

Научная статья
УДК 351.745.7

«Цифровая оперативно-розыскная деятельность» и цифровизация противодействия преступлениям

Виктор Иванович Шаров, доктор юридических наук, профессор

Нижегородская академия МВД России
Нижний Новгород (603950, Анкудиновское шоссе, д. 3), Российская Федерация
v-i-sharov@rambler.ru
<https://orcid.org/0009-0008-5196-1131>

Аннотация:

Введение. Развитие цифровых технологий и их применение в разных сферах современной жизни справедливо поднимает вопрос о цифровизации отдельных направлений правоохранительной практики, не исключая и оперативно-розыскную деятельность (далее – ОРД). Однако каким образом цифровые инновации влияют на оперативно-розыскную деятельность и корректируют ее содержание, как они должны включаться в теорию ОРД – эти вопросы остаются проблемными и требующими отдельного анализа.

Методы. В исследовании применялась совокупность методов. В первую очередь это категории диалектики (анализ, синтез, индукция, дедукция, обобщение) и общенаучные методы познания (наблюдение, описание, сравнение, включая методы теоретического уровня – классификацию, абстрагирование), а также частнонаучные методы. Использовались основные принципы системно-деятельностного и формально-логического подходов.

Результаты исследования заключаются в выводах о необходимости развития цифровых средств и методов оперативно-розыскной деятельности, но не в рамках теории «цифровой ОРД», понятие которой сформулировано расплывчато и противоречиво, а в виде самостоятельного направления оперативной работы, опирающегося как на негласные, так и на гласные методы сбора и анализа данных в цифровых сетях и интернете, получение цифровых следов, мониторинг интернета и данные киберразведки.

Ключевые слова:

оперативно-розыскная деятельность, цифровые методы оперативно-розыскной деятельности, цифровые следы, интернет, мониторинг интернета, анализ цифровых данных

Для цитирования:

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

Статья поступила в редакцию 10.04.2025;
одобрена после рецензирования 09.07.2025;
принята к публикации 25.09.2025.

Original article

“Digital operational-search activity” and digitalisation in counteracting crimes

Viktor I. Sharov, Doc. Sci (Jurid.), Professor

Nizhny Novgorod Academy of the MIA of Russia
3, Ankudinovskoye Hwy, Nizhny Novgorod, 603950, Russian Federation
v-i-sharov@rambler.ru
<https://orcid.org/0009-0008-5196-1131>

Abstract:

Introduction. The development of digital technologies and their application in various spheres of modern life raises the question of digitalisation of certain areas of law enforcement practice, not excluding operational-search activities. However, how digital innovations affect operational-search activity and its content, how they should be included in its theory – these issues remain problematic and require a separate analysis.

Methods. The research involved a set of methods. These are primarily the categories of dialectics (analysis, synthesis, induction, deduction, generalisation) and general scientific methods of cognition (observation, description, comparison, including methods of theoretical level – classification, abstraction), as well as private scientific methods. The main principles of system-activity and formal-logical approaches were used.

Keywords:

operational investigative activities, digital methods of operational investigative activities, digital traces, Internet, Internet monitoring, digital data analysis

For citation:

Sharov V. I. “Digital operational-search activity” and digitalisation in counteracting crimes // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 3 (107). P. 171–178.

© Шаров В. И., 2025



The results of the research include conclusions concerning the need for developing digital means and methods of operational-search activities. Such an idea should be implemented not within the framework of the theory of "digital operational-search activity", the concept of which is formulated vaguely and controversially, but as an independent area of operational work, relying on both covert and overt methods of collecting and analysing data in digital networks and the Internet, obtaining digital traces, monitoring the Internet and cyber intelligence data.

**The article was submitted April 10, 2025;
approved after reviewing July 9, 2025;
accepted for publication September 25, 2025.**

Введение

Развитие цифровых технологий и их применение в разных сферах современной жизни поднимает вопрос и о цифровизации отдельных направлений правоохранительной практики, не исключая и оперативно-розыскную деятельность. Стремительное развитие технологий и изменение характера преступности в цифровую эпоху, новые виды криминальных угроз (компьютерное мошенничество, торговля запрещенными товарами и услугами, кибератаки, манипулирование компьютерной информацией и т. д.) определяют актуальность применения цифровых технологий в оперативно-розыскной деятельности (далее – ОРД), создания новых методов оперативной работы.

В отдельных случаях даже используется весьма интересный термин – «цифровая ОРД». Если вдуматься, это понятие должно в корне менять само содержание оперативно-розыскной деятельности. Собственно, об особенностях, в т. ч. и терминологических, ОРД в цифровую эпоху мы и остановимся в настоящей статье.

Методы

Принятая в исследовании методология исследования опирается в первую очередь на категории диалектики. В частности, сделанные выводы синтезированы на основе анализа многих из имеющихся подходов к построению ОРД в цифровом мире, путем дедуктивных рассуждений получен основной вывод исследования о целесообразности преимущественного развития методов работы с цифровыми объектами. Использование абстрагирования позволило в лучшей степени понять содержание ключевого понятия «цифровое ОРД» и провести уточнение профессионального категориально-понятийного ряда, связанного с терминологией оперативно-розыскной деятельности в цифровой действительности. Основные принципы системности, деятельности, формальной логики определяли ход и результаты исследования.

Результаты

Результаты исследования заключаются в выводах о необходимости развития цифровых средств и методов оперативно-розыскной деятельности. В научной литературе появляются работы о «цифровой ОРД», что вызывает вопрос: неужели и правда рождается эта особенная отрасль правоохранительной деятельности?

Сразу заметим: анализ литературы показал, что большая часть работ, посвященных цифровой ОРД, по существу, раскрывает совершенно иные темы. Скорее, речь в них идет о цифровизации (цифровой трансформации), переходе к новым цифровым методам в этой сфере деятельности. Значительная часть таких работ представляет собой анализ проблем, которые возникают перед ОРД в связи с цифровизацией общества и использованием цифровых и информационных технологий преступниками, т. е. переходом преступности в цифровую сферу, а также предложения по нейтрализации новых видов угроз безопасности общества. Также подобные работы посвящены развитию новых технологий применительно к решению задач ОРД, исходя из возможностей, предоставляемых этими цифровыми технологиями, что, в общем-то, логично. Какие-то целостные концепции цифровой ОРД создать крайне трудно, поскольку мы пока плохо представляем эту новую реальность, в которой «оцифрованы» все стороны жизни общества.

Разговоры о цифровизации и виртуализации вызывают ассоциации с фантастическими сюжетами в стиле «Лабиринта отражений» Сергея Лукьяненко: человек садится за компьютер, подключается к нему, и его сознание улетает в виртуальные города, игровые пространства, созданные фантазией компьютерщиков. Сам же автор в одном из своих интервью говорит, что если будет создано полноценное виртуальное пространство, оно сможет заменить людям обыкновенную жизнь. Так это когда оно будет полноценно создано! Мы, конечно, туда стремимся, но непонятно, когда дойдем, и как это виртуальное пространство будет выглядеть. По всей видимости, и полицейский в таком же виртуальном образе будет следить за порядком, установленным в виртуальном мире (собственно, так у С. Лукьяненко и происходит). Однако реальность пока несколько иная, более традиционная, а цифровая «виртуальная действительность» еще впереди.

Похоже, ученые слишком торопятся, застолбив «цифровое ОРД» как термин, обозначающий целую сферу деятельности, новую и оригинальную, ранее не встречавшуюся в практике и теории, как «систему использования оперативно-розыскных сил, средств и методов в цифровой среде» [1, с. 36]. Фантазии же в стиле «цифрового полицейского» приводят лишь к заключению о том, «что в корне должен меняться подход к подбору, воспитанию и обучению цифрового полицейского – человека, стоящего на страже борьбы с преступностью» [2, с. 257], что не создает нового цифрового образа правоохранителя, а скорее, совершенствует имеющийся.

В некоторых работах с тегом «цифровая ОРД» констатируется необходимость совершенствования правового регулирования, поскольку оно значительно отстает от развития цифровых технологий. Существует глубокий разрыв между скоростью развития этих технологий и «нормативно-правовым регулированием вопросов цифрового пространства, научно-практическими обоснованиями технологических прорывов и морально-этическими нормами» [2, с. 258]. Сказанное верно отражает действительность. Право представляет собой ту область, которая, наряду с техническими вопросами, вплотную столкнулась с неизвестными реалиями. Однако законодатель, так же как и ученые, выжидает, когда новая реальность станет более очевидной, и пока ограничивается отдельными предложениями.

Конечно, содержащиеся в цитированной выше работе Ю. А. Лапуновой и А. Ю. Бегунова выводы во многом декларативны и очевидны. Опираясь на них, сложно делать какие-либо предположения о содержании цифровой ОРД, поэтому следует воспринимать эти выводы скорее как призыв, чем как серьезную научную концепцию. Концепции цифровой ОРД не существует, отсутствуют даже подходы к ее построению. Повторим, определены только отдельные направления. Тем не менее полагаем указанную выше работу крайне полезной, поскольку она позволяет оттолкнуться от приведенных положений и сделать некоторые предположения о месте ОРД в цифровой реальности.

Итак, о цифровом ОРД, по всей видимости, говорить нужно, но очень осторожно, как это делают многие ученые, анализируя проблемы развития оперативно-розыскной деятельности в цифровой сфере. Именно так сделали В. В. Семенчук и В. Б. Батоев, предложив свои направления совершенствования ОРД в новых условиях в статье «Развитие оперативно-розыскной деятельности в цифровой сфере» [3, с. 132–136]. Много из предложенного ими уже анализировалось в литературе, но не сложилось в единую конструкцию противодействия преступности в цифровой сфере. О цифровых методах ОРД пишет А. В. Варданян [4, с. 12]. Представляется вполне уместным анализ многочисленных аспектов современного ОРД, как это сделано в большей части сборника «Оперативно-розыскная деятельность в цифровом мире», вышедшего под редакцией профессора В. С. Овчинского [5].

О расширении перспектив оперативно-розыскной деятельности, связанных с цифровизацией общества и виртуализацией реальности [6, с. 150–172], и оперативно-розыскной деятельности в информационном обществе пишет А. Л. Осипенко [7, с. 38–46]. Нельзя не отметить работу П. И. Иванова, который рассматривает оперативно-розыскную деятельность в условиях цифровой реальности в контексте её научного обеспечения [8, с. 64–67]. О перспективах развития отдельных видов деятельности в условиях цифровизации общества, а также реализации оперативно-розыскной политики органами внутренних дел в условиях цифровой трансформации пишут и другие ученые.

Приведенные примеры свидетельствуют о целесообразности развития ОРД в цифровой сфере, а не о ее новом качестве. Полагаем, что подобный подход отвечает принципу преемственности в развитии оперативно-розыскной деятельности. По всей видимости, более уместно говорить: а) об оперативной работе в цифровой среде; б) использовании цифровых средств при проведении оперативно-розыскных мероприятий. При этом второй случай (использование цифровых средств) явно не предполагает революционных изменений и представляет собой плавный переход от одних средств (традиционных) к другим – цифровым, с максимальным использованием дополнительных возможностей, предоставляемых цифровой. На наш взгляд, преждевременно пытаться формулировать цифровую ОРД, которая должна иметь множество специфических признаков, отличных от настоящего состояния науки и практики в этой деятельности.

Уместно говорить о цифровой трансформации ОРД, ее условиях и задачах, тем более, что этот термин присутствует в Положении о ведомственных программах цифровой трансформации, утвержденном постановлением Правительства Российской Федерации от 10 октября 2020 г. № 1646¹, хотя в этом документе данный термин не раскрывается. Тем не менее анализ его использования в контексте показал, что под цифровой трансформацией вполне уместно понимать приспособление оперативно-розыскной деятельности к условиям развивающейся цифровой среды.

¹ О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий, финансовое обеспечение которых осуществляется (планируется осуществлять) за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов : постановление Правительства Российской Федерации от 10 октября 2020 г. № 1646 (ред. от 18.03.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2020. № 42 (ч. III). Ст. 6612.

Цифровые аспекты оперативно-розыскной деятельности можно также рассматривать как достаточно емкое, самостоятельное, отдельное направление оперативной работы, которое связано с использованием цифровых технологий и интернета для выявления, предупреждения и раскрытия преступлений.

Вместе с тем в этом направлении возможно выделить относительно самостоятельные элементы, что, собственно, и делается в литературе. Полагаем, что развитие техники и технологий скорректирует любые предположения, но тем не менее их анализ представляется актуальным.

Пожалуй, главное место занимает совершенствование нормативно-правовой базы оперативно-розыскной деятельности, проводимой в цифровой среде. Анализ ряда научных позиций из отдельных отраслей права позволил выделить ряд проблем, возникающих при попытках привязать ОРД к современной (и в большей степени будущей) цифровой действительности. Обратим внимание на одну из них: виртуализацию ОРД, включающую вывод, что эта деятельность в цифровой среде в корне другая, чем в обычной привычной жизни. Отличия ОРД в цифровом пространстве от привычной нам присутствуют, и нет оснований утверждать обратное. Но эти отличия представляются пока не такими уж и кардинальными. Остаются принцип негласности и методы его реализации, такие как маскировка и легендирование, остается, в конце концов, система оперативно-розыскных мероприятий как определяющий элемент ОРД. По существу сегодня речь идет о том, как на законных основаниях имеющейся совокупностью оперативно-розыскных мероприятий осуществлять оперативную работу в цифровом (информационном) пространстве, а не о разработке новых правовых инструментов. Да и традиционные методы не кажутся безнадежно устаревшими – по всей видимости, быстрее, надежнее и «законнее» будет запросить в банке справку о движении по счетам злоумышленника, чем взламывать его компьютер для извлечения следов проведенных финансовых операций в онлайн-банке.

Новые возможности для ОРД уже предоставлены. Основанием оперативной работы в цифровой среде выступают такие оперативно-розыскные мероприятия, как «Получение компьютерной информации», «Снятие информации с технических каналов связи». Однако эти мероприятия используют технически довольно сложные алгоритмы, недоступные для обычного оперативного подразделения, требуют специальной подготовки и реализуются преимущественно специалистами с использованием оперативно-технических сил и средств [9, с. 86]. Хотя при этом остается законодательно и нормативно неотрегулированными целый ряд элементов оперативно-розыскной деятельности в интернете. Например, как назвать блуждание по интернету с целью извлечения максимально полной информации об интересующем оперативного работника лице – наблюдение или наведение справок?

Виртуализация деятельности налицо, но специфика этого элемента пока еще не раскрыта в законодательстве.

Важно также развивать методы сбора и анализа данных в цифровых сетях, интернете [10, с. 154], включая как негласные, так и гласные методы (OSINT-технологии [11, с. 66]). Это должны быть не только информационно-аналитические мероприятия, реализуемые специальными оперативными подразделениями, которые сегодня созданы и успешно выполняют стоящие перед ними задачи, но и широкое проведение такой работы обычными оперативными работниками.

Особое значение приобретают методы, направленные на обнаружение и получение цифровых следов из интернета. Это требует изучения процессов обращения информации в компьютерных системах и сетях, особенностей функционирования отдельных информационных систем, взаимодействия пользователя и компьютера. Включая создание особых средств обеспечения «прозрачности» отдельных операций, как, например, это сейчас делается при обороте криптовалюты, с разработкой процедур доступа к такой «технологической» информации.

Можно согласиться с А. В. Вardanяном, который даже формирует группы этих способов работы, называя одни из их «цифровыми методами ОРД», а другие «условно цифровым методом». К первым он относит наряду с получением компьютерной информации также контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров [4, с. 11], ко вторым – ряд других оперативно-розыскных мероприятий, на самом деле довольно условно относящихся к работе в цифровой среде. Однако при всей дискуссионности данных положений, по всей видимости, речь должна идти о создании новых цифровых методов работы, реализуемых в рамках указанных мероприятий.

Это тесно пересекается с ранее отмеченными проблемами правового регулирования цифровых методов оперативной работы – на законодательном уровне следует отрегулировать работу оперативных подразделений с информацией в интернете.

Для реализации этих целей в литературе предлагается такой метод работы, как мониторинг интернета, который можно считать также методом сбора и анализа данных, обладающих определенной спецификой, связанной с выявлением и наблюдением за преступными проявлениями в сети, выявлением лиц, пропагандирующих преступное поведение и вовлекающих в преступную деятельность.

Еще одним самостоятельным элементом цифровизации оперативно-розыскной деятельности следует назвать киберразведку. При реализации данного метода используются

специальные программные средства для отслеживания действий преступников в цифровом пространстве, связанные со взломом защиты компьютерных систем, использованием программных закладок и т. д. Данные методы ассоциируются чаще всего с хакерами, с незаконным получением информации, но должны показать свою эффективность и в осуществлении оперативной работы.

Повторим, правовые вопросы использования данных методов не проработаны, однако полагаем, что они допустимы в процессе оперативной работы. Требуется на законодательном уровне прописать, какие действия допустимы, и определить условия их использования. Иначе это грозит применением к оперативному работнику мер уголовной ответственности за неправомерный доступ к компьютерной информации по ст. 272 Уголовного кодекса Российской Федерации² (далее – УК РФ).

Весьма специфичными выглядят отдельные элементы цифровизации ОРД. Например, лежащая на поверхности актуальная проблема информационной безопасности. Она относительно нова, в связи с чем далеко неясна во всех ее многочисленных аспектах. Хотя, казалось бы, все очевидно: оперативно-розыскной закон относит к числу задач ОРД (ст. 2 Федерального закона «Об оперативно-розыскной деятельности»³) добывание информации о событиях или действиях, создающих угрозу в т. ч. и информационной безопасности Российской Федерации, а в отдельных случаях, как отмечает Е. Н. Яковец, выступает и ее предполагаемым результатом [12, с. 128].

Но проблема представляется настолько обширной, что для ее решения методов ОРД явно недостаточно. Так, существенно более широкие возможности предусмотрены теорией информационной безопасности, практикой и законодательством в виде совокупности административных средств. Они носят превентивный характер и рассчитаны на недопущение инцидентов информационной безопасности. ОРД же включаются там и тогда, когда совокупность этих мер оказывается бессильной со стороны поступивших угроз. ОРД совместно с процессуальной деятельностью обеспечивает реализацию уголовно-правовых мер, но они гораздо менее «цифровые», чем возможности, предоставленные сегодня методам обеспечения информационной безопасности, к которым мы бы отнесли еще и всю мощь технического регулирования со стороны Роскомнадзора. Собственно, и полномочия у ОРД совсем иные. Тем не менее новая ОРД определяет действенность уголовно-правовых средств обеспечения информационной безопасности, что требует ее развития и в этом направлении.

Однако и сами уголовно-правовые средства, изложенные в УК РФ как преступления в сфере компьютерной информации, далеко не исчерпывают все проблемы информационной безопасности. Имевшая изначально три, а сейчас расширившаяся до шести статей гл. 28 УК РФ все равно не содержит всех противоправных деяний в анализируемой сфере – т. е. методы ОРД включаются в обеспечение информационной безопасности по довольно ограниченному набору инцидентов и совершенно не первичны и не характерны для данной сферы. Например, хакерским атакам сейчас нередко подвергаются официальные сайты государственных органов, банков. В этих действиях содержатся признаки преступления, но уголовных дел по этим фактам практически нет, хотя им активно и довольно успешно противостоят службы информационной безопасности. Представляется, что административные меры пока доминируют над уголовно-правовыми. Это, по всей видимости, правильно, но любому инциденту следует также давать уголовно-правовую оценку, вплоть до привлечения нарушителей к уголовно-правовой ответственности.

Полагаем, что для обеспечения информационной безопасности возникает необходимость в некоторых «цифровых» полицейских методах, но весьма специфических, объединяющих административные и уголовно-правовые меры воздействия на цифровые правонарушения и преступления. Иными словами, требуется некая подвижка ОРД в сторону административных мер, развития процедур использования результатов ОРД за пределами уголовного процесса (например, для блокировки сайтов с противоправным содержанием).

Развитие «цифровых» методов делает актуальной проблему того, как аккумулировать знания о применении цифровых технологий в решении задач, одной из которых выступает выявление и раскрытие преступлений, совершаемых в цифровой среде. Напрашивается вывод о создании некоторой теоретической конструкции в виде частной теории ОРД, или «теории цифровой ОРД» [2, с. 258], что, полагаем, синонимично.

Основания для конструирования научных основ цифровых методов ОРД представляются достаточно разнообразными. Конечно, они могут опираться на положения научного знания цифровой криминологии, как это указывается в литературе. Она активно развивается, но единства, свойственного самостоятельному разделу науки, еще не достигла. Задача создания цифровой ОРД неординарная, для ее решения нужны знания не только криминологии (мы бы даже сказали, не столько криминологии), но и иных наук, включая информатику. Пожалуй, более правильным было бы построение цифровой ОРД с опорой на компьютерную кримина-

² Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954.

³ Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ (ред. от 01.04.2025) // СЗ РФ. 1995. № 33. Ст. 334.

листику (форензику), переориентированную на решение проблем ОРД, с методов исследования компьютерной информации на ее получение негласными методами. Криминалистика все же ближе к оперативной работе, чем криминология, а ее наработки в сфере цифровой трансформации правоохранительной деятельности более обширны, чем в ОРД.

Очевидно, конструкция создаваемой теории будет определяться исследуемой областью, т. е. исходить из определенных в ее предмете закономерностей информационно-правовых (цифровых) отношений. Если исследуемые закономерности будут носить общий характер и слабо зависеть от сферы применения этой теории, т. е. от вида расследуемых преступлений, то мы и получим теоретическое построение, которое можно назвать частной теорией ОРД. В этом случае в частной теории следует изложить все выявленные закономерности движения цифровой информации и их использования в сфере выявления и раскрытия преступлений.

А если нет? Может получиться так, что логика построения научного знания потребует создать теорию более высокой степени общности, задающую лишь общие направления работы в цифровой среде и не содержащую решений конкретных практических задач. Такое не редкость в науке, например, общая теория судебной экспертизы не содержит конкретных методик экспертного исследования. Она включает в себя лишь структурированное знание о данной области, определяет только общее направление использования специальных знаний в расследовании преступлений (понятие предмета и объектов судебной экспертизы, экспертные методы и задачи, структуру экспертного познания, классификацию судебных экспертиз и т. д.). Конкретные же методики проведения отдельных видов экспертиз рассматриваются в других разделах.

В этом случае применительно к частной теории цифрового ОРД следует сформулировать еще и систему знаний, в которой нужно описывать особенности использования цифровых информационных технологий применительно к решению различных задач ОРД, расширяя имеющиеся традиционные знания. Структура этой теории, содержание разделов существенно расширяется, но тоже пока не просматривается.

Заметим, что речь идет именно о теории ОРД, а не о методике или иных формах рекомендаций для практики. К примеру, возьмем теорию документирования. Что там должно быть, относящееся к информационным цифровым технологиям? Наверное, а) методы и средства документирования в цифровой среде; б) цифровые средства документирования преступной деятельности. Но каково взаимоотношение теории документирования и частной теории цифрового ОРД? Каково взаимопроникновение одной в другую? Или вот еще интересный вопрос – а где пределы такой цифровизации? Некоторые ученые уже говорят об обратных процессах, поскольку повсеместное использование компьютерных технологий вызывает проблемы потребности «в структурах и средствах безопасности, соответствующих уровню угроз» [13, с. 108] или «цифровизации негласного сотрудничества граждан» [14, с. 182]. Пока не сформулирована частная теория ОРД, ответить на эти вопросы довольно сложно.

Итак, общая теория цифрового ОРД пока не создана ни в одном из предполагаемых видов.

Еще одно положение, свидетельствующее о несколько обособленном положении в теории ОРД системы знаний о цифровых технологиях.

В литературе, в частности, в работе А. Н. Позднякова, декларируется создание «частной теории оперативно-розыскной деятельности по борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий» [15, с. 121]. Не прибегая к анализу содержания предлагаемой частной теории, следует сказать, что по количеству входящих в нее рекомендаций данная теория предлагается чрезмерно громоздкой. И причины очевидны – с использованием информационных технологий совершается большое количество видов преступлений, почти весь УК РФ. Для каждого вида преступлений должны быть, по мнению автора, «выявление первичных оперативно-розыскных данных и документирование криминальной деятельности лиц, причастных к преступлениям, совершенным с использованием ИКТ-технологий». Включается в структуру теории и «оперативно-розыскное предупреждение преступлений, совершаемых с использованием ИКТ-технологий» и т. д. [15, с. 123]. И какой видится данная частная теория? Как рекомендации по противодействию преступлениям в сфере компьютерной информации (глава 28 УК РФ⁴)? А как же остальные преступные деяния, которые не относятся к компьютерным, но совершаются в цифровой среде: параллельно с обычными рекомендациями выстраивать еще одну структуру только для раскрытия тех же преступлений, совершенных с использованием информационных технологий?

Конечно, содержание и структура такой теории, и как следствие ее название, должны быть иными. Мы вообще с настороженностью относимся к частным теориям выявления, раскрытия или расследования отдельных видов преступлений. По существу, это та же методика той или иной степени общности и придавать такой методике статус частной теории представляется неправильным. Методика не может носить статус частной теории, поскольку она ориентирована на выдачу практических рекомендаций, а не на вскрытие закономерностей, из которых эти рекомендации вытекают. Такая теория может погрязнуть в деталях, сила же теории в обобщении знания и формулировании непротиворечивых конструктов.

⁴ СЗ РФ. 1996. № 25. Ст. 2954.

Тогда частная теория противодействия каким-либо видам преступлений, в данном случае совершенным с использованием информационных цифровых технологий, должна содержать только систему общих рекомендаций, построенных на обнаруженных закономерностях обращения информационных процессов и средств обработки информации, применительно к выявлению и раскрытию преступлений, а не конкретные рекомендации раскрытия преступлений, совершенных с их использованием. А это вызывает вопросы в целесообразности такого рода теорий. По всей видимости, не стоит назначать статус теории методическим рекомендациям, пусть и такого уровня общности. Если же не ставить под сомнение наличие такой теории, то, по крайней мере, над содержанием этой теории нужно еще думать.

Как уже было сказано, в современных условиях цифровой трансформации всех видов деятельности использование цифровых или информационных технологий становится рядовым инструментом деятельности и должно рассматриваться совместно с традиционными средствами.

О методике следует сказать отдельно. Сейчас по большей части рекомендации по использованию цифровых технологий или об особенностях раскрытия преступлений, совершенных с их использованием, сводятся в отдельные самостоятельные параграфы или разделы. Методика имеет традиционный вид, от оперативно-розыскной характеристики преступлений к их признакам, средствам выявления этих признаков и методам и средствам документирования преступного деяния, но этот вид дополняется отдельно выделенным материалом по использованию цифровых технологий и раскрытию преступлений в цифровой реальности.

Представляется, что это неправильно. Современная жизнь невозможна без информационных технологий, они сопровождают нас повсюду. Но также с их использованием совершается немало преступлений. Эти технологии органично вплетены в социальные и экономические процессы и неотделимы от естественного и очевидного хода событий. При этом даже обычные преступления, совершаемые без участия цифровых средств, раскрываются с использованием последних, и порой весьма интенсивным: оперативные работники проверяют подозреваемых по учетам, «пробивают» их по социальным сетям, осуществляют поиск сведений об интересующих лицах в интернете с использованием технологий OSINT и т. д. Поэтому рекомендации по выявлению и раскрытию преступлений должны быть адаптированы под современные условия и содержать сведения об оптимальных методах работы. И если они (эти методы) связаны с использованием цифровых технологий, то нужно рекомендовать, какие цифровые средства и методы использовать в этом случае, т. е. нужно ориентировать рекомендации на то, каким образом работать в информационном пространстве, что и где искать, каким инструментом пользоваться применительно к стоящей задаче. При этом следует рассматривать это не как отдельное направление деятельности, а как рядовое, обычное средство оперативной работы. Так, анализируя способы совершения преступления, следует обращать внимание и на те, что совершаются с использованием цифровых технологий, приводить наряду с традиционными признаки, характерные для таких способов совершения преступлений, обратить внимание на средства и методы выявления и раскрытия этих преступлений.

3 заключение

В современных условиях цифровизации всех видов деятельности использование цифровых или информационных технологий оперативно-розыскной деятельности не требует создания специальных частных теорий «цифровой ОРД» или «оперативно-розыскного противодействия преступлениям, совершаемым в цифровой среде». Цифровые возможности становятся обычным инструментом деятельности, и они должны рассматриваться как рядовое обычное средство оперативной работы вместе с традиционными средствами, дополняя их.

Основной вывод исследования состоит в необходимости развития цифровых средств и методов оперативно-розыскной деятельности, но не в рамках теории «цифровой ОРД», понятие которой сформулировано расплывчато и противоречиво, а в виде самостоятельного направления оперативной работы, опирающегося как на негласные, так и на гласные методы сбора и анализа данных в цифровых сетях и интернете, получение цифровых следов, мониторинг интернета и данные киберразведки.

Список источников

1. Васильченко Д. А. О Концепции цифровизации оперативно-розыскной деятельности / Петербургские пенитенциарные конференции : материалы конференций : в 4 т., г. Санкт-Петербург, 17–18 мая 2021 г. Санкт-Петербург : Санкт-Петербургский университет Федеральной службы исполнения наказаний, 2021. Т. II. С. 34–41.
2. Лапунова Ю. А., Бегунов А. Ю. Полемика о концептуальных основах цифровой оперативно-розыскной деятельности / Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов / под ред. В. С. Овчинского. Москва : ИНФРА-М, 2021. С. 253–260.
3. Семенчук В. В., Батоев В. Б. Предпосылки формирования концепции развития оперативно-розыскной деятельности в цифровой сфере (Часть 1) // Вестник Волгоградской академии МВД России. 2023. № 3 (66). С. 132–136. <https://doi.org/10.25724/VAMVD.A166>
4. Варданян А. В. Проблема систематизации цифровых методов оперативно-розыскной деятельности, используемых в борьбе с дистанционными хищениями, и их криминалистическое значение // Юристъ-Правоведь. 2022. № 2 (101). С. 7–13.

5. *Оперативно-розыскная деятельность в цифровом мире* : сборник научных трудов / под ред. В. С. Овчинского. Москва : ИНФРА-М, 2021. 630 с.
6. *Осипенко А. Л.* Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности / *Оперативно-розыскная деятельность в цифровом мире* : сборник научных трудов / под ред. В. С. Овчинского. Москва : ИНФРА-М, 2021. С. 150–173.
7. *Осипенко А. Л.* Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // *Научный вестник Омской академии МВД России*. 2019. № 4 (75). С. 38–46. <https://doi.org/10.24411/1999-625X-2019-14007>
8. *Иванов П. И.* Оперативно-розыскная деятельность в условиях цифровой реальности: её научное обеспечение // *Вестник Калининградского филиала Санкт-Петербургского университета МВД России*. 2022. № 2 (68) С. 64–67.
9. *Осипенко А. Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // *Вестник Воронежского института МВД России*. 2016. № 3. С. 83–90.
10. *Кубасов И. А., Лекарь Л. А.* Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети интернет, для обеспечения деятельности оперативных подразделений МВД России // *Труды Академии управления МВД России*. 2023. № 3 (67). С. 154–161. <https://doi.org/10.24412/2072-9391-2023-367-154-161>
11. *Батоев В. Б.* О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности // *Вестник Уфимского юридического института МВД России*. 2023. № 2 (100). С. 66–71.
12. *Яковец Е. Н.* Оперативно-розыскные меры полиции по обеспечению информационной безопасности Российской // *Труды Академии управления МВД России*. 2017. № 3 (43). С. 127–131.
13. *Ткачук Т. А., Курьесев К. Н.* Вопросы о децифровизации в аспекте осуществления оперативно-розыскной деятельности // *Вестник Владимирского юридического института*. 2023. № 1 (66). С. 107–111.
14. *Железняк И. Н.* Проблемы цифровизации негласного сотрудничества граждан с органами, осуществляющими оперативно-розыскную деятельность // *Вестник Восточно-Сибирского института МВД России*. 2022. № 2 (101). С. 181–192. <https://doi.org/10.55001/2312-3184.2022.93.64.016>
15. *Поздняков А. Н.* О частной теории оперативно-розыскной деятельности по борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий // *Труды Академии управления МВД России*. 2022. № 3 (63). С. 119–125. <https://doi.org/10.24412/2072-9391-2022-363-119-125>