Научная статья

УДК 343.98
DOI 10.25205/2542-0410-2025-21-3-104-113

# Проблемы построения единой цифровой экосистемы правоохранительных органов в период цифровой трансформации

**Александр Борисович Смушкин**

Саратовская государственная юридическая академия
Саратов, Россия

skif32@yandex.ru, https://orcid.org/0000-0003-1619-8325

*Аннотация*

В статье констатируется, что реализация платформенных решений является одним из элементов цифровой трансформации раскрытия расследования и предупреждения преступлений. Автором последовательно анализируются основные проблемные вопросы нового этапа развития цифровых платформ с позиций их возможной эволюции: однозначная идентификация и аутентификация пользователей; определение уровня и объема доступа; решение вопроса с архитектурой данной системы; решение вопроса с отсутствием дублирования электронного документооборота в бумажном виде и подписанием документов в электронной форме; решение вопроса о интеграции имеющихся информационных массивов отдельных правоохранительных органов при устранении дублирования информации; решение вопроса с обеспечением безопасности электронного документооборота; внедрение интеллектуальных систем.

*Ключевые слова*

цифровая платформа, цифровая экосистема правоохранительных органов, кросс-платформенное объединение, уголовное судопроизводство, цифровизация, оператор цифровой платформы

*Финансирование*

Исследование выполнено за счет гранта Российского научного фонда № № 24-28-00312, https://rscf.ru/project/24-28-00312/

*Для цитирования*

*Смушкин А. Б.* Проблемы построения единой цифровой экосистемы правоохранительных органов в период цифровой трансформации // Юридическая наука и практика. 2025. Т. 21, № 3. С. 104–113. DOI 10.25205/2542-0410-2025-21-3-104-113

# Problems of Building a Unified Digital Ecosystem of Law Enforcement Agencies in the Period of Digital Transformation

**Alexander B. Smushkin**

Saratov State Law Academy,
Saratov, Russian Federation

skif32@yandex.ru, https://orcid.org/0000-0003-1619-8325

*Abstract*

The article states that the implementation of platform solutions is one of the elements of the digital transformation of crime detection, investigation and prevention. The author consistently analyzes the main problematic issues of the new stage of development of digital platforms from the perspective of their possible evolution: unambiguous identification and authentication of users; determination of the level and volume of access; solving the problem with the architecture of this system; solving the problem with the absence of duplication of electronic document management in paper form

and signing documents in electronic form.; solving the issue of integrating the existing information arrays of individual law enforcement agencies while eliminating duplication of information; solving the issue of ensuring the security of electronic document management; introducing intelligent systems.

*Keywords*

digital platform, digital ecosystem of law enforcement agencies, cross-platform association, criminal proceedings, digitalization, digital platform operator

*Funding*

The research was carried out at the expense of a grant from the Russian Science Foundation No. 24-28-00312, https://rscf.ru/project/24-28-00312/

*For citation*

Smushkin A. B. Problems of building a unified digital ecosystem of law enforcement agencies in the period of digital transformation. *Juridical Science and Practice*, 2025, vol. 21, no. 3, pp. 104–113. (in Russ.) DOI 10.25205/2542-0410-2025-21-3-104-113

С развитием научно-технического прогресса, а также цифровой трансформации раскрытия, расследования и предупреждения преступлений, все большее внимание начинает уделяться следующему этапу эволюции отдельных цифровых платформ правоохранительных органов в единый синергетически функционирующий программно-аппаратный телекоммуникационный комплекс – цифровую экосистему правоохранительных органов. Л. Н. Масленникова предлагает характеризовать экосистему начального этапа уголовного судопроизводства как «систему, включающую множество взаимосвязанных и взаимообусловленных элементов, которая может быть представлена как сфера, регулируемая уголовно-процессуальным законом, обеспечивающая доступ к правосудию, обладающая замкнутой системой взаимосвязей ее компонентов (регистрация сообщения о преступлении, расследование, надзор прокурора, судебная власть), придающих ей стабильность, связанная с другими устойчивыми системами (судебной системой), имеющая определенную продуктивность по обеспечению доступа к правосудию» [1, с. 62 ].

Различные авторы предлагают разные подходы к формированию концепции экосистемы, выделяя тот или иной аспект и формируя различное содержание, однако для эффективного проектирования и бесперебойного функционирования целостной экосистемы либо информационно-телекоммуникационной инфраструктуры уголовного процесса важно последовательно решить ряд ключевых проблем: обеспечить надежную идентификацию и аутентификацию пользователей; установить четкий уровень и объем допуска; определить оптимальную архитектуру системы; устранить проблему параллельного существования электронных и бумажных форм документооборота путем внедрения цифровой подписи; интегрировать имеющиеся базы данных различных правоохранительных структур, исключив повторение сведений; гарантировать безопасность электронного взаимодействия; внедрить интеллектуальные технологии обработки данных.

Вопросы идентификации и аутентификации при доступе к государственным телекоммуникационным ресурсам многократно становились предметом изучения различных ученых. Так, подробную схему идентификации и аутентификации пользователя таких ресурсов предлагают в своей статье Д. И. Степаненко и А. А. Рудых [2]. Большой вклад в разработку данного вопроса внесли также О. А. Зайцев, П. С. Пастухов и другие авторы [3]. При этом верно утверждение П. С. Пастухова, что «главное преимущество эпохи цифровой идентификации заключается в ее дистанционном характере» [4, с. 211]. Авторы монографии «Высокотехнологичный уголовный процесс» подчеркивают, что «механизм удаленной идентификации с применением информационных технологий включает несколько информационных систем: регистр физических лиц единой системы, единую информационную систему персональных данных, единую биометрическую систему, единую систему идентификации и аутентификации, иные информационные

системы, обеспечивающие идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц» [5, с. 27].

Наибольшее значение имеет использование для идентификации единой государственной системы ЕСИА (Единая система идентификации и аутентификации). Эта система предназначена для обеспечения санкционированного доступа к иным базам данным. Среди иных средств идентификации пользователя, в самом общем виде, можно выделить следующие методы идентификации:

- предоставление логина и пароля и вход по данным идентификаторам. При этом логин и пароль сотруднику правоохранительных органов будет предоставлен с учетом положений приказа ФСБ № 524 от 24.10.2022 г[1]. Граждане же смогут получить логин и пароль по электронной почте, в МФЦ или иными способами, подтвердив свою личность лично или через кабинет госуслуг;
- вход на портал экосистемы непосредственно через личный кабинет госуслуг с помощью ЕСИА. При этом при отсутствии личного кабинета аккаунта на госуслугах (что уже становится редкостью), он может быть заведен в МФЦ, или сам процесс будет происходить через иные методы идентификации;
- получение доступа по биометрическим показателям при сопоставлении биометрической информации с использованием, например, устройств, оснащенных датчиками Face ID и Touch ID и баз данных Единой биометрической системы;
- с использованием кода направляемого в SMS, электронную почту или push-сообщения;
- с использованием разработок в области идентификации лица по клавиатурному почерку [6; 7].

При этом оптимальным представляется использование двухфакторной идентификации, например, сочетанием входа через личный кабинет госуслуг и подтверждением кодом, направленным на электронную почту либо с помощью биометрических показателей.

Подробно вопросы защиты персональных данных от различных киберугроз уже подвергались исследованиям в трудах отечественных криминалистов, специалистов в области уголовного права, IT-технологий [8; 9]. Для оптимального функционирования экосистем необходимо также решение отмеченных Р. Н. Боровских вопросов в области обеспечения их кибербезопасности и привлечения к ответственности нарушителей [10].

При определении уровня и объема доступа должны быть выделены несколько уровней доступа и типов информации. Представляется необходимым выделить следующие группы лиц: прежде всего, дифференцировать властных и невластных субъектов расследования, а также лиц, не имеющих отношения к расследованию. Невластные субъекты расследования должны быть дифференцированы по процессуальному положению участников судопроизводства, так как свидетель, потерпевший, подозреваемый (обвиняемый), с учетом соответствующих норм УПК РФ, имеют разный уровень доступа к информации о расследовании. Даже относительно обвиняемого имеет место разный период предоставления определенного доступа к информации расследования (наиболее полно с материалами расследования обвиняемые получают право ознакомиться только при предъявлении обвинительного заключения либо обвинительного акта). Властные субъекты расследования, в свою очередь, должны быть дифференцированы на имеющих отношение к расследованию данного конкретного уголовного дела и не имеющих отношения следователей данного и иных органов.

---

[1] Приказ Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» (рег. 23.11.2022 № 71073) // Портал официального опубликования нормативных актов http://publication.pravo.gov.ru/Document/View/0001202211230034?ysclid=m8e6rtw9ql546851478 (дата обращения: 18.03.2025).

Представляется, что весь объем информации, фигурирующей в экосистеме, может быть также разделен на общую информацию и нормативные акты, доступ к которым могут получать все; методическую информацию и иную информацию, распространение которой ограничено грифом «Для служебного пользования» (доступ к ней, на наш взгляд, должны иметь все сотрудники следственных органов); информацию, касающуюся обращения, ходатайства и ответов на них, соответственно, доступ к которым будет получать лицо, направившее это ходатайство; иную информацию уголовного дела, полный доступ к ознакомлению и редактированию которой может иметь только следователь, ведущий расследование. Доступ к ознакомлению будет получать также надзирающий прокурор, потерпевший и обвиняемый (при предъявлении обвинительного заключения/акта). При этом, при участии потерпевшего в процессе под псевдонимом, эта информация не должна предоставляться. Именно разноуровневые пользователи через единую точку входа максимально характеризуют экосистему как явление. Цифровая экосистема правоохранительных органов должна обеспечивать «бесшовное» взаимодействие.

Относительно архитектуры системы выбор стоит между монолитной и модульной структурой. При этом модульную структуру В. В. Тюрин описал как «концепцию архитектуры информационной системы, предусматривающей в качестве основной модели ее исполнения совокупность интегрированных между собой условно независимых программных модулей, каждый из которых выполняет определенную функцию, имеет свою защищенную логику реализации и программный интерфейс для взаимодействия» [11, с. 112]. Преимущества именно модульной организации подчеркивают как отечественные, так и зарубежные авторы [12; 13, с. 637]. Внутри структуры экосистемы должны быть выделены модули и микросервисы, используемые конкретными органами. Технически представляется разумным предусмотреть возможность установки в конкретном органе клиента цифровой экосистемы, ускоряющего доступ к функционалу экосистемы, но не ко всем элементам, а только к избранным. Подобная организация разгрузит тем самым мощности их компьютерных систем органов от лишней нагрузки, а также позволит установить ведомственные уровни доступа к информации.

Дублирование электронного документооборота в бумажном виде должно стать фактически анахронизмом, поскольку в подобной ситуации не только пропадает существенная часть смысла электронного документооборота, но и происходит удвоение необходимой деятельности сотрудника, и так протекающей в условиях дефицита времени. Проводимое в рамках докторского исследования анкетирование показало, что дублирование электронной и бумажной работ как одну из основных проблем выделяют респонденты – научно-педагогические работники (17,5 % опрошенных). Настаивают на полной цифровизации документооборота с использованием электронной цифровой подписи 44,2 % практических работников. Решение вопроса с подписанием электронного документа лежит в плоскости использования электронной подписи, не требующего его распечатки и последующего сканирования. Как отмечает П. С. Пастухов, «при подписании электронных документов посредством единой цифровой платформы могут использоваться: а) простая электронная подпись; б) усиленная квалифицированная электронная подпись; в) усиленная неквалифицированная электронная подпись, сертификат ключа проверки которой создан и используется в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» [14, с. 536]. Представляется, что следователи должны обеспечиваться усиленной квалифицированной электронной подписью централизованно. Иные участники уголовного судопроизводства в начале расследования своей подписью должны заверять согласие на использование усиленной неквалифицированной электронной подписи ими в рамках электронного документооборота.

