Владимир Юрьевич ЖАНДРОВ,
кандидат юридических наук, доцент
Московский университет МВД России имени В.Я. Кикотя (г. Москва)
доцент кафедры оперативно-разыскной деятельности и специальной техники
vaisvladimir74@gmail.com

Научная статья
УДК 343.102:[343.14:004]

ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ЦИФРОВОГО ОПЕРАТИВНОГО ПОИСКА

КЛЮЧЕВЫЕ СЛОВА. Оперативно-разыскная деятельность, оперативно-разыскное мероприятие, оперативный поиск, киберпреступность, цифровизация, цифровой след.

АННОТАЦИЯ. ***Введение***. *Цифровизация общественных отношений и массовый переход преступности в информационно-телекоммуникационную среду требуют пересмотра традиционных подходов к оперативно-разыскной деятельности. Оперативный поиск как инициативный метод выявления преступлений в новых технологических условиях сталкивается с отсутствием в российском законодательстве правового основания для его осуществления. Буквальное толкование закона фактически лишает оперативно-разыскную деятельность наступательности, сводя использование ее потенциала к ситуациям, когда признаки преступления уже проявились. Это особенно негативно сказывается на выявлении латентных киберпреступлений.* ***Методы***. *Проведение исследования опиралось на системно-структурный подход, позволивший сконструировать многоуровневую модель реализации цифрового оперативного поиска. Востребованным оказался сравнительно-правовой метод. Применены методы OSINT-аналитики, Data Mining, социально-сетевого, экономического и структурного анализа цифровых следов. Были также задействованы формально-юридический метод и метод моделирования оперативно-разыскных процессов.* ***Результаты***. *Обоснована необходимость закрепления в российском законодательстве отдельного основания для инициативного цифрового поиска с использованием возможностей OSINT-аналитики, фиксации цифровых следов и теней. В противном случае нарастают риски признания в уголовном процессе собранных цифровых данных недопустимыми доказательствами. Разработана пятиуровневая модель цифрового оперативного поиска. В ней объединены в единую методическую схему объектово-установочный, информационно-накопительный, верифицирующе-проверочный, аналитический и процессуально-интегративный уровни. Предложено реализовать меры по созданию межведомственного цифрового пространства, подготовке специалистов по OSINT-аналитике и цифровой криминалистике, совершенствованию ведомственных регламентов и стандартов документирования.*

ВВЕДЕНИЕ

Цифровизация и связанные с ней процессы перемещения криминальной активности в информационно-телекоммуникационную среду требуют обновления сложившихся в оперативно-разыскной деятельности (далее – ОРД) подходов к выявлению и документированию преступлений. В первую очередь это касается оперативного поиска – метода ОРД, традиционно занимающего в деятельности оперативных подразделений органов внутренних дел (далее – ОВД) значимое место и не теряющего своей актуальности в новых технологических условиях.

Осуществление оперативного поиска в цифровой среде (иначе – цифрового оперативного поиска) напрямую зависит от организационно-правового обеспечения. Речь идет прежде всего о правовом основании его проведения, а также использовании специальных приемов, способов и средств субъектами ОРД на всех этапах осуществления поискового процесса – от выявления до реализации оперативно значимой информации.

Основания проведения оперативно-разыскных мероприятий (далее – ОРМ) закреплены в ст. 7 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Федеральный закон «Об ОРД»). Однако такие инструменты, как OSINT-разведка[1] и фиксация цифровых следов, пока не имеют нормативно-правовой опоры. Представляется, что решение данной

[1] OSINT-разведка (OSINT-аналитика) – это сбор, анализ и систематизация данных из общедоступных источников (OSINT – от англ. Open Source Intelligence).

Vladimir Y. ZHANDROV,
Cand. Sci. (Jurisprudence), Associate Professor
Moscow University of the Ministry of the Interior
of Russia named after V.Ya. Kikot (Moscow, Russia)
Associate Professor of the Department of Operational
Investigative Activities and Special Equipment
vaisvladimir74@gmail.com

LEGAL AND ORGANIZATIONAL SUPPORT FOR THE IMPLEMENTATION OF DIGITAL OPERATIONAL SEARCH

KEYWORDS. Operational investigative activities, operational investigative measures, operational search, cybercrime, digitalization, digital footprint.

ANNOTATION. ***Introduction***. *The digitalization of social relations and the widespread migration of crime to the information and telecommunications environment require a revision of traditional approaches to operational investigative activities. Operational search, as a proactive method for detecting crimes in the new technological environment, faces the lack of a legal basis for its implementation in Russian legislation. A literal interpretation of the law effectively deprives operational investigative activities of their offensive potential, limiting their use to situations where the elements of a crime have already manifested themselves. This has a particularly negative impact on the detection of latent cybercrimes.* ***Methods***. *The study relied on a systems-structural approach, which made it possible to construct a multi-level model for implementing digital operational search. A comparative legal method proved to be in demand. Methods of OSINT analytics, data mining, social network, economic, and structural analysis of digital traces were applied. A formal legal method and a method for modeling operational investigative processes were also employed.* ***Results***. *The need to establish in Russian legislation a separate basis for proactive digital searches using OSINT capabilities and the recording of digital traces and shadows is substantiated. Otherwise, the risk of collected digital data being deemed inadmissible as evidence in criminal proceedings increases. A five-level model of digital operational search has been developed. It combines the object-identification, information-cumulative, verification-checking, analytical, and procedural-integrative levels into a single methodological framework. Measures are proposed to create an interdepartmental digital space, train specialists in OSINT intelligence and digital forensics, and improve departmental regulations and documentation standards.*

проблемы лежит в сфере совершенствования регулирования инициативности ОРД.

Перед исследованием, результаты которого представлены в статье, были поставлены цели обосновать необходимость формирования правовой и организационной базы для реализации ОВД цифрового оперативного поиска, а также разработать такую его модель, которая обеспечивала бы сохранность цифровых доказательств и их интеграцию в уголовный процесс.

МЕТОДЫ

Системно-структурный подход позволил сконструировать целостную пятиуровневую модель цифрового оперативного поиска, где каждый уровень логически связан с последующим. Сравнительно-правовой метод был использован для анализа законодательства России, Беларуси, Кыргызстана и директив ЕС с целью выявления оптимальных правовых решений для нормативного закрепления инициативного цифрового поиска как инструмента ОРД. Методы OSINT-аналитики и Data Mining применены для описания технологических приемов сбора, обработки и выявления скрытых закономерностей в больших массивах цифровых данных открытых источников. Социально-сетевой анализ был направлен на реконструкцию структуры онлайн-сообществ, деанонимизацию участников и выявление ролей в преступных группах. Экономический анализ оказался полезен для изучения финансовых потоков, схем воспроизводства преступной деятельности и идентификации ресурсной базы. С помощью структурного анализа исследована инфраструктура цифровой среды функционирования преступных объектов (серверы, платформы, сети) и определены ее уязвимые элементы. Формально-юридический метод обеспечил толкование норм Федерального закона «Об ОРД» и выявление правовых пробелов в регулировании инициативного поиска. Метод моделирования оперативно-разыскных процессов предоставил возможность построить алгоритм действий оперативных подразделений при выявлении, фиксации, верификации и правовой интеграции цифровых следов.

РЕЗУЛЬТАТЫ

Буквальное толкование ст. 7 Федерального закона «Об ОРД», как отмечают Е.В. Кузнецов и А.Е. Ступницкий, фактически лишает ОРД ее ключевых черт – инициативности и наступательности, сводя проведение мероприятий к ситуациям, когда признаки преступления уже проявились [1, с. 46]. В связи с этим оперативный поиск теряет разведывательно-поисковый потенциал, что особенно негативно отражается на процессах, направленных на выявление и раскрытие латентных деяний, например преступлений в сфере незаконного оборота наркотиков.

Аналогичные выводы сделаны и белорусским исследователем И.И. Шишковцом, отметившим, что эффективность оперативного поиска существенно ограничена отсутствием в национальном законодательстве специального правового основания для его проведения. Им было предложено закрепить в Законе Республики Беларусь от 15 ию-

ля 2015 г. № 307-З «Об оперативно-розыскной деятельности» в качестве такого основания необходимость обнаружения признаков латентных преступлений и лиц, к ним причастных [2, с. 82].

Показателен в данном случае законодательный опыт Кыргызской Республики. Здесь в Законе от 26 июня 2025 г. № 127 «Об оперативно-розыскной деятельности» закреплено такое самостоятельное ОРМ, как «оперативный поиск в информационных сетях и сети Интернет» (п. 6 ст. 2). Законодатель относит его к числу мер, не ограничивающих конституционные права граждан, в то время как действия, в большей степени ограничивающие эти права, – снятие информации с компьютерных систем, перехват телекоммуникаций и скрытое наблюдение – выведены в блок специальных мероприятий. Таким образом, кыргызский закон устанавливает нормативное разграничение между инициативной стадией ОРД, предусматривающей лишь меры с минимальным уровнем вмешательства, и мероприятиями, требующими особой процессуальной процедуры. Важно и то, что результаты сетевого поиска могут служить основанием для досудебного производства и использоваться в доказывании, если они соответствующим образом запротоколированы.

Идеи о необходимости законодательного закрепления отдельного правового основания для инициативного поиска, закрепляющего возможность осуществления ограниченного круга ОРМ (опрос, наведение справок, сбор образцов для сравнительного исследования, исследование предметов и документов, наблюдение), во многом близки подходу, реализуемому в Европейском союзе. Здесь допускается применение превентивных форм расследования (англ. – proactive investigation), предполагающих ограниченный мониторинг, сбор метаданных и скрытое наблюдение еще до выявления прямых признаков преступления. Нормативной основой выступает Директива (ЕС) 2016/680, в ст. 1(1) которой говорится о том, что обработка персональных данных компетентными органами разрешена не только для выявления и расследования преступлений, но и для их предупреждения (prevention)[1].

В отсутствие непосредственного правового основания цифрового оперативного поиска в российском законодательстве риски признания собранных таким образом данных недопустимыми в уголовном процессе значительно возрастают. До тех пор, пока законодатель не урегулирует этот вопрос, работа с цифровой оперативной информацией должна сопровождаться усиленными мерами по подтверждению ее достоверности.

В целях формирования актуальной модели поискового метода исследуемого нами вида был применен системно-структурный подход. Он позволил сконструировать модель так, чтобы она полностью соответствовала современным условиям цифровизации. Предлагаемая концепция цифрового оперативного поиска опирается на многоуровневую модель, где каждый уровень формирует основу для следующего и может быть воспроизведен в повторных циклах.

На первом (**объектово-установочном**) уровне структурная модель охватывает формулировку задачи поиска и определение источников цифровых следов и теней. Именно на нем закладывается фундамент для последующего анализа и обеспечивается непрерывность поискового процесса [3, с. 60]. Специальная цель первоначального этапа поиска – своевременное обнаружение признаков преступлений и причастных к ним лиц на ранних стадиях в рамках работы с неопределенным кругом объектов. Достижение указанной цели обеспечивается последовательным решением двух задач.

Первая – определение признаков, которые необходимо заложить в поисковую матрицу. В ходе этой деятельности уточняются объекты оперативного интереса и цифровые маркеры, выдвигаются рабочие гипотезы. Основным условием успешного решения поставленной задачи является минимизация так называемого «пузыря фильтров» [4, с. 173], прежде всего с помощью применения неперсонализированных запросов и специальных приемов обхода профилирования. Такая тактика снижает риск искажения информации и обеспечивает ее репрезентативность.

Вторая задача – выбор среды и источников информации. Это могут быть открытые сайты, закрытые разделы и базы данных, даркнет, распределенные сети или устройства интернета вещей [5, с. 211]. Как правило, проводимая на этом этапе работа связана с многоуровневым доступом к различным сегментам цифровой среды, поэтому поиск целесообразно строить по принципу постепенного продвижения от открытых источников (Surface Web) к менее доступным (Deep Web) и далее к скрытым и анонимным сетям (DarkNet, P2P-платформы). Такой маршрут позволяет постепенно расширять поле поиска и выявлять скрытые массивы информации.

Второй (**информационно-накопительный**) уровень поиска предусматривает извлечение и первичную фиксацию обнаруженной информации. Это не только сам сбор сведений, например визуальным способом, но и обязательное документирование условий их получения (время, обстоятельства доступа, технические параметры среды, контрольные хэши файлов). Надежность цифровых доказательств обеспечивается соблюдением совокупности требований, каждое из которых направлено на подтверждение их подлинности, сохранности и возможности независимой проверки [6, с. 76].

Одним из ключевых является требование *двойной фиксации*. Информация подлежит сохранению не менее чем двумя независимыми способами – в виде визуальной копии (например скриншота) и исходного файла, дополнительно подвергаемого хэшированию. Такой подход предоставляет возможность надежной проверки неизменности дан-

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and on the free movement of such data. EUR-Lex // URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj (дата обращения: 25.11.2025).

ных и существенно снижает риск их несанкционированной модификации.

Неотъемлемой составляющей фиксации цифровых следов выступает *маркировка источника*. В обязательном порядке документируются условия формирования следа: уровень среды (Surface, Deep, Dark, IoT), параметры доступа (используемый браузер, клиентское приложение, подключение через TOR/I2P-сети), IP-адрес, а также точные дата и время взаимодействия. Подобная детализация приобретает особую значимость в делах, связанных с организованной преступностью, где сторона защиты нередко ссылается на вероятность искажения или фальсификации доказательственной базы.

Отдельного внимания требует порядок *хранения верифицирующих метаданных*. Заголовки электронных писем, EXIF-информация, сетевые журналы и иные сведения технического характера должны фиксироваться и храниться отдельно от основного содержимого. Это позволяет обеспечить условия для их независимой проверки и экспертной атрибуции, повышая достоверность представленных цифровых объектов.

Третий (**верифицирующе-проверочный**) уровень охватывает меры, направленные на кросс-источниковую проверку достоверности извлеченной цифровой информации. Все значимые сведения должны быть сопоставлены с независимыми источниками, такими как альтернативные поисковые системы, журналы операторов связи, биллинговые данные [7, с. 26]. Сравнение сведений, полученных из разных источников, снижает вероятность ложных совпадений, позволяет исключить ошибки и способствует формированию более точного атрибутивного профиля цифрового следа.

Развитие организационно-правовой составляющей цифрового оперативного поиска невозможно без совершенствования ведомственных информационных систем, объединяющих внешние источники (OSINT, Deep Web, цифровые тени) с государственными централизованными регистрами. К числу ключевых технологических решений, используемых МВД России, относятся автоматизированные комплексы «Розыск-магистраль», «Папилон», «Безопасный город», «Паутина» и др., а также централизованные базы учета, содержащие данные о лицах, событиях и объектах, представляющих оперативный интерес [8, с. 27]. Эти ресурсы формируют массивы данных, доступ к которым возможен исключительно в соответствии с требованиями нормативных актов и на основании ведомственных инструкций.

Четвертый (**аналитический**) уровень поисковой работы включает в себя обработку собранной и зафиксированной надлежащим образом цифровой информации. Задача оперативно-аналитического этапа заключается в объединении инициативного сбора цифровых следов и теней с их аналитической обработкой, что позволяет превратить разрозненные сведения в целостную картину преступной активности и разработать систематизированные версии. Как отмечает Я.М. Мазунин, специфика оперативно-аналитического поиска состоит в сочетании оперативного и аналитического компонентов, что позволяет систематизировать полученные сведения и использовать их для решения тактических и стратегических задач [9, с. 8].

Методологическое ядро аналитического уровня формируется вокруг трех основных составляющих:

1) полноты информации, обеспечиваемой включением в аналитическую базу даже «второстепенных» сигналов и документов. Важен итеративный цикл «поиск → анализ → уточненный поиск», который позволяет последовательно конкретизировать гипотезы и повышать точность выводов. Такой контур демонстрирует внутреннюю согласованность цифрового оперативного поиска с классической логикой оперативного поиска («построение по признакам → проверка → редукция гипотез») и одновременно отражает его технологическую современность;

2) применения разных видов анализа:

- экономического (направлен на изучение финансовых потоков, схем воспроизводства преступной деятельности, идентификацию новых ее участников, позволяет выявить скрытую ресурсную базу криминальных формирований и увязать ее с организационной структурой);

- структурного (исследуется инфраструктура объектов оперативного интереса, а именно цифровая среда, в которой функционируют участники преступной деятельности; данный метод позволяет выяснить, как организована цифровая система преступной деятельности, определить ее уязвимые элементы и спрогнозировать возможные изменения);

- социально-сетевого (позволяет реконструировать структуру онлайн-сообществ, выявить распределение ролей внутри них, выделить ключевых участников, скрытые группы и связи между ними; задачей такого анализа становится деанонимизация цифровых субъектов);

3) систематизации данных (их упорядочение для решения тактических и стратегических задач). Систематизация любых доступных данных – от формальных документов до косвенных фактов – позволяет формировать целостные информационно-поисковые модели. Она предполагает не только техническое упорядочение цифровых следов, но и их правовое структурирование с учетом возможностей дальнейшего использования в процессуальной сфере. Особое значение здесь приобретают методы, позволяющие привести разнородные сведения – от OSINT-фрагментов до логфайлов и метаданных операторов связи – к единой аналитической форме.

Криминалистическая экспертиза как метод выявления закономерностей и аномалий в вещественных доказательствах получает в цифровой среде эквивалент в виде аналитики Big Data и Data Mining. Их преимущество заключается в задействовании алгоритмов искусственного интеллекта, способных обрабатывать колоссальные объемы информации, обнаруживать скрытые связи и строить статистические модели. Как подчеркивает В.И. Шаров, именно использование Big Data и Data Mining может вывести оперативный поиск на качественно новый уровень, оно позволяет выхо-

дить за пределы статистических сводок и производить идентификацию преступлений, лиц и их связей [10, с. 412]. Эффективность таких процедур напрямую зависит от корректности предварительной фиксации данных и сохранения их необработанного вида, что гарантирует возможность независимой проверки результатов.

И наконец, пятый (**процессуально-интегративный**) уровень обеспечивает соответствие поисковых процедур требованиям законодательства, документирование результатов и их интеграцию в процессуальную сферу уголовного судопроизводства [11, с. 13]. Его результативность определяется степенью минимизации возможных правовых рисков. Всего можно выделить три основных вида таких рисков.

Первый их вид связан с угрозой выхода за пределы допускаемого законом доступа к цифровым данным и нарушения режима конфиденциальности. Применение OSINT-разведки связано с риском необоснованного вторжения в частную жизнь. Даже если цифровые следы формально находятся в открытом доступе (например видеозаписи с камер наблюдения или данные от IoT-устройств), они могут содержать персональную информацию, защищаемую ст. 23 Конституции Российской Федерации и ст. 137 УК РФ. Ее использование без должных правовых оснований может привести к чрезмерному вмешательству в цифровую сферу жизнедеятельности граждан, признанию доказательств недопустимыми и подрыву доверия к оперативно-разыскной деятельности в целом [12, с. 216].

Второй вид рисков связан с несоблюдением порядка сбора и фиксации цифровой информации. Доказательственный аспект цифрового оперативного поиска имеет особое значение – цифровые следы и тени могут быть использованы в уголовном судопроизводстве только при условии их надлежащей аутентификации и фиксации в соответствии с процессуальными требованиями. Результативность поиска рассматриваемого вида определяется не только тем, насколько качественно производится извлечение и анализ информации, но и возможностью ее последующего использования в суде [13, с. 160].

Третий вид рисков связан с несоблюдением порядка легализации в национальном правовом поле цифровых данных, полученных в условиях трансграничного доступа. Вопрос международного перемещения такой информации приобретает особую важность именно в контексте цифрового оперативного поиска [14, с. 62]. Значительная часть серверов, облачных хранилищ и социальных сетей, где формируются ключевые цифровые следы, находится за пределами юрисдикции России. Это создает трудности в получении допустимых с точки зрения уголовного процесса доказательств и требует углубления международного сотрудничества [15, с. 123].

Таким образом, оперативный поиск в цифровой среде формируется в качестве пятиуровневой модели, в которой выявление источников цифровых данных, их инициативный сбор, верификация, последующая аналитическая обработка и правовая интеграция образуют единую методическую схему.

ЗАКЛЮЧЕНИЕ

Цифровому оперативному поиску необходима институализация в российском правовом поле и практике ОРД, что предполагает принятие ряда правовых и организационных мер.

1. На законодательном уровне должно быть закреплено отдельное основание для проведения оперативно-разыскных мероприятий, ориентированных на инициативный цифровой поиск. Это позволит узаконить работу с информацией, полученной в рамках OSINT-разведки и фиксации цифровых теней, снизить вероятность признания ее недопустимой в качестве доказательства и выстроить деятельность оперативных подразделений с учетом современных технологических реалий.

Для эффективного осуществления цифрового оперативного поиска требуется разработать и внедрить комплекс регламентов и стандартов. Прежде всего нужны ведомственные регламенты, которые будут закреплять порядок сбора и фиксации цифровых следов и теней, а также устанавливать минимальные требования к протоколам действий оперативных служб. Кроме того, следует подготовить стандарты документирования, которые должны предусматривать обязательное описание среды, в которой были получены цифровые данные, параметров метаданных, условий доступа и технических характеристик сеанса, а также использования контрольных хэш-сумм. Это обеспечит возможность повторного получения результатов и уменьшит риск их оспаривания в суде. Наконец, необходимы инструкции по взаимодействию с зарубежными сервисами и вопросам трансграничного обмена данными. Речь о том, что возникают сложности с допустимостью в качестве доказательства информации, которая хранится на серверах за пределами юрисдикции России. Унификация правил доступа к таким данным и их фиксации будет способствовать их включению в судебные процессы.

2. Важно наладить организационное обеспечение реализации цифрового оперативного поиска. Достижение этой цели возможно посредством создания устойчивых организационных структур, прежде всего за счет развития межведомственного взаимодействия, стандартизации обработки данных и подготовки специалистов с нужными цифровыми навыками.

Первым шагом на этом пути может стать повышение эффективности межведомственного сотрудничества. Это предполагает создание общего цифрового пространства, в котором оперативно значимая информация передается по согласованным правилам и в соответствии со стандартами безопасности. Расширение источников данных – от баз МВД России, ФСБ и Росфинмониторинга до региональных и муниципальных систем – позволит более точно анализировать ситуацию даже при высокой скрытности правонарушений.

Второй шаг – развитие профессиональных навыков реализующих цифровой оперативный поиск субъектов. Современные специалисты этой сферы должны обладать аналитическим мышлением и цифровой грамотностью: уметь работать

с большими данными, пользоваться инструментами OSINT-аналитики, фиксировать и подтверждать цифровые следы, разбираться в кибербезопасности и защите персональной информации. Для подготовки таких кадров необходимо внедрять в программы учебных заведений правоохранительных органов и государственных финансовых структур образовательные модули по тематике киберразведки, цифровой криминалистики, анализа сетевых структур и мониторинга блокчейна.

Повышение качества подготовки кадров и развитие межведомственного взаимодействия – основа для реализации цифрового оперативного поиска. Квалифицированные специалисты и единая система обмена информацией позволят достичь баланса между эффективностью оперативных действий и соблюдением правовых норм. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузнецов Е.В., Ступницкий А.Е. Основания для проведения оперативно-разыскных мероприятий: проблемы инициативности оперативного поиска // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2016. № 16-1. С. 46-47.

2. Шишковец И.И. О понятии, содержании и правовых основаниях оперативного поиска как целостной системы // Вестник Академии МВД Республики Беларусь. 2021. № 1 (41). С. 78-83.

3. Герасимов А.В., Поляков А.В. К вопросу информационного воздействия на объекты оперативной заинтересованности // X Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2022. С. 60-61.

4. Карпика А.Г. Актуальные вопросы поиска и анализа цифровых следов в оперативно-розыскной деятельности // Юристъ-Правоведъ. 2019. № 3 (90). С. 171-179.

5. Поляков А.В., Гринева Д.А. О возможностях использования информационных технологий в решении задач оперативно-розыскной деятельности // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 211-215.

6. Алексеева А.П. Киберпреступность: насколько реальна угроза // Научно-методический электронный журнал «Концепт». 2017. № Т31. С. 76-80.

7. Глубоковских Р.В., Гринева Д.А. Характеристика оперативно-розыскного инструментария при раскрытии хищения денежных средств с банковских счетов // XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2025. С. 25-27.

8. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.

9. Мазунин Я.М. Оперативно-аналитический поиск как направление борьбы с преступностью, связанной с незаконным оборотом наркотиков // Оперативно-розыскное противодействие наркопреступности: Материалы всероссийского научно-практического семинара. Ч. 1. Красноярск: Сибирский ЮИ МВД России, 2023. С. 7-10.

10. Шаров В.И. Поиск и анализ оперативно-розыскной информации в интернете // Юридическая техника. 2024. № 18. С. 411-416.

11. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы // Уголовное законодательство: вчера, сегодня, завтра: Материалы международной научно-практической конференции. СПб: СПбУ МВД России, 2024. С. 13-15.

12. Попов С.В. К вопросу об особенностях обнаружения признаков мошеннических действий в сети Интернет // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 216-219.

13. Желудков М.А., Алексеева А.П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. 2025. № 2 (106). С. 159-169.

14. Попов С.В. О некоторых вопросах развития оперативно-розыскной науки // XI Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2023. С. 62-63.

15. Катков С.В., Семененко Г.М., Костенко Н.С., Алексеева А.П. О мерах совершенствования организации работы оперативных и следственных подразделений МВД России по выявлению, раскрытию и расследованию хищений денежных средств с использованием банковских карт на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 123-128.

REFERENCES

1. Kuznetsov Ye.V., Stupnitskiy A.Ye. Osnovaniya dlya provedeniya operativno-razysknykh meropriyatiy: problemy initsiativnosti operativnogo poiska // Aktual'nyye problemy bor'by s prestupleniyami i inymi pravonarusheniyami. 2016. № 16-1. S. 46-47.

2. Shishkovets I.I. O ponyatii, soderzhanii i pravovykh osnovaniyakh operativnogo poiska kak tselostnoy sistemy // Vestnik Akademii MVD Respubliki Belarus'. 2021. № 1 (41). S. 78-83.

3. Gerasimov A.V., Polyakov A.V. K voprosu informatsionnogo vozdeystviya na ob"yekty operativnoy zainteresovannosti // X Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2022. S. 60-61.

4. Karpika A.G. Aktual'nyye voprosy poiska i analiza tsifrovykh sledov v operativno-rozysknoy deyatel'nosti // Yurist"-Pravoved". 2019. № 3 (90). S. 171-179.

5. Polyakov A.V., Grineva D.A. O vozmozhnostyakh ispol'zovaniya infor-matsionnykh tekhnologiy v reshenii zadach operativno-rozysknoy deyatel'nosti // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 211-215.

6. Alekseyeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». 2017. № T31. S. 76-80.

7. Glubokovskikh R.V., Grineva D.A. Kharakteristika operativno-rozysknogo instrumentariya pri raskrytii khishcheniya denezhnykh sredstv s bankovskikh schetov // XIII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2025. S. 25-27.

8. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.

9. Mazunin Ya.M. Operativno-analiticheskiy poisk kak napravleniye bor'by s prestupnost'yu, svyazannoy s nezakonnym oborotom narkotikov // Operativno-rozysknoye protivodeystviye narkoprestupnosti: Materialy vserossiyskogo nauchno-prakticheskogo seminara. Ch. 1. Krasnoyarsk: Sibirskiy YUI MVD Rossii, 2023. S. 7-10.

10. Sharov V.I. Poisk i analiz operativno-rozysknoy informatsii v internete // Yuridicheskaya tekhnika. 2024. № 18. S. 411-416.

11. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v sfere ustanovleniya ugolovnoy otvetstvennosti za nezakonnyye ispol'zovaniye i peredachu, sbor i khraneniye komp'yuternoy informatsii, soderzhashchey personal'nyye dannyye: problemy i perspektivy // Ugolovnoye zakonodatel'stvo: vchera, segodnya, zavtra: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2024. S. 13-15.

12. Popov S.V. K voprosu ob osobennostyakh obnaruzheniya priznakov moshennicheskikh deystviy v seti Internet // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 216-219.

13. Zheludkov M.A., Alekseyeva A.P. Obespecheniye zashchishchennosti biometricheskikh personal'nykh dannykh ot ispol'zovaniya v kriminal'nykh tselyakh // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2025. № 2 (106). S. 159-169.

14. Popov S.V. O nekotorykh voprosakh razvitiya operativno-rozysknoy nauki // XI Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2023. S. 62-63.

15. Katkov S.V., Semenenko G.M., Kostenko N.S., Alekseyeva A.P. O merakh sovershenstvovaniya organizatsii raboty operativnykh i sledstvennykh podrazdeleniy MVD Rossii po vyyavleniyu, raskrytiyu i rassledovaniyu khishcheniy denezhnykh sredstv s ispol'zovaniyem bankovskikh kart na territorii Rossiyskoy Federatsii // Vestnik Volgogradskoy akademii MVD Rossii. 2020. № 4 (55). S. 123-128.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Жандров В.Ю. Правовое и организационное обеспечение реализации цифрового оперативного поиска // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2026. № 2 (84). С. 50-56.