

Подольный Н. А.

ТЕХНИКО-ИНСТРУМЕНТАЛЬНОЕ СОКРЫТИЕ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ: ЛАТЕНТНОСТЬ СЛЕДА И ПОТРЕБНОСТЬ В СПЕЦИАЛЬНЫХ ЗНАНИЯХ

Аннотация. Применение различных видов сервисов VPN и анонимайзеров с целью скрыть противоправные действия делает ряд информационных инцидентов юридически неопределимыми, при этом невозможно однозначно квалифицировать такое нейтральное действие как преступление. В то же время традиционный способ проведения осмотра места происшествия неприменим к информационной сфере вследствие высокой вероятности удаленного уничтожения/изменения информации — это диктует необходимость разработки новых способов фиксации и сохранения доказательств. Актуальность представленной статьи состоит в необходимости решения проблемы несоответствия роста сложности IT-инфраструктуры (экспоненциальный рост) к возможностям следственных органов. Новизна статьи состоит в обосновании базиса алгоритма интеграции специальных технических знаний в процесс построения достоверной и законной доказательственной базы при проведении расследования.

Ключевые слова: преступления, совершённые с применением цифровых технологий; цифровые следы; расследование; латентность преступлений; доказательства; специальные знания; специалист

Для цитирования: Подольный Н. А. Техничко-инструментальное сокрытие цифровых преступлений: латентность следа и потребность в специальных знаниях // Проблемы права. 2026. № 3 (103). С. 168–174. DOI: 10.24412/2075-7913-2026-3(103)-168-174

Podolnyy N. A.

TECHNICAL AND INSTRUMENTAL CONCEALMENT OF DIGITAL CRIMES: TRACE LATENCY AND THE NEED FOR SPECIAL KNOWLEDGE

Abstract. The use of various types of VPN services and anonymizers in order to conceal illegal actions makes a number of information incidents legally undefinable, and it is impossible to unambiguously classify such a neutral action as a crime. At the same time, the traditional method of conducting a scene of crime is not applicable to the information sphere due to the high probability of remote destruction/modification of information, which necessitates the development of new methods for capturing and preserving evidence. The relevance of this article lies in the need to address the issue of the discrepancy between the growing complexity of IT infrastructure (exponential growth) and the capabilities of investigative bodies. The novelty of the article lies in the justification of the basis for integrating specialized technical knowledge into the process of building a reliable and legal evidence base during investigations.

Keywords: crimes committed using digital technologies; digital traces; investigation; crime latency; evidence; specialized knowledge; specialist

For citation: Podolnyy N. A. Technical and Instrumental Concealment of Digital Crimes: Trace Latency and the Need for Special Knowledge. *Problemy*



Понятие борьбы с преступностью исторически определяется через введение уголовно-правового запрета на совершение преступления и применение наказания в отношении лица, его совершившего. Но только факт жесткости меры наказания недостаточен для реализации предупреждающего действия. Ничто не так важно как осведомленность вероятного преступника о возможности выявления им совершенных действий, идентификации личности и ее дальнейшего привлечения к ответственности. Данная особенность для деяний, связанных с использованием информационных технологий имеет особую актуальность — удаленный способ совершения деяния, возможность автоматизировать процесс совершения преступления, применение технических приспособлений для маскировки позволяют виновному чувствовать себя неуязвимым.

Поэтому неотвратимость ответственности следует понимать не как формальное наличие уголовно-правового запрета, а как реально действующую систему обнаружения, раскрытия и доказывания преступлений [1, с. 168–176]. Если технически сложные деяния выявляются лишь случайно, а установление причастного лица зависит от допущенной им грубой ошибки, предупредительное значение уголовного закона снижается. Совсем наоборот — умение правоохранительных органов выявлять неочевидные цифровые следы, связывать отдельные эпизоды в единую цепочку фактов и фиксировать их на процессуальном уровне значительно повышает субъективный уровень угрозы привлечения к ответственности.

Следовательно, гарантия неотвратимости ответственности по данной категории дел достигается не только уголовным наказанием [2, с. 297–303]. Гарантирует её определенный уровень технического обеспечения службы правопорядка, квалификация сотрудников, информационное взаимодействие между ними, применение специальных знаний.

