Научная статья
УДК 343.985.7:004.8





ЦИФРОВОЙ ПОВЕДЕНЧЕСКИЙ ПРОФИЛЬ: ПРАВОВЫЕ ОСНОВАНИЯ И МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ

Лада Ярославовна Смирнова,
Московский областной филиал Московского ордена Почёта университета МВД России имени В.Я. Кикотя, Московская область, Россия,
smirnov_0303@mail.ru
Эльвира Тагировна Хайруллова,
Казанский юридический институт МВД России, Казань, Россия,
elv_hai@mail.ru

Аннотация

Введение: работа посвящена теоретико-правовому осмыслению цифрового поведенческого профиля (далее ЦПП) как комплексного средства раскрытия и расследования преступлений, совершаемых через информационно-телекоммуникационные сети; тема актуальна на фоне сохраняющегося высокого уровня IT-преступности и нерешённости вопроса об алгоритмических доказательствах.

Цель: предложить авторское определение ЦПП, систематизировать источники данных для его построения и разработать трёхмодульную методику анализа.

Материалы и методы: основу составили 47 уголовных дел судов Республики Татарстан и соседних регионов за 2020–2024 годы, опрос 57 следователей МВД России и анализ зарубежного нормативного и доктринального опыта; применялись системный анализ, сравнительное правоведение и структурно-функциональное моделирование.

Результаты: предложена классификация источников данных, разработана трёхмодульная методика построения профиля, обоснованы дополнения к ч. 2 ст. 74 УПК РФ о самостоятельном виде электронных доказательств.

Обзор литературы выявил отсутствие в отечественной криминалистике целостной концепции ЦПП как самостоятельного процессуального инструмента.

Обсуждение и заключение: внедрение профиля в следственную практику требует специального ведомственного акта МВД России и законодательного закрепления алгоритмической объяснимости как условия допустимости доказательств.

Ключевые слова: цифровой поведенческий профиль; цифровой след; машинное обучение; криминалистическое профилирование; раскрытие преступлений; электронные доказательства; большие данные; кросс-платформенный анализ; уголовное судопроизводство; искусственный интеллект

© Смирнова Л.Я., Хайруллова Э.Т., 2026

Для цитирования: Смирнова Л.Я., Хайруллова Э.Т. Цифровой поведенческий профиль: правовые основания и методология формирования // Вестник Казанского юридического института МВД России. 2026. Т. 17. № 3 (65). С. 127 –134.

Scientific article
UDC 343.985.7:004.8

DIGITAL BEHAVIORAL PROFILE: LEGAL FOUNDATIONS AND METHODOLOGY OF FORMATION

Lada Yaroslavovna Smirnova,
Moscow Regional Branch of the Moscow Order of Honor University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, Moscow, Russia,
smirnov_0303@mail.ru
Elvira Tagirovna Khairullova,
Kazan Law Institute Ministry of MIA of Russia, Kazan, Russia,
elv_hai@mail.ru

Abstract

Introduction: the article offers a theoretical and legal analysis of the digital behavioral profile (DBP) as a composite tool for detecting and investigating crimes committed through information and telecommunications networks; the topic is timely given the persistently high level of IT crime and the unsettled status of algorithmic evidence.

The purpose is to propose an original definition of the DBP, to systematize the data sources used to build it and to design a three-module analytical methodology.

Materials and Methods: the study rests on 47 criminal cases heard by courts of the Republic of Tatarstan and neighbouring regions in 2020–2024, a survey of 57 investigators of the Russian Ministry of Internal Affairs and an examination of foreign regulatory and doctrinal experience; systemic analysis, comparative law and structural-functional modelling were applied.

Results: a classification of data sources is proposed, a three-module methodology for building the profile is developed, and amendments to Part 2 of Article 74 of the Criminal Procedure Code introducing a distinct type of electronic evidence are justified.

Literature review revealed the absence, in Russian forensic science, of a coherent concept of the DBP as an independent procedural tool.

Discussion and Conclusions: bringing the profile into investigative practice calls for a dedicated departmental act of the Ministry of Internal Affairs and for making algorithmic explainability a statutory condition of admissibility.

Keywords: digital behavioral profile; digital footprint; machine learning; forensic profiling; crime detection; electronic evidence; big data; cross-platform analysis; criminal proceedings; artificial intelligence

© Smirnova L.Y., Khairullova E.T., 2026

For citation: Smirnova L.Y., Khairullova E.T. Digital Behavioral Profile: Legal Foundations and Methodology of Formation. Bulletin of the Kazan Law Institute of MIA of Russia. 2026;17(3):127-134. (In Russ.).

