Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра оперативно-розыскной деятельности

ДИПЛОМНАЯ РАБОТА

на тему: «Интернет-сеть как источник оперативно-розыскной информации»

Выполнил: Зайцев Максим Владимирович
(фамилия, имя, отчество)

40.05.02 Правоохранительная деятельность, набор 2021 г., 211 учебная группа
лейтенант полиции
(специальность, год набора, № группы)

Руководитель:
Преподаватель кафедры ОРД
полковник полиции в отставке
(ученая степень, ученое звание, должность)

Макаров Александр Семенович
(фамилия, имя, отчество)

Рецензент:
Заместитель начальника УНК МВД
по Удмуртской Республике
подполковник полиции
(должность, специальное звание)

Мингазутдинов Рустам Ильдарович
(фамилия, имя, отчество)

Дата защиты: «___» _____2026 г. Оценка_____

Казань 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования обусловлена следующими обстоятельствами. В XXI веке интернет стал не только основным средством коммуникации и обмена информацией, но и важной инфраструктурной платформой, на которой развиваются различные сферы деятельности – от бизнеса до образования. Однако динамичное развитие сети сопровождается ростом числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

По данным МВД России, за январь-август 2025 года число преступлений в сфере IT выросло более чем на 38% по сравнению с аналогичным периодом 2024 года, при этом значительная их часть связана с мошенничеством, распространением экстремистских материалов, незаконным оборотом наркотических веществ, детской порнографией, а также кибератаками. Более 80% таких преступлений совершаются с использованием социальной инженерии, а их планирование и осуществление зачастую проходит через социальные сети и мессенджеры[1].

Важнейшей особенностью интернет-пространства является сохранение цифровых следов деятельности пользователей: метаданных сообщений, записей движений денежных средств, истории действий в социальных сетях, геолокационных отметок. Эти данные могут быть использованы правоохранительными органами как источники оперативно-розыскной информации, обеспечивая возможность выявления преступных намерений и членов преступных групп до момента совершения правонарушений.

Правовая база России также закрепляет возможность использования интернет-данных в оперативно-розыскной работе. Так, Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон

[1] Состояние преступности в Российской Федерации за январь-август 2025 года // МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/70644759/ (дата обращения: 25.11.2025).

об ОРД)[1] предусматривает право органов, осуществляющих ОРД, собирать сведения, необходимые для выявления, предупреждения и раскрытия преступлений, включая материалы, размещённые в сети интернет. Дополнительно, Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон «Об информатизации…»)[2] регулирует порядок доступа к данным и взаимодействие с операторами связи.

Международная практика также подтверждает актуальность использования интернет-ресурсов для правоохранительной деятельности: в США, странах ЕС и Китае действуют системы, позволяющие осуществлять мониторинг открытых и закрытых онлайн-площадок в целях борьбы с терроризмом, киберпреступностью и организованной криминальной деятельностью[3].

Таким образом, исследование интернета как источника оперативно-розыскной информации является крайне актуальным по следующим причинам:

– Технологическая необходимость: интернет является ключевым каналом коммуникации и среды для совершения преступлений;

– Рост преступности в сети: ежегодное увеличение числа IT-преступлений требует совершенствования методов их выявления и расследования;

– Правовое закрепление: отечественное и международное законодательство предусматривает возможность использования сетевых данных в оперативно-розыскных целях;

– Практическая значимость: своевременное получение информации из сети позволяет предупреждать и пресекать преступления ещё на стадии их подготовки.

---

[1] Федеральный закон от 12.08.1995 г. № 144-ФЗ (ред. от 01.04.2025 г.) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. – 14.08.1995. – № 33. – Ст. 3349.

[2] Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 24.06.2025 г.) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 31.07.2006. – № 31 (1 ч.). – Ст. 3448.

[3] Пинкевич, Т.В. Международная практика применения современных цифровых решений в правоохранительной деятельности / Т.В. Пинкевич // Юристъ-Правоведъ. – 2023. – № 4(107). – С. 180-185.

Степень научной разработанности темы исследования. Вопросы, связанные с информационным обеспечением ОРД ОВД, широко представлены в специальной литературе. Существенный вклад в разработку различных аспектов данной проблематики внесли такие ученые, как В.М. Атмажитов, Ю.С. Блинов, В.Г. Бобров, Н.П. Водько, С.С. Галахов, В.Ю. Голубовский, Д.В. Гребельский, Н.А. Климов, В.П. Кувалдин, В.Д. Ларичев, А.Г. Лекарь, В.А. Лукашов, В.Ф. Луговик, С.С. Овчинский, А.С. Овчинский, В.Н. Омелин, Г.К. Синилов, Е.Н. Яковец и другие.

Целью настоящего исследования является комплексный анализ Интернет-сети как источника оперативно-розыскной информации.

Для достижения поставленной цели следует решить поставленные задачи:

– представить анализ интернет-сети (понятие, программно-технические особенности, использование виртуального пространства в преступной деятельности);

– охарактеризовать особенности сбора оперативной информации и отслеживания «цифровых» следов в сети Интернет;

– проанализировать особенности выдвижения и проверки оперативно-розыскных версий и планирование дальнейших этапов получения оперативно-розыскной информации по раскрытию преступлений;

– исследовать проблемы и пути решения организационно-правового обеспечения оперативно-розыскной деятельности в сети Интернет;

– разработать рекомендации по повышению эффективности деятельности ОВД при организации решения оперативно-розыскных задач в сети Интернет.

Объектом исследования выступают общественные отношения, связанные с организацией, тактикой выявления и документирования оперативными подразделениями ОВД преступлений в сети Интернет.

Предметом исследования являются правовые нормы, материалы правоприменительной практики, теоретический данные и доктрины о преступлениях, совершенных в сети Интернет.

Краткая характеристика основных положений дипломной работы:

1. Интернет как объект оперативно-розыскного анализа:

– Интернет-сеть является глобальной распределённой системой, объединяющей различные сервисы и технологии, и одновременно выступает как среда совершения противоправных действий;

– Основными особенностями интернет-пространства, значимыми для ОРД, являются: трансграничность, анонимизация участников, децентрализованное хранение данных и наличие скрытых сегментов (Deep Web, Darknet).

2. Рост киберпреступности и её специфика:

– Статистика МВД РФ фиксирует устойчивый рост числа преступлений в сфере IT, значительная часть которых связана с мошенничеством, незаконным оборотом наркотических средств, распространением экстремистских материалов и кибератаками;

– Более 80% преступлений совершаются с использованием методов социальной инженерии, а подготовка часто проходит через мессенджеры и социальные сети.

3. Цифровые следы как источник оперативной информации:

– К цифровым следам относятся регистрационные данные, IP-адреса, метаданные, контент публикаций, сетевые связи и поведенческие паттерны;

– Для их сбора используются методы OSINT, специализированные программные средства парсинга, краулеры, а также технологии анализа изображений и распознавания лиц.

4. Методика ОРД в цифровой среде:

– Сбор информации включает мониторинг ресурсов, выявление объектов, извлечение данных, корреляцию сведений, анализ и документирование;

– Особое место занимают примеры применения цифровой криминалистики в раскрытии различных преступлений, от поиска пропавших лиц до расследования DDoS-атак и кибермошенничества с криптовалютами.

5. Выдвижение и проверка оперативно-розыскных версий:

– Процесс выдвижения версий адаптирован к цифровой среде и опирается на анализ цифровых следов, атрибуцию объектов и корреляционный анализ;

– Планирование дальнейших этапов получения информации учитывает высокую изменчивость интернет-среды, необходимость стратегической и тактической последовательности и возможность проведения имитационно-поведенческих мероприятий.

6. Основные организационно-правовые проблемы ОРД в сети Интернет:

– Отсутствие унифицированного механизма для онлайн-ОРД, трудности взаимодействия с интернет-провайдерами и платформами, ведомственная разобщённость баз данных;

– Рост применения анонимайзеров, VPN и шифрования, правовые коллизии по границе между публичными и закрытыми данными, разрыв между скоростью технологических процессов и изменением законодательства.

7. Предложения по совершенствованию деятельности ОВД:

– Закрепление специальных процедур ОРД в цифровой среде в законодательстве;

– Создание единой межведомственной платформы («Цифровой ОРД») с автоматическим обменом данными между ведомствами;

– Разработка стандартов взаимодействия с IT-компаниями и международными партнёрами;

– Внедрение современных аналитических комплексов для мониторинга и анализа больших данных, криптовалютных транзакций, активности в Darknet;

– Повышение квалификации сотрудников в области компьютерной криминалистики и OSINT;

– Развитие профилактики цифровых угроз и повышение уровня киберграмотности населения.

8. Научная и практическая новизна работы:

– Систематизированы методы получения, обработки и анализа цифровых следов для применения в ОРД;

– Выработаны рекомендации по правовому и организационному обеспечению оперативно-розыскных мероприятий в интернет-среде;

– Предложена модель комплексного подхода, объединяющего нормативные, технические и кадровые меры для повышения эффективности ОВД.

Методологическая основа исследования представлена диалектико-материалистическим методом научного познания, общенаучными и частными научными методами. В числе общих методов научного познания были использованы сравнение, анализ, синтез, индукция, дедукция; из частно-научных – правой анализ, следственной и судебной практики, методы исследования эмпирических данных.

Нормативную базу исследования составили Конституция Российской Федерации[1], Уголовный кодекс Российской Федерации (далее – УК РФ)[2], федеральные законы и другие нормативно-правовые акты по теме исследования.

Эмпирическая основа включает в себя: материалы правоприменительной и судебной практик, статистические данные Министерства внутренних дел Российской Федерации и иных правоохранительных органов.

Теоретическая и практическая значимость исследования. Изучение данной темы позволит систематизировать методы добывания и анализа интернет-данных, выработать рекомендации по их применению в рамках действующего законодательства и повысить эффективность работы оперативных подразделений.

Достоверность и обоснованность выводов, полученных в результате исследования, подтверждается использованием соответствующей методологии, изучением достаточного объема научной литературы, нормативной базы, а также

---

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 г.) // Официальный текст Конституции РФ, включающий новые субъекты Российской Федерации - Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации http://pravo.gov.ru, 06.10.2022.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 29.12.2025 г.) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

оперированием эмпирическими данными, собранными в ходе прохождения производственной (преддипломной) практики[1].

Поставленные цель и задачи определили структуру работы: она состоит из введения, двух глав, объединяющих пять параграфов, заключения, списка использованной при написании работы литературы.

В первой главе работы проанализированы организационно-правовые аспекты получения оперативно-розыскной информации в сети Интернет.

Во второй главе работы представлены рекомендации по совершенствованию деятельности по получению информации, представляющей интерес для решения задач оперативно-розыскной деятельности.

В заключении сделаны выводы по проделанной работе.

[1] Материалы производственной (преддипломной) практики слушателя КЮИ МВД России Зайцева М.В. (место практики: отдел ОУР ОМВД России «Завьяловский», сроки прохождения практики: с 27.05.2025 г. по 21.07.2025 г.).

ГЛАВА 1. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ПОЛУЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

§1. Интернет-сеть: понятие, программно-технические особенности, использование виртуального пространства в преступной деятельности

Интернет сегодня представляет собой один из наиболее значимых феноменов современного информационного общества, оказывая колоссальное влияние на политическую, экономическую, культурную и социальную жизнь. Он является глобальной распределённой системой компьютерных сетей, соединённых между собой на основе стандартных протоколов передачи данных, позволяющих осуществлять обмен информацией между миллионами устройств в реальном времени. В широком смысле Интернет можно рассматривать как коммуникационную инфраструктуру, которая объединяет различные сервисы и технологии – от электронной почты и веб-ресурсов до потокового вещания и облачных вычислений.

С точки зрения права и криминалистики, Интернет представляет собой не только технологическую, но и социально-информационную среду, формирующую уникальные условия для коммуникации, хранения и обработки данных. Особенностью данной среды является виртуальность взаимодействий, анонимность или псевдонимность участников, а также территориальная децентрализация, когда передача информации происходит вне географических и государственных границ. Эти особенности одновременно обеспечивают предельно широкие возможности для законной деятельности и создают предпосылки для использования сети в противоправных целях[1].

Интернет-сеть представляет собой глобальную распределённую систему взаимосвязанных компьютерных сетей, функционирующих на основе

[1] Анциферова, Э.Ю. Правовой статус сети Интернет / Э.Ю. Анциферова // Ученые записки Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. – 2021. – № 18. – С. 64-68.

протоколов передачи данных TCP/IP и обеспечивающих доступ к информационным ресурсам, коммуникационным сервисам и цифровым услугам на международном уровне. С точки зрения правового регулирования в Российской Федерации, определение и основные положения, касающиеся Интернета и информационной инфраструктуры, содержатся в Федеральном законе от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В нём закреплены принципы правового оборота информации, обязанности операторов информационных систем, а также правила защиты информации от несанкционированного доступа, что непосредственно связано с задачами обеспечения национальной и общественной безопасности.

В научной и технической литературе термин «Интернет» определяется как совокупность аппаратных средств, программного обеспечения и коммуникационных протоколов, объединённых для обеспечения передачи данных между пользователями, независимо от их местонахождения[1]. Ядром сети служит система протоколов TCP/IP, обеспечивающих адресацию пакетов, управление потоками данных, маршрутизацию и контроль корректности передачи.

Инфраструктура Интернета включает:

– Аппаратную часть: серверы, маршрутизаторы, коммутаторы, линии связи (оптоволоконные, спутниковые, беспроводные), узлы доступа, центры обработки данных (ЦОД);

– Программное обеспечение: операционные системы серверов, веб-сервера, DNS-сервера, приложения для передачи данных и управления сетью, системы шифрования и защиты;

– Организационно-административные элементы: региональные интернет-регистраторы, провайдеры услуг, национальные сегменты сети;

---

[1] Гуцко, Е.Г. Характеристики сети интернет, способствующие совершению преступлений / Е.Г. Гуцко // Инновационный потенциал развития юридической науки и практики в современном мире: Сборник научных статей / Редколлегия: С.Е. Чебуранова (гл. ред.) [и др.]. – Гродно: Гродненский государственный университет имени Янки Купалы, 2023. – С. 312.

– Стандарты и протоколы: HTTP/HTTPS, FTP, SMTP, POP3/IMAP, DNS, SNMP, SIP и другие.

Сеть имеет многоуровневую архитектуру: уровень физической инфраструктуры, уровень сетевых протоколов, прикладной уровень (сервисы, приложения). Такое построение позволяет интегрировать разнородные системы и устройства, обеспечивая единую среду передачи информации[1].

Программно-технические особенности Интернет-сети:

Интернет представляет собой глобальную распределённую сеть передачи данных, не имеющую единого централизованного органа управления или контроля. Архитектура сети основана на принципах децентрализации, что означает наличие множества взаимосвязанных узлов (серверов, маршрутизаторов, клиентских устройств), принадлежащих различным организациям и частным лицам. Обмен информацией между участниками сети осуществляется посредством маршрутизации IP-пакетов, которые проходят через инфраструктуру большого числа независимых интернет-провайдеров.

Данная организационная модель исключает возможность установления абсолютного контроля за всей передаваемой информацией и создаёт предпосылки для анонимного или неконтролируемого обмена данными. В результате мониторинг цифрового трафика требует применения сложных, многоуровневых технических и программных средств, сочетающих алгоритмы фильтрации, анализа и корреляции данных в режиме реального времени.

К основным программно-техническим особенностям функционирования Интернет-сети относятся:

1. Использование унифицированных протоколов связи. Базовый стек протоколов TCP/IP обеспечивает совместимость и стандартизированный формат обмена данными между устройствами различных типов, работающими под управлением неоднородных операционных систем. Стандартизация позволяет

[1] Магомадова, Э.И. Правовое регулирование сети Интернет. Сеть Интернет: ее архитектура / Э.И. Магомадова, М.М. Саркарова // Журнал прикладных исследований. – 2023. – № 7. – С. 103-106.

интегрировать сеть с самыми разнообразными аппаратными и программными платформами, обеспечивая её универсальность и масштабируемость.

2. Децентрализованное хранение информации. Цифровые данные распределяются между множеством серверов, физически расположенных в разных странах и регионах. Часто реализуется репликация (дублирование) данных на отдельных узлах для повышения устойчивости к сбоям и отказам, а также для ускорения доступа пользователей. Такой подход затрудняет удаление информации и обеспечивает высокую степень её сохранности в случае атак на отдельные хосты.

3. Шифрование и анонимизация передачи данных. Современные технологии, включая протокол HTTPS, виртуальные частные сети (VPN), сеть анонимизации TOR и иные средства криптографической защиты, позволяют пользователям скрывать своё физическое местоположение, IP-адрес и персональные данные. Это снижает возможности отслеживания и идентификации участников сетевого взаимодействия, создавая дополнительные препятствия для правоохранительных органов.

4. Высокая пропускная способность каналов связи. Развитая телекоммуникационная инфраструктура позволяет передавать значительные объёмы данных с минимальной задержкой. Такая скорость особенно важна для реализации сложных распределённых систем, онлайн-сервисов и, к сожалению, для функционирования противозаконных схем, требующих оперативного обмена информацией.

5. Динамическая система доменных имён и IP-адресов. Благодаря механизмам переадресации, использованию временных (Disposable) доменных имён, а также размещению ресурсов на анонимных хостингах, отслеживание источников информации становится значительно затруднённым. Постоянное изменение привязки доменов и адресов препятствует долговременной блокировке ресурсов[1].

[1] Магомадова, Э.И. Указ. соч. – С. 105.

Особый интерес для исследования представляют сегменты сети, получившие названия deep web (глубокая сеть) и darknet (теневая сеть). Эти области находятся вне зоны индексирования стандартными поисковыми системами, что делает их недоступными для обычных методов поиска. Для входа в такие сегменты требуется специализированное программное обеспечение (например, браузер TOR), а коммуникация между пользователями обычно осуществляется в зашифрованной форме, исключающей перехват и анализ содержимого сообщений[1].

С точки зрения криминологии и кибербезопасности, эти скрытые сегменты сети играют ключевую роль в организации нелегальных торговых площадок, анонимных форумов и каналов передачи конфиденциальных данных, что требует разработки специализированных методов их выявления и мониторинга[2].

Развитие телекоммуникаций и цифровых технологий обусловило появление новых форм преступности. Интернет как среда взаимодействия стал не только инструментом легальной коммерции и коммуникации, но и пространством для преступной активности.

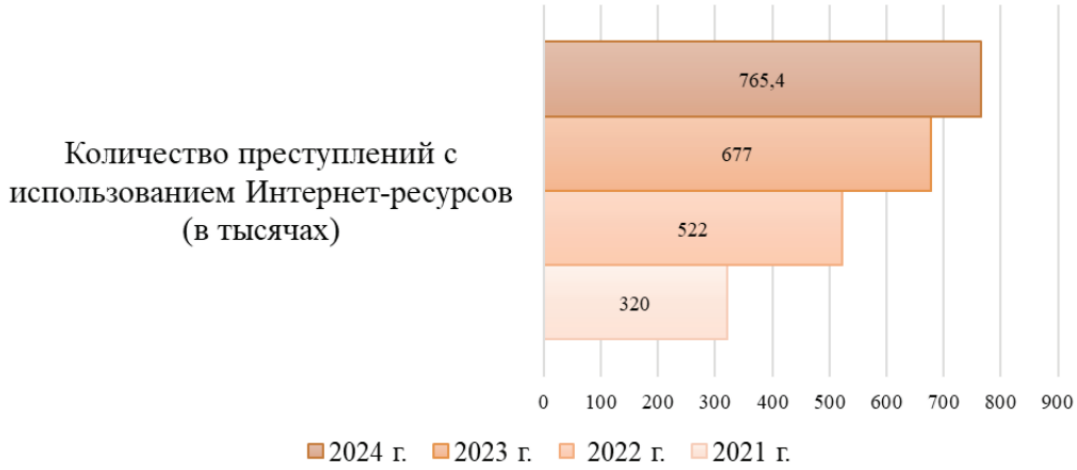
Из года в год в мире совершаются тысячи преступлений. В настоящее время преступность в сети Интернет – одна из международных проблем, наносящая значительный вред обществу, в том числе и государству в целом. В силу того, что возможности «всемирной паутины» растут с каждым днем, а информационные технологии выходят на новый уровень, появляются новые формы совершения противоправных действий. Технические средства довольно прочно закрепились в повседневной жизни граждан, сейчас практически у каждого человека есть гаджет с возможностью выхода в цифровое пространство. С его помощью возможно осуществлять различные действия: искать информацию, обучаться, общаться, совершать покупки, работать и т.д. Интернет

---

[1] Deep web, dark web, darknet и surface web – в чем разница? // Kaspersky daily. URL: https://blog.kaspersky.kz/deep-web-dark-web-darknet-surface-web-difference/23507/ (дата обращения: 25.11.2025).

[2] Поздняков, А.Н. Интернет и его функции в виртуальном пространстве: оперативно-розыскной аспект / А.Н. Поздняков // Академическая мысль. – 2024. – № 4 (29). – С. 47-52.

– мощнейший инструмент получения данных, которые, к сожалению, могут быть использованы злоумышленниками в корыстных целях. Согласно статистическим данным МВД около 40% от общего числа преступности составляют деяния, совершаемые в сетевом информационном пространстве[1]. Ниже на диаграмме представлены сведения о количестве зафиксированных преступлений за 2021-2024 г. с использованием Интернет-ресурсов:



Через сеть Интернет правонарушители преследуют незаконные цели для удовлетворения личных интересов. Так, информационное поле может выступать не только средством общения и обмена информацией между субъектами преступного мира, но и площадкой, на которой происходит реализация преступных замыслов. В целях предупреждения, пресечения и раскрытия данных преступлений, а также выявления и установления лиц, подготавливающих, совершающих или совершивших преступления, согласно Закона об ОРД свою деятельность организуют сотрудники оперативных отделов. Оперативные мероприятия в социально-технологической среде имеют свою специфику, в силу этого изменяется стратегия и тактика проведения оперативно-розыскных мероприятий. Сеть интернет помогает преступникам более тщательно скрыть следы преступления и остаться инкогнито. Можно выделить следующие особенности информационного пространства, которые необходимо учитывать при организации оперативной деятельности в сети Интернет:

[1] Состояние преступности в Российской Федерации за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 25.11.2025).

– онлайн-среда не имеет географических границ. В соответствии с этим возникает сложность определения места совершения преступления, в связи с нечеткостью его выражения (использование правонарушителями различных серверов, приложений VPN и иных способов, позволяющих скрыть место нахождения). Злоумышленник может совершать преступное деяние, находясь в любой точке мира, что существенно затрудняет проведение оперативно-розыскных мероприятий в отношении лиц, находящихся за границей. Процедура международного сотрудничества в отношении преступлений, имеющих трансграничный характер на данный момент, имеет определенные проблемы и весьма длительна;

– высокая скрытность, достигаемая, например, путем шифрования информации;

– изменчивость, постоянная смена огромного объема материалов, находящихся во всеобщем доступе. Данные из информационных потоков могут рассматриваться в качестве информации, представляющей оперативный интерес, а сеть Интернет – инструментом, выступающим в качестве ее поиска. Информационное пространство содержит в себе все глобальное количество информации, дополняющейся ежедневно, однако из-за большого количества ложной информации сетевое пространство не может являться полным источником ее получения для работы сотрудников оперативных отделов;

– еще одним фактором выступает скорость. Она проявляется как в совершении преступлений в режиме реального времени и скрытии следов преступления, так и в прогрессе программного обеспечения и процессе устаревания информации. Все это требует высокой оснащенности сотрудников техническими средствами и постоянной модернизации способов борьбы с преступностью в цифровом пространстве;

– на период 2024 года число пользователей Интернет ресурсами зарегистрировано более 130,4 миллиона человек, что из общего числа населения

Российской Федерации (144,2 миллиона) составляет около 90,4%[1]. Можно сказать, что доступ к информационной среде является свободным и имеет крайне мало ограничений, в следствии чего злоумышленнику не составляет труда найти себе жертву. Достаточное число пользователей не обладает высоким уровнем интернет-грамотности, а соответственно они потенциально становятся легкой добычей для правонарушителей;

– зачастую преступления совершаются во взаимодействии значительного количества лиц, в большинстве не знакомых между собой, что создает проблему в их поиске, идентификации и деанонизации. Использование фальшивых (поддельных) аккаунтов позволяет действовать от чужого имени, скрывая свою личность, а пользование анонимными площадками дает возможность лидерам свободно координировать, планировать преступность и организовывать взаимосвязь между друг другом;

– дистанционный характер совершения преступлений представляет возможность преступнику действовать напрямую без физического контакта с жертвой;

– существование различных социальных сетей и площадок упрощает коммуникацию между друг другом. Участники преступных сообществ мгновенно могут «пускать» в массы преступные взгляды и установки (пропаганда насилия, ненависти, терроризма и т.д.), негативно влияя на широкую аудиторию. Так же возможно распространение ложной информации в целях сокрытия следов преступления.

К основным категориям противоправного использования можно отнести:

– Киберпреступность – преступления, направленные на несанкционированный доступ к компьютерным системам, хищение данных, повреждение или блокировку информации. Примеры: взлом банковских систем, распространение вредоносного ПО (malware, ransomware), атаки типа DDoS.

[1] Сколько пользователей интернета в мире? (2025) // ИНКЛИЕНТ. URL: https://inclient.ru/users-internet-stats/ (дата обращения: 25.11.25025).

– Мошенничество и финансовые преступления – использование поддельных сайтов и сервисов (фишинг), обман в электронных платежных системах, аферы в интернет-торговле.

– Незаконный оборот товаров и услуг – анонимные торговые площадки в darknet предоставляют возможность приобретения наркотиков, оружия, поддельных документов, вредоносных программ.

