KonsultantPlus» [SPS Consultant]. Available at: <https://www.consultant.ru> [Accessed: 01.04.2025].
9. Shestakova L.A., Kochnev M.E. (2024) Problemy i perspektivy ispol'zovaniia tsifrovyykh tekhnologii v ugovnom sudoproizvodstve RF [Problems and Prospects of Using Digital Technologies in Criminal Proceedings of the Russian Federation]. Iuridicheskii analiticheskii zhurnal [Legal Analytical Journal], 19(1), pp. 15-25.
10. Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii ot 18.12.2001 № 174-FZ (red. ot 12.10.2023) [Criminal Procedure Code of the Russian Federation No. 174-FZ of December 18, 2001 (as amended on October 12, 2023)]. SPS «KonsultantPlus» [SPS Consultant]. Available at: <https://www.consultant.ru> [Accessed: 01.04.2025].
11. Verkhovnyi Sud Rossiiskoi Federatsii. (2023) *Opredelenie Sudebnoi kollegii po ugovnym delam ot 2 fevralia 2023 g. № 19-UD22-34-A3* [Ruling of the Judicial Collegium for Criminal Cases of February 2, 2023 No. 19-UD22-34-A3]. SPS «KonsultantPlus» [SPS Consultant]. Available at: <https://www.consultant.ru> [Accessed: 16.04.2025].

-
12. Volosova N.Yu. (2023) Perspektivy ispol'zovaniia iskusstvennogo intellekta v ugovnom sudoproizvodstve i formirovanie novoi etiki pravosudiia [Prospects for Using Artificial Intelligence in Criminal Proceedings and the Formation of a New Ethics of Justice]. Mezhdunarodnaia assotsiatsiia sodeistviia pravosudiiu [International Association for Promoting Justice]. Available at: <https://www.iuaj.net/node/3360> [Accessed: 02.04.2025].
 13. Zuev S.V., Zazulin A.I. (2024) IT-sledovatel' v tsifrovoi srede ugovnogo sudoproizvodstva [IT-Investigator in the Digital Environment of Criminal Proceedings]. Pravoporiadok: istoriia, teoriia, praktika [Law and Order: History, Theory, Practice], 2(41), pp. 48–54.