Введение

Цифровые технологии изменили большинство сфер общественной жизни, и преступность не стала исключением. Аналитики компании IDC прогнозируют, что мировой объём создаваемых и потребляемых данных продолжит стремительный рост и к 2030 году превысит 700 зеттабайт [1]. Сопоставимый масштаб проникновения цифровых технологий в противоправную деятельность отражает и российская статистика: по сведениям Генеральной прокуратуры Российской Федерации, число преступлений, совершённых с использованием информационных технологий, достигло пика в 2024 году (765,4 тыс.), а по итогам 2025 года впервые за несколько лет снизилось – до около 675 тыс. (на 11,8% меньше, чем годом ранее); тенденция сохранилась и в первом полугодии 2026 года – около 253 тыс. зарегистрированных преступлений (на 31,9% меньше, чем за тот же период 2025 года)[1]. Вместе с тем их доля в общей структуре преступности остаётся высокой – порядка 38%, а причиняемый ущерб и технологическая сложность применяемых схем продолжают расти.

[1] Состояние преступности в Российской Федерации: статистические сборники Генеральной прокуратуры РФ за январь – декабрь 2025 года и январь – июнь 2026 года. Москва, 2026. URL: https://epp.genproc.gov.ru/web/gprf/activity/statistics (дата обращения: 05.09.2026).

Любое действие в цифровой среде оставляет след. Сведения о лице накапливаются в телекоммуникационных сетях, на серверах интернет-сервисов, в платёжных системах, в памяти устройств Интернета вещей, и объём таких данных велик. Сложность в другом: следы разрознены и слабо структурированы. Проведённое нами анкетирование 57 следователей МВД России показало, что трудность сведе́ния цифровых данных из разных источников в единую картину 67,8% респондентов назвали главным препятствием при расследовании IT-преступлений.

Отсюда вытекает потребность в методике, которая объединяла бы отдельные цифровые следы в связную аналитическую модель поведения подозреваемого. Такую модель мы обозначаем как цифровой поведенческий профиль (далее – ЦПП). За рубежом это направление известно под названием Digital Behavioral Profiling, однако отечественная криминалистика разработала его слабо: единых требований к построению ЦПП не выработано, процессуальное положение получаемых сведений не определено, вопрос об их допустимости в суде не решён.

Настоящая статья ставит целью сформировать теоретическую базу концепции ЦПП и предложить методику его построения. Для этого решаются четыре задачи: дать авторское определение цифрового поведенческого профиля; классифицировать источники данных; изложить трёхмодульную методику формирования профиля; оценить правовые препятствия его применения в уголовном судопроизводстве и предложить поправки в законодательство. Новизна работы в том, что ЦПП впервые описывается как целостный самостоятельный инструмент криминалистики.

Материалы и методы

Исследование опирается на диалектический метод познания. В его рамках задействованы системный анализ – при построении трёхмодульной методики; структурно-функциональное моделирование – при описании связей между её компонентами; сравнительно-правовой метод – при сопоставлении подходов США, Германии, Нидерландов и Великобритании к регулированию алгоритмических доказательств; формально-юридический метод – при разборе норм УПК РФ и ведомственных актов МВД России; статистический метод – при обработке результатов анкетирования.

Эмпирическую основу образуют четыре группы материалов. Первую составили 47 уголовных дел, рассмотренных судами Республики Татарстан, Самарской и Нижегородской областей в 2020-2024 годах по преступлениям в сфере ИКТ: 24 дела о мошенничестве, 11 – о сбыте наркотиков через интернет, 8 – об экстремизме, 4 – прочие. Вторую – данные опроса 57 следователей Следственного департамента МВД России, проведённого в 2023-2024 годах. Третью – аналитические доклады Европола IOCTA за 2025 и 2026 годы и материалы Центра цифровых расследований ФБР США за 2022-2026 годы. Четвёртую – технические стандарты ISO/IEC 27037:2012 и ISO/IEC 27042:2015.