Для устранения дублирования в базах следственных органов первоначально необходимо приведение их к единым стандартам и форматам. После унификации баз устранения дублиро-

вания возможно программным способом, например с использованием программного комплекса CCleaner или функционала Total Comander, а также иных программ.

Представляется, что оптимальную организацию документооборота и информационных блоков можно провести с использованием разработок в области цифровой криминалистической логистики, предлагаемых Е. В. Христининой. С точки зрения ее подхода, термин «цифровая криминалистическая логистика» следует понимать как «систему управления информационными потоками в процессе расследования по уголовным делам, когда вся электронная документация и иная цифровая информация, имеющая криминалистическое значение, используется следователем в качестве логических (оптимальных) цепочек (алгоритмов), позволяющих эффективно решать задачи по раскрытию и расследований преступлений, используя единую цифровую среду» [15, с. 129].

Обеспечению безопасности судопроизводства в электронном формате и электронного документооборота, в частности, было посвящено достаточно много работ. Среди новых методов можно отметить использование облачных сервисов и блокчейна. Применение облачных сервисов для цифровой среды уголовного судопроизводства не только обосновывается учеными [16; 17], но и получает отражение в нормативных актах[2]. Использование облачных сервисов повышает кибербезопасность вследствие того, что «облачная информация» не сконцентрирована на одном сервере или одном носителе. Она распределена по значительному количеству серверов, и злоумышленнику для получения неправомерного доступа необходимо преодолеть все уровни защиты множества носителей и скомпоновать распределенную информацию. Сатоши Накамото относительно используемой технологии блокчейна указывал, что «система работает по следующим правилам:

1. Новые транзакции рассылаются всем узлам.
2. Каждый узел объединяет пришедшие транзакции в блок.
3. Каждый узел пытается подобрать хеш блока, удовлетворяющий текущей сложности.
4. Как только такой хеш найден, этот блок отправляется в сеть.
5. Узлы принимают этот блок, только если все транзакции в нем корректны и не используют уже потраченные средства.
6. Свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хеш предыдущего в качестве новых исходных данных»[3].

При использовании технологии блокчейна будет отсутствовать единый депозитарий и единая база, размещенная на определенных серверах. Информация будет распределена, а у каждого пользователя будет реестр информации. Каждая новая транзакция, произведенная с информацией, отражается во всей цепочке блоков. Посредством блокчейна информация через распределенные записи децентрализуется, последовательно хешируется (от англ. hashing – перемешивание, преобразование) и зашифровывается, что делает практически невозможным для злоумышленников ее выявление и осмысление[4]. Блокчейн считается практически не взламываемой технологией, что дает основание многим авторам рекомендовать ее использование для электронного уголовного дела [18, с. 80; 19, с. 229].

Интеграция элементов интеллектуальных систем в экосистему может существенно повысить ее эффективность. При этом интеллектуальные системы могут быть алгоритмизирован-

[2] Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года утверждена Распоряжением Правительства от 1 ноября 2013 г. № 2036-р (в ред. от 18.10.2018 г.) // Собрание законодательства Российской Федерации от 18 ноября 2013 г № 46. Ст. 5954.

[3] Накамото Сатоши. Биткоин: цифровая пиринговая наличность (2009) / перевод // Coinspot: сайт. 21 декабря 2013 г. URL: http://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/ (дата обращения: 16.07.2020).

[4] LuffC. Cybersecurity and the future of blockchain technology. URL: http://www.gingermaypr.com/ cyb ersecurity-blockchain-technology.htm (дата обращения: 31.03.2025).

ными, т. е. построены на заранее запрограммированном порядке действий, и неалгоритмизированными, прошедшими машинное обучение (например, нейроморфными). Среди первых можно назвать предложенные В. Б. Веховым автоматизированные методики расследования [20] (так, специализированная территориально-распределенная автоматизированная система (СТРАС-СК), действующая в Следственном департаменте при МВД России, содержит подсистему гибридного интеллекта «Расследование», направленную на поддержку следователя при принятии процессуальных и иных решений, также работающую на принципах автоматизированных методик расследований), а также разработки профессора В. Ю. Толстолуцкого с коллегами – программа ФорВер [21]. К уже имеющимся нейроморфным разработкам можно отнести исследования профессора Д. В. Бахтеева в области нейросетей, направленных на выявление подделки подписей [22], а также разработка профессора А. А. Бессонова в области использования искусственного интеллекта при расследовании серийных[5] и иных преступлений [23].

Следующим вопросом является, безусловно, определение единого оператора данной экосистемы. А. Ю. Чурикова отмечает, что «у цифровой платформы, если ее рассматривать не как платформенное решение, позволяющее создавать децентрализованные интегрируемые информационные системы, а как некий отдельный самостоятельный ресурс, должен быть единый оператор. Возможно ли в сфере уголовного судопроизводства выделить орган, который бы стал единым оператором цифровой платформы и это не нарушило бы принципы уголовного процесса и не перегрузило бы данный орган несвойственной ему работой? Считаем, что нет. На эту роль с учетом обозначенных критериев не подходят ни ВС РФ, ни Генеральная прокуратура, ни СК, ни МВД» [24, с. 110]. Л. А. Воскобитова указывает, что «при создании единой межведомственной цифровой платформы «Цифровое уголовное судопроизводство» администратором-держателем этой платформы также должна оставаться Генеральная прокуратура РФ. Она сможет выступать не только органом надзора за законностью производства по уголовному делу на всех стадиях процесса, обеспечивающим в том числе как соблюдение прав человека, так и уголовное преследование в рамках закона, но и выполнять в известной мере функции координации использования, а также дальнейшего совершенствования такой платформы. Более того, такая позиция и роль Прокуратуры позволит обеспечивать контроль безопасности платформы и ее модулей: защиту от различных киберугроз; сохранность и неизменность всей информации уголовного судопроизводства; законность решений по вопросам доступа или его ограничения при пользовании процессуальной информацией невластными участниками процесса, когда в этом возникает процессуально-правовая необходимость и появляются для этого правовые основания, и т. п.» [25, с. 24–25].

По-нашему же мнению, решение проблемы определения единого оператора цифровой экосистемы должно лежать в контексте создания государственной некоммерческой организации, в функции которой будут входить обеспечение автоматизированной обработки информации и обеспечение доступа к этой информации. Кроме того, следует учитывать возможность использования технологии частично распределенной информации (аналогичной принципам работы BitTorrent), при которой единый HTTP-сервер, управляемый единым общим оператором, организует связь модулей, управляемых ведомственными операторами между собой. Подобный подход с использованием распределенных реестров снизит нагрузку на оборудование единого оператора (и, соответственно, требования к нему). При этом общий оператор будет фактически только направлять векторы движения информационных потоков, что обусловливает отсутствие необходимости получения допуска к конфиденциальной информации со стороны его сотрудников. При этом, на основании п. 1.14 федерального проекта «Информационная

[5] *Бессонов А. А.* Искусственный интеллект против серийных преступников // Искусственные общества. 2023. Т. 18, вып. 3. URL: https://artsoc.jes.su/s207751800027535-7-1/. DOI: 10.18254/S207751800027535-7 (дата обращения: 31.03.2025).

безопасность» национальной программы «Цифровая экономика Российской Федерации»[6], следует сразу определять стандарт связи и функционирования цифровой среды взаимодействия на базе сетей пятого поколения 5G стандарта LTE- 450. При этом, с учетом требований импортозамещения и технологического суверенитета, данный стандарт должен быть основан на применении отечественных технологий.

Подводя итог, можно отметить, что, безусловно, указанными вопросами не исчерпывается полный спектр проблем построения единой экосистемы правоохранительных органов. В процессе их построения будет выявляться множество нормативных, организационных, методологических проблем. Однако представляется, что откладывать их решение будет критической ошибкой в связи с активной цифровой трансформацией расследования.

## Список литературы


1. **Масленникова Л. Н.** Концептуальный подход к построению уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий // Вестник Ун-та им. О. Е. Кутафина. 2020. № 10 (74) С. 52–65.
2. **Степаненко Д. А., Рудых А. А.** К вопросу об использовании механизма удаленной идентификации и аутентификации в правоохранительной деятельности // Технологии XXI века в юриспруденции: материалы III Междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / под ред. Д. В. Бахтеева. Екатеринбург: Урал. гос. юрид. ун-т, 2021. С. 318–326.
3. **Зайцев О. А., Пастухов П. С.** Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского ун-та. Юридические науки. 2022. № 56. С. 281–308.
4. **Пастухов П. С.** Эволюция криминалистической идентификации как метода научного познания в информационном обществе // Пенитенциарная система и общество: опыт взаимодействия: сб. материалов IX Международной науч.-практ. конф. (Пермь, 6–8 апреля 2022 года) / сост. А. И Согрина. Пермь, 2022. С. 211–215.
5. Высокотехнологичный уголовный процесс: моногр. / под ред. д-ра юрид. наук С. В. Зуева; д-ра юрид. наук Л. Н. Масленниковой. М.: Юрлитинформ, 2023. 212 с.
6. **Перегудов А. В.** Анализ клавиатурного почерка. Способы его применения // Интерактивная наука. 2018. № 6 (28). С. 59–60.
7. **Протасевич А. А., Фойгель Е. И.** О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности // Всероссийский криминологический журнал. 2020. Ч. 14. № 3. С. 471–480.
8. **Зайнутдинова Е. В.** Конфиденциальность персональных данных в ситуации киберугроз // Юридическая наука и практика. 2023. Т. 19, № 3. С. 38–46.
9. **Карунная Я. А.** Проблемы защиты персональных данных в условиях цифровой трансформации // Юридическая наука и практика. 2023. Т. 19, № 3. С. 47–56.
10. **Боровских Р. Н.** Уголовно-правовые аспекты кибербезопасности // Юридическая наука и практика. 2023. Т. 19, № 3. С. 17–22.
11. **Тюрин В. В.** Управление цифровой трансформацией. Основные тезисы и понятия. [б. м.]: Издательские решения, 2023. 322 с.
12. **Ghazawneh A., Henfridsson O.** A paradigmatic analysis of digital application marketplaces // Journal of Information Technology. 2015. Vol. 30, is. 3. P. 198–208.


[6] Федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» // Официальный сайт Министерства цифрового развития РФ. URL: https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/vedomstvennyj-proektnyj-ofis-vpo/administrirovanie-soprovozhdenie-ispolneniya-naczionalnoj-programmy-czifrovaya-ekonomika-rossijskoj-federaczii/informaczionnaya-bezopasnost (дата обращения: 31.03.2025).

13. **Гелисханов И. З., Юдина Т. Н.** Цифровые платформы: особенности и перспективы развития // Сб. материалов 71-й Всерос. науч.-техн. конф. студентов, магистрантов и аспирантов вузов с междунар. участием. Ярославль: Изд. дом ЯГТУ, 2018. С. 637–640.
14. **Пастухов П. С.** Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юрид. альманах. 2023. № 6. С. 521–540.
15. **Христинина Е. В.** К вопросу о применении цифровой логистики в уголовном процессе и криминалистике // Юридический вестник Самар. ун-та. 2020. Т. 6. № 3. С. 128–132.
16. **Тагиров З. И.** Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики // Вопросы безопасности. 2018. № 4. С. 28–51.
17. **Жевняк О. В.** Соотношение облачных технологий и цифровых платформ // Правовая информатика. 2024. № 2. С. 143–151.
18. **Перов В. А.** Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учеб.-метод. пособие. М.: Юрлити нформ, 2017. 197 с.
19. **Бертовский Л. В.** Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226–230.
20. **Вехов В. Б.** Автоматизированные методики расследования преступлений как новое направление в криминалистической технике // Известия Тульского гос. ун-та. Экономические и юридические науки. 2016. Вып. 3. Ч. II. С. 8–11.
21. **Толстолуцкий В. Ю., Казарян К. С.** Использование компьютерной программы «ФОРВЕР» в процессе взаимодействия следователя и сотрудников органа, осуществляющего оперативно-розыскную деятельность // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2010. № 2 (13). С. 242–246.
22. **Бахтеев Д. В.** Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. 2020. Т. 17, № 4. С. 514–522.
23. **Бессонов А. А.** Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: моногр. М.: Проспект, 2021. 816 с.
24. **Чурикова А. Ю.** Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование: дис. … д-ра юрид. наук. Саратов, 2024. 498 с.
25. **Воскобитова Л. А.** Цифровая трансформация российского уголовного судопроизводства и роли прокуратуры как организатора такой трансформации // Вестник Ун-та им. Кутафина. 2024. № 1. С. 18–31.

## References

1. **Maslennikova L. N.** A conceptual approach to the construction of criminal justice, ensuring access to justice in the context of the development of digital technologies. *Bulletin of the O E. Kutafin University*, 2020, no. 10 (74), pp. 52–65. (in Russ.)
2. **Stepanenko D. A., Rudykh A. A.** On the use of remote identification and authentication mechanisms in law enforcement activities. *Technologies of the XXI century in jurisprudence : materials of the Third International Scientific and Practical Conference. (Yekaterinburg, May 21, 2021)* / edited by D. V. Bakhteev. Yekaterinburg : Ural State Law. Univ., 2021, pp. 318–326. (in Russ.)
3. **Zaitsev O. A., Pastukhov P. S.** The digital profile of a person as an element of an information technology strategy for investigating crimes. *Bulletin of Perm University. Legal sciences*, 2022, no. 56, pp. 281–208. (in Russ.)

4. **Pastukhov P. S.** The evolution of forensic identification as a method of scientific knowledge in the information society. *The penal system and society: experience of interaction: collection of materials of the IX International Scientific and Practical Conference* (Perm, April 6–8, 2022) / comp. A. And. Sogrin. Perm, 2022, pp. 211–215. (in Russ.)
5. High-tech criminal procedure: a monograph / ed. by Dr. jurid. of Sciences S. V. Zueva; Doctor of Sciences. jurid. L. N. Maslennikova, M.: Yurlitinform, 2023, 212 p. (in Russ.)
6. **Peregudov A. V.** Analysis of keyboard handwriting. Methods of its application. *Interactive science,* 2018, no. 6 (28), pp. 59–60. (in Russ.)
7. **Protasevich A. A., Voigel E. I.** On the possibilities of criminalistic habitoscopy in the implementation of measures to counter modern cybercrime. *All-Russian Journal of Criminology*, 2020, part 14, no. 3, pp. 471–480. (in Russ.)
8. **Zainutdinova E. V.** Confidentiality of personal data in the context of cyber threats. *Legal science and practice*, 2023, vol. 19, no. 3, pp. 38–46. (in Russ.)
9. **Karunnaya Ya. A.** Problems of personal data protection in the context of digital transformation. *Legal science and practice*, 2023, vol. 19, no. 3, pp. 47–56. (in Russ.)
10. **Borovskikh R. N.** Criminal and legal aspects of cybersecurity. *Legal science and practice*, 2023, vol. 19, no. 3, pp. 17–22. (in Russ.)
11. **Tyurin V. V.** Digital transformation management. Basic theories and concepts. [B. M.]: Publishing decisions, 2023, 322 p. (in Russ.)
12. **Ghazawneh A., Henfridsson O.** A paradigmatic analysis of digital appli-cation marketplace. *Journal of Information Technology*, 2015, vol. 30, is. 3, pp. 198–208. (in Russ.)
13. **Geliskhanov I. Z., Yudina T. N.** Digital platforms: features and development prospects. *Collection of materials of the Seventy-first All-Russian Scientific and Technical Academy. conference of students, undergraduates and postgraduates of higher educational institutions with international participation.Yaroslavl: Publishing house of YSTU*, 2018, pp. 637–640.
14. **Pastukhov P. S.** Digital platforms as the basis of electronic document management in criminal proceedings. Perm Law Almanac, 2023, no. 6, pp. 521–540. (in Russ.)
15. **Khristinina E. V.** On the issue of the use of digital logistics in criminal procedure and criminalistics. *Law Bulletin of the Samara University*, 2020, vol. 6, no. 3, pp. 128–132. (in Russ.)
16. **Tagirov Z. I.** Digital operational environment, a person's digital name and network (digital) law enforcement activities in the national model of the digital economy. *Security issues*, 2018, no. 4, pp. 28–51. (in Russ.)
17. **Zhevnyak O. V.** The ratio of cloud technologies and digital form boards. *Legal Informatics*, 2024, no. 2, pp. 143–151. (in Russ.)
18. **Perov V. A.** Identification, qualification and organization of investigation of crimes committed using cryptocurrencies: textbook. Moscow: Yurliti nform, 2017. 197 p. (in Russ.)
19. **Bertovsky L. V.** Blockchain technology in criminal proceedings as an element of digital legal proceedings. *Problems of economics and legal practice*. 2017. no. 6. pp. 226–230. (in Russ.)
20. **Vekhov V. B.** Automated methods of crime investigation as a new direction in criminalistic technology. *Proceedings of Tula State University. Economic and legal sciences*, 2016, issue 3, ch. P, pp. 8–11. (in Russ.)
21. **Tolstolutsky V. Yu., Kazaryan K. S.** The use of the computer program "FORVER" in the process of interaction between the investigator and the staff of the body carrying out operational investigative activities. *Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2010, no. 2 (13), pp. 242–246. (in Russ.)
22. **Bakhteev D. V.** Features of human signature forgery recognition as primary criteria for the development of an artificial intelligence system. *Siberian Law Review*, 2020, vol. 17, no. 4, pp. 514–522. (in Russ.)
23. **Bessonov A. A.** Artificial intelligence and mathematical statistics in the criminalistic study of crimes: Monograph. Moscow, Prospekt publ., 2021, 816 p. (in Russ.)

24. **Churikova A. Y.** The use of information technologies and systems in criminal proceedings: opportunities, risks, legal regulation. Dissertation ... Saratov University of Law, 2024, 498 p. (in Russ.)
25. **Voskobitova L. A.** Digital transformation of the Russian criminal justice system and the role of the prosecutor's office as the organizer of such a transformation. *Bulletin of the University named after Kutafina*, 2024, no. 1, pp. 18–31. (in Russ.)

## Информация об авторе

**Смушкин Александр Борисович,** кандидат юридических наук, ведущий научный сотрудник проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии
SPIN 7360-6396

## Information about the Author

**Alexander Borisovich Smushkin,** PhD in Law, Senior Researcher at the Project Office of Scientific Programs and Research of the Federal State Budgetary Educational Institution of Higher Education "Saratov State Law Academy", Associate Professor at the Department of Criminology of the Federal State Budgetary Educational Institution of Higher Education "Saratov State Law Academy"; Saratov, Russian Federation
SPIN 7360-6396

*Статья поступила в редакцию 01.04.2025;*
*одобрена после рецензирования 05.05.2025; принята к публикации 30.06.2025*

*The article was submitted 01.04.2025;*
*approved after reviewing 05.05.2025; accepted for publication 30.06.2025*