Существенным препятствием на пути её практического обеспечения является несоответствие между сложностью применяемых преступниками технологий и технической подготовкой правоприменителя. Следователь не обладает достаточным объемом технических знаний, позволяющим самостоятельно оценивать все про-

цессы, происходящие в современных информационных системах. Такое положение нельзя объяснять лишь недостатками профессионального обучения. Оно имеет объективную основу: следователь является прежде всего юристом, владеющим нормами уголовного и уголовно-процессуального права, положениями криминалистики и методиками расследования. Одновременно быть квалифицированным программистом, сетевым администратором, специалистом по мобильным устройствам, облачной инфраструктуре, компьютерной криминалистике, анализу вредоносного программного обеспечения и криптографическим средствам защиты практически невозможно.

Вместе с тем именно следователь принимает процессуальные решения, определяет направление расследования, выдвигает версии и устанавливает предмет доказывания. Поэтому определенное понимание принципов работы цифровых технологий ему необходимо. Оно позволяет увидеть возможный источник информации, грамотно поставить задачу перед оперативным подразделением, специалистом или экспертом, а также критически оценить полученные результаты. Но знание следователем некоторых особенностей цифровой технологии не может заменить специалиста в сфере цифровых технологий, имеющего специальное образование и опыт работы, хотя оно, несомненно, полезно для качества проводимого расследования. Более того, поверхностная техническая осведомленность иногда создаёт дополнительный риск, если следователь переоценивает собственные возможности и совершает необратимые действия с электронным устройством.

Техническая сложность противоправных действий влияет на их восприятие правоохранительными органами. Традиционное преступление обычно оставляет понятные внешние признаки: повреждение имущества, телесные повреждения, недостатку, следы проникновения. В цифровой среде внешнее проявление события нередко нейтрально. Оно может выглядеть как штатный сетевой запрос, обычная авторизация, программная ошибка, автоматическая операция или использование предусмотренной разработчиком функции.

Это меняет привычную логику обнаружения преступления. Внешне нейтральное





техническое действие приобретает противоправный характер не в силу названия использованного инструмента, а с учётом полномочий лица, цели, последовательности операций и наступивших последствий. Использование штатной функции выгрузки данных может быть обычной служебной операцией, а может выступать способом хищения коммерчески значимой информации. Дистанционное соединение с персональным компьютером возможно в рамках технического обслуживания; однако в других случаях является элементом несанкционированного проникновения. Передача цифровых ценностей по адресам — сама по себе еще ничего не говорит о сути происходящего, если не смотреть на то откуда пришли деньги, кто контролирует адреса и как эта операция связана с остальными фактами.

Возможно, что преступник и не будет «ломать» систему, а использует законные программы, штатное программное обеспечение для администрирования, облачные технологии, реальные пароли. Именно поэтому эта схема стала популярной — ведь сам по себе легальный инструмент ничего не говорит о незаконности применения. Важно всё остальное — ситуация, порядок выполнения операций, права доступа к системе, задача операции, результат её проведения.

С этим непосредственно связана латентность преступлений, совершённых с применением цифровых технологий [3, с. 146–155]. В наиболее общем виде она означает, что фактически совершённое преступление остаётся неизвестным правоохранительным органам либо не получает правильной уголовно-правовой оценки и потому не отражается как преступление в официальном учёте [4, с. 179–183]. В цифровой среде можно говорить о нескольких последовательно возникающих уровнях латентности. Сначала сам потерпевший может не знать об имевшем место вмешательстве. Затем, обнаружив необычное событие, он может принять его за техническую неисправность. Организация, установившая признаки атаки, иногда сознательно не сообщает о ней из опасения репутационного ущерба. Наконец, поступившая информация может быть ошибочно воспринята правоохранительными органами как описание гражданско-правового конфликта, нарушения договора или технического инцидента.

Для того, чтобы скрыть свою деятельность преступники применяют VPN серви-

сы, прокси-узлы, анонимные сети, используют виртуальные машины, временные номера, подставные аккаунты, арендуют серверы, пользуются криптовалютой и автоудалением сообщений. Криминальные действия делят на несколько человек и технических средств. Первый — получает доступ; второй — организует технические условия; третий — выводит деньги; четвертый — работает с жертвами. Отдельное цифровое событие может казаться не заслуживающим внимания из-за незначительности либо легитимным, а криминальный смысл проявляется лишь при наличии совокупности фактов в целостном контексте.