Результаты исследования

1. Авторское определение и структура ЦПП. Проведённый анализ позволяет предложить следующее определение. Цифровой поведенческий профиль – упорядоченная совокупность проверенных сведений о цифровых следах конкретного лица, собранных из разнородных информационно-телекоммуникационных источников и систематизированных с помощью кросс-платформенного корреляционного анализа и методов машинного обучения; такая совокупность даёт возможность установить идентификационные признаки лица, его поведенческие паттерны, круг социальных связей и последовательность действий в цифровой среде для целей раскрытия и расследования преступлений.

Предложенное определение отграничивает ЦПП от близких понятий. В отличие от классического «профиля преступника» (Criminal Profiling), профиль опирается не на психологический прогноз, а только на объективно зафиксированные данные. От «цифрового следа» его отличает интегративность: ЦПП представляет собой не единичный след, а продукт агрегации и упорядочивания множества следов, поступивших из разных систем.

В структуре профиля выделяются три уровня. Идентификационный объединяет учётные данные, аппаратные идентификаторы (MAC, IMEI, IMSI) и биометрические маркеры. Поведенческий охватывает паттерны сетевой активности, временны́е закономерности и коммуникативные связи. Событийный фиксирует конкретные действия лица, сопоставленные с обстоятельствами расследуемого события.

2. Классификация источников данных для формирования ЦПП. Опираясь на следственную практику и технические возможности информационных систем, мы сгруппировали источники данных так, как показано в таблице 1.

Распределение источников по изученным делам оказалось неравномерным. Телекоммуникационные данные фигурировали во всех делах (100%), сведения платёжных систем – в 34 делах (72,3%), материалы OSINT – в 32 (68,1%), дан-

Таблица 1. Классификация источников данных для формирования ЦПП
Table 1. Classification of data sources for DBP formation

Категория / Category	**Виды данных / Data types**	**Правовое основание / Legal basis**
Операторы связи и телекоммуникационные сети	Детализация звонков, SMS; геолокация (базовые станции); история интернет-сессий (СОРМ-3); сведения об абоненте	Ст. 186.1 УПК РФ; ФЗ «Об ОРД»
Цифровые платформы и интернет-сервисы	Учётные записи в соцсетях; история запросов; геометки публикаций; переписка в мессенджерах; электронная почта	Ст. 182, 183 УПК РФ; MLAT
Электронные платёжные системы и банки	История транзакций; сведения о счетах; криптовалютные переводы; IP-адреса при операциях	Ст. 183 УПК РФ; ФЗ «О банках и банковской деятельности»
Устройства Интернета вещей (IoT)	Смарт-часы, фитнес-трекеры; навигационные системы автомобилей; умные колонки; системы «умный дом»	Ст. 182, 183 УПК РФ; нормы о персональных данных
Системы видеонаблюдения и биометрии	Камеры с распознаванием лиц; анализ походки (Gait Recognition); голосовая биометрия	Ст. 185.1 УПК РФ; ФЗ «О персональных данных»
Открытые источники (OSINT)	Публичные профили в соцсетях; реестры WHOIS; государственные реестры (ЕГРЮЛ, Росреестр)	Специального основания не требует

ные социальных сетей – в 30 (63,8%), видеозаписи с распознаванием – в 8 (17%), информация с устройств Интернета вещей – лишь в 4 (8,5%). Последняя цифра говорит о недооценке этого источника, тогда как в зарубежной практике записи IoT-устройств не раз становились решающим доказательством[1].

3. Трёхмодульная методология формирования ЦПП. Методика построения профиля складывается из трёх модулей.

Модуль I – *сбор и агрегация данных* (Data Collection & Aggregation). Он включает следственные и оперативно-розыскные мероприятия по получению сведений из всех перечисленных категорий источников. Работа модуля подчинена нескольким принципам: охват должен быть полным, каждое действие – законным, фиксация – своевременной (цифровые следы недолговечны), а целостность данных – подтверждённой криптографически (хеш-функция SHA-256). Практически это означает запросы операторам связи по ст. 186.1 УПК РФ[2], выемку и осмотр носителей по правилам ст. 182–183 УПК РФ, обращения в иностранные юрисдикции по каналам MLAT, а также оперативно-розыскные мероприятия «снятие информации с технических каналов связи» и «получение компьютерной информации»[3].