– Распространение экстремистских и террористических материалов – сети используются для идеологической пропаганды, координации действий группировок, обучения участников, распространения инструкций по изготовлению оружия.

– Нарушение авторских прав и пиратство – незаконное копирование и распространение программ, фильмов, музыкальных и литературных произведений.

– Сексуальные преступления – распространение порнографических материалов с участием несовершеннолетних, вербовка и эксплуатация жертв через социальные сети.

Фактическая безграничность Интернета в географическом плане позволяет преступникам действовать вне юрисдикции конкретного государства, что создаёт значительные сложности для правоохранительных органов.

Для органов, осуществляющих оперативно-розыскную деятельность (ОРД), Интернет является источником ценнейшей информации, позволяющей:

– выявлять лиц, причастных к противоправным действиям;

– отслеживать финансовые транзакции;

– анализировать коммуникации в социальных сетях;

– получать данные о перемещениях и активности подозрительных лиц;

– выявлять места концентрации криминального контента[1].

[1] Филатова, В.А. Особенности получения оперативно-розыскной информации в сети интернет / В.А. Филатова // Вопросы деятельности служб и подразделений органов внутренних дел Российской Федерации: Сборник статей вузовской научно-практической конференции, Тверь, 07 апреля 2021 года. Том Выпуск 2. – Тверь: Тверской государственный университет, 2021. – С. 182-184.

Виртуальное пространство содержит как открытые источники данных (OSINT), так и закрытые сегменты, доступ к которым требует специальных технических средств и оперативных мероприятий. Важное значение имеют мониторинг форумов и сетевых сообществ, анализ поведения пользователей, корреляция сетевых идентификаторов с реальными личностями.

Отдельно следует отметить Значение Федерального закона от 07.07.2003 № 126-ФЗ «О связи»[1], который регламентирует обязанности операторов связи по хранению и предоставлению данных, необходимых для проведения ОРД. В рамках так называемого «пакета Яровой»[2] предусмотрены технические условия для хранения данных о соединениях, переданных сообщениях и содержимом трафика, что создаёт возможности для документирования противоправных действий в сети[3].

Использование Интернета в преступной деятельности связано с высокой динамикой технологий, поэтому методы ОРД должны постоянно совершенствоваться, включая применение искусственного интеллекта, машинного обучения, систем автоматического анализа больших данных (big data) и средств распознавания речевых и визуальных образов.

Итак, Интернет-сеть, обладая сложной мультиуровневой структурой и уникальными техническими характеристиками, является одновременно глобальным инструментом прогресса и средой повышенного риска. Программно-технические особенности сети обеспечивают открытость и доступность информации, но в то же время создают условия для анонимной,

---

[1] Федеральный закон от 07.07.2003 г. № 126-ФЗ (ред. от 31.07.2025 г.) «О связи» // Собрание законодательства РФ. – 14.07.2003. – № 28. – Ст. 2895.

[2] Пакет направлен на противодействие терроризму и экстремизму с использованием интернета, а также на упрощение расследования таких дел. Название закон получил по имени одного из авторов – депутата Госдумы Ирины Яровой.

[3] Федеральный закон от 06.07.2016 г. № 374-ФЗ (ред. от 29.12.2022 г.) «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. – 11.07.201. – № 28. – Ст. 4558; Федеральный закон от 06.07.2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. – 11.07.2016. – № 28. – Ст. 4559.

транскордонной преступной активности. Виртуальное пространство всё активнее используется преступными группами, что требует от правоохранительных структур не только совершенствования технических средств мониторинга и контроля, но и выработки комплексных правовых и организационных механизмов реагирования.

Таким образом, Интернет-сеть является не только средой, в которой совершаются преступления, но и мощным инструментом получения оперативно-розыскной информации. При этом децентрализованный характер сети, сочетание легальных и нелегальных сегментов, а также использование технологий шифрования создают дополнительные вызовы для правоохранительных органов, требуя постоянного совершенствования методов мониторинга, анализа и противодействия преступной деятельности в цифровой среде.

§2. Сбор оперативной информации и отслеживание «цифровых» следов в сети Интернет

Через сеть Интернет правонарушители преследуют незаконные цели для удовлетворения личных интересов. Так, информационное поле может выступать не только средством общения и обмена информацией между субъектами преступного мира, но и площадкой, на которой происходит реализация преступных замыслов. В целях предупреждения, пресечения и раскрытия данных преступлений, а также выявления и установления лиц, подготавливающих, совершающих или совершивших преступления, согласно Закона об ОРД, свою деятельность организуют сотрудники оперативных отделов. Оперативные мероприятия в социально-технологической среде имеют свою специфику, в силу этого изменяется стратегия и тактика проведения оперативно-розыскных мероприятий[1].

[1] Кривонос, А.А. Особенности получения оперативно-розыскной информации в сети интернет / А.А. Кривонос, М.С. Дзырук // Техника и безопасность объектов уголовно-исполнительной

Рассмотрим, какие существуют формы получения оперативно-розыскной информации в сети Интернет:

Оперативно-розыскной мониторинг представляет собой изучение, поиск, наблюдение сотрудниками оперативных отделов за ресурсами информационной среды, для установления сайтов, используемых в противозаконных целях, а также выявление платформ и страниц, на которых размещена, запрещенная к пропаганде информация, в целях их дальнейшего блокирования и привлечения виновных лиц к юридической ответственности. По факту это оперативное мероприятие, осуществляемое оперативным сотрудником в рамках общего познания, или с конкретной целью, при этом базой таких действий выступает ОРМ «наведение справок». Чаще всего данный метод имеет продолжительный характер. Для осуществления интернет мониторинга используются всеми известные поисковые системы. В рамках проведения мониторинга может осуществляться какое-либо оперативно-розыскное мероприятие (наведение справок, оперативное внедрение, наблюдение, опрос).

Для аккумулирования, категоризации и детального изучения большого объема данных на наличие в текстах, изображениях, на сайтах, форумах, блогах, платформах, иных информационных ресурсах, сведений об обстановке криминальной среды, информации, запрещенной к пропаганде, признаках готовящихся преступлений или о лицах, состоящих в преступных организациях, а также иной информации, представляющей оперативный интерес, реализуется направление контент-анализа. С помощью данного аналитического метода информация, полученная оперативником, подвергается обработке, исследованию и обобщению. Данные действия возможно соотнести с ОРМ «исследование предметов и документов».

Как упоминалось выше, участники криминальной среды, как правило, общаются посредством так называемого «теневого общения». Каналы, закрытые от общего доступа, не индексируются поисковыми серверами. Ввиду этого

системы: Сборник материалов Международной научно-практической конференции. В 4-х томах, Воронеж, 14–15 мая 2025 года. – Воронеж: ИП Копыльцов П.И., 2025. – С. 368-372.

необходимо применение более сложных алгоритмов для их обнаружения и непосредственное наблюдение за данными зонами. Еще одним направлением является получение информации от гражданских лиц. Например, с помощью специализированных сайтов, заполнив форму, граждане вправе анонимно подать сообщение о подготавливаемых преступлениях и иных признаках преступной деятельности. Так, на официальном сайте федеральной службы безопасности Российской Федерации можно передать значимую информацию для оперативных подразделений.

В настоящее время возрастает объем участия людей в обмене информацией, в том числе в электронном виде, при котором используются их персональные данные в рамках получения той или иной государственной, коммерческой либо другой услуги, что также становится фактором обеспечения социальной деятельности и эффективного общения. Причем большинство людей не имеют исчерпывающей информации о том, какие персональные данные, с какой целью, кому и в каком объеме передаются. Современный уровень развития и проникновения информационных технологий таков, что человек ежеминутно предоставляет огромное количество информации о себе самым различным компаниям. При этом мельчайшие частицы такой информации, включая кажущиеся совсем незначительными, могут комбинироваться друг с другом с помощью применения цифровых технологий, воссоздавая полный образ человека.

Цифровое присутствие неизбежно сосуществует с такими явлениями, как «цифровой след» и «цифровая тень».

Интернет заполнен множеством цифровых следов и теней, которые могут использоваться для анализа поведения пользователя.

Цифровая тень – это информация, создаваемая о людях автоматически посредством деятельности и устройств третьих лиц[1].

[1] Анохов, И.В. Цифровая тень как инструмент для исследования отрасли / И.В. Анохов // E-Management. – 2022. – Т. 5, № 1. – С. 80-92.

Цифровой след – это совокупность данных, образующихся в результате взаимодействия субъекта с цифровой средой, фиксирующих его активность в сети и при использовании электронных устройств. Он может быть явным (открыто публикуемые сообщения, фото, видео) и скрытым (метаданные файлов, логи сервисов, геоинформация, технические идентификаторы)[1].

Для целей ОРД цифровые следы условно делятся на:

1. Регистрационные данные – имя, логин, адрес электронной почты, номер телефона, использованные при регистрации в сервисах.

2. Трафиковая информация – IP-адреса, MAC-адреса устройств, протоколы подключений, временные метки.

3. Контентные следы – сообщения, изображения, видеозаписи, комментарии, тексты на форумах, блогах.

4. Метаданные – техническая информация, сопровождающая контент: геолокация фото, модель используемого устройства, время создания и модификации.

5. Сетевые связи – перечень контактов, подписок, переписка, пересылки и репосты.

6. Поведенческие паттерны – типичное время активности в сети, реакция на события, характер поисковых запросов[2].

Этапы технологического цикла сбора цифровых следов. ОРД по выявлению цифровых следов в Интернете происходит поэтапно:

1. Мониторинг – непрерывное наблюдение за открытыми и условно закрытыми ресурсами: социальные сети, форумы, блоги, мессенджеры, маркетплейсы, даркнет-площадки.

2. Выявление объекта – определение аккаунтов и идентификаторов, связанных с целевым лицом или группой.

---

[1] Делягин, М.Г. «Цифровой след» личности – новый смысл существования человечества и некоторые следствия этого / М.Г. Делягин // Свободная мысль. – 2021. – № 2 (1686). – С. 5-14.
[2] Сарычев, М.М. Особенности выявления и фиксации цифровых следов преступлений в рамках ОРД / М.М. Сарычев // Научные исследования XXI века. – 2024. – № 2(28). – С. 146-150.

3. Извлечение данных – парсинг контента, выгрузка логов, фиксация метаданных, сбор публикаций и медиафайлов.

4. Корреляция и сопоставление – увязка разрозненных сведений: установление совпадений по никнеймам, IP-адресам, геолокации.

5. Анализ – применение инструментов OSINT, графовых моделей связей, сетевого картографирования.

6. Сохранение и легализация – документирование информации для дальнейшего использования в процессуальной деятельности, оформления доказательственной базы.

Методы и источники (OSINT в ОРД). OSINT (Open Source Intelligence) – открытая разведка, предполагающая сбор информации из общедоступных источников. В ОРД применяются:

– Поисковые системы и метапоиск (Google, Bing, Yandex, DuckDuckGo) – поиск упоминаний, документов, изображений.

– Социальная аналитика: инструменты типа SocialMention, Brandwatch, SentiOne, позволяющие отслеживать активность в социальных сетях и настроения аудитории.

– Фото- и видеопоиск: TinEye, Google Image Search – поиск оригинала изображения и мест его размещения.

– Анализ WHOIS[1] и DNS – установление владельцев и истории доменов, IP-адресов.

– Геолокационные сервисы – получение данных о местоположении авторов контента.

– Парсеры и краулеры – автоматизированный сбор информации с сайтов.

В рамках ОРД эти методы интегрируются в специализированные комплексы мониторинга, учитывающие вопросы правового регулирования.

Пример 1: В ходе расследования случаев мошенничества с использованием онлайн-платежных систем одной из основных улиц поиска стало установление

[1] Сервис по предоставлению выделенных серверов. URL: https://www.whois-service.ru. (дата обращения: 25.11.2025).

IP-адресов, с которых осуществлялись операции. Благодаря корреляции данных от провайдеров и анализа активности в социальных сетях удалось выявить лиц, находящихся в другом регионе, а также установить их связь с другими преступными эпизодами[1].

Пример 2: При выявлении группы, занимающейся сбытом наркотических средств через условно закрытые Telegram-каналы, сотрудники ОРД применили метод контентной аналитики. Использовалась автоматическая выгрузка ключевых слов, а также определение временных паттернов публикаций, что позволило выйти на организаторов[2].

Пример 3: Выявление организаторов DDoS-атаки на государственный портал. В одном из регионов Российской Федерации в 2023 году была зафиксирована массовая DDoS-атака на портал государственных услуг, приведшая к временной недоступности ресурса. Оперативными подразделениями был произведён анализ сетевого трафика, зафиксированного службами кибербезопасности. Сопоставление IP-адресов с данными зарубежных провайдеров показало, что атака инициировалась с арендованных серверов в нескольких странах Восточной Азии. Через выявленные цифровые следы – данные об учетных записях на хостинговых платформах, время регистрации, привязанные электронные кошельки – удалось установить организационную группу лиц, занимающуюся подобными атаками по заказу[3].

Пример 4: Расследование кибермошенничества с криптовалютами. В ходе оперативно-розыскных мероприятий по делу о хищении криптовалюты у пользователей инвестиционной платформы информация была собрана из

---

[1] Приговор Иволгинского районного суда (Республика Бурятия) № 1-37/2020 1-466/2019 от 05.02.2020 г. по делу № 1-37/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/sn2BltwAV8H8/ (дата обращения: 25.11.2025).

[2] Приговор Ухтинского городского суда (Республика Коми) № 1-283/2020 от 14.07.2020 г. по делу № 1-283/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Ppfg23ryMwHT/ (дата обращения: 25.11.2025).

[3] Атаки на портал госуслуг // TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%90%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB_%D0%B3%D0%BE%D1%81%D1%83%D1%81%D0%BB%D1%83%D0%B3 (дата обращения: 25.11.2025).

блокчейна – открытой распределённой базы данных транзакций. Анализ транзакционных «цепочек» позволил выявить кошельки, на которые переводились похищенные активы. Далее через мониторинг специализированных форумов (в т.ч. в даркнете) были обнаружены объявления о продаже криптовалюты с использованием этих адресов. Соотнесение никнеймов и метаданных публикаций позволило выйти на конкретных участников преступной группы. Этот случай показал, что даже децентрализованные и анонимные системы хранения данных оставляют цифровые следы, которые поддаются аналитическому исследованию[1].

Пример 5: Поиск несовершеннолетнего по активности в социальных сетях. В одной из российских областей органы внутренних дел проводили поиск пропавшего подростка. Мониторинг социальных сетей показал, что аккаунт пропавшего оставался активным – были отметки «онлайн» в мессенджере и публикации в сообществе знакомств. Анализ геотегов в двух новых фотографиях позволил установить фактическое местоположение автора в соседнем городе. Это дало возможность оперативно выехать на место, где несовершеннолетнего нашли в компании знакомых. Здесь цифровой след сыграл ключевую роль в ускорении поиска и установлении контакта[2].

Пример 6: Анализ цифровых следов при выявлении экстремистской группы. В рамках межведомственного расследования правоохранительные органы вели наблюдение за несколькими аккаунтами в социальных сетях, распространявших материалы экстремистского характера. Автоматизированный сбор постов и публикаций, их тематическая категоризация по ключевым словам («призывы», «акции», «ответственность») позволили выявить круг постоянных комментаторов и активных участников групп. Построение графа социальных связей показало, что большинство из них состоят в закрытом чате мессенджера.

---

[1] Приговор Пролетарского районного суда г. Ростова-на-Дону (Ростовская область) № 1-272/2023 от 16.08.2023 г. по делу № 1-272/2023 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/0zHE4yQknvoN/ (дата обращения: 25.11.2025).

[2] Найден, жив! Правовые аспекты поиска пропавших в России // РАПСИ. URL: https://rapsinews.ru/publications/20210611/307135480.html (дата обращения: 25.11.2025).

После оперативного внедрения сотрудника под прикрытием в этот чат стало возможным получать данные о планируемых незаконных акциях[1].

Пример 7: Применение цифровой криминалистики при расследовании убийства. В одном из дел по расследованию тяжкого преступления следователи использовали цифровые следы из смартфона подозреваемого. Анализ метаданных фотографий показал, что снимки были сделаны вблизи места происшествия за несколько часов до события. Кроме того, в кэш-файлах приложений сохранились координаты перемещений, совпадающие с временной линией преступления. Такой цифровой анализ стал важным элементом доказательной базы в суде[2].

Отдельно подробнее остановимся на анализе программных средств сбора и анализа информации из Интернет-источников.

Программные средства в автоматизированном режиме собирающие данные из Интернет-источников способны не только анализировать содержимое web-страниц, но и имитировать действия реальных пользователей для доступа к данным, которые Интернет-ресурс предоставляет только убедившись, что имеет дело с живым человеком, использующим программу-браузер для доступа к сайту. Примеры таких программных средств приведены, например, для социальной сети Вконтакте[3]. Это две библиотеки BeatifulSoup и lxml, позволяющие проводить сбор и анализ текста Интернет-ресурсов, а также набор программных средств Selenium (Selenium WebDriver, Selenium RC, Selenium Server, Selenium Grid, Selenium IDE), позволяющих имитировать действия

---

[1] Иващенко, М.А. Расследование преступлений экстремистской направленности, совершенных с использованием сети Интернет: учебно-методическое пособие / М.А. Иващенко. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – 105 с.

[2] Шаров, В.И. «Цифровая оперативно-розыскная деятельность» и цифровизация противодействия преступлениям / В.И. Шаров // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 3(107). – С. 171-178.

[3] Амирханова, Х.А. Характеристика сети Интернет / Х.А. Амирханова // Интеллектуальный потенциал общества как драйвер инновационного развития науки: Сборник статей Международной научно-практической конференции в 2 частях, Иркутск, 17 января 2023 года. Том Часть 1. – Уфа: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2023. – С. 16.

пользователей, работающих через программы-браузеры с Интернет-ресурсом. Примеры построения и применения систем имитирующих работу пользователей приведены, например, в следующих работах[1].

Интересной тенденцией в настоящее время выступает возможность распространения противозаконной информации посредством изображений, которые могут при этом содержать и текстовую информацию внутри себя, но не распознаваемую напрямую как текст. Для его автоматизированного извлечения необходимо проведение анализа изображения. Однако особый интерес при анализе графической информации Интернет-ресурсов представляет идентификация лиц пользователей, позволяющая приблизиться к раскрытию преступления, установив его фигурантов. В настоящее время существует большое количество программных средств, позволяющих осуществлять анализ массивов графической информации на Интернет-ресурсах с целью идентификации портретов пользователей и сопоставления их с конкретными лицами. Для решения подобных задач используются реализованные в программных средствах нейронные сети, выполняющие когнитивные функции, присущие ранее только живому человеческому мозгу[2]. В качестве примеров следует указать зарубежные программы FaceNet компании Google и Amazon Rekognition компании Amazon, Deep Dense Face Detector компании Yahoo.

---

[1] Алейников, Д.П. Анализ цифрового контента социальных сетей на предмет выявления оперативно значимой информации / Д.П. Алейников, М Б. Руденко // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года / Под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2020. – С. 40-44; Калытюк, И.С. Начальные этапы проектирования системы сбора и предиктивного анализа данных социальных медиа / И.С. Калытюк, Г.А. Французова, А.В. Гунько // Системы анализа и обработки данных. – 2021. – № 1(81). – С. 73-84; Купин, А.Ф. Организация использования возможностей сети Интернет при раскрытии преступлений / А.Ф. Купин, А.А. Павлова // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 года. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 142-146.

[2] Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering. URL: https://arxiv.org/pdf/1503.03832.pdf (дата обращения: 25.11.2025).

Обзоры возможностей этих программных средств можно найти в источниках[1]. Российские разработчики также готовы предложить инструменты для решения подобных задач, например: FindFace Pro компании NTechLab, Face-Интеллект компании ITV, широкий спектр программно-аппаратных средств компании Vocord, сравнительное описание можно найти в исследованиях[2].

Представляется перспективным направлением деятельности подразделений специальных технических мероприятий территориальных органов МВД России комбинированное использование описанных программных средств для решения правоохранительных задач по выявлению, раскрытию и расследованию преступлений. Отмечая, что в настоящее время в органах внутренних дел применяется ряд разрозненных программных средств по мониторингу Интернет-ресурсов, следует проработать задачу создания комплексного целевого программного продукта, акцентированного на поиске противоправных проявлений в Интернет-пространстве, установлении на основе текстовой информации обстоятельств и профилей пользователей, связанных с криминальной активностью, а также анализ графической информации социальных сетей для отождествления виртуальных профилей и реальных лиц.

При этом учитывая специфику деятельности органов внутренних дел, подобные системы могут служить лишь в качестве систем поддержки принятия решений, дополняя результаты оперативных и аналитических мероприятий.

Сбор информации из Интернета должен строго соответствовать Федеральному закону № 144-ФЗ от 12.08.1995, а также нормам Закона о персональных данных (№ 152-ФЗ)[3] и Закона о связи (№ 126-ФЗ).

Особо важно учитывать:

---

[1] Farfade S.S., Saberian M., Li L.-J. Multi-view Face Detection Using Deep Convolutional Neural Networks. URL: https://arxiv.org/pdf/1502.02766.pdf (дата обращения: 25.11.2025); Amazon Rekognition. URL: ttps://aws.amazon.com/ru/rekognition/ (дата обращения: 25.11.2025); MIT Technology Review. URL: https://www.technologyreview.com (дата обращения: 25.11.2025).

[2] Купин, А.Ф. Использование современных программных средств распознавания изображений в правоохранительной деятельности / А.Ф. Купин, О.А. Баринова, В.М. Егорова // Вестник Волгоградской академии МВД России. – 2017. – № 3(42). – С. 105-111.

[3] Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 24.06.2025 г.) «О персональных данных» // Собрание законодательства РФ. – 31.07.2006. – № 31 (1 ч.). – Ст. 3451.

– порядок санкционирования получения данных, составляющих тайну связи (ст. 8 Закона об ОРД);

– исключения, допускающие сбор сведений без согласия лица при наличии угрозы государственной или общественной безопасности;

– необходимость документального оформления каждого этапа извлечения данных для обеспечения их допустимости как доказательств.

Развитие технологий электронной форензики в странах ЕС и США показывает высокую эффективность сотрудничества государственных и частных структур. Перспективно для РФ:

– создание межведомственных центров OSINT-анализа;

– унификация форматов хранения цифровых следов;

– развитие алгоритмов предварительного прогнозирования угроз.

Проблемы и риски:

1. Правовые коллизии – несоответствие между скоростью техпроцессов и динамикой изменения законодательства.

2. Анонимизация и шифрование – использование VPN, TOR, прокси усложняет атрибуцию следа.

3. Избыточность данных – необходимость фильтровать огромные массивы информации.

4. Этические вопросы – баланс между безопасностью и неприкосновенностью частной жизни.

Итак, сбор оперативной информации и отслеживание цифровых следов в сети Интернет – это сочетание технических, организационных и правовых мер, направленных на выявление, фиксацию и анализ сетевой активности. Эффективное проведение таких мероприятий требует высокой квалификации сотрудников, современного технического оснащения и правовой грамотности. Системный подход, включающий OSINT, анализ больших данных и традиционные методы ОРД, обеспечивает возможность получения достоверной информации, необходимой для раскрытия и предупреждения преступлений в условиях цифровой эпохи.

§3. Выдвижение и проверка оперативно-розыскных версий и планирование дальнейших этапов получения оперативно-розыскной информации по раскрытию преступлений

В практике органов, уполномоченных на осуществление оперативно-розыскной деятельности, своевременное и обоснованное выдвижение оперативно-розыскных версий является базовым методическим приёмом, определяющим направления поиска, установления и фиксации фактических данных, способных приобрести доказательственное значение в уголовном судопроизводстве. В условиях цифровизации общественных отношений, глобальной информатизации и интенсивного развития информационно-телекоммуникационных технологий сеть Интернет становится комплексным источником сведений, позволяющим получать значительный объём информации как о событиях, имеющих признаки преступления, так и о лицах, вовлечённых в противоправную деятельность. При этом специфика виртуальной среды обуславливает необходимость адаптации классических алгоритмов выдвижения и проверки версий к особенностям цифрового пространства[1].

1. Методологические основы выдвижения оперативно-розыскных версий.

Выдвижение версии в рамках ОРД представляет собой формулирование обоснованного предположения, основанного на совокупности выявленных признаков и фактов, полученных в ходе анализа информационных массивов, связанных с преступлением. Согласно ч. 1 ст. 2 Закона об ОРД, одной из задач ОРД является выявление, предупреждение, пресечение и раскрытие преступлений. В условиях цифровой среды этот процесс включает системно-аналитическую обработку общедоступных данных (Open Source Intelligence, OSINT), результатов негласных поисковых мероприятий, а также информации,

[1] Шаров, В.И. «Цифровая оперативно-розыскная деятельность» и цифровизация противодействия преступлениям / В.И. Шаров // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 3(107). – С. 176.

поступающей из специализированных сегментов сети или от конфиденциальных источников.

Примером может служить ситуация выявления признаков организованного мошенничества с использованием электронных платёжных систем. Оперативный сотрудник, анализируя цифровые следы (лог-файлы, активность аккаунтов в социальных сетях, сообщения на криминальных форумах), может сформировать несколько рабочих гипотез, касающихся личности предполагаемого преступника, структуры преступной группы, способов совершения и маскировки противоправных действий.

Такая технология описана, например, в работе С.М. Ховавко, который указывает на необходимость применения «комбинированных техник цифрового профилирования в структуре выдвижения версий»[1].

2. Процедуры проверки версий в цифровой среде

Проверка версий в контексте ОРД предполагает реализацию комплекса мероприятий, направленных на подтверждение либо опровержение исходных гипотез. Основными требованиями к цифровым доказательствам выступают полнота, достоверность и верифицируемость. При проверке версия должна сопоставляться с результатами иных оперативно-розыскных мероприятий, предусмотренных законодательством (например, получение информации о соединениях в электросвязи – ст. 6 Закона об ОРД).

В условиях Интернета важна многоуровневая система верификации, включающая:

– Корреляционный анализ данных из различных онлайн-источников;

– Цифровую атрибуцию объектов (определение владельца аккаунта, IP-адреса, криптокошелька);

– Кросс-проверку фактов с привлечением негласных действий;

---

[1] Ховавко, С.М. Влияние фактора цифровизации на оперативно-розыскную деятельность органов внутренних дел/ С.М. Ховавко // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2023. – Т. 9 (75). № 4. – С. 283-286.

– Проведение компьютерно-технической экспертизы[1];

– Лингвистический и семантический анализ коммуникаций в цифровой среде.

Так, при проверке версии о причастности группы лиц к фишинговым атакам был применён метод контент-анализа, основанный на поиске идентичной семантики в переписке, извлечённой с закрытого форума и перехваченной в локальной сети[2].

3. Планирование дальнейших этапов получения информации

Планирование дальнейших этапов получения оперативно-розыскной информации в Интернете предполагает стратегическую расстановку приоритетов по маршрутам сбора данных, распределение ресурсов доступа к закрытым сегментам и обеспечение технологического потенциала для перехвата и анализа потоков сетевого трафика. Долгосрочное планирование осуществляется с учётом динамики сетевых тенденций, появления новых коммуникационных платформ, изменения алгоритмов поисковых систем и политики модерации контента. Например, при выявлении признаков формирования преступного сообщества в закрытых группах мессенджеров дальнейшие этапы могут включать имитационно-поведенческое внедрение оперативного сотрудника в цифровое сообщество, систематический мониторинг переписки, выявление каналов поступления и распределения финансовых средств, фиксацию задокументированных фактов с последующим процессуальным оформлением.

Планирование этапов получения оперативно-розыскной информации при использовании сети Интернет:

Организация деятельности по выявлению и сбору оперативно-розыскной информации в цифровом пространстве предполагает построение процесса на

---

[1] Хатунцев, Н.А. Судебная компьютерно-техническая экспертиза в свете цифровизации общества / Н.А. Хатунцев // Эксперт-криминалист. – 2020. – № 2. – С. 18-20.

[2] Кобец, П.Н. Фишинговые атаки как один из самых распространенных видов киберпреступности и меры по противодействию / П.Н. Кобец // Научный портал МВД России. – 2023. – № 1(61). – С. 82-89.

основе принципов как стратегической, так и тактической последовательности действий. Стратегическое планирование направлено на определение долгосрочных приоритетов, учитывающих системные изменения в инфраструктуре сети и динамику развития цифровых технологий, тогда как тактическая составляющая связана с реализацией конкретных оперативных мероприятий, согласованных с текущими условиями информационной среды.

В рамках долгосрочного планирования внимание сосредотачивается на ряде ключевых факторов:

– Тенденции эволюции сетевых платформ – анализ направлений развития социальных сетей, мессенджеров, электронных торговых площадок и других интернет-сервисов, включая прогнозы изменения их функциональности и уровня защищённости.

– Появление новых каналов коммуникации – выявление и изучение перспективных или нишевых инструментов передачи данных, которые могут стать популярными в целевых аудиториях, включая децентрализованные приложения, peer-to-peer сети и специализированные анонимные сервисы.

– Изменения алгоритмов поисковых систем – отслеживание модификаций механизмов ранжирования и индексирования веб-ресурсов, которые могут влиять на доступность определённых сегментов информации, а также на эффективность применения OSINT-методов.

– Развитие технологических мер противодействия – учет и анализ применения инструментов анонимизации и защиты цифрового трафика (VPN-сервисы, сеть Tor, алгоритмы криптографического шифрования), которые снижают возможности идентификации и слежения, усложняя сбор достоверных данных.

Таким образом, планирование в оперативно-розыскной деятельности, связанной с использованием сети Интернет, должно основываться на комплексном подходе, включающем прогнозирование технологических тенденций, оценку изменений в цифровой инфраструктуре и разработку адаптивных методик применения аналитических и технических средств.

При выявлении преступного сообщества в закрытых чатах мессенджеров, например, может быть предусмотрено имитационно-поведенческое внедрение оперативного сотрудника в цифровое сообщество, систематический мониторинг переписки, фиксация задокументированных фактов с последующим процессуальным оформлением – при обязательном соблюдении требований ст. 5 Закона об ОРД о законности методов получения информации.

В план также закладывается возможность проведения оперативного эксперимента в цифровой среде, например, создание заведомо интересующего фигуранта контента (объявления о продаже запрещённых предметов) для инициирования его активности и последующего наблюдения за реакцией. Как отмечает С.Н. Маслов, имитационные мероприятия в Интернете требуют «аккуратного сочетания технических средств и психологической настройки оперативного сотрудника»[1].

4. Прогнозирование и адаптация планов

В условиях высокой изменчивости цифровой информации версии должны быть устойчивыми к изменению ситуации, а план – гибким и опираться на модульный принцип. Это предполагает возможность быстрой интеграции вновь обнаруженных данных, параллельную проверку нескольких версий и оперативное перераспределение ресурсов.

Таким образом, выдвижение и проверка оперативно-розыскных версий в сети Интернет представляет собой многоэтапный, научно обоснованный процесс, требующий сочетания аналитических методик, технологических инструментов и строгого нормативного регулирования. Применение сетевых источников позволяет существенно увеличить массив данных, но требует тщательного планирования, контроля достоверности и адаптации к условиям киберпространства.

---

[1] Маслов, С.Н. О некоторых актуальных вопросах интенсификации и модернизации профессиональной подготовки сотрудников органов внутренних дел Российской Федерации с использованием имитационных средств обучения / С.Н. Маслов, Е.С. Бондаренко // Закон и право. – 2025. – № 3. – С. 221-224.

ГЛАВА 2. СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ПОЛУЧЕНИЮ ИНФОРМАЦИИ, ПРЕДСТАВЛЯЮЩЕЙ ИНТЕРЕС ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

§1. Проблемы и пути решения организационно-правового обеспечения оперативно-розыскной деятельности в сети Интернет

Организационно-правовое обеспечение оперативно-розыскной деятельности в сети Интернет в условиях цифровизации общества приобретает особую значимость, поскольку глобальная сеть стала ключевым каналом коммуникаций, коммерческой активности и, одновременно, площадкой для совершения противоправных действий.

В последние годы законодательство Российской Федерации претерпело изменения, направленные на адаптацию правовых инструментов к цифровым угрозам. Так, внесены поправки в Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», расширяющие перечень оперативных мероприятий в электронном формате, и в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи», закрепляющие обязанность операторов связи по хранению и передаче определённых категорий данных («пакет Яровой»).

Однако анализ правоприменительной практики (материалы Судебного департамента при Верховном Суде РФ[1]; отчёты МВД России за 2023-2024 гг.[2]) показывает, что существующие нормы не полностью охватывают специфику онлайн-розыска и порождают значимые организационные и правовые проблемы.

Проблема 1. Отсутствие унифицированного правового механизма для онлайн-ОРД.

---

[1] Судебная статистика. Судебный департамент при Верховном суде. URL: https://cdep.ru/index.php?id=5 (дата обращения: 25.11.2025).

[2] Состояние преступности в Российской Федерации за январь-декабрь 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 25.11.2025); Состояние преступности в Российской Федерации за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 25.11.2025).

Несмотря на то, что ст. 6 Закона об ОРД допускает проведение оперативных мероприятий с использованием технических средств связи, порядок их осуществления в трансграничной цифровой среде чётко не регламентирован. В практике российских правоохранительных органов неоднократно возникали ситуации, когда собранные в ходе анализа сетевой активности доказательства признавались недопустимыми из-за того, что получение данных велось через зарубежные серверы без международного запроса по линии правовой помощи[1]. Международная правовая база, в частности Будапештская конвенция о киберпреступности (2001 г.)[2], предусматривает упрощённый обмен цифровыми доказательствами, но Россия формально не участвует в её механизмах, опираясь на двусторонние договоры, что снижает оперативность реагирования.

Проблема 2. Взаимодействие с интернет-провайдерами и платформами.

В соответствии со ст. 64 Закона «О связи» операторы обязаны обеспечивать хранение и предоставление информации по запросам уполномоченных органов. На практике фиксируются случаи неполного предоставления данных или задержек в ответах, особенно при запросах к международным IT-компаниям (пример: переписка в мессенджере WhatsApp в деле № 1-216/2025 Раменского городского суда)[3]. Российские суды неоднократно указывали на необходимость стандартизации форматов передачи данных (см. апелляционное определение Санкт-Петербургского городского суда от 28.11.2017 г. № 33-23595/2017 по делу № 2-4865/2017)[4].

Проблема 3. Отсутствие единой межведомственной платформы.

---

[1] Напр., приговор Центрального районного суда г. Читы (Забайкальский край) № 1-1223/2019 1-43/2020 от 26.07.2020 г. по делу № 1-1223/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/pQ3MyHNrVIZp/ (дата обращения: 25.11.2025).

[2] Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Заключена в г. Будапеште 23.11.2001 г.) (с изм. от 28.01.2003 г.) // СПС «КонсультантПлюс».

[3] Приговор Раменского городского суда (Московская область) № 1-216/2025 от 28.04.2025 г. по делу № 1-216/2025 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/ynmMtPjjPq6l/ (дата обращения: 25.11.2025).

[4] Апелляционное определение Санкт-Петербургского городского суда от 28.11.2017 г. № 33-23595/2017 по делу № 2-4865/2017 // СПС «КонсультантПлюс».

Базы данных, формируемые ФСБ, МВД, Следственным комитетом и Роскомнадзором, остаются ведомственно-замкнутыми, что затрудняет комплексный анализ угроз. Примером негативных последствий стала утечка данных пользователей в одном из дел, когда информация, доступная одному ведомству, не была своевременно передана другому, что затянуло оперативную работу[1].

Проблема 4. Рост использования средств анонимизации.

В уголовных делах, связанных с распространением запрещённого контента (ст. 242.1 УК РФ – распространение детской порнографии, ст. 205.2 УК РФ – публичные призывы к терроризму), оперативные сотрудники фиксируют использование сетей Tor, VPN, а также мессенджеров с end-to-end шифрованием (Telegram, Signal), что снижает возможности мониторинга. Несмотря на то, что в 2025 году в России были ужесточены требования к идентификации пользователей в интернете и значительно увеличены штрафы за нарушения (в том числе по Законам 152-ФЗ «О персональных данных» и Закону «Об информации»)[2], обход этих требований с помощью анонимайзеров остаётся распространённым.

Теоретико-правовые проблемы в российской юриспруденции касаются уточнения понятия «оперативно-розыскная информация» применительно к цифровым источникам. Постановление Конституционного Суда РФ от 17 октября 2017 г. № 24-П указало, что сведения, полученные без судебного решения в рамках ОРД, могут быть допустимы при условии соблюдения принципа соразмерности[3]. Однако, в сети Интернет грань между публичными

---

[1] Парфенов, А.В. Некоторые проблемы взаимодействия оперативных подразделений органов, осуществляющих оперативно-розыскную деятельность, по борьбе со взяточничеством, совершаемым с использованием информационно-телекоммуникационных технологий / А.В. Парфенов, Д.М. Фарахиев // Вестник Уральского юридического института МВД России. – 2025. – № 3(47). – С. 138-144.

[2] Федеральный закон от 30.11.2024 г. № 420-ФЗ (ред. от 23.05.2025 г.) «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ. – 02.12.2024. – № 49 (часть IV). – Ст. 7411.

[3] Постановление Конституционного Суда РФ от 17.10.2017 г. № 24-П «По делу о проверке конституционности пункта 5 части четвертой статьи 392 Гражданского процессуального

данными (например, в открытом профиле пользователя в соцсети) и закрытыми сведениями (переписка, приватные фото) нередко размыта, что требует дополнительных правовых разъяснений.

Возможные пути решения:

1. Закрепление специальных процедур ОРД в цифровой среде – внесение в ФЗ «Об ОРД» отдельной главы, описывающей алгоритмы получения, фиксации, хранения и представления в суде цифровых доказательств.

Предлагается дополнить Федеральный закон «Об оперативно-розыскной деятельности» отдельной главой, посвященной особенностям работы с цифровыми доказательствами. В данной главе следовало бы детально регламентировать алгоритмы их получения из сетевых источников, методы фиксации в неизменном виде, порядок безопасного хранения с применением криптографических технологий, а также механизмы представления этих доказательств в судебных органах. Такая правовая стандартизация позволит обеспечить их допустимость и надежность с точки зрения процессуальных норм, исключая возможность подтасовки или утраты данных.

2. Реформа межведомственного взаимодействия – создание единой федеральной платформы («Цифровой ОРД»), обеспечивающей автоматическую синхронизацию данных между ФСБ, МВД, СК и Роскомнадзором; аналогичные системы работают в ЕС (проект Europol Data Exchange).

Рекомендуется разработать и внедрить единую федеральную цифровую платформу условно под названием «Цифровой ОРД». Эта платформа должна осуществлять автоматическую синхронизацию данных и аналитических материалов между ключевыми субъектами оперативно-розыскной деятельности: Федеральной службой безопасности, Министерством внутренних дел, Следственным комитетом и Роскомнадзором. Платформа будет функционировать по принципу защищенного обмена данными с использованием протоколов высокой степени шифрования, минимизируя риск информационных

кодекса Российской Федерации в связи с жалобами граждан Д.А. Абрамова, В.А. Ветлугаева и других» // Вестник Конституционного Суда РФ. – № 6. – 2017.

утечек. Подобная инфраструктура уже получила развитие в Европейском союзе – примером служит проект Europol Data Exchange, позволяющий правоохранительным органам разных стран работать в едином информационном пространстве.

3. Разработка стандартов взаимодействия с IT-компаниями – закрепление на законодательном уровне обязательных форматов передачи данных и сроков их предоставления; использование зарубежной практики (Австралийский закон Assistance and Access Act 2018[1]).

На законодательном уровне следует утвердить обязательные форматы передачи данных, а также чётко обозначить регламентированные сроки их предоставления правоохранительным органам. В качестве ориентира может быть использован международный опыт, в частности положения Австралийского закона Assistance and Access Act 2018, который регулирует доступ государственных структур к информации, находящейся в распоряжении технологических компаний. Установление подобных стандартов в России позволило бы не только ускорить процесс получения ключевых цифровых доказательств, но и повысить их юридическую значимость в рамках судебного рассмотрения.

4. Инвестиции в технические средства анализа трафика – применение систем распознавания анонимных соединений и анализа больших данных (Big Data Intelligence) в совокупности с судебным контролем.

Необходима интеграция в деятельность органов ОРД систем, способных выявлять и распознавать анонимные соединения (в том числе через сети типа Tor или VPN), а также проводить масштабный анализ структурированных и неструктурированных данных (Big Data Intelligence). Реализация подобных технических решений должна сопровождаться обязательным судебным

[1] Assistance and Access Act 2018 (официальное название – Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018) – закон об шифровании, принятый в Австралии 6 декабря 2018 года. URL: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (дата обращения: 25.11.2025).

контролем, чтобы соблюсти баланс между обеспечением национальной безопасности и защитой прав и свобод граждан.

5. Повышение квалификации сотрудников – включение в программу подготовки оперативников и следователей курсов по компьютерной криминалистике, OSINT, анонимайзерам и криптографическим протоколам.

В систему профессиональной подготовки оперативных сотрудников и следователей следует включить специализированные курсы по компьютерной криминалистике, методам открытой разведки (OSINT), функционированию анонимайзеров, а также по принципам работы криптографических протоколов. Такой подход обеспечит готовность специалистов к эффективной работе с современными технологиями, включая анализ цифровых следов и выявление скрытой информации.

6. Расширение международного обмена по двусторонним соглашениям – заключение договоров с государствами, где размещены ключевые серверы, для ускоренной легализации цифровых доказательств.

Целесообразно активизировать заключение межгосударственных соглашений с теми странами, где на территории располагаются серверы или дата-центры, имеющие ключевое значение для расследований. Эти договоры должны предусматривать упрощённые и ускоренные процедуры легализации цифровых доказательств, что позволит значительно сократить время их внедрения в процессуальную базу и обеспечить соответствие международным стандартам.

Таким образом, решение организационно-правовых проблем ОРД в сети Интернет возможно только при комплексной модернизации законодательства, технического обеспечения и системы взаимодействия субъектов, с учётом конституционных гарантий права на тайну связи и международных обязательств Российской Федерации.

§2. Рекомендации по повышению эффективности деятельности ОВД при организации решения оперативно-розыскных задач в сети Интернет

В условиях стремительной цифровизации всех сфер общественных отношений, а также глобального проникновения и повсеместного распространения интернет-технологий, формируется объективная необходимость глубокой и системной трансформации организационных, тактических и методологических основ оперативно-розыскной деятельности органов внутренних дел. Такая трансформация должна учитывать специфические характеристики информационной среды сети Интернет, где действуют собственные законы информационного обмена, коммуникации и анонимизации субъектов.

Современная практика выявления, предупреждения и раскрытия противоправных деяний, совершаемых с применением информационно-телекоммуникационных технологий, убедительно подтверждает, что эффективность оперативно-розыскных мероприятий является функцией целого комплекса взаимосвязанных факторов. К их числу относятся уровень технической оснащённости подразделений ОВД, степень профессиональной подготовки и компетентности кадрового состава, полнота и точность нормативно-правовой базы, а также качество механизма межведомственного взаимодействия внутри страны и координации усилий с международными партнёрами.

Решающее значение при этом приобретает способность оперативно комбинировать технические средства мониторинга и анализа цифрового контента, навыки использования специализированного программного обеспечения, а также умение интегрировать результаты межведомственного и межгосударственного обмена данными в единую систему оперативного реагирования. В существующих реалиях оперативно-розыскная деятельность в киберпространстве выступает не как узкоспециализированная сфера, а как

многоуровневый комплекс, объединяющий правовое регулирование, технологические инструменты и человеческий фактор в целях обеспечения национальной безопасности и правопорядка.

В целях повышения эффективности деятельности ОВД по организации решения оперативно-розыскных задач в сети Интернет представляется целесообразным определить и систематизировать ряд специализированных рекомендаций, учитывающих как правовые, так и организационно-технические аспекты функционирования органов внутренних дел.

1. Совершенствование нормативно-правовой базы с учётом динамики интернет-пространства.

Одним из наиболее значимых факторов, определяющих результативность оперативно-розыскной деятельности (ОРД) в информационно-телекоммуникационных сетях, выступает наличие актуальной и детально проработанной нормативно-правовой базы. Поскольку интернет-среда характеризуется непрерывным развитием технологических платформ, изменением архитектуры сетевого взаимодействия, появлением новых сервисов и способов передачи информации, правовое регулирование должно носить не статичный, а адаптивный характер. Иными словами, правовые акты, регламентирующие порядок проведения ОРМ в цифровом пространстве, обязаны своевременно обновляться и отражать новейшие угрозы и технологии.

Особое значение приобретает гармонизация национальных правовых норм с международными договорами и соглашениями, что позволит минимизировать противоречия в правоприменительной практике разных юрисдикций и обеспечит унификацию методологических подходов к сбору, фиксации и последующей оценке цифровых доказательств. Так, интеграция положений Конвенции Совета Европы о киберпреступности (Будапештская конвенция, 2001 г.) в российскую правовую систему создаст правовую основу для совместной работы с иностранными правоохранительными органами, а также позволит

сохранять процессуальную состоятельность доказательственной базы в трансграничных расследованиях.

В целях практической реализации данных задач целесообразно разработать комплекс методических материалов, утверждаемых МВД России, которые определяли бы нормативный порядок применения положений Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в условиях функционирования интернет-инфраструктуры. Указанные рекомендации должны охватывать вопросы:

– Легитимности использования специализированного программного обеспечения для мониторинга сетевого трафика, анализа открытых источников (OSINT), а также проведения перехвата информации при наличии законных оснований.

– Правового режима работы с цифровыми следами и данными, извлеченными из публично доступных ресурсов, в том числе из социальных сетей, блог-платформ, интернет-форумов и каналов в мессенджерах.

– Процедуры взаимодействия с российскими и иностранными операторами связи, включая оперативный обмен данными в рамках действующих межправительственных соглашений и двусторонних протоколов.

– Регламентации использования программно-аппаратных комплексов для сетевого анализа с целью выявления противоправной деятельности в онлайн-сообществах, включая скрытые и зашифрованные каналы коммуникации.

Следует отметить, что действующая редакция Федерального закона № 144-ФЗ по-прежнему содержит ряд лакун в части регулирования специфических особенностей интернет-пространства. В частности, отсутствует детальная процедура мониторинга открытых данных социальных сетей, а также четкие правовые механизмы осуществления законного перехвата сетевого трафика, когда часть информационного обмена происходит за пределами

национальной юрисдикции. Устранение подобных пробелов позволит повысить прозрачность и правовую устойчивость методов работы ОВД, а также предотвратить спорные интерпретации в судебных процессах.

Системная модернизация правовой базы в сочетании с адаптацией к международным стандартам должна рассматриваться как один из ключевых факторов формирования современной модели оперативно-розыскной деятельности в условиях глобальной цифровой среды.

2. Повышение технической оснащённости и внедрение современных аналитических инструментов.

Современное интернет-пространство представляет собой высокодинамичную информационную среду, отличающуюся масштабной трансграничностью и повышенной степенью анонимности коммуникаций. Эти характеристики создают объективные сложности для идентификации участников противоправных действий в цифровой сфере и требуют применения целого комплекса специализированных инструментов, ориентированных на извлечение, обработку и многоуровневую интерпретацию значительных массивов данных.

В условиях постоянного роста объема и разнообразия циркулирующей в сети информации эффективное реагирование возможно лишь при использовании программно-аппаратных решений, сочетающих автоматизированные алгоритмы поиска релевантных данных с технологиями искусственного интеллекта. Такие решения позволяют оперативно выявлять аномальные поведенческие паттерны, признаки целенаправленной деструктивной деятельности, а также формировать доказательственную базу, пригодную к процессуальной эксплуатации в уголовном производстве.

В связи с этим для повышения результативности работы в данной сфере рекомендуется реализовать комплекс следующих мер:

– Создание централизованных информационных хранилищ цифровых инцидентов, обеспеченных возможностями межведомственной интеграции, где

данные будут синхронизироваться с ведомственными базами, что способствует оперативному обмену информацией и формированию целостной картины угроз.

– Внедрение систем обработки и анализа больших данных (Big Data), способных моделировать и выявлять устойчивые закономерности и поведенческие модели, характерные для участников киберпреступных группировок.

– Использование аналитических платформ для отслеживания криптовалютных транзакций, предусматривающих выявление межкошельковых связей, а также установление скрытых цепочек взаимодействия между субъектами, причастными к противоправной деятельности.

– Применение ОСИНТ-технологий (Open Source Intelligence) для масштабного мониторинга открытых источников, извлечения и интерпретации метаданных с изображений, звуковых файлов и аудиовизуальных материалов с целью выявления скрытых элементов идентификации.

Техническая инфраструктура органов внутренних дел должна строиться на основе сертифицированных средств и комплексов, обеспечивающих не только оперативное извлечение информации из различных источников, но и её корректную подготовку для последующего экспертного анализа в рамках судебного разбирательства. Такая комплексная модернизация позволит повысить эффективность противодействия киберугрозам, минимизировать временные затраты на обработку данных и обеспечить высокий уровень достоверности получаемых результатов.

3. Специализированная подготовка и повышение квалификации сотрудников ОВД.

Результативность деятельности ОВД в условиях современной интернет-среды находится в прямой зависимости от глубины и комплексности профессиональных знаний, навыков и компетенций сотрудников, непосредственно задействованных в оперативно-розыскной работе с использованием цифровых технологий. В условиях стремительного прогресса

информационно-коммуникационных систем и сложной трансформации киберугроз особенно актуальным становится целенаправленное совершенствование подготовки кадров.

Одним из приоритетных направлений оптимизации кадрового потенциала следует считать организацию регулярных и структурированных курсов повышения квалификации. Такие программы должны включать углубленное изучение приемов и инструментов OSINT (Open Source Intelligence – разведка по открытым источникам информации), специализированных методик анализа и отслеживания транзакций с применением криптовалют, а также детальную разработку тактических алгоритмов выявления, фиксации и экспертной интерпретации цифровых следов преступной деятельности.

Неотъемлемой составляющей совершенствования компетенций является формирование межведомственных учебно-методических центров нового поколения. Эти структуры должны обеспечивать внедрение актуальных образовательных программ, ориентированных на ключевые тенденции и эволюцию киберпреступности. Особое внимание необходимо уделять изучению технологий социальной инженерии, механизмов фишинга, способов распространения различных видов вредоносного программного обеспечения, а также методов применения сервисов анонимизации для сокрытия криминальных действий в сети.

Комплексная реализация данных мероприятий позволит создать гибкую и адаптивную систему повышения профессионального уровня сотрудников ОВД, способную своевременно реагировать на динамику киберугроз и изменяющуюся криминальную среду, обеспечивая при этом высокую эффективность оперативно-розыскной деятельности в цифровом пространстве.

4. Развитие межведомственного и международного сотрудничества.

В условиях глобализации цифровых коммуникаций и трансграничного характера преступной активности в сети Интернет эффективность оперативно-розыскной деятельности (ОРД) во многом зависит от уровня интеграции

национальных правоохранительных структур в систему международного информационного обмена и совместных действий. Специфика интернет-преступлений заключается в их высокой мобильности, распределённости сетевых инфраструктур и возможности использования удалённых серверов, находящихся за пределами юрисдикции одной страны. Это предопределяет необходимость построения устойчивых каналов взаимодействия, позволяющих оперативно получать, передавать и анализировать сведения о киберугрозах, а также осуществлять координацию мер реагирования.

Ключевым направлением укрепления международного сотрудничества является активная интеграция в деятельность специализированных межгосударственных структур, таких как Интерпол, Европол и другие организации, обладающие компетенцией в области противодействия киберпреступности. В рамках этих платформ возможно не только оперативное распространение информации о новых методах и инструментах преступной деятельности, но и унификация подходов к её предотвращению.

Особую практическую значимость имеет заключение двусторонних и многосторонних международных соглашений, регламентирующих совместное проведение оперативных мероприятий, обмен технологическими решениями, а также согласование процедур получения, верификации и передачи цифровых доказательств в правовом поле различных государств. Такие договорённости позволяют минимизировать временные затраты на реагирование, устранить юридические коллизии и обеспечить допустимость цифровых материалов в судебных процессах.

Международный аспект работы правоохранительных органов приобретает критическую важность в делах, связанных с мошенничеством, транснациональным оборотом наркотических средств и оружия, а также распространением контента, имеющего незаконный характер (включая материалы, нарушающие законодательство в сфере защиты прав человека и детей). Совместная координация усилий и обмен ресурсами создают

предпосылки для формирования единой глобальной системы безопасности, способной эффективно противостоять эволюционирующим угрозам цифрового пространства.

5. Внедрение систем внутреннего аудита и аналитической оценки результативности.

В условиях стремительного развития информационно-телекоммуникационных технологий, а также роста числа правонарушений, совершаемых с их использованием, особую значимость приобретает обеспечение высокого уровня эффективности оперативно-служебной деятельности соответствующих подразделений. Для достижения данной цели необходимо систематическое внедрение продуманных механизмов внутреннего аудита, которые позволяют осуществлять постоянный мониторинг текущих процессов, выявлять скрытые недостатки и оперативно реагировать на возникающие угрозы.

Речь идёт не только о фиксации и документировании выявленных проблемных зон, но и о внедрении структурированных инструментов аналитической обработки данных. Такие инструменты должны обеспечивать формирование развернутых отчётов, содержащих полный спектр количественных и качественных показателей. В частности, представляется целесообразным включать в эти отчёты сведения о фактах обнаруженных угроз информационной безопасности, количестве предотвращённых правонарушений, а также статистические данные, отражающие динамику раскрываемости преступлений, связанных с использованием информационно-телекоммуникационных систем.

Полученные аналитические материалы следует подвергать многоуровневой экспертной оценке, проводимой на уровне руководящего состава соответствующих структурных единиц. На основе выявленных тенденций и закономерностей возможно корректирование стратегических и тактических планов, а также совершенствование применяемых методик

оперативной работы. В конечном счёте, системное использование механизмов внутреннего аудита и аналитической оценки результативности позволяет создать основу для непрерывного повышения качества деятельности в сфере противодействия преступлениям в информационной среде.

6. Формирование культуры цифровой безопасности среди населения.

В современных условиях, когда информационно-телекоммуникационные технологии прочно интегрированы во все сферы общественной и экономической жизни, эффективность деятельности правоохранительных органов в значительной степени определяется уровнем правосознания, общей цифровой грамотности и информационной культуры граждан. Недостаточная осведомлённость населения о потенциальных угрозах в сети Интернет, а также отсутствие навыков безопасного поведения в цифровой среде создают благоприятные условия для реализации противоправных действий со стороны киберпреступников.

Поэтому одной из ключевых задач правоохранительных структур и государственных институтов является разработка и внедрение целостной системы профилактических мероприятий, ориентированных на формирование у граждан устойчивых знаний, практических умений и навыков по обеспечению цифровой безопасности. Такая система должна включать комплекс информационно-разъяснительных программ, охватывающих следующие направления:

– популяризация сведений о наиболее распространённых формах и механизмах интернет-мошенничества;

– обучение простым и доступным методам защиты персональных данных и конфиденциальной информации;

– формирование у населения навыков критического восприятия цифрового контента и способности идентифицировать вероятные признаки противоправной активности в сети.

Важным элементом данной работы является использование разнообразных каналов коммуникации – от традиционных средств массовой информации до социальных сетей, онлайн-платформ и интерактивных обучающих сервисов. Это позволит охватить как молодёжную аудиторию, обладающую высоким уровнем активности в цифровом пространстве, так и менее технологически подготовленные группы населения.

Реализация системных информационно-просветительских и профилактических проектов в области кибербезопасности способствует снижению числа потенциальных жертв преступных посягательств, укреплению доверия граждан к правоохранительным органам, а также повышает эффективность взаимодействия между населением и органами внутренних дел при выявлении, фиксации и передаче сведений о противоправном контенте. Таким образом, формирование культуры цифровой безопасности является стратегическим направлением в обеспечении устойчивой защиты общества от киберугроз и факторов цифрового риска.

Комплексная реализация представленных рекомендаций требует целостного, взаимосвязанного внедрения правовых, организационных и технических механизмов, а также системной подготовки высококвалифицированных специалистов и активного расширения международного партнерства. Такая интеграция предполагает разработку и поэтапное внедрение нормативно-правовых реформ, согласованных с современными тенденциями цифровизации, модернизацию технических средств и инфраструктуры оперативно-розыскной деятельности, а также создание эффективной системы профессиональной подготовки кадров, способных адаптироваться к постоянным изменениям технологической среды.

В условиях стремительного прогресса информационно-коммуникационных технологий ключевым направлением становится не только оперативное реагирование на существующие и потенциальные угрозы, но и их заблаговременное прогнозирование. Это обеспечивает формирование

превентивной составляющей работы органов, осуществляющих оперативно-розыскную деятельность, что позволяет минимизировать риски и повышать уровень цифровой безопасности. Прогностическая аналитика должна базироваться на комплексном мониторинге и сопоставлении данных, с обязательным учетом международных методик и опыта правоохранительных органов иных государств.

Системная реализация указанных мер требует тесного взаимодополнения технических, организационных и нормативно-правовых инструментов, что в совокупности формирует устойчивую и функционально оптимальную основу для повышения эффективности деятельности в рамках противодействия угрозам в сети Интернет. Адаптация органов внутренних дел к динамично трансформирующейся цифровой среде должна носить непрерывный и планомерный характер. Она должна включать регулярное обновление технологических средств, постоянное повышение квалификации сотрудников, активное внедрение результатов научных исследований, а также интеграцию международных стандартов и передовых практик, обеспечивающих унификацию и координацию усилий в глобальном масштабе. Такой подход позволит ОВД действовать проактивно, с максимальным использованием современных технических и аналитических возможностей.

ЗАКЛЮЧЕНИЕ

В ходе проведённого исследования интернет-сети как источника оперативно-розыскной информации были рассмотрены теоретические, правовые, организационные и технические аспекты применения информационно-телекоммуникационных технологий в оперативной деятельности органов внутренних дел. Анализ показал, что глобальная сеть Интернет одновременно является мощнейшей платформой для социально-экономического прогресса и средой повышенного риска, формирующей новые вызовы для обеспечения правопорядка и безопасности.

Развитие интернет-инфраструктуры, её многоуровневая архитектура, распределённый характер и трансграничность информационных потоков создают уникальные условия как для законной деятельности, так и для совершения преступлений, включая кибератаки, мошенничество, незаконный оборот запрещённых товаров, распространение экстремистских материалов и сексуальные преступления с использованием цифровых средств. Анонимизация, шифрование и технологии скрытых сегментов сети (Darknet, Deep Web) существенно затрудняют идентификацию преступников и фиксацию доказательств.

Особое значение в современных условиях приобретает анализ цифровых следов, включающих регистрационные данные, контентные публикации, метаданные, сетевые связи и поведенческие паттерны. Применение методов OSINT (Open Source Intelligence), технологий анализа больших данных, графовых моделей связей и автоматизированных парсеров позволяет выявлять и документировать противоправную активность в онлайн-среде, включая недоступные для открытого поиска сегменты. Рассмотренные примеры из практики подтверждают эффективность таких подходов при раскрытии преступлений различного характера – от мошенничества в платёжных системах до поиска пропавших лиц и противодействия экстремистским группам.

Выдвижение и проверка оперативно-розыскных версий в цифровом пространстве требует адаптации классических алгоритмов ОРД к особенностям интернет-среды. Это подразумевает системно-аналитическую обработку разнородных массивов данных, цифровую атрибуцию объектов, корреляционный анализ информации из разных источников, проведение компьютерно-технических экспертиз и лингвистического анализа коммуникаций. Ключевым условием эффективности таких мероприятий является планирование – стратегическое и тактическое, с учётом динамики появления новых платформ и технологий, а также использование модульной схемы, позволяющей оперативно адаптироваться к изменению обстановки.

Исследование выявило ряд организационно-правовых проблем в обеспечении ОРД в сети Интернет. Среди них – отсутствие унифицированного правового механизма для онлайн-розыска, недостаточная стандартизация взаимодействия с интернет-провайдерами, ведомственная разобщённость баз данных, рост применения средств анонимизации и шифрования, а также размытость границы между публичными и закрытыми цифровыми сведениями. Эти проблемы дополняются техническими вызовами, связанными с необходимостью фильтрации огромных массивов информации и соблюдения баланса между безопасностью и правом на неприкосновенность частной жизни.

Пути решения указанных проблем включают формирование специализированных процедур ОРД в цифровой среде, создание единой межведомственной платформы для обмена данными («Цифровой ОРД»), разработку стандартов взаимодействия с IT-компаниями, инвестиции в технические средства анализа цифрового трафика и повышение квалификации сотрудников. Не менее важным является расширение международного обмена информацией, заключение двусторонних и многосторонних соглашений для оперативной легализации цифровых доказательств.

В числе практических рекомендаций по повышению эффективности деятельности ОВД в сети Интернет выделены:

– актуализация нормативно-правовой базы в соответствии с динамикой интернет-пространства и гармонизация её с международными стандартами;

– внедрение современных аналитических инструментов и комплексных систем мониторинга, объединяющих OSINT, анализ больших данных и автоматизированную обработку криптовалютных транзакций;

– системная подготовка кадров, включающая обучение компьютерной криминалистике, методам анализа цифровых следов и средствам обхода анонимайзеров;

– развитие межведомственного и международного сотрудничества, включая обмен технологиями и согласование процедур передачи цифровых доказательств;

– формирование системы внутреннего аудита и аналитической оценки результативности оперативных мероприятий;

– повышение цифровой грамотности и информационной безопасности населения для профилактики преступлений.

Комплексный подход, объединяющий правовые реформы, техническую модернизацию, подготовку квалифицированных специалистов и расширенное сотрудничество с международными структурами, позволит существенно повысить результативность оперативно-розыскной работы в цифровой среде. При этом необходимо помнить о соблюдении конституционных гарантий права на тайну связи и защиты персональных данных, что требует соразмерности принимаемых мер и прозрачности правовых процедур.

В условиях стремительного развития цифровых технологий и постоянно меняющихся угроз задача органов внутренних дел – не только реагировать на факты противоправной активности, но и обеспечивать прогнозирование и предупреждение преступлений на ранних стадиях. Интернет как источник оперативно-розыскной информации обладает уникальным потенциалом для решения этих задач, однако его использование требует высокой профессиональной подготовки, современного технического оснащения и прочной нормативно-правовой базы.

Проведённое исследование подтверждает, что эффективность ОРД в интернете напрямую зависит от способности правоохранительных органов интегрировать аналитические методики, технологические инструменты и правовые механизмы в единую систему. Такой системный подход позволит обеспечить защиту общества от киберугроз, сохранить стабильность правового порядка и повысить уровень безопасности граждан в цифровую эпоху.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные акты и иные официальные документы

1. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Заключена в г. Будапеште 23.11.2001 г.) (с изм. от 28.01.2003 г.) // СПС «КонсультантПлюс».
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 г.) // Официальный текст Конституции РФ, включающий новые субъекты Российской Федерации - Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации http://pravo.gov.ru, 06.10.2022.
3. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 29.12.2025 г.) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
4. Федеральный закон от 12.08.1995 г. № 144-ФЗ (ред. от 01.04.2025 г.) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. – 14.08.1995. – № 33. – Ст. 3349.
5. Федеральный закон от 07.07.2003 г. № 126-ФЗ (ред. от 31.07.2025 г.) «О связи» // Собрание законодательства РФ. – 14.07.2003. – № 28. – Ст. 2895.
6. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 24.06.2025 г.) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 31.07.2006. – № 31 (1 ч.). – Ст. 3448.
7. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 24.06.2025 г.) «О персональных данных» // Собрание законодательства РФ. – 31.07.2006. – № 31 (1 ч.). – Ст. 3451.
8. Федеральный закон от 07.02.2011 г. № 3-ФЗ (ред. от 15.12.2025 г.) «О полиции» // Собрание законодательства РФ. – 14.02.2011. – № 7. – Ст. 900.

9. Федеральный закон от 06.07.2016 г. № 374-ФЗ (ред. от 29.12.2022 г.) «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. – 11.07.201. – № 28. – Ст. 4558.
10. Федеральный закон от 06.07.2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. – 11.07.2016. – № 28. – Ст. 4559.
11. Федеральный закон от 30.11.2024 г. № 420-ФЗ (ред. от 23.05.2025 г.) «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ. – 02.12.2024. – № 49 (часть IV). – Ст. 7411.
12. Приказ МВД России от 31.03.2023 г. № 199 «Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность» (Зарегистрировано в Минюсте России 17.08.2023 г. № 74840) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 18.08.2023.

II. Монографии, учебники, учебные пособие

1. Авдонина, Т.М. Правоохранительные органы России: учебник / Т.М. Авдонина, Е.Н. Асташкина, Е.В. Богатова [и др.]; под. ред. Е.Н. Асташкиной; Саратовская государственная юридическая академия. – Саратов: Изд-во Сарат. гос. юрид. акад., 2024. – 461 с.
2. Аврутин, Р.Ю. Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России: учебно-практическое пособие /

Р.Ю. Аврутин, О.С. Габова, А.О. Шихалов; Санкт-Петербургский университет МВД России. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. – 156 с.

3. Арутюнян, А.А. Курс уголовного процесса / А.А. Арутюнян, Л.В. Брусницын, О.Л. Васильев и др. под ред. Л.В. Головко. – М.: Статут, 2022. – 964 с.
4. Балашов, Д.Н. Криминалистика: учебник / Д.Н. Балашов, Н.М. Балашов, С.В. Маликов. – М.: ИНФРА-М, 2024. – 449 с.
5. Дубоносов, Е.С. Оперативно-розыскная деятельность: учебник для вузов / Е.С. Дубоносов. – М.: Юрайт, 2025. – 399 с.
6. Иващенко, М.А. Расследование преступлений экстремистской направленности, совершенных с использованием сети Интернет: учебно-методическое пособие / М.А. Иващенко. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – 105 с.
7. Маркушин, А.Г. Оперативно-розыскная деятельность: учебник и практикум для вузов / А.Г. Маркушин. – М.: Юрайт, 2025. – 375 с.
8. Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. – М.: ИНФРА-М, 2025. – 795 с.

III. Статьи, научные публикации

1. Алейников, Д.П. Анализ цифрового контента социальных сетей на предмет выявления оперативно значимой информации / Д.П. Алейников, М Б. Руденко // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года / Под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2020. – С. 40-44.

2. Амирханова, Х.А. Характеристика сети Интернет / Х.А. Амирханова // Интеллектуальный потенциал общества как драйвер инновационного развития науки: Сборник статей Международной научно-практической конференции в 2 частях, Иркутск, 17 января 2023 года. Том Часть 1. – Уфа: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2023. – С. 15-16.
3. Анохов, И.В. Цифровая тень как инструмент для исследования отрасли / И.В. Анохов // E-Management. – 2022. – Т. 5, № 1. – С. 80-92.
4. Анциферова, Э.Ю. Правовой статус сети Интернет / Э.Ю. Анциферова // Ученые записки Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. – 2021. – № 18. – С. 64-68.
5. Бадашин, Д.С. Оперативное сопровождение при расследовании уголовных дел / Д.С. Бадашин // Экономика и социум. – 2020. – № 4(71). – С. 177-183.
6. Гирько, С.И. Некоторые вопросы оперативно-розыскного обеспечения раскрытии и расследовании преступлений / С.И. Гирько, С.В. Харченко // Военное право. – 2024. – № 2(84). – С. 86-91.
7. Гуцко, Е.Г. Характеристики сети интернет, способствующие совершению преступлений / Е.Г. Гуцко // Инновационный потенциал развития юридической науки и практики в современном мире: Сборник научных статей / Редколлегия: С.Е. Чебуранова (гл. ред.) [и др.]. – Гродно: Гродненский государственный университет имени Янки Купалы, 2023. – С. 310-313.
8. Делягин, М.Г. «Цифровой след» личности – новый смысл существования человечества и некоторые следствия этого / М.Г. Делягин // Свободная мысль. – 2021. – № 2 (1686). – С. 5-14.
9. Ермакова, Я.В. Взаимодействие подразделений МВД при расследовании различных категорий преступлений / Я.В. Ермакова // Юридический факт. – 2021. – № 152. – С. 39-41.

10. Калытюк, И.С. Начальные этапы проектирования системы сбора и предиктивного анализа данных социальных медиа / И.С. Калытюк, Г.А. Французова, А.В. Гунько // Системы анализа и обработки данных. – 2021. – № 1(81). – С. 73-84.
11. Кобец, П.Н. Фишинговые атаки как один из самых распространенных видов киберпреступности и меры по противодействию / П.Н. Кобец // Научный портал МВД России. – 2023. – № 1(61). – С. 82-89.
12. Кривонос, А.А. Особенности получения оперативно-розыскной информации в сети интернет / А.А. Кривонос, М.С. Дзырук // Техника и безопасность объектов уголовно-исполнительной системы: Сборник материалов Международной научно-практической конференции. В 4-х томах, Воронеж, 14–15 мая 2025 года. – Воронеж: ИП Копыльцов П.И., 2025. – С. 368-372.
13. Купин, А.Ф. Использование современных программных средств распознавания изображений в правоохранительной деятельности / А.Ф. Купин, О.А. Баринова, В.М. Егорова // Вестник Волгоградской академии МВД России. – 2017. – № 3(42). – С. 105-111.
14. Купин, А.Ф. Организация использования возможностей сети Интернет при раскрытии преступлений / А.Ф. Купин, А.А. Павлова // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): Сборник статей Международной научно-практической конференции, Москва, 18 мая 2018 года. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2018. – С. 142-146.
15. Магомадова, Э.И. Правовое регулирование сети Интернет. Сеть Интернет: ее архитектура / Э.И. Магомадова, М.М. Саркарова // Журнал прикладных исследований. – 2023. – № 7. – С. 103-106.
16. Макаров, А.С. Выявление и документирование с помощью оперативно-розыскной деятельности ОВД преступлений, совершенных с использованием электронного банкинга / А.С. Макаров, Е.В. Кувина //

Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе: материалы всероссийской научно-практической конференции, Казань, 07 июня 2019 года. – Казань: Казанский юридический институт Министерства внутренних дел Российской Федерации, 2019. – С. 131-135.

17. Маслов, С.Н. О некоторых актуальных вопросах интенсификации и модернизации профессиональной подготовки сотрудников органов внутренних дел Российской Федерации с использованием имитационных средств обучения / С.Н. Маслов, Е.С. Бондаренко // Закон и право. – 2025. – № 3. – С. 221-224.
18. Найден, жив! Правовые аспекты поиска пропавших в России // РАПСИ. URL: https://rapsinews.ru/publications/20210611/307135480.html (дата обращения: 25.11.2025).
19. Парфенов, А.В. Некоторые проблемы взаимодействия оперативных подразделений органов, осуществляющих оперативно-розыскную деятельность, по борьбе со взяточничеством, совершаемым с использованием информационно-телекоммуникационных технологий / А.В. Парфенов, Д.М. Фарахиев // Вестник Уральского юридического института МВД России. – 2025. – № 3(47). – С. 138-144.
20. Пинкевич, Т.В. Международная практика применения современных цифровых решений в правоохранительной деятельности / Т.В. Пинкевич // Юристъ-Правоведъ. – 2023. – № 4(107). – С. 180-185.
21. Поздняков, А.Н. Интернет и его функции в виртуальном пространстве: оперативно-розыскной аспект / А.Н. Поздняков // Академическая мысль. – 2024. – № 4 (29). – С. 47-52.
22. Родивилина, В.А. Проблемы противодействия использованию анонимности в сети Интернет в преступных целях / В.А. Родивилина, И.П. Родивилин, В.В. Коломинов // Криминалистика: вчера, сегодня, завтра. – 2021. – № 4(20). – С. 68-76.

23. Сарычев, М.М. Особенности выявления и фиксации цифровых следов преступлений в рамках ОРД / М.М. Сарычев // Научные исследования XXI века. – 2024. – № 2(28). – С. 146-150.
24. Сервис по предоставлению выделенных серверов. URL: https://www.whois-service.ru (дата обращения: 25.11.2025).
25. Сколько пользователей интернета в мире? (2025) // ИНКЛИЕНТ. URL: https://inclient.ru/users-internet-stats/ (дата обращения: 25.11.25025).
26. Филатова, В.А. Особенности получения оперативно-розыскной информации в сети интернет / В.А. Филатова // Вопросы деятельности служб и подразделений органов внутренних дел Российской Федерации: Сборник статей вузовской научно-практической конференции, Тверь, 07 апреля 2021 года. Том Выпуск 2. – Тверь: Тверской государственный университет, 2021. – С. 182-184.
27. Хатунцев, Н.А. Судебная компьютерно-техническая экспертиза в свете цифровизации общества / Н.А. Хатунцев // Эксперт-криминалист. – 2020. – № 2. – С. 18-20.
28. Ховавко, С.М. Влияние фактора цифровизации на оперативно-розыскную деятельность органов внутренних дел / С.М. Ховавко // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2023. – Т. 9 (75). № 4. – С. 283-286.
29. Шаров, В.И. «Цифровая оперативно-розыскная деятельность» и цифровизация противодействия преступлениям / В.И. Шаров // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 3(107). – С. 171-178.

IV. Эмпирические материалы

1. Постановление Конституционного Суда РФ от 17.10.2017 г. № 24-П «По делу о проверке конституционности пункта 5 части четвертой статьи 392 Гражданского процессуального кодекса Российской Федерации в связи с

жалобами граждан Д.А. Абрамова, В.А. Ветлугаева и других» // Вестник Конституционного Суда РФ. – № 6. – 2017.

2. Апелляционное определение Санкт-Петербургского городского суда от 28.11.2017 г. № 33-23595/2017 по делу № 2-4865/2017 // СПС «КонсультантПлюс».
3. Материалы производственной (преддипломной) практики слушателя КЮИ МВД России Зайцева М.В. (место практики: отдел ОУР ОМВД России «Завьяловский», сроки прохождения практики: с 27.05.2025 г. по 21.07.2025 г.).
4. Приговор Иволгинского районного суда (Республика Бурятия) № 1-37/2020 1-466/2019 от 05.02.2020 г. по делу № 1-37/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/sn2BltwAV8H8/ (дата обращения: 25.11.2025).
5. Приговор Ухтинского городского суда (Республика Коми) № 1-283/2020 от 14.07.2020 г. по делу № 1-283/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Ppfg23ryMwHT/ (дата обращения: 25.11.2025).
6. Приговор Центрального районного суда г. Читы (Забайкальский край) № 1-1223/2019 1-43/2020 от 26.07.2020 г. по делу № 1-1223/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/pQ3MyHNrVIZp/ (дата обращения: 25.11.2025).
7. Приговор Пролетарского районного суда г. Ростова-на-Дону (Ростовская область) № 1-272/2023 от 16.08.2023 г. по делу № 1-272/2023 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/0zHE4yQknvoN/ (дата обращения: 25.11.2025).
8. Приговор Раменского городского суда (Московская область) № 1-216/2025 от 28.04.2025 г. по делу № 1-216/2025 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/ynmMtPjjPq6l/ (дата обращения: 25.11.2025).

9. Состояние преступности в Российской Федерации за январь-декабрь 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 25.11.2025).
10. Состояние преступности в Российской Федерации за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 25.11.2025).
11. Состояние преступности в Российской Федерации за январь-август 2025 года // МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/70644759/ (дата обращения: 25.11.2025).

IV. Ресурсы сети Интернет

1. Судебная статистика. Судебный департамент при Верховном суде. URL: https://cdep.ru/index.php?id=5 (дата обращения: 25.11.2025).
2. Атаки на портал госуслуг // TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%90%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB_%D0%B3%D0%BE%D1%81%D1%83%D1%81%D0%BB%D1%83%D0%B3 (дата обращения: 25.11.2025).
3. Amazon Rekognition. URL: ttps://aws.amazon.com/ru/rekognition/ (дата обращения: 25.11.2025).
4. Assistance and Access Act 2018 (официальное название – Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018) – закон об шифровании, принятый в Австралии 6 декабря 2018 года. URL: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (дата обращения: 25.11.2025).

5. Deep web, dark web, darknet и surface web – в чем разница? // Kaspersky daily. URL: https://blog.kaspersky.kz/deep-web-dark-web-darknet-surface-web-difference/23507/ (дата обращения: 25.11.2025).
6. Farfade S.S., Saberian M., Li L.-J. Multi-view Face Detection Using Deep Convolutional Neural Networks. URL: https://arxiv.org/pdf/1502.02766.pdf (дата обращения: 25.11.2025).
7. MIT Technology Review. URL: https://www.technologyreview.com (дата обращения: 25.11.2025).
8. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering. URL: https://arxiv.org/pdf/1503.03832.pdf (дата обращения: 25.11.2025).