Умышленные действия преступников направлены на то, чтобы скрыть результаты преступления за счет отнесения их к естественным событиям. Изменение цены актива, когда оно искусственно достигается посредством соответствующих манипуляций, представляется как нормальная рыночная ситуация; недоступность ресурсов сети Internet объясняется перегрузкой, наступившей в результате повышения пользовательской активности или неисправностью оборудования; безобидное списание небольших сумм — комиссией, округлением или изменением расчетной базы. Потерю клиентов можно интерпретировать как обычный переход к конкурентам, а искажение результатов автоматизированной системы — как ошибку в программном обеспечении. Маскировка особенно удачно работает, когда преступный умысел реализуется не через явную незаконную операцию, а через ряд формально допустимых действий, которые вместе приводят к желаемому результату.

В рамках расследованных уголовных дел выделяется категория цифровых преступников, которых можно назвать «дилетантами». Такие лица обладают базовыми пользовательскими навыками, умеют находить готовые руководства, покупать программное обеспечение и применять чужие разработки, однако не обладают глубоким пониманием принципов их работы. Они используют общедоступные инструменты анонимизации, готовые фишинговые пакеты, чужое вредоносное программное обеспечение или стандартные схемы социальной инженерии для совершения своих преступлений.

«Дилетант» часто ошибочно считает, что применение одного инструмента анонимизации обеспечит полную скрытность его личности. В реальности же он использует

личные и подконтрольные ему учетные записи с единого устройства, повторно применяя электронные адреса, псевдонимы и номера телефонов. Часто на его компьютере сохраняются исходные файлы, пароли, отрывки программного кода, история поиска и информация о применяемой инфраструктуре, что может привести к раскрытию его идентичности. Выплаты осуществляются через счета, которые непосредственно или косвенно связаны с виновным или его близкими. Ошибки могут быть допущены не только во время совершения преступления, но и на этапах, связанных с оплатой сервера, регистрацией почты, восстановлением пароля или общением с соучастниками.

Данные виды преступлений в большинстве случаев не сложны для расследования при условии изъятия устройств, получения информации у операторов и служб сервиса, изучения финансовых транзакций и привлечения эксперта. Расследование осуществляется за счет наличия связи цифрового следа с определенным субъектом.

Принципиально иная ситуация возникает, когда преступник глубоко понимает архитектуру информационных систем, способен самостоятельно создавать вредоносное программное обеспечение и заранее прогнозирует действия правоохранительных органов. Такой субъект не зависит от готового инструмента и может разработать программный код для конкретной цели, изменить его после каждого применения, отказаться от сохранения файлов на носителе либо встроить преступную функцию в легитимную программу. Знает, какие журналы записывает система; в каком месте хранится временная информация; как формируется маршрутизация по сети; какую информацию можно взять у оператора/провайдера.

Суть проблемы заключается не в выявлении самого факта наличия злонамеренного поведения в цифровом пространстве. Она состоит в установлении личности субъекта управления инфраструктурой; в ответе на вопросы: кто разрабатывал или применял программное обеспечение? Кто знал о природе своих действий? И на что был направлен умысел? Определение IP-адреса, устройства или аккаунта — это еще не определение исполнителя преступления.

В то же время — техническая атрибуция не равнозначна идентификации виновного лица. IP-адрес характеризует подключение к сети — человек при этом далеко не всегда идентифицируется; аккаунт мо-

жет передаваться, вороваться либо использоваться издали; наличие файла на устройстве еще не доказывает факт его создания владельцем, запуска им и осведомленности о целях использования; даже совпадение кусков программного кода имеет множество интерпретаций (например, применение публичной библиотеки или клонирование чужого программного обеспечения). Чем выше подготовка виновного, тем сложнее перейти от обнаружения технического события к доказанному выводу о сознательных действиях конкретного лица.

Основной проблемой при проведении предварительного следствия по уже совершённым преступлениям является переход от технических сведений к относимым, допустимым и достоверным доказательствам о фактах юридического значения [5, с. 423–426]. Сведения могут свидетельствовать с достаточной степенью вероятности об участии конкретного человека — однако они еще не являются доказательством.