Модуль II – *кросс-платформенный корреляционный анализ* (Cross-Platform Correlation Analysis). Здесь применяются четыре инструмента. Анализ социальных сетей (Social Network Analysis, SNA) вскрывает коммуникативные связи лица и его роль в преступной группе; в делах о мошенничестве он помог установить соучастников в 11 случаях из 24. Анализ временны́х закономерностей (Temporal Pattern Analysis, TPA) обнаруживает устойчивые хроноритмы активности. Геопространственный анализ (Geospatial Analysis, GA) сводит разрозненные сведения о местоположении в общую карту перемещений. Обработка естественного языка (Natural Language Processing, NLP) выявляет особенности идиолекта и связывает псевдонимные аккаунты с их владельцем.

Модуль III – *нейросетевая верификация* (Neural Network Verification). На этом этапе про-

[1] State v. Bates, Pulaski County Circuit Court (Arkansas), No. 60CR-17-325, 2017. Суд рассматривал допустимость записей умной колонки Amazon Echo в качестве доказательства по уголовному делу об убийстве. URL: https://www.courtlistener.com/docket/5783524 (дата обращения: 05.09.2026).

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 10.06.2026) // Собрание законодательства РФ. 2001. № 52 (ч. 1), ст. 4921. СПС «КонсультантПлюс» (дата обращения: 05.09.2026).

[3] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025) // Собрание законодательства РФ. 1995. № 33, ст. 3349. СПС «КонсультантПлюс» (дата обращения: 05.09.2026).

филь проверяется ансамблевыми методами машинного обучения (Ensemble Learning): градиентным бустингом, случайным лесом, нейронными сетями с механизмом внимания (Attention-based Neural Networks). Обязательное условие – алгоритмическая объяснимость (Explainable AI, XAI): каждый вывод системы должен сопровождаться отсылкой к исходным данным, на которых он построен. Без этого профиль нельзя проверить в суде, а сторона защиты лишается возможности его оспорить. Требование объяснимости согласуется и с национальной стратегией развития искусственного интеллекта[1].

4. Правовые проблемы использования ЦПП в уголовном судопроизводстве. Применение профиля упирается в четыре нерешённых вопроса.

Первый – в перечне доказательств нет такого их вида, как электронные данные. Часть 2 статьи 74 УПК РФ[2] среди допустимых доказательств их не называет. На практике алгоритмически полученные сведения приобщают либо как «иные документы» (п. 6 ч. 2 ст. 74 УПК РФ), либо как вещественные доказательства, что не соответствует природе ЦПП – результата аналитической обработки данных.

Второй – неясен статус доказательств, добытых средствами машинного обучения. Нейросетевые модели работают по принципу «чёрного ящика» (Black Box): суд не может проверить их методологию, а защита – предметно оспорить полученный вывод. Показателен спор Loomis v. Wisconsin (2016), где Верховный суд штата Висконсин оценивал конституционность применения системы COMPAS при назначении наказания[3].

Третий – почти не урегулирована агрегация данных из разных источников. Порядок получения каждого вида сведений закон описывает, но норм о сведении разнородных данных в единый аналитический продукт не содержит; остаётся открытым вопрос, каким следственным действием оформляется само построение профиля.

Четвёртый – агрегация угрожает правам личности. Соединение отдельных фрагментов данных выводит вмешательство в частную жизнь на новый уровень; в литературе это называют «мозаичным эффектом» (Mosaic Effect). Действующее регулирование обработки персональных данных[4] под такую специфику не рассчитано и требует корректировки.

5. Предложения по совершенствованию законодательства. На основе изложенного предлагается ряд изменений.

Во-первых, дополнить ч. 2 ст. 74 УПК РФ пунктом 7: «7) электронные (цифровые) доказательства – любые данные в электронной форме, полученные, хранящиеся или переданные с использованием компьютерных систем, а также результаты их аналитической обработки с использованием автоматизированных информационных систем, если они имеют значение для уголовного дела».

Во-вторых, ввести в УПК РФ статью 164.2 «Особенности получения электронных доказательств», закрепив в ней обязательную криптографическую верификацию данных, порядок удалённой выемки у отечественных и зарубежных провайдеров и требование алгоритмической объяснимости при работе автоматизированных аналитических систем.

В-третьих, издать приказ МВД России об утверждении методических рекомендаций по формированию ЦПП. В них следует определить перечень источников данных, порядок доступа к каждому из них, технические требования к программно-аппаратным средствам и форму протокола с обязательным указанием применённых алгоритмов.

В-четвёртых, установить критерии допустимости алгоритмических доказательств, ориентируясь на американский стандарт Дауберта (Daubert Standard): результат должен быть проверяемым, погрешность метода – известной, а сам метод – признанным в научном сообществе.

Обзор литературы

Отечественная наука обратилась к цифровому следу как объекту криминалистики в конце 1990-х годов. Теорию компьютерно-технической экспертизы существенно продвинули Е.Р. Россинская и Е.И. Галяшина: они классифицировали виды цифровых следов и заложили научную основу их исследования [2]. Проблематику расследования преступлений в сфере компьютерной информации разрабатывал В.А. Мещеряков, приложивший теорию цифро-

[1] О Национальной стратегии развития искусственного интеллекта на период до 2030 года: Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) // Собрание законодательства РФ. 2019. № 41, ст. 5700.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 10.06.2026), ч. 2 ст. 74 «Доказательства» // Собрание законодательства РФ. 2001. № 52 (ч. 1), ст. 4921.

[3] Loomis v. State, 881 N.W.2d 749 (Wis. 2016). Wisconsin Supreme Court. Certiorari denied, 137 S. Ct. 2290 (2017). URL: https://scholar.google.com/scholar_case?case=5456278755958704579 (дата обращения: 05.09.2026).

[4] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. 2006. № 31 (1 ч.), ст. 3451.

вой криминалистики к российской следственной практике [3].

За рубежом фундамент дисциплины составили работы Э. Кейси [4], предложившего модель оценки достоверности цифровых доказательств, и Б. Кэрриера [5], построившего теорию криминалистического анализа файловых систем. Организационным ориентиром долгое время служила модель DFRWS (Digital Forensic Research Workshop, 2001). Все эти построения, однако, рассчитаны прежде всего на работу с уже изъятыми носителями и не затрагивают комплексный поведенческий анализ, ведущийся в реальном времени.

Отдельный пласт зарубежных исследований посвящён большим данным и машинному обучению в правоохранительной сфере. Х. Чен, М. Чау и Я. Ван [6] обобщили методы Crime Data Mining, включая алгоритмы кластеризации и поиска ассоциаций для нужд расследования. К этому примыкает тема выявления мошеннических транзакций средствами нейросетевого анализа, напрямую связанная с задачами построения ЦПП.

Правовую сторону вопроса освещают В.В. Конин и А.А. Давлетов: они констатируют, что в действующем УПК РФ специальных норм об электронных доказательствах нет [7]. К такому же выводу применительно к европейским правопорядкам приходят Б. Шварц и Р. Коэн [8], предупреждая, что алгоритмически непрозрачные системы подрывают состязательность процесса. Обсуждается в доктрине и риск «алгоритмического суверенитета» следователя, когда профессиональное усмотрение вытесняется автоматическими выводами системы.

Складывается характерная картина: технологический инструментарий цифрового анализа развит, правовая доктрина об электронных доказательствах обширна, но связующего теоретико-методологического звена между ними нет. Восполнить этот пробел и призвана концепция ЦПП.

Обсуждение и заключение

Проведённое исследование позволяет сформулировать несколько выводов.

Первый. ЦПП следует рассматривать как новый криминалистический инструмент, главное свойство которого – интегративность. Соединяя данные многих разнородных источников в одну аналитическую конструкцию, профиль даёт о поведении лица в цифровой среде куда более полное представление, чем любой отдельно взятый след.

Второй. Предложенная методика удерживает равновесие между технологической эффективностью и правовой допустимостью результата. Её опорным звеном выступает требование XAI: именно оно открывает возможность судебной проверки профиля и обеспечивает состязательность сторон.

Третий. Практика обнажает разрыв между тем, что умеют системы цифрового анализа, и тем, как это обеспечено нормативно. Правовой вакуум чреват признанием доказательств недопустимыми и не даёт гражданам гарантий от произвольного вторжения в частную жизнь.

Четвёртый. Зарубежный опыт – Директива ЕС 2016/680 и Принципы применения искусственного интеллекта в правосудии, утверждённые Консультативным советом европейских судей [9], – показывает, что при продуманном регулировании алгоритмические инструменты и защита прав личности вполне совместимы.

Дальнейшую работу мы связываем с созданием видовых методик ЦПП-анализа под отдельные категории преступлений, изучением ЦПП как возможного объекта нового рода судебной экспертизы и проработкой вопросов трансграничного получения данных с опорой на нормы международного уголовно-процессуального права.

СПИСОК ИСТОЧНИКОВ

1. Worldwide IDC Global DataSphere Forecast, 2026–2030: IDC Market Forecast (Doc. № US53425426). Needham: IDC, 2026.
2. Россинская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2021. 464 с.
3. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та, 2019. 408 с.
4. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. London: Academic Press, 2022. 936 p.
5. Carrier B. File System Forensic Analysis. Boston: Addison-Wesley, 2005. 600 p.
6. Chen H., Chau M., Wang Y. Crime Data Mining: An Overview and Case Studies // International Journal of Digital Crime and Forensics. 2020. Vol. 12. № 3. P. 1–22. doi: 10.4018/IJDCF.2020070101.

7. Конин В.В., Давлетов А.А. Электронные доказательства в уголовном процессе: современное состояние и перспективы регулирования // Вестник Московского университета. Серия 11: Право. 2022. № 4. С. 87–104.
8. Schwartz B., Cohen R. Algorithmic Accountability in Criminal Justice: A Comparative Study // European Journal of Crime, Criminal Law and Criminal Justice. 2021. Vol. 29. № 2. P. 133–162. doi: 10.1163/15718174-29020001.
9. Consultative Council of European Judges (CCJE). Opinion No. 22 on the Role of Judicial Officers in the Digital Age. Strasbourg: Council of Europe, 2019. 18 p.

REFERENCES

1. Worldwide IDC Global DataSphere Forecast, 2026–2030: IDC Market Forecast (Doc. № US53425426). Needham: IDC, 2026.
2. Rossinskaya E.R., Galyashina E.I. Nastol'naya kniga sud'i: sudebnaya ekspertiza. Moskva: Prospekt, 2021. 464 s.
3. Meshcheryakov V.A. Prestupleniya v sfere komp'yuternoj informacii: osnovy teorii i praktiki rassledovaniya. Voronezh: Izd-vo Voronezh. gos. un-ta, 2019. 408 s.
4. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 4th ed. London: Academic Press, 2022. 936 p.
5. Carrier B. File System Forensic Analysis. Boston: Addison-Wesley, 2005. 600 p.
6. Chen H., Chau M., Wang Y. Crime Data Mining: An Overview and Case Studies // International Journal of Digital Crime and Forensics. 2020. Vol. 12. № 3. P. 1–22. doi: 10.4018/IJDCF.2020070101.
7. Konin V.V., Davletov A.A. Elektronnye dokazatel'stva v ugolovnom processe: sovremennoe sostoyanie i perspektivy regulirovaniya // Vestnik Moskovskogo universiteta. Seriya 11: Pravo. 2022. № 4. S. 87–104.
8. Schwartz B., Cohen R. Algorithmic Accountability in Criminal Justice: A Comparative Study // European Journal of Crime, Criminal Law and Criminal Justice. 2021. Vol. 29. № 2. P. 133–162. doi: 10.1163/15718174-29020001.
9. Consultative Council of European Judges (CCJE). Opinion No. 22 on the Role of Judicial Officers in the Digital Age. Strasbourg: Council of Europe, 2019. 18 p.

Информация об авторах:
Смирнова Лада Ярославовна, кандидат экономических наук, доцент, начальник кафедры социально-экономических и гуманитарных дисциплин Московского областноого филиала Московского ордена Почёта университета МВД России имени В.Я. Кикотя, Московская область, Россия, e-mail: smirnov_0303@mail.ru
Хайруллова Эльвира Тагировна, кандидат педагогических наук, доцент, начальник кафедры криминалистики Казанского юридического института МВД России, Республика Татарстан, Россия, e-mail: elv_hai@mail.ru
Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:
Smirnova Lada Ya., candidate of Economic Sciences, Associate Professor, Head of the Department of Social, Economic, and Humanitarian Disciplines, Moscow Regional Branch of the Moscow Order of Honor University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, e-mail: smirnov_0303@mail.ru
Khairullova Elvira T., candidate of Pedagogical Sciences, Associate Professor, Head of the Department of Criminalistics of Kazan Law Institute Ministry of MIA of Russia, e-mail: elv_hai@mail.ru
The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов
Смирнова Лада Ярославовна – концепция и инициация исследования; осуществление критического анализа и доработка текста.
Хайруллова Эльвира Тагировна – подготовка первоначального варианта текста; анализ нормативных правовых актов и научных материалов; формирование выводов; поиск аналитических материалов в официальных источниках.

Статья получена: 13.04.2026.
Статья принята к публикации: 30.09.2026.
Статья опубликована онлайн: 30.09.2026.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаем.