Дата поступления рукописи в редакцию: 14.10.2026 г. DOI: 10.24412/3033-7518-2026-3-35-39
Дата принятия рукописи в печать: 28.10.2026 г.

АНДРЕЕВА К. М.,
адъюнкт Ростовского юридического института МВД России,
e-mail: kristina-andreeva-96@internet.ru

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья посвящена комплексному теоретико-правовому и организационно-тактическому анализу использования информации из открытых источников (OSINT) в оперативно-розыскной деятельности (ОРД) органов внутренних дел. Актуальность исследования обусловлена стремительной цифровизацией преступности и геополитическими факторами, ограничивающими международное сотрудничество российских правоохранительных органов с зарубежными ИТ-гигантами. В этих условиях автономный поиск в открытом сегменте Интернета становится приоритетным направлением. Опираясь на положения Конституции РФ и Федерального закона «Об информации...» № 149-ФЗ, доказывается бесконфликтный и легитимный характер сбора общедоступных данных. В работе сопоставляются методы OSINT с нормами ФЗ «Об оперативно-розыскной деятельности» № 144-ФЗ. Обосновано, что поиск по открытым источникам нормативно реализуется через два ОРМ: «наведение справок» (запросы в реестры и базы данных) и «наблюдение» (мониторинг соцсетей и мессенджеров). В статье предложена авторская классификация массивов открытых данных по технико-содержательному признаку: коммуникативно-социальный сегмент, технические метаданные (EXIF-данные) и инфраструктурно-сетевые параметры. Сформулированы тактические этапы оперативно-розыскного поиска от постановки задачи до верификации. Систематическое внедрение методов анализа OSINT модернизирует тактику ОВД, позволяя автономно извлекать цифровые следы, устанавливать геолокацию и формировать психологический портрет проверяемых лиц без нарушения их конституционных прав.

Ключевые слова: оперативно-розыскная деятельность, открытые источники информации, OSINT, общедоступные данные, сеть Интернет, наведение справок, наблюдение, цифровые следы, метаданные.

ANDREEVA K. M.,
postgraduate student at the Rostov Law Institute
of the Ministry of Internal Affairs of Russia

THE USE OF OPEN-SOURCE INFORMATION IN OPERATIONAL-SEARCH ACTIVITIES

Annotation. The article is devoted to a comprehensive theoretical, legal, organizational, and tactical analysis of using open-source intelligence (OSINT) in the operational-search activity of internal affairs bodies. The relevance of the research is driven by the rapid digitalization of crime and geopolitical factors that limit international cooperation between Russian law enforcement and foreign IT companies. Under these conditions, autonomous searching in the public segment of the Internet becomes a priority. The Relies on the provisions of the Constitution of the Russian Federation and Federal Law No. 149-FZ «On Information...», proving the conflict-free and legitimate nature of public data collection. The paper correlates OSINT methods with the norms of Federal Law No. 144-FZ «On Operational-Search Activity». It is substantiated that open-source searching is normatively implemented through two operational-search measures: «inquiring» (queries to registries and databases) and «surveillance» (monitoring social media and messengers). The article proposes an author's classification of open data arrays based on technical and content characteristics: the communicative-social segment, technical metadata (EXIF data), and infrastructural/network parameters. The tactical stages of the operational-search process from task setting to verification are formulated. The systematic implementation of OSINT analysis methods modernizes the tactics of law enforcement, allowing them to autonomously extract digital footprints, establish geolocation, and profile subjects without violating their constitutional rights.

Key words: operational-search activity, open source intelligence, OSINT, public data, Internet, inquiring, surveillance, digital footprints, metadata.

Динамичное развитие информационных технологий, глобальная доступность сети Интернет и появление новых коммуникационных платформ существенно изменили структуру современной преступности. В сложившейся оперативной обстановке перед оперативными подразделениями органов внутренних дел (ОВД) остро встала задача модернизации существующих тактических приемов и методов выявления, пресечения и раскрытия преступлений. Традиционные методы оперативно-розыскной деятельности (ОРД), ориентированные преимущественно на физическое пространство, сталкиваются с объективными трудностями при переносе их в цифровую среду. Одним из наиболее перспективных, доступных и законных направлений совершенствования аналитической работы правоохранительных органов является систематическое использование информации из открытых источников (в международной и отечественной научно-практической терминологии часто обозначаемой как OSINT — Open Source Intelligence).

Как верно, указывает В.Ю. Иванов на то, что анализ информации, содержащейся в социальных сетях и на иных сайтах, хранящих персональные данные, открывает большие возможности для сбора информации о конкретном лице [1]. Актуальность теоретического осмысления и практического развития методов работы с открытыми цифровыми источниками обусловлена также геополитическими факторами. В условиях существенного ограничения международного правового и информационного взаимодействия отечественных правоохранительных органов с зарубежными ИТ-компаниями и администрациями коммуникационных платформ получение данных по классическим каналам международных запросов оказалось затруднительным. Это предопределило необходимость перехода к автономным формам поиска оперативно значимых сведений, основанным на самостоятельном извлечении и глубоком интеллектуальном анализе информации, находящейся в открытом, общедоступном сегменте сети Интернет.

Для интеграции методов поиска по открытым источникам в доктрину оперативно-розыскной деятельности необходимо четко определить их правовую природу. Основным нормативно-правовым актом, регулирующим общественные отношения в исследуемой сфере, является Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ [2]. Согласно статье 7 указанного закона, к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Такая информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений на распространение такой информации.

В контексте теории оперативно-розыскной деятельности открытые источники информации представляют собой массив данных, размещенный пользователями, организациями или государственными органами в свободном доступе, для ознакомления с которыми не требуется преодолевать системы технической защиты, подбирать пароли или получать специальные санкции судебных органов. В криминалистической науке феномен накопления таких сведений содержательно описывается через концепцию «цифровых следов». Как справедливо отмечает Е. П. Ищенко, в России формируется информационное общество – такое общество, в котором большинство работающих людей занято производством, хранением, переработкой и реализацией информации (знаний), а наряду с традиционным материальным миром возникает специфическая среда существования – компьютерные нейронные сети – кибернетическое пространство, обладающее рядом специфических признаков [3]. И указанное кибернетическое пространство, по моему мнению, сегодня выступает неисчерпаемым источником криминалистически значимой информации, требующей специфических методов фиксации и декодирования. Полноценная обработка данных следов в рамках OSINT позволяет оптимизировать первоначальный этап оперативно-розыскного прогнозирования и моделирования.

Поскольку пользователи сети Интернет размещают указанные сведения добровольно и делают их доступными для неограниченного круга лиц, сбор и анализ такой информации оперативными подразделениями не может рассматриваться как вмешательство в частную жизнь, личную и семейную тайну или нарушение конституционных прав на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, 24 Конституции РФ) [4]. На основании вышеизложенного можно отметить, что мониторинг открытых интернет-ресурсов (социальных сетей, блогов, публичных каналов) не вторгается в сферу охраняемой законом личной или семейной тайны, поскольку пользователь изначально придал публикуемым материалам публичный статус. Следует учитывать справедливое мнение А.В. Сидоренко и К.И. Масленникова о том, что интенсификация информационных потоков и активное развитие поисковых технологий позволяет рассматривать Интернет в качестве особого инструмента информационного поиска [5].

В системе оперативно-розыскных мероприятий (ОРМ), предусмотренных статьей 6 Федерального закона «Об оперативно-розыскной деятельности» № 144-ФЗ [6], работа с открытыми источниками информации находит свое нормативное воплощение в рамках двух ключевых мероприятий:

1. «Наведение справок». Данное ОРМ в цифровой среде реализуется посредством направления автоматизированных или ручных поисковых запросов в открытые информационные системы, государственные реестры, справочные базы дан-

ных, WHOIS-сервисы доменных имен и специализированные ведомости. В ходе наведения справок оперативник собирает формализованные сведения о владельцах сетевых узлов, регистрационных данных организаций или идентифицирующих признаках технических средств.

2. «Наблюдение». В электронной форме наблюдение представляет собой негласный или гласный визуальный мониторинг открытых веб-страниц, форумов, каналов в мессенджерах и тематических сообществ в социальных сетях. Сотрудник оперативного подразделения осуществляет непрерывное или дискретное отслеживание динамики размещения контента, фиксацию активности конкретных учетных записей и анализ их коммуникативного поведения, не вступая при этом в непосредственное взаимодействие (диалог) с проверяемыми лицами и не выдавая своего присутствия.

Теоретический анализ юридической литературы показывает, что использование открытых данных в оперативно-розыскной деятельности носит исключительно бесконфликтный характер на этапе их сбора, поскольку действия сотрудника полностью легитимны и осуществляются в общедоступном пространстве. Бесконфликтность ОРМ в цифровой среде обеспечивает высокую сохранность тактического замысла и оперативность получения первичных проверочных материалов.

Справедливо указывает К.С. Белова, на то, что Интернет в силу своего содержания и специфического устройства является самостоятельным объектом познания – элементом функциональной стороны криминальной и антикриминальной деятельности [7].

Для систематизации аналитической работы в процессе оперативно-розыскного поиска представляется целесообразным разделить массивы открытых данных, циркулирующих в сети Интернет, на несколько взаимосвязанных категорий на основе их технической и содержательной специфики.

1. Коммуникативно-социальный сегмент (социальные медиа и мессенджеры). Данная группа источников включает в себя персональные профили пользователей в социальных сетях, открытые группы, сообщества, блоги и публичные каналы в мессенджерах. В научной литературе подчеркивается, что социальные медиа выступают ключевой платформой для цифрового профилирования. В частности, В.Ю. Жандров отмечает, что сбор данных в форме цифрового оперативного поиска позволяет отслеживать коммуникационные связи, предпочтения, перемещения, цифровые следы и даже эмоциональные реакции пользователей [8]. Информация, полученная из этого сегмента, позволяет установить анкетные данные, социально-демографические характеристики, круг связей и контактов проверяемого лица, а также психологический портрет на основе публикуемого контента.

2. Технические метаданные цифровых объектов. Любой файл, размещаемый в сети Интернет (фотоизображение, видеозапись, текстовый документ), содержит в себе скрытую, но доступную для извлечения служебную информацию. Наибольший интерес для ОРД представляют EXIF-данные графических файлов. С помощью открытых утилит для анализа метаданных оперативный сотрудник может получить сведения о точной дате и времени создания файла, модели и серийном номере технического устройства, а также географических координатах места съемки, что позволяет с высокой точностью установить локацию проверяемого лица.

3. Инфраструктурные и сетевые параметры (сетевой аудит). К этой категории относятся открытые данные о техническом устройстве интернет-ресурсов, используемых в противоправных целях. Используя сервисы проверки доменных имен, открытые базы данных IP-адресов и маршрутизации, оперативные сотрудники получают сведения об IP-адресах серверов, хостинг-провайдерах, регистраторах доменов и географическом расположении серверов сайтов. Установление базовых инфраструктурных параметров криминальных интернет-ресурсов служит незаменимым фундаментом для определения технической основы всей преступной деятельности и планирования последующих оперативно-технических мероприятий.

Тактика использования открытых источников в ОРД строится на принципах системности, последовательности и верифицируемости. Процесс работы с общедоступными данными включает в себя несколько последовательных тактических этапов:

Таблица 1.

[Постановка задачи] →
[Сбор данных] →
[Фильтрация информации] →
[Анализ и синтез] →
[Верификация].

Этап 1: Определение поисковых индикаторов (Постановка задачи). На основе первичных материалов оперативный сотрудник формулирует ключевые параметры поиска: уникальные текстовые маркеры, идентификаторы учетных записей (ники, юзернеймы), телефонные номера, адреса электронной почты или специфический сленг.

Этап 2: Сбор информации и преодоление «информационного шума». Главной сложностью этого этапа является колоссальный объем неструктурированных данных в сети Интернет. Тактика сотрудника заключается в правильном комбинировании автоматизированных поисковых алгоритмов (включая специализированное поисковое ПО) и ручного веб-серфинга для отсечения нерелевантных данных.

Этап 3: Фильтрация и структурирование информации. На данном этапе происходит агрегация собранного массива, исключение дублирующих сведений и группировка объектов по хронологическому или тематическому признаку. Эффективная фильтрация на 70% сокращает временные затраты на аналитическую обработку сетевых данных.

Этап 4: Анализ и синтез данных. Сотрудник сопоставляет разрозненные сведения (например, совпадение геолокации из метаданных фото с кругом связей в социальной сети), выявляя скрытые причинно-следственные связи и формируя целостную картину противоправной деятельности.

Этап 5: Верификация. Проверка достоверности полученных сведений через альтернативные независимые открытые источники или путем сопоставления со сведениями, уже имеющимися в распоряжении оперативного подразделения.

Важнейшим условием эффективности использования открытых данных является их последующее введение в уголовный процесс. Информация, полученная из сети Интернет, приобретает статус доказательства только после прохождения процедуры легализации в соответствии со ст. 11 ФЗ «Об ОРД» и уголовно-процессуальным законодательством.

Тактический алгоритм фиксации и легализации открытых данных включает:

1. Документирование хода ОРМ. Осуществляется составление рапорта об обнаружении признаков преступления либо справки о проведении оперативно-розыскного мероприятия (наведения справок, наблюдения), в котором подробно фиксируются: дата, время проведения, технические характеристики используемых ЭВМ и программного обеспечения, точные URL-адреса веб-страниц, а также сетевые реквизиты (IP-адреса).

2. Хеш-верификация и техническое закрепление. В целях исключения обвинений в модификации цифровых данных, оперативный сотрудник осуществляет зеркальное копирование интернет-страниц, запись сетевого трафика в файлы формата .pcap и обязательный расчет хэш-функций (MD5, SHA-256) полученных файлов. К материалам приобщаются скриншоты страниц и оптические или электронные носители информации.

3. Процессуальное представление. Оформленные результаты ОРД направляются в орган предварительного расследования, где следователь производит осмотр представленных документов и электронных носителей, после чего они признаются вещественными доказательствами. В случаях, когда существует риск оперативного удаления информации проверяемыми лицами до возбуждения дела, тактически оправданным шагом выступает привлечение механизмов нотариального обеспечения доказательств.

Подводя итог проведенному исследованию, необходимо сделать вывод о том, что использование открытых источников информации в оперативно-розыскной деятельности представляет собой высокоэффективное, экономически доступное и полностью легитимное средство противодействия современной преступности. В условиях смещения криминальной активности в цифровое пространство и снижения эффективности международных правовых механизмов разведка по открытым источникам (OSINT) становится базовым элементом суверенного оперативно-розыскного поиска.

Нормативно-правовая база Российской Федерации предоставляет оперативному правоприменителю достаточные основания для проведения OSINT-мероприятий в рамках существующих оперативно-розыскных мероприятий «Наблюдение» и «Наведение справок», не нарушая при этом конституционных прав гражданина на неприкосновенность частной жизни и тайну переписки.

Вместе с тем дальнейшее развитие данного направления требует совершенствования методического обеспечения сотрудников ОВД. Необходима разработка унифицированных ведомственных стандартов фиксации и хеширования цифровых данных, а также создание специализированных обучающих программ для оперативного состава по тактике преодоления «информационного шума» и верификации интернет-сведений. Это позволит существенно повысить качество формируемой доказательной базы и эффективность раскрытия высокотехнологичных преступлений.

Список литературы:

[1] Иванов В.Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. – 2023. – № 1. – С. 62-66.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ: [ред. от 26.06.2026] // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1). – Ст. 3448.

[3] Ищенко Е. П. У истоков цифровой криминалистики // Вестник Университета имени О.Е. Кута-

фина (МГЮА). – 2019. – № 3. – С. 15–28.

[4] Российская Федерация. Конституция (1993). Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. – Москва : Эксмо, 2023. – 76 с – с.9.

[5] Сидоренко А.В., Масленников К.И. Оперативный поиск информации в сети интернет о лицах, подготавливающих и совершающих наркопреступления // Журнал правовых и экономических исследований. – 2025, 2 – С. 217-222.

[6] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ: [ред. от 01.04.2025] // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

[7] Белова К.С. Диссертация на соискание ученой степени кандидата юридических наук Тактико–организационные основы использования сети Интернет при расследовании преступлений // ФГАОУ ВО «МГЮА им. О.Е. Кутафина». – 2026. – С. 75.

[8] Жандров В.Ю. Методы оперативно-разыскной деятельности: теоретическая основа трансформации в условиях цифровизации // Проблемы правоохранительной деятельности. – 2025. – № 4. – С. 31-40.

References:

[1] Ivanov V.Yu. The Use of OSINT in the Detection and Investigation of Crimes // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. – 2023. – No. 1. – pp. 62–66.

[2] On Information, Information Technologies, and Information Protection: Federal Law No. 149-FZ of July 27, 2006 [as amended on June 26, 2026] // Collected Legislation of the Russian Federation. – 2006. – No. 31 (Part 1). – Art. 3448.

[3] Ishchenko E. P. At the Origins of Digital Forensics // Bulletin of the O.E. Kutafin University (MSAL). – 2019. – No. 3. – pp. 15–28.

[4] Russian Federation. Constitution (1993). Constitution of the Russian Federation: adopted by popular vote on December 12, 1993, with amendments approved during the all-Russian vote on July 1, 2020. – Moscow: Eksmo, 2023. – 76 p. – p. 9.

[5] Sidorenko A.V., Maslennikov K.I. Operational Search for Information on the Internet Regarding Individuals Preparing or Committing Drug-Related Crimes // Journal of Legal and Economic Research. – 2025, No. 2. – pp. 217–222.

[6] On Operational-Search Activity: Federal Law No. 144-FZ of August 12, 1995 [as amended on April 1, 2025] // Collected Legislation of the Russian Federation. – 1995. – No. 33. – Item 3349.

[7] Belova K.S. Dissertation for the degree of Candidate of Legal Sciences: Tactical and Organizational Foundations for Using the Internet in Criminal Investigations // Kutafin Moscow State Law University (MSAL). – 2026. – P. 75.

[8] Zhandrov V.Yu. Methods of Operational-Investigative Activity: Theoretical Basis for Transformation in the Context of Digitalization // Problems of Law Enforcement Activity. – 2025. – No. 4. – Pp. 31–40.