В ходе предварительного расследования необходимо обеспечить проверяемость происхождения цифровых данных и их неизменности после обнаружения. Для этого фиксируются характеристики носителя и информационной системы, последовательность выполненных действий, применённые аппаратные и программные средства, условия копирования, временные параметры и контрольные значения. Но даже технически безупречно полученная информация должна быть связана с обстоятельствами, входящими в предмет доказывания. Для суда это значит — важно не просто видеть объект цифрового документа, а знать — что он удостоверяет; как его получили; почему в него можно верить.

Достоверность доказательств необходимо обосновать источником их получения, способом получения и мерами, предпринятыми для их сохранения, принадлежностью к определенному устройству/аккаунту, сохранением неизменности при выемке, смысловой нагрузкой в контексте соответствующего эпизода совершения преступления. При формировании копий цифровых материалов важную роль играют контрольные суммы хэш-алгоритмов, информация о программном обеспечении и оборудовании для дублирования данных; версия программного обеспечения, время создания копии и непрерывность их хранения.

В ходе проверки сообщений о преступлениях, совершенных с использованием





цифровых технологий, становится особенно очевидной недостаточность знаний следователя, работающего на уровне «пользователя». Владение компьютером и распространенными приложениями не подразумевает понимания того, где физически располагаются данные, как изменяются метаданные и какие последствия могут возникнуть после выключения устройства. Информация, отображаемая на экране, может быть хранима не на изъятом устройстве, а на удаленном сервере, что требует от следователя более глубоких технических знаний. Отключение работающей системы может привести к потере данных, хранящихся в оперативной памяти, или к блокировке зашифрованного раздела. С другой стороны, поддержание соединения с сетью может повлечь за собой удаленное уничтожение информации. Не существует универсального решения для этой ситуации; оно принимается с учетом особенностей конкретной системы.

Отсюда вытекает необходимость участия специалиста по ст. 58 УПК РФ — его участие должно быть системным (не эпизодическим), в рамках той части расследования, что касается работы с цифровыми данными [6, с. 104–108]. Не обязательно присутствие одного специалиста в ходе всего расследования, при проведении всех процессуальных действий, их может быть несколько — для проведения разных действий [7, с. 68–69]. Необходимо постоянное сопровождение специалистом всего хода расследования — от организации сбора информации о цифровых следах до определения необходимости дальнейшего сбора доказательств и формирования вопросов экспертам [8, с. 108–110].

До проведения следственного действия специалист осуществляет предварительную оценку возможных мест нахождения информации; оценивает архитектуру информационно-системы; определяет возможные потери данных. Специалист привлекается для информирования следователя о наличии шифрования, удаленного управления, синхронизации в облачных сервисах, дублировании/архивировании и специфике эксплуатации технических средств [9, с. 210–217]. В присутствии специалиста определяются технические способы сбора доказательств, устанавливается порядок действий, формулируется предмет поиска информации. Данная мера исключает бессмысленную конфискацию всего оборудования — что может привести к остановке деятельности предприятия

и в тоже время не даст возможности получить необходимую информацию.

При проведении следственного действия специалист проводит анализ устройств и элементов инфраструктуры, фиксирует работоспособность системы, выявляет действующие связи, осуществляет оценку возможности изменения содержания информации; при необходимости — участвует в процессе сохранения информации из оперативной памяти, создания копии, расчета хеш-значений, упаковки носителей информации. Также он информирует следователя о том, что происходит в данный момент — эта информация помогает ему разобраться с ситуацией. Помощь специалиста имеет тактический характер — влияет как на технические моменты в проведении расследования, так и на тактику проведения отдельных следственных действий (своевременное использование тактических приемов, позволяющих получить доказательства).

При составлении протокола специалист помогает сформулировать корректные выражения, указание на параметры устройства, программное обеспечение примененного при работе с данными; как именно были получены данные, когда и при каких условиях они были скопированы. Необходимо фиксировать не только сам факт «выявления переписки» либо «наличия вирусов», но и указывать место хранения информации (какое приложение), способ открытия данных, принадлежность к какому пользователю или учетной записи, которая была сделана на устройстве. Неполнота технического описания может привести к невозможности перепроверить доказательства и вызывает вопросы об их достоверности.

Специалист по своей сути не является следователем или экспертом. Он не осуществляет процессуальные действия, не квалифицирует правоотношения и не устанавливает вины конкретного лица [10, с. 263–270]. При необходимости установить отдельные обстоятельства совершенного деяния должно проводиться самостоятельное исследование с целью формулирования заключения эксперта — то есть назначается судебная компьютерно-техническая экспертиза. Проведение экспертизы и привлечение специалиста — это два параллельных действия следователя, они дополняют друг друга при получении доказательств, а не являются взаимоисключающими.

В ходе возбуждения уголовного дела и на стадии предварительного расследования следователь сохраняет роль организатора расследования и лица, принимающего процессуальные решения. Несмотря на то, что знание им специфики цифровых технологий не может полностью заменить специалиста с соответствующим образованием и опытом, оно существенно улучшает качество расследования и делает взаимодействие более плодотворным. Для успешного проведения следственных действий, выявления и фиксации цифровых следов, а также для копирования данных, оценки технических угроз, составления заключений и формулирования вопросов эксперту требуется присутствие специалиста в данной области.

Знание следователем особенностей применения цифровых технологий способствует повышению эффективности работы, исключает возможные ошибки и облегчает коммуникацию со специалистом в сфере компьютерной техники и программного

обеспечения. Но при этом такое знание не подменяет собой профессиональную квалификацию и стаж работы специалиста. Понимание данного обстоятельства не умаляет процессуальной самостоятельности следователя — напротив, оно служит гарантом реализации этой самостоятельности в содержательном смысле. Самостоятельность следователя применительно к цифровому миру не означает того, что он должен стремиться выполнить любую техническую задачу самостоятельно, а состоит в умении вовремя определить необходимость специализированных знаний, привлечь к работе компетентного специалиста, четко сформулировать ему задачу и эффективно использовать полученные результаты в рамках требований уголовно-процессуального законодательства. Данный методологический подход позволяет способствовать снижению скрытности цифровых преступлений и позволяет реализовывать принцип неотвратимости уголовной ответственности.

Литература

1. Силкин В. П. Неотвратимость уголовной ответственности в законе, теории и правоприменительной практике // *Ius Publicum et Privatum*. — 2023. — № 2(22). — С. 168–176.
2. Николаев И. А. Теоретико-правовая проблема реализации принципа неотвратимости юридической ответственности // *Моя профессиональная карьера*. — 2025. — Т. 1, № 73. — С. 297–303.
3. Поляков В. В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня // *Всероссийский криминологический журнал*. — 2023. — Т. 17, № 2. — С. 146–155.
4. Палий Е. С. К вопросу о латентности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // *Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики* (памяти профессора С. Е. Вицина) (к 50-летию образования Московской высшей школы милиции МВД СССР): Сборник научных трудов Всероссийской научно-практической конференции, Москва, 18 июня 2025 года. — Москва: Московский университет МВД РФ им. В. Я. Кикотя, 2025. — С. 179–183.
5. Ахъядов Э. С. М. Основные характеристики преступлений, совершаемых в сфере обращения цифровой информации // *Аграрное и земельное право*. — 2026. — № 1. — С. 423–426.
6. Молохов А. В. Эволюция роли специалиста в уголовном процессе // *Устав уголовного судопроизводства 1864 г. и его влияние на современный уголовный процесс* (Памяти Николая Андреевича Буцковского (1811–1873): Материалы Всероссийской научно-практической конференции, Москва, 16 ноября 2023 года. — Москва: Московская академия Следственного комитета Российской Федерации, 2024. — С. 104–108.
7. Темирханова М. Т. Специалист как субъект уголовного процесса // *NovalInfo. Ru*. — 2021. — № 124. — С. 68–69.
8. Хачикян С. А. Особенности участия специалиста в уголовном процессе на стадии возбуждения уголовного дела // *Тенденции развития науки и образования*. — 2023. — № 97–6. — С. 108–110.
9. Лукошкина С. В. Проблемы изъятия электронного носителя информации в контексте участия специалиста и назначения судебных экспертиз // *Всероссийский криминологический журнал*. — 2024. — Т. 18, № 2. — С. 210–217.
10. Сотников К. И. Тактико-правовые нюансы участия специалиста при проведении следственных действий, связанных с изъятием и копированием электронной информации // *Судебная экспертиза: прошлое, настоящее и взгляд в будущее: Материалы международной научно-практической конференции, Санкт-Петербург, 16 мая 2025 года*. — Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2025. — С. 263–270.



References

1. Silkin V. P. Neotvratimost' ugovnoy otvetstvennosti v zakone, teorii i pravoprime-nitel'noj praktike // *Ius Publicum et Privatum*. — 2023. — № 2(22). — S. 168–176.
2. Nikolaev I. A. Teoretiko-pravovaya problema realizacii principa neotvratimosti yuridicheskoy otvetstvennosti // *Moya professional'naya kar'era*. — 2025. — T. 1, № 73. — S. 297–303.
3. Polyakov, V. V. Latentnost' vy'sokotekhnologichny'x prestuplenij: ponyatie, struk-tura, metody' ocenki urovnya // *Vserossijskij kriminologicheskij zhurnal*. — 2023. — T. 17, № 2. — S. 146–155.
4. Palij E. S. K voprosu o latentnosti prestuplenij, sovershaemy'x s ispol'zovaniem informacionno-telekommunikacionny'x tehnologij // *Voprosy' sovershenstvovaniya pravooxranitel'noj deyatel'nosti: vzaimodejstvie nauki, normotvorchestva i prakti-ki (pamyati professora S. E. Vicina) (k 50-letiyu obrazovaniya Moskovskoj vy'sshej shkoly' milicii MVD SSSR): Sbornik nauchny'x trudov Vserossijskoj nauchno-prak-ticheskoy konferencii, Moskva, 18 iyunya 2025 goda*. — Moskva: Moskovskij univer-sitet MVD RF im. V. Ya. Kikotya, 2025. — S. 179–183.
5. Ax'yadov E'. S. M. Osnovny'e karakteristiki prestuplenij, sovershaemy'x v sfere obrashheniya cifrovoj informacii // *Agrarnoe i zemel'noe pravo*. — 2026. — № 1. — S. 423–426.
6. Moloxov A. V. E'voluciya roli specialista v ugovnom processe // *Ustav ugovlov-nogo sudoproizvodstva 1864 g. i ego vliyaniye na sovremenny'j ugovny'j process (Pamyati Nikolaya Andreevicha Buczkovskogo (1811–1873): Materialy' Vserossijskoj nauchno-prakticheskoy konferencii, Moskva, 16 noyabrya 2023 goda*. — Moskva: Moskovskaya akademiya Sledstvennogo komiteta Rossijskoj Federacii, 2024. — S. 104–108.
7. Temirxanova M. T. Specialist kak sub'ekt ugovnogo processa // *NovalInfo.Ru*. — 2021. — № 124. — S. 68–69.
8. Xachikyan S. A. Osobennosti uchastiya specialista v ugovnom processe na sta-dii vzbuzhdeniya ugovnogo dela // *Tendencii razvitiya nauki i obrazovaniya*. — 2023. — № 97–6. — S. 108–110.
9. Lukoshkina S. V. Problemy' iz'`yatiya e'lektronnogo nositelya informacii v kon-tekste uchastiya specialista i naznacheniya sudebny'x e'kspertiz // *Vserossijskij kriminologicheskij zhurnal*. — 2024. — T. 18, № 2. — S. 210–217.
10. Sotnikov K. I. Taktiko-pravovy'e nyuansy' uchastiya specialista pri provedenii sledstvenny'x dejstvij, svyazanny'x s iz'`yatiem i kopirovaniem e'lektronnoj infor-macii // *Sudebnaya e'kspertiza: proshloe, nastoyashhee i vzglyad v budushhee: Materialy' mezhdunarodnoj nauchno-prakticheskoy konferencii, Sankt-Peterburg, 16 maya 2025 goda*. — Sankt-Peterburg: Sankt-Peterburgskij universitet MVD RF, 2025. — S. 263–270.

Сведения об авторе

Подольный Н. А. — доктор юридических наук, профессор, заведующий кафедрой уголовного процесса и криминалистики, Казанский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России). Казань. E-mail: ipk-saransk@yandex.ru

Information about the author

Podolnyy Nikolai A. — Doctor of juridical sciences, professor, head of the sub-department of criminal procedure and criminalistics, Kazan Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia). Kazan. E-mail: ipk-saransk@yandex.ru

Конфликт интересов отсутствует.
There is no conflict of interest.

Дата поступления статьи / Received: 15.08.2026

Дата рецензирования / Received: 23.08.2026

Дата принятия к опубликованию / Accepted: 25.08.2026

