

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

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность (специализация
Оперативно-розыскная деятельность, профиль образовательной программы –
Деятельность оперуполномоченного уголовного розыска), очная форма
обучения, набор 2021 года

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

**ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ
РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С
НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ
«ИНТЕРНЕТ»**

Выполнил:

Слушатель учебной группы П 2102-УР
младший лейтенант полиции
Ермаков Даниил Андреевич

Руководитель:

Профессор кафедры криминалистики,
кандидат юридических наук., доцент
полковник полиции
Шинкевич Дмитрий Валерьевич

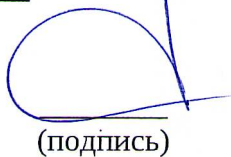
Дата защиты:

«24» июня 2026 г.

Оценка: отлично

Председатель ГЭК

полковник Шинкевич
(специальное звание)


(подпись)

А.В. Шинкевич
(инициалы, фамилия)

Красноярск 2026

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

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность (специализация
Оперативно-розыскная деятельность, профиль образовательной программы –
Деятельность оперуполномоченного уголовного розыска), очная форма
обучения, набор 2021 года

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

**ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ
РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С
НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ
«ИНТЕРНЕТ»**

Выполнил:

Слушатель учебной группы П 2102-УР
младший лейтенант полиции
Ермаков Даниил Андреевич

Руководитель:

Профессор кафедры криминалистики,
кандидат юридических наук., доцент
полковник полиции
Шинкевич Дмитрий Валерьевич

Дата защиты:

« ____ » _____ 2026 г.

Оценка: _____

Председатель ГЭК

(специальное звание)

(подпись)

(инициалы, фамилия)

Красноярск 2026

Оглавление

Введение.....	3
ГЛАВА I. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И ТИПОЛОГИЯ СЛЕДСТВЕННЫХ СИТУАЦИЙ ПРИ РАССЛЕДОВАНИИ НАРКОПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СРЕДЕ.....	7
§ 1.1. Структурно-криминалистическая характеристика преступлений в сфере НОН, опосредованных использованием ИТС.....	7
§ 1.2. Цифровые следы как элемент криминалистической характеристики: классификация и особенности обнаружения.....	13
§ 1.3. Типичные исходные следственные ситуации и алгоритмы построения следственных версий.....	18
ГЛАВА II. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С УЧЕТОМ СПЕЦИФИКИ ЦИФРОВОЙ СРЕДЫ.....	24
§ 2.1. Тактика осмотра цифровых носителей информации и изъятия электронных доказательств.....	24
§ 2.2. Тактические приемы допроса при расследовании «бесконтактных» сбытов наркотических средств.....	28
§ 2.3. Организация и тактика обыска (выемки) у лиц, осуществляющих дистанционное управление наркотрафиком.....	34
ГЛАВА III. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАССЛЕДОВАНИЯ И ПРОФИЛАКТИКА ЦИФРОВЫХ НАРКОПРЕСТУПЛЕНИЙ.....	40
§ 3.1. Организация взаимодействия следователя с оперативно- розыскными подразделениями и экспертными учреждениями.....	40
§ 3.2. Роль судебных экспертиз в доказывании по делам о наркопреступлениях, совершенных через ИТС.....	44
§ 3.3. Криминалистическое прогнозирование и меры профилактики с учетом развития цифровых технологий.....	48
Заключение.....	53
Список использованной литературы.....	57

Введение

Актуальность темы исследования. Современный этап развития общественных отношений характеризуется стремительной цифровизацией всех сфер жизнедеятельности человека. Информационно-телекоммуникационные сети, включая сеть «Интернет», стали неотъемлемым элементом социальной коммуникации, экономики, государственного управления и повседневной жизни граждан. Однако наряду с позитивными эффектами цифровая среда предоставляет беспрецедентные возможности для криминальной активности, трансформируя традиционные механизмы совершения преступлений. В полной мере это относится к незаконному обороту наркотических средств (далее – НОН), который в последние годы приобрел выраженный «цифровой» характер, интегрируясь в даркнет-площадки, анонимные мессенджеры, криптовалютные платежные системы и автоматизированные интернет-магазины.

Статистические данные убедительно свидетельствуют о масштабах и динамике данной угрозы. По итогам 2025 года в России зафиксирован значительный рост наркопреступности: общее число зарегистрированных преступлений в сфере НОН достигло 186 тысяч, что на 11% превышает показатели предыдущего года. Более половины из них (54,5%) совершаются с использованием сети «Интернет». При этом, как отмечает МВД РФ, всего по стране предварительно расследовано 126 145 наркопреступлений, причем лидерами по их количеству стали Москва (свыше 10,4 тыс.), Московская (около 5,8 тыс.) и Челябинская области (5,1 тыс.). Объем изъятых из незаконного оборота наркотических средств также впечатляет: в 2025 году изъято более 35,7 тонны наркотиков, 828 кг психотропных веществ и свыше 46 тонн прекурсоров. В ряде регионов доля «цифровых» наркопреступлений достигает критических значений: в Нижегородской области 83% преступлений данной категории совершаются с использованием ИТ-

технологий, в Кемеровской области этот показатель составил 76,7%, а на Сахалине зафиксировано увеличение на 27,8% числа таких преступлений.

Особую тревогу вызывает не только количественный рост, но и качественная трансформация наркобизнеса. Преступные группы используют разветвленные иерархические структуры с четким распределением функций, активно применяют системы шифрования, средства анонимизации (VPN, TOR, I2P) и криптовалюты для расчетов, что существенно затрудняет процесс выявления и документирования преступлений. В этих условиях классические криминалистические методики, ориентированные на «контактные» способы совершения преступлений, оказываются недостаточно эффективными. Возникает объективная необходимость переосмысления организационных и тактических основ расследования, адаптации следственного аппарата к работе с цифровыми следами, электронными доказательствами и анонимными средами. Сказанное определяет высокую теоретическую и практическую значимость настоящего исследования.

Степень научной разработанности проблемы. Вопросы противодействия незаконному обороту наркотических средств традиционно находились в поле зрения отечественных криминалистов. Значительный вклад в разработку теоретических и методических основ расследования данной категории преступлений внесли такие ученые, как В.Ф. Васюков, А.Н. Залескина, Е.Л. Глушаков, С.И. Земцова, А.М. Моисеев, С.В. Кондратюк и другие. Исследователи анализировали способы совершения наркопреступлений, личность преступника, особенности первоначального этапа расследования, а также вопросы взаимодействия следователя с оперативными подразделениями.

Однако, как свидетельствует анализ научной литературы, большинство существующих работ были выполнены до активной цифровизации наркобизнеса и ориентированы преимущественно на «контактные» способы сбыта. Отдельные аспекты, касающиеся тактики осмотра цифровых носителей, допроса участников бесконтактного наркотрафика и обыска у лиц,

использующих криптовалютные активы, освещены в работах К.Т. Саркисян (расследование незаконного оборота наркотических средств, совершенного с использованием компьютерных сетей), О.Ю. Введенской (первоначальный этап расследования), а также в публикациях И.Р. Аминова, А.А. Белякова, В.Р. Вареной, посвященных тактическим аспектам работы с электронно-цифровыми следами. Вместе с тем комплексного исследования организационно-тактических особенностей расследования наркопреступлений, совершаемых с использованием информационно-телекоммуникационных сетей, с учетом современных способов анонимизации и криптовалютных расчетов, в криминалистической науке не проводилось. Настоящая работа призвана восполнить указанный пробел.

Объектом исследования являются общественные отношения, складывающиеся в процессе оперативно-розыскной и следственной деятельности при противодействии преступлениям в сфере незаконного оборота наркотических средств, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет».

Предметом исследования выступают организационно-тактические закономерности, формы и методы расследования указанной категории преступлений, а также особенности выявления, фиксации и использования в доказывании цифровых следов и электронных носителей информации.

Цель исследования заключается в разработке комплекса научно обоснованных рекомендаций по совершенствованию организации и тактики расследования преступлений, связанных с незаконным оборотом наркотических средств через сеть «Интернет» и иные информационно-телекоммуникационные сети, с учетом современных криминалистических вызовов и тенденций развития цифровой среды.

Задачи исследования:

1. Определить криминалистически значимые признаки и структурные элементы преступлений в сфере незаконного оборота наркотиков,

опосредованных использованием цифровых технологий, на основе анализа современных способов их совершения.

2. Выявить типичные исходные следственные ситуации, возникающие на первоначальном этапе расследования, и разработать алгоритмы построения следственных версий для каждой из них.
3. Разработать тактические рекомендации по производству отдельных следственных действий (осмотра цифровых носителей, допроса, обыска) с учетом специфики цифровой среды и психологических особенностей участников «бесконтактного» наркотрафика.
4. Проанализировать организационные проблемы взаимодействия следователя с оперативно-розыскными подразделениями и экспертными учреждениями в процессе раскрытия и расследования данной категории преступлений.
5. Сформулировать предложения по повышению эффективности доказывания и профилактики указанных преступлений с учетом прогнозируемого развития информационных технологий и изменений в методах противодействия расследованию.

Теоретическую основу исследования составляют фундаментальные труды ведущих отечественных криминалистов в области криминалистической методики и тактики, теории судебной экспертизы, а также концептуальные положения о цифровых следах. В работе использованы научные работы Е.Р. Россинской, В.Б. Вехова, В.А. Мещерякова, Н.П. Яблокова, А.Г. Филиппова, а также диссертационные исследования К.Т. Саркисян и публикации, посвященные тактическим и организационным аспектам расследования наркопреступлений в цифровой среде.

Нормативную основу исследования составляют: Конституция Российской Федерации; Уголовный кодекс Российской Федерации; Уголовно-процессуальный кодекс Российской Федерации; Федеральный закон «Об оперативно-розыскной деятельности»; Федеральный закон «О наркотических средствах и психотропных веществах»; постановления Пленума Верховного

Суда Российской Федерации; ведомственные нормативные правовые акты МВД России, регламентирующие деятельность по выявлению и расследованию преступлений в сфере НОИ.

Эмпирическую основу исследования составляют: опубликованные материалы следственной и судебной практики по уголовным делам о преступлениях, предусмотренных ст. 228–228.1 УК РФ, совершенных с использованием информационно-телекоммуникационных сетей; статистические данные Министерства внутренних дел Российской Федерации о состоянии наркопреступности и результатах противодействия ей за 2022–2025 годы; обзоры следственной практики и методические рекомендации следственных подразделений МВД России;

Методологическую основу исследования составляют общенаучные и частно-научные методы познания: диалектический метод, системно-структурный анализ, формально-юридический метод, сравнительно-правовой метод, историко-правовой метод, метод статистического анализа, метод моделирования, логический метод, а также методы криминалистической тактики и методики расследования.

Теоретическая значимость исследования состоит в том, что сформулированные в работе выводы и предложения развивают и дополняют криминалистическую теорию в части организационно-тактического обеспечения расследования преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных сетей. Предложенная классификация типичных следственных ситуаций и алгоритмы действий следователя могут быть использованы при дальнейшей разработке частных криминалистических методик расследования высокотехнологичных преступлений.

Практическая значимость исследования состоит в том, что разработанные автором тактические рекомендации по производству осмотра, допроса и обыска, а также предложения по совершенствованию взаимодействия следователя с оперативно-розыскными подразделениями и

экспертными учреждениями могут быть непосредственно использованы в практической деятельности органов предварительного следствия и дознания. Материалы исследования могут быть применены в учебном процессе при подготовке учебных пособий и методических рекомендаций по курсу «Криминалистика», а также в программах повышения квалификации следователей и оперативных сотрудников.

Значение разработки проблемы для деятельности органов внутренних дел. Учитывая устойчивую тенденцию к трансформации наркоторговли в высокотехнологичную, транснациональную и анонимную сферу, результаты данного исследования обладают прямым практическим значением для сотрудников следственных и оперативно-розыскных подразделений МВД России. Разработанные рекомендации направлены на повышение эффективности раскрытия и расследования наркопреступлений, совершаемых с использованием ИТС, минимизацию рисков утраты доказательственной информации, а также на совершенствование организационных механизмов взаимодействия между участниками уголовно-процессуальной деятельности.

Работа состоит из введения, 3 глав, включающих 9 параграфов, заключения и списка использованной литературы

ГЛАВА I. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА И ТИПОЛОГИЯ СЛЕДСТВЕННЫХ СИТУАЦИЙ ПРИ РАССЛЕДОВАНИИ НАРКОПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СРЕДЕ

§ 1.1. Криминалистически значимые элементы преступного оборота наркотиков, опосредованного телекоммуникационными технологиями

Интеграция наркобизнеса в глобальное цифровое пространство привела к его радикальной трансформации. Ранее торговля веществами на нелегальном рынке базировалась преимущественно на личных контактах между участниками сделки. В современных условиях произошла трансформация модели сбыта: доминирующей практикой стало бесконтактное взаимодействие, осуществляемое через анонимные площадки в сети Интернет. По экспертным оценкам, большая часть современных наркопотребителей приобретают запрещённые вещества посредством интернет-коммуникации. Правоохранительная статистика последних лет фиксирует устойчивую восходящую динамику регистрации деяний, квалифицируемых по ст. 228.1 УК РФ и сопряжённых с использованием телекоммуникационных каналов.

Криминалистическая модель рассматриваемых деликтов представляет собой взаимосвязанную систему базовых компонентов, охватывающих объект преступного посягательства, алгоритм противоправных действий, обстановочные условия, механизм следообразования и характерологические свойства субъекта преступления. Каждая из перечисленных составляющих приобретает уникальное смысловое наполнение в контексте дистанционных практик сбыта наркотиков.

Объектный состав противоправной деятельности претерпел существенные изменения вследствие вовлечения в теневой оборот широкого спектра новых психоактивных соединений, позиционируемых как «дизайнерские» наркотики. Отличительная черта современного этапа — применение так называемых «наркоконструкторов» и вовлечение в незаконные операции «дизайнерских» прекурсорных веществ. Подобная тактика позволяет криминальным структурам оперативно реагировать на изменения

нормативной базы, выводя из-под прямого запрета новые модификации химических соединений.

Способ совершения преступного посягательства в криминалистической доктрине традиционно трактуется как трёхфазная конструкция, объединяющая этапы приготовления, реализации и сокрытия. Однако специфика бесконтактных наркотических сбытов состоит в том, что обозначенные стадии утрачивают чёткую хронологическую последовательность: маскирующие мероприятия инициируются уже на подготовительном этапе и продолжаются на всём протяжении криминальной активности. В силу множественности эпизодов в рамках единого продолжаемого преступления границы между этапами оказываются размытыми, а способ исполнения и способ конспирации фактически сливаются в единый непрерывный процесс.

Содержание преступных операций варьируется в зависимости от процессуальной позиции участника в иерархической системе наркотического сбыта. Для исполнителей низшего звена подготовительная фаза предполагает: установление контакта с сетевым наркомаркетом через специализированные интернет-платформы или защищённые каналы связи; получение координат крупной партии из оптового тайника; расфасовку полученного объёма на дозированные единицы; рекогносцировку территории для последующего оборудования закладок. Непосредственная реализация криминального замысла включает обустройство тайников-закладок, их фотофиксацию с привязкой к географическим координатам и последующую передачу описательных данных оператору сетевого магазина. Конспиративные мероприятия реализуются посредством использования технических средств с предустановленным специализированным программным обеспечением, изменения внешнего облика, привлечения номинальных лиц, смены локаций, противодействия следствию путём сообщения заведомо ложных сведений и

эксплуатации многоуровневых финансовых конструкций для вывода средств из теневого оборота.

Обстановочные условия обладают двойственной природой, совмещая физическое пространство (тайниковые точки в городской и природной среде, используемые для фасовки помещения, транспортные средства) и виртуальную плоскость (анонимные торговые площадки, криптозащищённые мессенджеры, платёжные системы на основе блокчейн-технологий). Эмпирический материал свидетельствует о том, что местонахождение наркосодержащих объектов определяется посредством GPS-координат с применением как общедоступных картографических сервисов, так и специализированного программного обеспечения, повышающего точность геолокации до одного метра. К координатам прилагается детализированное описание локации с приложением фотоизображения, размещаемого на интернет-хостингах и пересылаемого в виде ссылок внутри преступного сообщества.

Следообразовательная картина демонстрирует специфическое сочетание материальных и виртуальных следов. Материально-фиксируемые следы представлены дактилоскопическими отпечатками на упаковках, самими психоактивными веществами в тайниковых точках, упаковочными материалами, транспортными средствами. Цифровой компонент включает IP-адреса, идентификаторы сетевого оборудования, геолокационные маркеры, транзакционные записи в электронных платёжных системах, текстовые массивы переписки, интернет-историю. Приоритеты в доказывании всё более отчётливо смещаются в сторону электронных информационных носителей, что обусловлено объективными тенденциями цифровизации преступной среды.

Субъектный состав в сфере дистанционного наркотрафика отличается высокой степенью ролевой дифференциации. Криминалистическая практика позволяет выделить следующие функциональные позиции:

Высшее звено (организационный центр) — субъект, занимающий доминирующее положение в иерархической структуре. В его компетенцию входят: организация стабильных каналов поступления наркотических средств, создание и администрирование интернет-ресурса, ценовое регулирование, предпродажная подготовка, стратегическое руководство, разработка конспиративных протоколов, подбор новых участников, контроль финансовых потоков.

Региональный менеджер (куратор) — субъект, ответственный за организацию регионального сегмента сбытовой сети. Его функции включают селекцию и адаптацию участников для работы на закреплённой территории, координацию их деятельности, разрешение конфликтных ситуаций. Куратор контролирует работу операторского звена и обеспечивает соблюдение режима конспирации на региональном уровне.

Операторское звено («диспетчер», «селлер») — субъект, обеспечивающий медиацию между конечными потребителями и закладочным персоналом через цифровые каналы связи. Оператор аккумулирует заявки от потребителей, определяет способ оплаты, контролирует поступление средств, после чего передаёт координаты закладки. В компетенцию оператора входит также внесение крупного депозита организатору, найм экспедиторов, передача адресов оптовых партий лицам, ответственным за складское хранение, размещение адресов в системе моментальных интернет-магазинов, мониторинг продаж. Всё более широкое распространение получают системы на основе искусственного интеллекта, полностью замещающие оператора и обеспечивающие автоматизированное информирование клиентов об ассортименте, стоимости и оформлении заказов.

Исполнительское звено («закладчик») — субъект, непосредственно размещающий тайниковые точки с наркотическими средствами. Закладчик получает от оператора адреса с небольшими партиями наркотиков, расфасовывает их на розничные единицы, размещает в тайниках, производит

фотофиксацию и передаёт координаты оператору. Статистика свидетельствует, что именно закладчики являются наиболее уязвимым элементом криминальной цепочки и чаще других привлекаются к уголовной ответственности.¹

Представленная классификация дополняется такими ролевыми позициями, как вербовщик (осуществляет рекрутинг закладчиков через интернет-форумы), хранитель мини-склада (принимает от оператора адреса с небольшими партиями и осуществляет их фасовку), кассир (финансовый менеджер, обеспечивающий консультирование по финансовым вопросам, аккумуляцию отчётов о продажах, обналичивание средств, открытие электронных кошельков), системный администратор (консультирует членов группы по техническим аспектам безопасности, обеспечивает функционирование интернет-ресурса).

Конспиративные мероприятия, применяемые в криминальной среде, формируют многоуровневую систему противодействия правоохранительным органам. К числу наиболее востребованных мер относятся: использование криптостойких мессенджеров с OTR-шифрованием; эксплуатация анонимных интернет-площадок в сети TOR, специализирующихся на наркосбыте; применение электронных денег и криптовалютных инструментов; привлечение подставных лиц для регистрации финансовых операций; установка специализированных программ-сейфов, создающих зашифрованные контейнеры и изолированные сегменты в операционных системах мобильных устройств.

Организационно-структурные параметры преступных формирований демонстрируют вариативность в зависимости от масштаба деятельности. Разветвлённая структура с задействованием всех перечисленных ролевых позиций характерна для межрегиональных криминальных сетей.

¹ Моисеев, А.М. Криминалистические признаки наркосбыта посредством Интернет / А.М. Моисеев, С.В. Кондратюк // Балканско научно обозрение. — 2017. — № 1. — С. 29-33.

Региональные группы имеют более компактную конфигурацию, часто совмещая несколько функций в рамках одного субъекта, что сводит их организацию к 3–4 ролевым составляющим. Типовая схема функционирования регионального формирования выглядит следующим образом: организаторы приобретают оптовые партии, осуществляют фасовку, изготавливают закладки с запасом на несколько суток и передают описания операторам. Операторы через социальные сети или сайты вакансий подбирают курьеров, предлагая привлекательную оплату, после трудоустройства передают им адрес закладки с мелкооптовой партией. Курьеры размещают розничные дозы по тайниковым точкам и информируют оператора, который принимает заказы от потребителей, определяет способ оплаты, контролирует поступление средств и сообщает данные о местонахождении закладки.

Резюмируя изложенное, следует констатировать, что структурно-криминалистическая модель преступлений, связанных с незаконным оборотом наркотических средств с использованием телекоммуникационных сетей, отражает качественно новый уровень организации наркобизнеса. Интеграция цифровых технологий на всех этапах — от коммуникации и расчётов до сокрытия следов — в сочетании с жёсткой иерархией, функциональной специализацией и многоуровневой конспирацией существенно осложняет деятельность по предупреждению, выявлению, раскрытию и расследованию таких деликтов. Указанные обстоятельства настоятельно требуют переосмысления устоявшихся методических подходов и выработки специализированных тактических рекомендаций, адекватных современным реалиям наркокриминала.

§ 1.2. Цифровые следы как элемент криминалистической характеристики: классификация и особенности обнаружения

Современный этап эволюции криминалистической науки ознаменован активным переосмыслением классической теории следов под влиянием тотальной цифровизации общественных отношений. Практика показывает, что процессы цифровизации привели к появлению новой разновидности следов — цифровых. В структуре преступлений, сопряжённых с незаконным оборотом наркотических средств с использованием телекоммуникационных сетей, на первый план выходит специфическая разновидность следовой информации — цифровые следы, выступающие в качестве ключевого источника доказательственной информации. Согласно мнению различных авторов, при расследовании более 90 % всех зарегистрированных преступлений обнаруживаются цифровые следы¹, которые в результате многоэтапных процессов обнаружения, фиксации и изъятия преобразуются в такой вид доказательств, как цифровые доказательства.

Понятие и юридическая природа цифрового следа. Вопросы терминологического определения и сущностной характеристики цифровых следов выступают предметом активной научной дискуссии. В литературе встречаются различные подходы к обозначению данного феномена. В. А. Мещеряков вводит понятие «виртуальные следы», понимая под ними любое изменение состояния автоматизированной информационной системы, связанное с событием преступления, представленное в виде компьютерной

¹ Беляков, А.А. Тактические особенности работы с электронно-цифровыми следами на месте происшествия / А.А. Беляков, В.Ю. Иванов // Криминалистика: вчера, сегодня, завтра. — 2021. — № 4 (20). — С. 18.

информации и зафиксированное на материальном носителе.¹ В.Б. Вехов, в свою очередь, оперирует категорией «электронные следы», подразумевая информацию, содержащуюся на определённых электронных носителях. Наиболее доктринально разработанным представляется понятие «цифрового следа», предложенное Е.Р. Россинской, которая определяет его как «криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде, в процессе её возникновения, обработки, хранения и передачи».²

Принципиальное значение для понимания процессуального статуса цифровых следов имеет вопрос об их отнесении к материальным либо идеальным следам. Р.А. Дерюгин и А.А. Жижелева полагают, что цифровые следы занимают промежуточное положение между материальными и идеальными, не будучи в полной мере отнесёнными ни к одной из этих категорий. В.Б. Вехов, Б.П. Смагоринский и С.А. Ковалев характеризуют компьютерную информацию как «невидимые материальные следы». Однако наиболее аргументированной представляется позиция Е.Р. Россинской, согласно которой «по природе цифровые следы являются следами материальными», поскольку они содержатся на материальных носителях и неотделимы от них. Данный вывод имеет важное процессуальное значение, поскольку определяет возможность применения к работе с цифровыми следами общих правил собирания, фиксации и изъятия материальных объектов, предусмотренных уголовно-процессуальным законодательством.

Классификация цифровых следов применительно к наркопреступлениям. В криминалистической науке предложены различные основания для систематизации цифровых следов. Е.Р. Россинская классифицирует их по

¹ Мещеряков, В.А. Виртуальные следы в раскрытии и расследовании преступлений / В.А. Мещеряков // Информационное право. – 2017. – № 3. – С. 22–27.

² Россинская, Е.Р. Цифровые следы как объект судебной экспертизы / Е.Р. Россинская // Теория и практика судебной экспертизы. – 2019. – № 1. – С. 8–15.

месту хранения, выделяя следы: 1) на отдельных носителях; 2) в компьютерных системах и сетях. В контексте преступлений, связанных с незаконным оборотом наркотических средств, наиболее актуальным является рассмотрение цифровых следов, хранящихся именно в компьютерных сетях, что обусловлено спецификой бесконтактных способов сбыта.

К числу наиболее часто встречающихся цифровых следов по исследуемой категории дел относятся: IP-адреса, фотографии на мобильном устройстве закладок и тайников с наркотическим средством, переписки в мессенджерах с участниками преступной группы или ботом интернет-магазина, подписки на тематические Telegram-каналы, используемые как площадка для размещения интернет-магазина, зарегистрированный аккаунт на сайте интернет-магазина. Кроме того, в процессе расследования фиксируются такие сведения, как идентификаторы сетевого оборудования (MAC-адреса, IMEI-коды), протоколы соединений, криптовалютные транзакции, метаданные мультимедийных файлов (геотеги фотографий закладок, время создания).

Специфика обнаружения цифровых следов в условиях анонимизации. Деятельность преступных групп в сфере наркотрафика характеризуется активным применением мер конспирации, направленных на сокрытие цифровых следов. В этих целях злоумышленники используют средства анонимизации: VPN-сеть, TOR, SSH-туннели. Например, сеть TOR позволяет скрыть IP-адрес с помощью направления интернет-трафика через анонимные прокси-серверы, что позволяет сохранять анонимность пользователя. В последние годы наркорынок преимущественно эмигрировал на площадку мессенджера «Telegram», что объясняется простотой его использования, общедоступностью и гарантированной анонимностью. На просторах «Telegram» можно найти как открытые, так и закрытые каналы (чаты, боты), которые предоставляют пользователям информацию о наркотических средствах и их воздействии, о способах изготовления и

производства наркотиков, способах приобретения приспособлений для употребления.

Особую сложность для правоохранительных органов представляет доступ к ресурсам сети Даркнет (Tor, I2P). Исследования показывают, что усилия по расследованию и деанонимизации подозрительных пользователей сталкиваются с трудностями из-за роста Даркнета и ограничений существующих инструментов и методов. Именно поэтому даркнет-площадки являются основной средой функционирования крупных интернет-магазинов по продаже наркотиков.

Вместе с тем, как подчеркивают специалисты, полностью скрыть своё присутствие в сети невозможно. Даже малозначительные действия любой давности могут предоставить информацию о личности пользователя. Для установления реального IP-адреса злоумышленника, использующего анонимайзеры, следователи могут направлять запросы владельцам сервисов анонимизации, однако не все из них ведут журналы посещений, что создаёт дополнительные препятствия.

Процессуальные аспекты фиксации и изъятия цифровых следов. Важнейшей проблемой, выявляемой следственной практикой, является отсутствие унифицированной методики работы с цифровыми следами, что приводит к ситуации, когда имеющие значение для дела цифровые следы не становятся в результате процессуальных действий доказательствами. Сложность заключается в том, что цифровые следы представляют собой компьютерную информацию, которая не может быть воспринята органами чувств непосредственно и неотделима от своего материального носителя.

Для эффективной фиксации цифровых следов — переписки, объявлений, транзакций — следователям рекомендуется привлекать специалистов в области компьютерных технологий. Участие специалиста необходимо как при

осмотре технического средства подозреваемого, так и при изъятии информации из телекоммуникационного пространства. Как подчёркивается в научной литературе, следователь, даже самый опытный, не обязан разбираться в технических тонкостях работы операционных систем, шифрования и удалённого доступа; его задачей является сохранение данных в неизменном виде и предотвращение их дистанционного удаления.

В протоколе следственного действия должна быть зафиксирована история переписки, относящаяся к событию преступления, а также сведения о приложениях для электронных платежей, переводах денежных средств, номерах счетов. При изъятии электронных носителей подозреваемых и ознакомлении с хранящейся на них перепиской процессуальных проблем не возникает, поскольку УПК РФ предусматривает такое следственное действие, как осмотр предметов. Однако получение переписки у оператора связи сопряжено с необходимостью получения судебного решения, поскольку в силу ст. 23 Конституции РФ тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений охраняется законом. Переписка, сохранившаяся на жестком диске пользователя, уже выбыла из ведения оператора связи, соответственно, на неё не распространяется режим тайны связи.¹

Таким образом, система цифровых следов в преступлениях, связанных с незаконным оборотом наркотиков через телекоммуникационные сети, представляет собой сложный многоуровневый комплекс, требующий для своего обнаружения, фиксации и изъятия применения специальных познаний в области компьютерных технологий, а также выработки унифицированных тактико-криминалистических подходов, отвечающих динамике развития цифровой среды и конспиративных приёмов, используемых криминальными структурами.

¹ Карлов, А.Л. Проблемы получения электронной переписки в уголовном судопроизводстве / А.Л. Карлов // Уголовное судопроизводство. — 2018. — № 4. — С. 41.

§ 1.3. Типичные исходные следственные ситуации и алгоритмы построения следственных версий

Результативность расследования преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием телекоммуникационных сетей, напрямую зависит от того, насколько точно следователь способен идентифицировать исходную следственную ситуацию и на её основе выдвинуть обоснованные версии. Как отмечают исследователи, современная наркопреступность характеризуется высокой степенью организованности и многоуровневостью, действуя без привязки к каким-либо регионам, а способы подготовки и осуществления преступлений последовательно усложняются с развитием информационных технологий.

Понятие и классификация следственных ситуаций. Под следственной ситуацией в криминалистике понимается совокупность условий, в которых на определённом этапе осуществляется расследование, включающая наличие и характер доказательственной и ориентирующей информации, возможности субъекта доказывания и иные факторы, оказывающие влияние на выбор направления и методов расследования. Многие авторы выделяют четыре базовых варианта развития следственной ситуации, наиболее характерных для современной правоприменительной практики.

Первая ситуация: задержание курьера-закладчика с поличным. Данная ситуация признаётся наиболее благоприятной для расследования. Она

складывается, когда лицо задерживается сотрудниками полиции непосредственно в момент совершения преступления либо сразу после его окончания. В распоряжении следователя имеются протокол изъятия наркотического средства, результаты исследования изъятых веществ, показания задержанного, а также его мобильное устройство, содержащее координаты тайников, переписку с оператором и сведения о произведённых платежах.

В рамках данной ситуации критически значимым становится немедленное изъятие и процессуальное закрепление данных мобильного телефона задержанного. Как обоснованно подчёркивается в научной литературе, именно в мессенджерах (Telegram, WhatsApp) и приложениях для заметок чаще всего хранятся координаты тайников, фотоматериалы с изображением мест закладок, а также переписка с куратором.¹ Осмотр смартфона позволяет трансформировать исходно простую ситуацию (задержание лица с наркотическим средством) в перспективную с точки зрения установления и документирования цепочки сбыта.

Алгоритм действий предполагает: незамедлительное проведение личного обыска задержанного; изъятие и осмотр мобильного устройства с соблюдением процессуального порядка; документирование геолокационных данных; допрос задержанного с использованием тактических приёмов, направленных на получение информации об организаторах преступной схемы и иных соучастниках.

Вторая ситуация: обнаружены наркотические средства, однако лицо, их оставившее, не установлено. Такая конфигурация складывается при выявлении тайников-закладок случайными гражданами или сотрудниками полиции без одновременного задержания курьера. Характерной особенностью

¹ Иванова, К.С. Расследование незаконного сбыта наркотических средств: специфика следственных действий в цифровой среде / К.С. Иванова // Молодой ученый. — 2025. — № 49 (600). — С. 336.

данной ситуации является отсутствие установленного субъекта преступления, что предопределяет особую направленность деятельности следователя.

В соответствии со ст. 144 УПК РФ в этом случае проводится осмотр места происшествия. Ключевая проблема — отсутствие установленного субъекта преступления, что требует максимально детальной фиксации особенностей упаковки (характер изолянты, тип зип-лок-пакета, наличие магнита и т. п.), поскольку способ упаковки нередко позволяет отнести тайник к определённому интернет-магазину. Назначается дактилоскопическая и молекулярно-генетическая экспертиза изъятых упаковочных материалов, проводится анализ биллинга и соединений абонентских номеров в зоне обнаружения тайника в предполагаемый период его закладки. Следственные версии строятся вокруг гипотетических моделей преступной группы: является ли обнаруженный тайник разовым действием или элементом систематической деятельности, действует ли преступник один или в составе группы.

Третья ситуация: поступила оперативная информация о готовящемся либо уже начавшемся сбыте, личность предполагаемого участника известна. Данная ситуация характеризуется наличием опережающей (превентивной) информации и развивается по логике реализации результатов оперативно-розыскной деятельности. Следователь в тесном взаимодействии с оперативными подразделениями разрабатывает план задержания. Наиболее результативным инструментом выступает проведение ОРМ — наблюдение или проверочная закупка (включая дистанционные форматы).

Особенностью рассматриваемой ситуации является необходимость системного документирования цифровых финансовых операций. Если ранее проверочная закупка связывалась с передачей меченых денежных купюр, то сегодня речь чаще идёт о переводе криптовалюты или фиатных средств на электронные кошельки. Следователь обязан заблаговременно привлечь специалиста, способного обеспечить фиксацию электронных следов

транзакций и скриншотов переписки, поскольку преступники нередко удаляют чаты дистанционно.

Четвёртая ситуация: лицо задержано после приобретения наркотического средства (потребитель). В таком случае следственная ситуация приобретает дуалистический характер: одновременно расследуется эпизод приобретения/хранения (ст. 228 УК РФ) и эпизод сбыта неустановленным лицом (ст. 228.1 УК РФ). Приоритетной задачей становится проверка показаний на месте: задержанный демонстрирует точное место, где им был поднят «клад». Осмотр соответствующего участка местности позволяет зафиксировать географические координаты и соотнести их с данными, содержащимися в мобильном телефоне задержанного.¹

Существенный аспект связан с необходимостью целенаправленной работы с задержанным, направленной на получение доступа к его аккаунту в теневом интернет-магазине. Это открывает возможности для изучения «витрины» магазина, используемых способов оплаты и, в ряде случаев, для выхода на организаторов преступной деятельности посредством анализа блокчейн-транзакций.

Методика построения следственных версий. Независимо от исходной ситуации, процесс построения версий должен основываться на тщательном анализе всей доступной информации и учитывать современные способы сокрытия преступлений в цифровой среде. Как показано на примерах завершённых расследований, преступные группы используют разветвлённые иерархические структуры с чётким распределением функций: от получения оптовых партий и фасовки до розничной реализации через систему тайников. При этом организация поставок, хранения и коммуникации между

¹ Залескина, А.Н. Бесконтактный сбыт наркотических средств как элемент криминалистической характеристики преступлений / А.Н. Залескина, И.А. Яцкина, В.С. Замашников // Философия права. — 2025. — № 4 (115). — С. 109-110.Ф

участниками осуществляется с использованием сети Интернет и мессенджеров.

Проверка выдвинутых версий осуществляется путём производства следственных действий и оперативно-розыскных мероприятий. При этом следственная ситуация более не ограничивается исключительно физическим пространством; она неизбежно включает виртуальную составляющую (облачные хранилища, мессенджеры и иные цифровые сервисы), доступ к которой должен быть обеспечен в наиболее ранние часы после выявления преступления.

Таким образом, успешное расследование преступлений в сфере бесконтактного наркотрафика невозможно без чёткого представления о типичных исходных следственных ситуациях и владения алгоритмизированными методиками построения и проверки следственных версий. Каждая из описанных ситуаций требует специфического тактического подхода, однако всех их объединяет необходимость максимально полного использования цифровых следов и организации эффективного взаимодействия с оперативными подразделениями на всех этапах расследования. Именно оперативное получение и процессуальное закрепление цифровых следов становится ключевым условием успешного расследования преступлений, предусмотренных ст. 228–228.1 УК РФ.

ГЛАВА II. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С УЧЁТОМ СПЕЦИФИКИ ЦИФРОВОЙ СРЕДЫ

§ 2.1. Тактика осмотра цифровых носителей информации и изъятия электронных доказательств

Осмотр цифровых носителей и изъятие электронных доказательств занимают центральное место в системе следственных действий при расследовании наркопреступлений, совершаемых с использованием телекоммуникационных сетей. Как справедливо отмечается в научной литературе, при расследовании более 90 % всех зарегистрированных преступлений обнаруживаются цифровые следы, которые в результате процессуального оформления трансформируются в цифровые доказательства. Вместе с тем отсутствие унифицированных подходов к работе с электронными носителями нередко приводит к тому, что значимая для следствия информация не приобретает доказательственного статуса, что негативно сказывается на эффективности расследования.

Понятие цифрового следа и его процессуальное значение. Вопросы терминологического определения цифровых следов остаются дискуссионными в научной среде. В. А. Мещеряков ввёл понятие

«виртуальные следы», понимая под ними любое изменение состояния автоматизированной информационной системы, связанное с событием преступления. В.Б. Вехов оперирует категорией «электронные следы», подразумевая информацию, содержащуюся на электронных носителях. Наиболее разработанным представляется понятие «цифрового следа», предложенное Е.Р. Россинской, которая определяет его как «криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде, в процессе её возникновения, обработки, хранения и передачи».

Принципиальное значение имеет вопрос об отнесении цифровых следов к материальным либо идеальным. Р.А. Дерюгин и А.А. Жижелева полагают, что цифровые следы занимают промежуточное положение между этими категориями. В.Б. Вехов, Б.П. Смагоринский и С.А. Ковалев характеризуют компьютерную информацию как «невидимые материальные следы». Е.Р. Россинская аргументированно утверждает, что «по природе цифровые следы являются следами материальными», поскольку они содержатся на материальных носителях и неотделимы от них. Данный вывод имеет важное процессуальное значение, определяя возможность применения к работе с цифровыми следами общих правил собирания и изъятия материальных объектов.

Правовое регулирование изъятия электронных носителей. С 8 января 2019 года в УПК РФ действует ст. 164.1¹, закрепляющая особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. Указанная норма устанавливает, что изъятие электронных носителей допускается только в случаях, когда: вынесено постановление о назначении судебной экспертизы; изъятие

¹ Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. — 2001. — № 52 (ч. 1), ст. 4921 (в ред. от 02.08.2019). — Ст. 164.1.

производится на основании судебного решения; либо на носителях содержится информация, полномочиями на хранение которой владелец не обладает, либо копирование может повлечь утрату или изменение информации. Критически важным является требование об изъятии электронных носителей исключительно с участием специалиста.

Как отмечает В.М. Герасенков, изъятие и осмотр электронных носителей без разрешения суда нарушает основополагающие принципы законности, поскольку следователь одномоментно получает доступ к личной переписке, контактам, сведениям о расчётных счетах и вкладах.¹

Осмотр мобильных устройств. Среди всех видов цифровых носителей наиболее значимыми являются мобильные телефоны и смартфоны, в памяти которых содержится информация о преступных контактах, координатах тайников и финансовых операциях. Первоочередной задачей при обнаружении мобильного устройства является его изоляция от внешних сетей во избежание дистанционной блокировки или удаления информации. На практике данная мера реализуется путём перевода устройства в режим «полёта» либо помещения его в экранирующий контейнер (пакет Фарадея).

Для извлечения криминалистически значимой информации применяются специализированные аппаратно-программные комплексы. Среди зарубежных разработок наиболее распространён UFED (Universal Forensic Extraction Device, «Универсальное устройство для извлечения криминалистических данных») компании Cellebrite, позволяющий извлекать данные с обходом блокировок, восстанавливать удалённую информацию и работать с повреждёнными устройствами. Применение UFED позволяет извлекать полную информацию из памяти мобильных устройств, включая удалённые

¹ Герасенков, В.М. Процессуальные аспекты изъятия электронных носителей информации / В.М. Герасенков // Российский следователь. — 2020. — № 7. — С. 35.

данные, фотографии мест с географическими координатами, переписки в мессенджерах.¹

Отечественным аналогом является программное обеспечение «Мобильный Криминалист» компании Oxygen Software. Данный АПК позволяет: получать общую информацию об устройстве; изучать SMS, MMS, фотографии, аудио- и видеозаписи; восстанавливать удалённые данные; прослеживать маршруты передвижения владельца. Программное обеспечение включает технологии искусственного интеллекта, позволяющие ускорить анализ цифровых доказательств, в том числе распознавать текст на изображениях. Как подчёркивается в исследованиях, «Мобильный Криминалист» способен извлекать информацию из облачных хранилищ (iCloud, Google, Dropbox) даже с заблокированных устройств.

Фиксация результатов осмотра. Процессуальное оформление результатов осмотра цифровых носителей имеет определяющее значение для последующего использования полученной информации в качестве доказательства. В протоколе осмотра должны быть отражены: внешнее состояние изъятых устройств; способы доступа к информации; перечень обнаруженных файлов с указанием наименований, размеров, дат создания и модификации; содержание текстовых сообщений, относящихся к событию преступления; сведения о финансовых операциях; координатные данные.

Особую роль играет использование технических средств документирования. Как показывает судебная практика, обязательной является фиксация следователем с помощью фото- и видеосъёмки всего процесса использования аппаратно-программных комплексов, с последующим приобщением фототаблицы к протоколу осмотра. Полное отсутствие каких-

¹ Белей, А.В. Тактика применения современных технико-криминалистических средств при сборании криминалистически значимой информации / А.В. Белей // Российский следователь. — 2022. — № 8. — С. 4.

либо средств фиксации должно влечь недопустимость полученных доказательств.

При изъятии цифровых носителей следует избегать негативного воздействия на них: прямых солнечных лучей, нагрева, грубого физического или электромагнитного воздействия, которое может повредить хранящуюся информацию. При этом, как справедливо отмечается в литературе, следователь не обязан разбираться в технических тонкостях работы операционных систем; его задачей является сохранение данных в неизменном виде и предотвращение их дистанционного удаления, для чего и привлекается специалист.

Таким образом, осмотр цифровых носителей при расследовании наркопреступлений, совершаемых через телекоммуникационные сети, представляет собой комплексное следственное действие, успешность которого определяется сочетанием процессуальной грамотности, тактической продуманности и технической оснащённости. Соблюдение требований ст. 164.1 УПК РФ, правильное применение специализированных АПК и надлежащая фиксация результатов создают необходимые условия для формирования допустимых и достоверных доказательств по уголовным делам данной категории.

§ 2.2. Тактические приемы допроса при расследовании «бесконтактных» сбытов наркотических средств

Допрос участников преступной деятельности в сфере бесконтактного сбыта наркотиков признаётся одним из наиболее сложных следственных действий, что обусловлено как спецификой самой противоправной деятельности, так и психологическими особенностями лиц, вовлечённых в сетевой наркобизнес. Широкое применение интернет-технологий в распространении синтетических наркотиков ставит перед правоохранительными органами серьёзные вызовы. Затруднения при производстве допросов усугубляются тем, что участники сетевых наркопреступлений активно используют анонимные и зашифрованные каналы связи, включая мессенджеры и торговые площадки в даркнете, что значительно усложняет процесс идентификации фигурантов и документирования доказательств их причастности к преступной деятельности.

Дифференциация допрашиваемых лиц. При допросе лиц, входящих в структуру интернет-магазина, специализирующегося на незаконном сбыте наркотических средств, тактические приёмы должны дифференцироваться в зависимости от процессуального положения допрашиваемого и его функционального места в преступной иерархии. На основе изучения материалов уголовных дел сформулирован перечень вопросов, подлежащих выяснению при допросе участников организованных преступных формирований, занимающихся наркоторговлей через интернет-площадки. В этом контексте особого внимания заслуживают тактические особенности допроса организатора, оператора, наркокурьера и закладчика.

Допрос закладчика. Закладчики признаются наиболее уязвимым звеном преступной цепи и чаще иных участников привлекаются к уголовной ответственности. Как показывает эмпирический материал, закладчик, как правило, не знаком лично с другими членами преступного сообщества, общение осуществляется через мессенджеры, а личность оператора остается для него неизвестной. В связи с этим тактика допроса закладчика должна быть направлена на получение максимально полной информации о структуре

преступной организации и методах взаимодействия её участников. Методика допроса закладчика предполагает выяснение следующих обстоятельств: квалификационные требования¹, предъявлявшиеся к закладчику при трудоустройстве; процедуры, предпринятые для оформления на работу; методы уведомления о принятии на работу; наличие специфических указаний от оператора или курьера; дополнительные обязанности, включая продолжительное хранение, фасовку и упаковку наркотиков; условия оплаты и размер вознаграждения за выполнение каждой закладки; особенности взаимодействия с другими участниками преступной деятельности.

Допрос организатора. Организатор занимает высшую ступень в преступной иерархии и располагает наиболее полной информацией о деятельности всей преступной сети. Однако допрос организатора, как правило, протекает в конфликтной ситуации, поскольку данное лицо осознаёт тяжесть предъявляемого обвинения и активно противодействует следствию. Тактические приёмы допроса организатора должны учитывать его высокий интеллектуальный уровень, осведомлённость в вопросах конспирации и нежелание давать правдивые показания. В ходе допроса организатора необходимо выяснить: каналы поставки наркотических средств; создание и администрирование интернет-ресурса; ценовое регулирование и предпродажную подготовку; структуру руководства деятельностью группы; разработку мер безопасности и конспирации; способы вовлечения новых участников; контроль финансовых потоков и распределение доходов. При этом тактически значимым является использование цифровых доказательств (переписки, транзакций, логов доступа) для изобличения организатора, а также проведение очных ставок с изобличающими его соучастниками.

¹ Саркисян, К.Т. Расследование незаконного оборота наркотических средств, совершенного с использованием компьютерных сетей : дис. ... канд. юрид. наук / К. Т. Саркисян. — М., 2020. — С. 96-98.

Допрос оператора. Оператор выступает в качестве посредника между организатором, закладчиками и потребителями. Его функционал включает приём и обработку заказов, координацию деятельности закладчиков, контроль оплаты, ведение отчётности о продажах. В ходе допроса оператора подлежат выяснению: способы коммуникации с закладчиками и потребителями; используемые мессенджеры и иные средства связи; применяемые системы шифрования и анонимизации; порядок передачи координат закладок; финансовые схемы и способы получения вознаграждения; информация об организаторе и иных соучастниках; технические средства, используемые для обеспечения деятельности. Тактически значимым является оперативное проведение допроса оператора сразу после задержания, когда фактор внезапности ещё не утратил своего воздействия.

Допрос свидетелей. Тактика допроса свидетелей по делам о бесконтактном сбыте наркотиков также имеет свою специфику. На основе анализа уголовных дел выделяются четыре группы свидетелей: 1) непосредственно участвовавшие в документировании преступных действий (сотрудники полиции, понятые); 2) оказавшиеся очевидцами преступления либо задержания подозреваемых; 3) имеющие опосредованное отношение к лицам, совершившим преступление, месту преступления (например, предоставившие квартиру в аренду закладчикам); 4) не имеющие отношения к деятельности интернет-магазина, но владеющие важной информацией для раскрытия и расследования незаконного сбыта.¹

Допрос свидетелей первой группы осуществляется в бесконфликтной ситуации. В ходе допроса сотрудников полиции необходимо получить полное представление о событии преступления, источниках информации о нём, проведённых мероприятиях. Круг вопросов включает: в каком подразделении

¹ Введенская, О.Ю. Первоначальный этап расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий : учебное пособие / О.Ю. Введенская. — Краснодар: Краснодарский университет МВД России, 2023. — С. 82-83.

проходит службу; в какой период и в отношении кого осуществлялись оперативно-розыскные мероприятия; осуществлялось ли задержание и при каких обстоятельствах; производился ли досмотр задержанных; были ли обнаружены объекты и их внешний вид.

Психологические аспекты допроса. Проведение первичного допроса обязывает следователя к максимальной концентрации и тщательному наблюдению за психофизиологическими реакциями допрашиваемого. Как правило, допрос инициируется либо по итогам комплекса оперативно-розыскных мероприятий, либо в результате задержания лица на месте преступления. Для формирования доверительного контакта рекомендуется придерживаться тактики вежливого общения: проявить участие к состоянию здоровья задержанного и выразить корректное сожаление о необходимости проведения следственных действий. Оптимальным началом беседы станет обсуждение нейтральных тем, предпочтительно связанных с личностью самого допрашиваемого.

Как показывает практика, допрос членов организованных преступных формирований, особенно первоначальный, всегда происходит в конфликтной ситуации: допрашиваемый либо не даёт никаких показаний, либо даёт показания ложные. Поскольку незаконные действия с наркотическими средствами преступниками тщательно маскируются, оперативной информации о составе преступного формирования, его руководителе и иных обстоятельствах на первоначальном этапе бывает недостаточно. Поэтому получить такую информацию можно только от одного из задержанных членов формирования.

На изменение конфликтной ситуации в бесконфликтную по делам, связанным с незаконным оборотом наркотических средств, влияют следующие моменты: разъяснение особенностей досудебного соглашения о сотрудничестве и применения мер государственной защиты; психическое состояние допрашиваемого; его личностные особенности; интерес к

семейному положению допрашиваемого; его прошлому; сочувствие к допрашиваемому.

Специфика предмета допроса. Как показывает анализ уголовных дел, подозреваемые и обвиняемые в большинстве случаев не только не сообщают каких-либо ценных для расследования показаний, но и пытаются использовать допрос в своих интересах. В ходе допроса подозреваемого необходимо сопоставлять данные, имеющиеся в распоряжении следователя, и данные, полученные от самого подозреваемого. О совершенном преступлении от допрашиваемого следует добиваться детального рассказа выяснять причину совершения преступления, его действия, действия его соучастников. Если в совершении преступления участвовало несколько лиц, а задержан только один, то у допрашиваемого выясняется информация о его сообщниках, их именах, прозвищах, характерных привычках, внешнем виде, месте жительства.

При допросе подозреваемого в незаконном обороте наркотических средств целесообразно придерживаться следующего перечня вопросов:

1. обстоятельства приобретения (источник, время, место, стоимость, способ оплаты);
2. сведения о продавце (личность, контактные данные, приметы);
3. цель приобретения (личное потребление или сбыт);
4. в случае установления цели сбыта — детали планируемой преступной деятельности (каналы реализации, круг потенциальных покупателей, ценообразование);
5. условия хранения изъятых веществ;
6. наличие связей в среде потребителей и распространителей наркотических средств.

Таким образом, эффективность допроса в рамках расследования бесконтактного сбыта наркотиков напрямую зависит от применения

дифференцированного подхода к субъектам, установления доверительного контакта и стратегического использования цифровых следов для опровержения ложных показаний. Ключевым фактором является разъяснение подозреваемому правовых последствий сотрудничества со следствием, так как искреннее содействие может быть учтено судом при назначении наказания.

§ 2.3. Организация и тактика обыска (выемки) у лиц, осуществляющих дистанционное управление наркотрафиком

Обыск и выемка относятся к числу ключевых следственных действий при расследовании уголовных дел о незаконном обороте наркотических средств, совершаемом с применением информационно-телекоммуникационных технологий. В отличие от «классических» наркопреступлений, бесконтактная модель сбыта характеризуется наличием разветвлённой системы тайников, использованием цифровых средств коммуникации и хранения информации, а также применением многоуровневых мер конспирации. В связи с этим тактика производства обыска и выемки приобретает существенные особенности, игнорирование которых снижает эффективность расследования.

Подготовительный этап обыска. Организационные мероприятия перед проведением обыска в ходе расследования бесконтактного наркотрафика включают ряд специальных действий, отсутствующих при традиционных наркопреступлениях. Обыск по таким делам рассматривается как неотложное следственное действие и обычно проводится в первые сутки после

возбуждения уголовного дела. Задержка в проведении недопустима, поскольку наиболее важные доказательства, подтверждающие факт преступления, обнаруживаются именно в ранний период после его совершения. Подготовка к обыску должна быть максимально быстрой и обязательно предусматривать элемент внезапности, поскольку без него существует высокая вероятность уничтожения улик как самим подозреваемым, так и его сообщниками.

Существенным элементом подготовки является полный анализ исходной информации о личности подозреваемого, его образе жизни, связях, маршрутах передвижения, способах и средствах совершения наркопреступления. Сбор данной информации, однако, иногда представляет проблему, поскольку не всегда возможно без проблем получить эти сведения, а от их изучения определяется тактика расследования. Кроме того, требуется определить круг лиц, подлежащих обыску, и последовательность проведения обысков. При расследовании преступлений, совершаемых организованной группой, высокую эффективность принесёт групповой обыск, проводимый несколькими следователями в одно и то же время в нескольких местах и у разных лиц, в целях предотвращения утечки информации о планируемых следственных мероприятиях среди участников преступных групп.

Для повышения результативности обыска следователю необходимо привлекать специалистов: сотрудников химических лабораторий, специалистов в области компьютерных технологий, а при наличии оснований — кинолога со специально обученной на обнаружение наркотиков собакой. Участие специалиста необходимо для правильного изъятия компьютерной техники, проведения первичного осмотра цифровых носителей и ориентирования на месте обыска в особенностях возможных наркотических средств и способов их маскировки.

Основанием производства обыска является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться

орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела. Обыск производится на основании постановления следователя, а в жилище — на основании судебного решения. Исключения составляют случаи, не терпящие отлагательства, когда обыск в жилище может быть произведён без судебного решения, однако следователь обязан не позднее трёх суток уведомить об этом судью и прокурора. Если судья признает действия незаконными, все полученные доказательства будут признаны недопустимыми.¹

Согласно действующему законодательству, перед началом обыска следователь обязан предложить лицу добровольно выдать предметы и документы, подлежащие изъятию. Однако данная процедура содержит правовой пробел: добровольная выдача части запрещенных веществ (например, наркотических средств) не гарантирует отсутствия у лица иных предметов, подлежащих изъятию. Кроме того, оценочное понятие «отсутствие оснований опасаться сокрытия» не имеет законодательной конкретизации. В связи с этим целесообразно закрепить обязательное проведение обыска вне зависимости от факта добровольной выдачи объектов.

Тактика обыска жилых и нежилых помещений. При обыске помещений, используемых участниками бесконтактного наркотрафика, следователь должен исходить из того, что данные помещения могут использоваться для различных целей: хранение наркотических средств, фасовка, оборудование мини-складов, временное проживание закладчиков, размещение серверного оборудования.

Поиск в местах, где осуществляется фасовка и складирование запрещенных веществ, должен охватывать как сами наркотики, так и инструменты, применяемые для их упаковки. Главная трудность состоит в

¹ Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 02.08.2019) // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. 1), ст. 4921. – Ст. 182.

том, что небольшие дозы психотропных препаратов способны незаметно скрываться в самых неожиданных предметах: от скрытых отсеков в стенах, мебели или подоконниках до обычных детских игрушек, продуктов питания, грунта в горшках с цветами, домашней аптечки (где они имитируют легальные лекарства) и даже пустот в книгах или каблуках обуви.

При проведении обыска приоритетной задачей является поиск цифровых носителей. Подлежат изъятию стационарные и портативные персональные компьютеры, смартфоны, флеш-накопители, маршрутизаторы, банковские карты, а также бумаги с паролями и данными о местоположении тайников. Лицам, находящимся на месте, категорически запрещается касаться техники. Важно корректно завершить работу программ перед обесточиванием (если это возможно), записать все ключи доступа и оградить устройства от сильных магнитных полей. Категорически недопустимо выключать работающую аппаратуру без фиксации текущих процессов, так как это грозит потерей данных, хранящихся в оперативной памяти.

Тактика обыска транспортных средств. Транспортные средства активно используются участниками бесконтактного наркотрафика для перевозки наркотических средств, а также для перемещения между тайниками. Во время осмотра автотранспорта важно помнить, что для тайного размещения запрещенных веществ могут использоваться самые разные участки машины: от стандартных ниш, приборной панели и дверных обшивок до моторного отсека и зоны запасного колеса. Отдельного внимания заслуживает изъятие навигаторов, бортовых компьютеров и видеорегистраторов, поскольку эти устройства часто хранят информацию о маршрутах и перемещениях владельца автомобиля.

Особенности изъятия криптовалютных активов. Растущая популярность криптовалют в незаконном обороте наркотических средств обуславливает необходимость приобретения следователем специфических компетенций при проведении обысков. В ходе осмотра объектов, принадлежащих

пользователям цифровых активов, следует обращать особое внимание на поиск и изъятие следующих элементов: физических носителей аппаратных кошельков; носителей информации, содержащих приватные ключи; записей с учётными данными для доступа к криптобиржам и обменным пунктам; а также специализированного программного обеспечения для управления криптовалютой, установленного на мобильных устройствах. Важно помнить, что криптовалюта может храниться в облачных хранилищах, и для её изъятия требуется своевременное направление соответствующих запросов. Современные методы анализа криптовалютных транзакций с использованием специализированных сервисов (например, Crystal blockchain) позволяют прослеживать транзакции, выявлять незаконные операции, связанные с наркоторговлей, а также фиксировать, изымать и арестовывать криптовалютные активы.

Фиксация результатов обыска. Процессуальная фиксация результатов обыска должна производиться с особой тщательностью, поскольку любое нарушение порядка изъятия может привести к признанию доказательств недопустимыми. В протоколе обыска должны быть подробно отражены: места обнаружения предметов и документов; их индивидуальные признаки; техническое состояние изъятых устройств; меры, принятые для обеспечения сохранности цифровой информации. Изъятые предметы, документы и ценности предъявляются понятым и другим присутствующим лицам, упаковываются и опечатываются на месте, что удостоверяется подписями указанных лиц.

Копия протокола вручается лицу, в помещении которого был произведён обыск, либо совершеннолетнему члену его семьи. При изъятии компьютерной техники рекомендуется составлять отдельную опись изымаемых устройств, а также фиксировать средствами фото- и видеосъёмки все этапы работы с устройствами на месте обыска. Изъятие осуществляется с участием понятых,

техника упаковывается с мерами по предотвращению разукомплектования и повреждения носителей информации.

Ключевым этапом сбора доказательств в рамках расследования бесконтактной наркоторговли выступает изъятие цифровых данных у хостинг-провайдеров, телекоммуникационных компаний, служб поддержки мессенджеров и площадок для криптовалютных операций. Процедура может осуществляться непосредственно на территории организации или путем отправки официальных запросов. Для установления фактов соединений абонентов требуется направлять запросы операторам сотовой связи, сопровождая их данными о базовых станциях и IMEI-номерах устройств. При этом важно учитывать, что не все интернет-провайдеры сохраняют логи посещений, а ряд администраторов мессенджеров отказывает правоохранным органам в предоставлении истории переписки пользователей. В подобных ситуациях необходимо прибегать к другим доступным источникам информации.

Таким образом, тактика обыска и выемки при расследовании преступлений в сфере бесконтактного наркотрафика представляет собой сложный комплекс организационных и тактических мероприятий, требующих учёта специфики цифровой среды, особенностей преступной иерархии и применяемых мер конспирации. Только комплексный подход, объединяющий традиционные криминалистические методы и современные технологии, позволяет обеспечить эффективное собирание доказательств по данной категории дел.

ГЛАВА III. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАССЛЕДОВАНИЯ И ПРОФИЛАКТИКА ЦИФРОВЫХ НАРКОПРЕСТУПЛЕНИЙ

§ 3.1. Организация взаимодействия следователя с оперативно-розыскными подразделениями и экспертными учреждениями

Эффективность противодействия преступлениям в сфере незаконного оборота наркотических средств, совершаемым с использованием телекоммуникационных сетей, находится в прямой зависимости от налаженного взаимодействия следователя с оперативно-розыскными подразделениями и экспертными учреждениями. По данным прокурорского надзора, в ряде регионов менее трети уголовных дел о наркопреступлениях раскрываются, а совершённые с использованием сети «Интернет» раскрываются в единичных случаях, что во многом обусловлено отсутствием слаженного взаимодействия заинтересованных ведомств.¹

Взаимодействие следователя с органами дознания регламентируется нормами Уголовно-процессуального кодекса РФ и Федерального закона «Об оперативно-розыскной деятельности»². Под взаимодействием

¹ Доклад Генеральной прокуратуры РФ о состоянии законности в сфере противодействия наркопреступности. — 2024. — URL: <https://genproc.gov.ru>

² Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (ред. от 02.12.2019) // Собрание законодательства Российской Федерации. – 1995. – № 33, ст. 3349

подразумевается скоординированная работа, опирающаяся на правовые нормы, между следственными и дознавательными структурами, которые обладают самостоятельностью в рамках своих полномочий. Такая деятельность направлена на расследование и предотвращение конкретного преступления посредством оптимального объединения специфических методов и инструментов, характерных для каждого из этих ведомств. Принципиальное значение имеет разграничение компетенций: следователь не вправе осуществлять оперативно-розыскные мероприятия, а сотрудник органа дознания может производить следственные действия лишь по поручению следователя.

Уголовно-процессуальный закон предусматривает несколько процессуально-правовых форм взаимодействия: уведомление следователя органом дознания о выявленном преступлении с принятием мер по охране места происшествия; осуществление оперативно-розыскных мероприятий по делам, переданным следователю, если лицо, совершившее преступление, осталось неизвестным; производство органом дознания отдельных следственных действий по поручению следователя; содействие сотрудников органа дознания следователю при производстве отдельных следственных действий. При этом следователь уполномочен давать органу дознания обязательные для исполнения письменные поручения о производстве следственных и иных процессуальных действий, а также об организации участия в следственном действии лица, участие которого признано необходимым.

Оптимальным механизмом координации действий считается формирование следственно-оперативных отрядов, куда входят следователи, оперативники, эксперты-криминалисты, кинологи и другие профильные специалисты. Именно создание таких узкоспециализированных подразделений обеспечивает наивысшую результативность взаимодействия,

позволяя максимально и всесторонне задействовать все ресурсы и возможности внутренних органов.

Ключевую роль играет согласованная организация работы по уголовному делу, включающая разработку межведомственного письменного плана, в котором фиксируется перечень требуемых следственных мероприятий и задачи для оперативных работников. Такая скоординированная деятельность особенно актуальна при расследовании тяжких и особо тяжких преступлений, если личность виновного не установлена. При этом совместное обсуждение стратегии расследования может проводиться многократно, если в процессе следствия возникают новые обстоятельства.

Тактические аспекты взаимодействия при расследовании наркопреступлений. Специфика бесконтактного наркотрафика предъявляет особые требования к организации взаимодействия. Как отмечают исследователи, структура дистанционного незаконного сбыта наркотических средств включает коммуникационную основу (мобильная связь, IP-телефония, интернет-мессенджеры), финансовую основу (электронные платёжные системы, криптовалюта, банковские карты), материально-техническую и логистическую основу, а также интеллектуальную основу — соучастников с чётким распределением ролей.¹ Сложная структура данного явления обуславливает необходимость применения интегрированной стратегии расследования, в рамках которой оперативные работники занимаются обнаружением и фиксацией противоправных действий, тогда как следователь осуществляет официальное оформление полученных материалов.

Важнейшим направлением взаимодействия является использование метода ретроспективного выяснения обстоятельств, подлежащих установлению. Данный метод применяется, когда первоначально необходимо

¹ Саркисян, К.Т. Расследование незаконного оборота наркотических средств, совершенного с использованием компьютерных сетей : дис. ... канд. юрид. наук / К. Т. Саркисян. — М., 2020. — С. 56.

установить максимально широкий круг лиц, имеющих отношение к преступной цепочке, начиная от наркопотребителей. