DOI: 10.25806/mr-65

Ссылка для цитирования: Лытнев А.М. Перспективы использования открытых источников информации в оперативно-розыскной деятельности оперативных подразделений системы МВД России: комплексное исследование возможности внедрения технологий разведки по открытым источникам (OSINT) // Modern Review of Academic Problems. 2026. № 3. - URL: https://modernreview.ru/index.php/journal/article/view/65

How to cite: Lytnev A.M. Prospects for the use of open-source information in the operational-search activities of law enforcement units within the Russian ministry of internal affairs: a comprehensive study on the feasibility of implementing open-source intelligence (OSINT) technologies // Modern Review of Academic Problems. 2026. No. 3. - URL: https://modernreview.ru/index.php/journal/article/view/65

Научная статья / Original article

УДК 343.2.7

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ СИСТЕМЫ МВД РОССИИ: КОМПЛЕКСНОЕ ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ РАЗВЕДКИ ПО ОТКРЫТЫМ ИСТОЧНИКАМ (OSINT)

Лытнев А.М.

Брянский филиал Орловского юридического института МВД России имени В.В. Лукьянова, Брянск, email: sabi47@yandex.ru

Аннотация
Данная статья направлена на комплексное изучение вопроса интеграции технологий разведки по открытым источникам (OSINT) в деятельность оперативных подразделений системы МВД России. Целью работы является не только использование общедоступных данных, но и выявление системных противоречий между скоростью технологического развития общества и существенным отставанием правового регулирования в данной сфере в системе МВД. На основе анализа официальных источников, актуальной судебной практики арбитражных судов и судов общей юрисдикции за 2024 и 2025 годы, а также материалов правоприменительной практики органов внутренних дел, последовательно разберём три взаимосвязанных аспекта, имеющие наибольшие противоречия. Первый блок будет посвящен трансформации доказательственной базы оперативно-розыскной деятельности и легализации цифровых следов OSINT в уголовном процессе. Второй блок посвящен влиянию искусственного интеллекта и автоматизации на тактику оперативной-розыскной деятельности, а третий существенной угрозе информационной безопасности при работе с большими массивами открытых данных. Методологическую основу составляет взаимодействие сравнительно-правового анализа законодательства РФ, анализа судебных решений Верховного Суда РФ и моделирования различных оперативно-розыскных ситуаций. Необходимо переходить от эпизодического использования интернета, к созданию непрерывного аналитического цикла обработки открытых данных, как неотъемлемой части современной правоохранительной системы, требующей пересмотра нормативной базы и в частности Федерального закона №144-ФЗ «Об ОРД».

Ключевые слова: открытые источники информации, OSINT, оперативно-розыскная деятельность, цифровые следы, искусственный интеллект, легализация доказательств, персональные данные, киберпреступность, межведомственное взаимодействие, хеш-сумма.

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Статья поступила в редакцию 10.10.2026, одобрена после рецензирования 13.11.2026, опубликована 16.11.2026.

PROSPECTS FOR THE USE OF OPEN-SOURCE INFORMATION IN THE OPERATIONAL-SEARCH ACTIVITIES OF LAW ENFORCEMENT UNITS WITHIN THE RUSSIAN MINISTRY OF INTERNAL AFFAIRS: A COMPREHENSIVE STUDY ON THE FEASIBILITY OF IMPLEMENTING OPEN-SOURCE INTELLIGENCE (OSINT) TECHNOLOGIES

Lytnev A.M.

Bryansk Branch of the Oryol Law Institute of the Ministry of Internal Affairs of Russia, Bryansk, email: sabi47@yandex.ru

Abstract
This article is aimed at a comprehensive study of the integration of Open-Source Intelligence (OSINT) technologies into the activities of operational units within the system of the Ministry of Internal Affairs of Russia. The objective of the work is not only the utilization of publicly available data but also the identification of systemic contradictions between the rapid pace of technological development in society and the significant lag in legal regulation within this sphere in the MVD system. Based on the analysis of official sources, current judicial practice of arbitration courts and courts of general jurisdiction for the period of 2024 and 2025, as well as materials from the law enforcement activities of internal affairs bodies, the author sequentially examines three interconnected aspects that contain the most significant contradictions. The first aspect is dedicated to the transformation of the evidentiary basis of operational-investigative activity and the legitimization of digital OSINT traces in the criminal process. The second aspect examines the impact of artificial intelligence and automation on the tactics of operational-investigative activity, while the third addresses the critical threat to information security when working with large arrays of open data. The methodological basis consists of the interplay of comparative legal analysis of the legislation of the Russian Federation, analysis of judicial decisions of the Supreme Court of the Russian Federation, and the modeling of various operational-investigative situations. It is necessary to transition from episodic internet usage to the creation of a continuous analytical cycle for processing open data as an integral part of the modern law enforcement system, which requires a revision of the regulatory framework, in particular Federal Law No. 144-FZ "On Operational-Investigative Activity".

Keywords: open sources of information, OSINT, operational investigative activities, digital footprints, artificial intelligence (AI), admissibility of evidence, personal data, cybercrime, interagency cooperation, hash value.

The article was received by the editorial office on 10/10/2026, approved after review on 13/11/2026, accepted for publication on 16/11/2026.

Введение

Оперативно-розыскная деятельность (далее ОРД), в основном всегда, строилась на получение сведений, скрытых от публичного доступа. Однако современная работа по сбору и анализу оперативно-значимой информации характеризуется противоречиями: значительная часть подготовки, организации и сокрытия тяжких и особо тяжких преступлений оставляет «цифровые следы» в открытом сегменте информационно-телекоммуникационной сети Интернет. Получение информации из открытых источников OSINT [11] перестает быть

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

вспомогательным инструментом сбора справок, а переходит в отдельное и самостоятельное направление информационного обеспечения борьбы с преступностью, в том числе с её организованными формами. Современные подходы борьбы с преступностью требует перехода от эпизодического использования интернета в сборе доказательной базы, к его постоянному мониторингу и дальнейшей легализации добытой информации в ОРД. Это подразумевает создание непрерывного аналитического цикла мониторинга открытых данных, позволяющего выявлять, в том числе и латентные преступления на этапе их подготовки, когда физического состава преступления еще нет, но в цифровом пространстве уже фиксируются аномалии: массовая скупка сим-карт, поиск уязвимостей в информационной инфраструктуре учреждений различных форм собственности, в том числе и критической инфраструктуре.

Результаты исследования и их обсуждение

Наиболее точное определение «цифровому следу», используемое в системе МВД, дано профессором А.Л. Осипенко [6], под ним понимается отражение криминального события или деятельности лица в памяти ЭВМ, на машинных носителях или в сигналах данных, циркулирующих в сети интернет. Ключевой признак здесь объективность: след существует независимо от воли преступника как побочный продукт использования современных технологий. В трудах профессора А.Л. Осипенко, цифровизация общества привела к виртуализации реальности, что усложняет вызовы, для правоохранительных органов, но одновременно и расширяет, для них горизонт возможностей, за счет доступности больших объёмов данных. Еще 3 года назад изучение профиля подозреваемого или обвиняемого в совершении преступления, в социальной сети, было личной инициативой отдельного сотрудника, то на сегодняшний день, это должно стать обычным алгоритмом проверки информации на любой стадии ОРД.

1. Необходимо изменить правовой статус цифровой информации, определить переход от обычного скриншота с экрана ПК к превращению его в доказательство.

В российском законодательстве и ведомственных актах МВД понятие «цифровые следы» не имеет единого легального определения в одном предложении, однако его содержание раскрывается через совокупность норм и доктринальных документов.

Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» [10] создавался в эпоху аналоговой связи, когда еще в системе МВД практически не было ПК и тем более специалистов в этой сфере. Его терминологический аппарат ориентирован на материальные носители. Это порождает первую проблему: отсутствие легального определения «цифровой оперативной информации».

В своей статье В.Ю. Жандров правильно указывает, на то, что сложившиеся современные условия требуют формализации данного понятия, как самостоятельного объекта правового режима [1]. Под таковой следует понимать сведения, извлекаемые из IT-среды (социальные сети, мессенджеры, облачные хранилища), подвергнутые первичной верификации и потенциально способные превращаться в процессуально допустимые доказательства.

Из анализа судебной практики 2025-2026 годов становится понятным, что судебная система демонстрирует постепенный отход от постоянного стремления заверять у нотариуса абсолютно любые документы, в том числе и электронные доказательства. Долгое время суды низших инстанций признавали ничтожными скриншоты, полученные оперативным путем, ссылаясь на невозможность установить автора публикации или факт отсутствия монтажа, однако позиция вышестоящих судов в настоящее время постепенно меняется.

Согласно п. 55 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10, распечатки материалов, размещенных в сети интернет, являются допустимыми доказательствами при наличии адреса страницы и времени получения. Эта позиция была подтверждена и усилена в практике 2024 года. Так, Судебная коллегия по гражданским делам Верховного Суда РФ в Определении от 07.02.2024 (дело № 5-КГ23-144-К2) прямо

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

указала, что отсутствие нотариального протокола осмотра сайта не лишает скриншот доказательственной силы, если сторона, против которой он представлен, не заявляет о его фальсификации [15].

Арбитражная практика подтверждает эти изменения. В Постановлении Арбитражного суда Московского округа от 26.07.2024 по делу № А40-11205/2024 суд отказался принимать довод ответчика о недопустимости незаверенных скриншотов личного кабинета налогоплательщика, сославшись на ч. 3 ст. 75 АПК РФ [16].

Алгоритм фиксации данных из различных каналов сети интернет:

1. Фиксация метаданных канала (username, ID).2. Выгрузка публичных сообщений с фиксацией URL-адреса каждого сообщения и созданием хеш-суммы файла выгрузки (для подтверждения неизменности файла).

3. Использование сервисов веб-архивирования, для фиксации истории изменений названия канала.

4. Проведение оперативно-розыскного мероприятия «Наблюдение» с использованием технических средств: фото-видеофиксации экрана монитора в присутствии двух незаинтересованных лиц, с составлением акта осмотра интернет-ресурса.

Однако остается острая проблема разграничения публичной и частной информации. Согласно ст. 24 Конституции РФ и ст. 6 ФЗ № 152-ФЗ «О персональных данных», сбор любых сведений о гражданине требует законных оснований. Сбор досье из открытых источников находится в так называемой «серой зоне». Поправки в КоАП РФ (ст. 13.11) и УК РФ (ст. 137), вступившие в силу в 2023–2024 годах, ужесточили ответственность за обработку биометрических данных без согласия субъекта [14].

Особую сложность представляет анализ общедоступных ссылок в сети интернет. Зачастую информация, размещенная в открытом доступе (например, в профиле социальной сети без ограничений приватности), юридически считается публичной. Однако, автоматический парсинг подобных данных программными средствами, может быть расценен, как нарушение неприкосновенности частной жизни, если целью является формирование систематизированного досье.

Для сотрудников правоохранительных органов, это означает необходимость строгого регламентирования парсинга: автоматизированный поиск и сбор фотографий лиц находящихся в оперативной разработке, а также подозреваемых и обвиняемых, может быть признан незаконным, тогда как, ручной мониторинг открытых связей фигуранта, по конкретным ссылкам полностью легитимен. Кроме того, сбор данных из закрытых чатов, куда оперативный сотрудник заходит под легендой, требует санкции суда согласно ст. 8 № 144-ФЗ «об ОРД», так как активное внедрение конфидента, в закрытый чат общения, нарушает тайну связи, даже если техническая ссылка на чат, была передана третьим лицам.

2. Необходимость изменения традиционных оперативно-розыскных мероприятий под влиянием OSINT.

Классический перечень оперативно-розыскных мероприятий (ОРМ), закрепленный в ст. 6 Федерального закона №144-ФЗ «об ОРД», претерпевает качественное изменение содержания [10].

ОРМ «наведение справок» превратилось, в том числе и в масштабный анализ и сбор информации из открытых источников информации в сети интернет. Вместо направления обычных бумажных запросов в ЗАГС или Росреестр, оперативные подразделения внедряют электронные запросы, со своего ПК, расположенном на рабочем месте, к государственным информационным системам (СМЭВ, СУДИС).

В 2025 году МВД России, проведен анализ работы сотрудников ведомства с автоматизированными системами, по результатам которого составлен отчет. Установлено, что использование автоматизированных систем перекрестной проверки позволило сократить время отработки связей фигурантов на 53%. Особое значение имеет интеграция с

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

коммерческими агрегаторами данных, которые собирают и аккумулируют информацию из десятков тысяч утекших баз данных.

Как отмечается в работах В.Б. Батоева, технологии поиска по OSINT позволяют выявить аффилированность коррупционера, через цепочки владения офшорами [7].

Снятие информации с технических каналов связи (СИТКС), граница между СИТКС и пассивным наблюдением размывается. Мониторинг открытых радиочастот и перехват незащищенного трафика Wi-Fi в общественных местах стало стандартом работы Управлений по борьбе с киберпреступностью (далее УБК) [11]. При этом возникает противоречие с конституционным правом на тайну переписки. Позиция Конституционного Суда РФ (Постановление от 06.06.2017 № 14-П) гласит, что технические средства защиты тайны связи должны применяться всегда, кроме случаев, когда пользователь сам сделал коммуникацию общедоступной.

Изучение «цифрового профиля» лица, до проведения с ним разведбеседы, стало обязательным элементом подготовки оперативно-розыскного мероприятия «опрос». Анализ профилей позволяет составить психологический портрет, выявить уязвимости (долги, зависимости, конфликты) и скорректировать залегендированную беседу.

Нельзя приуменьшать роль быстрого развития искусственного интеллекта. Внедрение нейросетей в поиск информации меняет её качественный объём и скорость самого поиска. Современные языковые модели способны самостоятельно генерировать запросы на основе описания цели, главное правильно поставить задачу, для ИИ агента. Вместе с тем, как предупреждают эксперты IT отрасли, те же инструменты используют и криминальные элементы, для генерации дипфейков и с помощью их совершать противоправные деяния, так в 2025 году зафиксирован первый случай использования подделки голоса начальника отдела полиции, для санкционирования незаконного проведения ОРМ.

Внедрение в свою деятельность ИИ и нейросетей открывает, для органов внутренних дел новые возможности быстрой аналитики, огромного массива данных. Системы на базе ИИ практически в режиме реального времени способны анализировать потоки данных из городских систем видеонаблюдения, социальных сетей и транспортных узлов, выявляя поведение характерное, для подготовки террористических актов или массовых беспорядков, устанавливать место нахождения лиц, находящихся в розыске, а также лиц без вести пропавших. Однако использование ИИ требует создания отечественных платформ, исключающих утечку оперативных данных на зарубежные серверы и возможность одномоментного отключения доступа ко всем базам данных.

3. Кадровый кризис системы МВД и его истоки.

По официальным данным, озвученным Министром внутренних дел Российской Федерации В.А. Колокольцевым на расширенной коллегии МВД в марте 2026 года, количество незаполненных вакансий в ведомстве превысило критическую отметку в 212 тысяч единиц, из них 186,5 тысячи, это сотрудники, находившиеся на аттестованных должностях.

Наиболее сложная ситуация сложилась в высокотехнологичных подразделениях. Некомплект экспертов в IT-сфере достигает 30%, а специалистов по анализу данных более 40%. Причина кроется не только в большом разрыве оплаты труда, но и в уменьшении образовательных учреждений по данному направлению. Система ведомственного образования (университеты МВД) не успевает за рынком: выпускник 2026 года знает нормативную базу, но зачастую не владеет языками программирования, для самостоятельного написания скриптов автоматизированной поисковой системы.

А.А. Майдыков и соавторы отмечают, что без кардинального повышения социального статуса технического специалиста, любые закупки дорогостоящего оборудования и программного обеспечения превращаются в нецелевую трату бюджетных денежных средств [5].

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Ведомственная разобщенность подразделений ОВД -это вторая не менее важная проблема в системе МВД. Как показывают исследования В.А. Усова и С.Д. Богачевой, информационные системы уголовного розыска, подразделений экономической безопасности и специализированных отделов УБК часто разобщены на уровне баз данных [3] и не хотят делиться ими, т.к. обладание оперативной информацией, напрямую влияет на показатели в оценке деятельности каждого подразделения отдельно.

Следственно-оперативная группа (СОГ), как форма взаимодействия также требует изменений: часто следователь превращает оперативного сотрудника, владеющего навыками киберразведки, в обычного технического помощника, обязанного лишь распечатывать предоставляемые скриншоты, вместо того чтобы участвовать в выработке стратегии расследования на основе глубокого анализа полученных им данных. Возможно пришло время внедрения понятия «цифрового следователя», в должностные обязанности которого, будет входить и процессуальное закрепление результатов работы IT-аналитиков, не давая им превращаться в простых операторов ЭВМ.

Выводы

Анализ, проведенный в данной статье, свидетельствует о том, что перспективы использования открытых источников в ОРД лежат не в плоскости простого увеличения штата сотрудников ОВД, а требуют системной реформы, включающей в себя:

1. Законодательный уровень: Внесение изменений в ФЗ об ОРД и ведомственные приказы, регламентирующих порядок проведения «удаленного осмотра информационных ресурсов» как самостоятельного вида документирования, с четким описанием требований к фиксации хеш-сумм и метаданных. Необходимо ввести новую правовую норму, регламентировав её как отдельный вид документирования результатов ОРД, а не просто часть «наведения справок». В связи с чем в последствии необходимо будет внести изменения в ведомственный приказ МВД РФ N 776 от 27.09.2013 года "Об Утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд".

2. Процессуальный уровень: Закрепление на уровне постановления Пленума ВС РФ специального регламента оценки доказательств, полученных из открытых источников, где презумпция добросовестности будет распространяться на должностное лицо, оформившее акт осмотра ресурса.

3. Кадровый уровень: Создание специализированной федеральной службы аналитики данных в структуре МВД с системой оплаты труда, конкурентной рынку IT, и введение обязательной цифровой грамотности для всего оперативного состава. В специализированных подразделениях МВД необходимо ввести обязательный зачет по основам OSINT и работе с нейросетями для всех сотрудников, допущенных к аналитическим панелям.

4. Технологический уровень: Переход от закупаемых иностранных программных комплексов к отечественным платформам на базе искусственного интеллекта, способным обрабатывать петабайты неструктурированных данных даркнета и соцсетей в режиме реального времени.

Именно такой подход к новым реалиям позволит правоохранительной системе сохранять наступательность в условиях тотальной цифровизации преступности, обеспечивая баланс между эффективностью раскрытия и соблюдением конституционных прав граждан.

Литература

1. Жандров В.Ю. Цифровая оперативная информация: нормативное регулирование и правовой режим использования в уголовном преследовании. Вестник Института права Башкирского государственного университета. 2025. Т. 8. № 3. С. 172-186. DOI: 10.33184/vest-law-bsu-2025.27.17 EDN: YEYXTG.

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

2. Волков К.А. Искусственный интеллект в российском правосудии: перспективы и риски // Российский судья. 2025. № 8. С. 44-48. DOI: 10.18572/1812-3791-2025-8-44-48 EDN: BVHDLE3.
Усов В.А., Богачева С.Д. Проблемы и перспективы развития взаимодействия подразделений органов внутренних дел при осуществлении оперативно-розыскной деятельности // Социальное управление. 2026. Т. 8. № 1. С. 54-60. EDN: FNJOGX.
4. Шаров В.И. "Цифровая оперативно-розыскная деятельность" и цифровизация противодействия преступлениям // Вестник Санкт-Петербургского университета МВД России. 2025. № 3. С. 171-178. EDN: AQKZJC.
5. Майдыков А.А., Огурцов А.Е., Конашенков С.О. Защита государственной тайны в оперативно-розыскной деятельности: современные проблемы в условиях цифровизации // Пробелы в российском законодательстве. 2025. Т. 18. № 2. С. 122-131. EDN: RTMLWZ.
6. Осипенко А. Л. Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. 2019. № 4 (75). С. 38-46. DOI: 10.24411/1999-625X-2019-14007 EDN: NFEFEI.
7. Батоев В.Б. О технологии поиска по открытым источникам "OSINT" в оперативно-розыскной деятельности // Вестник Уфимского юридического института МВД России. 2023. № 2. С. 66-71. EDN: HTHORH.
8. Семенчук В.В., Батоев В.Б. Предпосылки формирования концепции развития оперативно-разыскной деятельности в цифровой сфере (часть 1) // Вестник Волгоградской академии МВД России. 2023. № 3 (66). С. 132-136. DOI: 10.25724/VAMVD.A166 EDN: SMENIU.
9. Конституция Российской Федерации от 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020.
10. Федеральный закон от 12.08.1995 г. №144-ФЗ "Об оперативно-розыскной деятельности".
11. Распоряжение Правительства РФ от 30.12.2024 № 4154-р "Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий".
12. Приказ МВД России, Минобороны РФ, ФСБ РФ, ФСО РФ, ФТС РФ, СВР РФ, ФСИН РФ, ФСКН РФ, СК России от 27.09.2013 № 776/703/509/507/1820/42/535/398/68 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд".
13. Постановление Пленума Верховного Суда РФ от 23.04.2019 г. №10 "О применении части четвертой Гражданского кодекса Российской Федерации".
14. Федеральный закон от 27.07.2006 г. №152-ФЗ "О персональных данных".
15. Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 07.02.2024 (дело № 5-КГ23-144-К2).
16. Постановление Арбитражного суда Московского округа от 26.07.2024 по делу № А40-11205/2024.

References

1. Zhandrov V.Yu. Digital operational information: regulatory framework and legal regime of use in criminal prosecution. Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta. 2025. Vol. 8. No. 3. P. 172–186. DOI: 10.33184/vest-law-bsu-2025.27.17. EDN: YEYXTG. (In Russ.).
2. Volkov K.A. Artificial intelligence in Russian justice: prospects and risks. Rossiyskiy sudya. 2025. No. 8. P. 44–48. DOI: 10.18572/1812-3791-2025-8-44-48. EDN: BVHDLE. (In Russ.).
3. Usov V.A., Bogacheva S.D. Problems and prospects for developing cooperation between internal affairs departments in conducting operational-search activities. Sotsial'noe upravlenie. 2026. Vol. 8. No. 1. P. 54–60. EDN: FNJOGX. (In Russ.).

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

4. Sharov V.I. “Digital operational-search activity” and digitalization of crime prevention. Vestnik of Saint Petersburg University of the Ministry of Internal Affairs of Russia. 2025. No. 3. P. 171–178. EDN: AQKZJC. (In Russ.).
5. Maydykov A.A., Ogurtsov A.E., Konashenkov S.O. Protection of state secrets in operational-search activities: current challenges in the context of digitalization. Gaps in Russian Legislation. 2025. Vol. 18. No. 2. P. 122–131. EDN: RTMLWZ. (In Russ.).
6. Osipenko A.L. Operational-search activities in the information society: adaptation to digital reality. Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia. 2019. No. 4(75). P. 38–46. DOI: 10.24411/1999-625X-2019-14007. EDN: NFEFEI. (In Russ.).
7. Batoev V.B. On the technology of open-source intelligence (OSINT) in operational-search activities. Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii. 2023. No. 2. P. 66–71. EDN: HTHORH. (In Russ.).
8. Semenchuk V.V., Batoev V.B. Prerequisites for developing a concept for operational-search activities in the digital sphere (Part 1). Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2023. No. 3(66). P. 132–136. DOI: 10.25724/VAMVD.A166. EDN: SMENIU. (In Russ.).
9. Constitution of the Russian Federation of December 12, 1993, with amendments approved by the nationwide vote on July 1, 2020. (In Russ.).
10. Federal Law No. 144-FZ of August 12, 1995, “On Operational-Search Activities”. (In Russ.).
11. Order of the Government of the Russian Federation No. 4154-r of December 30, 2024, “On Approval of the Concept of the State System for Counteracting Unlawful Acts Committed Using Information and Communication Technologies”. (In Russ.).
12. Joint Order of the Ministry of Internal Affairs of Russia, Ministry of Defence of the Russian Federation, Federal Security Service of the Russian Federation, Federal Protective Service of the Russian Federation, Federal Customs Service of the Russian Federation, Foreign Intelligence Service of the Russian Federation, Federal Penitentiary Service of the Russian Federation, Federal Drug Control Service of the Russian Federation, and Investigative Committee of Russia No. 776/703/509/507/1820/42/535/398/68 of September 27, 2013, “On Approval of the Instruction on the Procedure for Submitting the Results of Operational-Search Activities to an Inquiry Body, Investigator or Court”. (In Russ.).
13. Resolution of the Plenum of the Supreme Court of the Russian Federation No. 10 of April 23, 2019, “On the Application of Part Four of the Civil Code of the Russian Federation”. (In Russ.).
14. Federal Law No. 152-FZ of July 27, 2006, “On Personal Data”. (In Russ.).
15. Ruling of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation of February 7, 2024, Case No. 5-KG23-144-K2. (In Russ.).
16. Resolution of the Commercial Court of the Moscow District of July 26, 2024, in Case No. A40-11205/2024. (In Russ.).

Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.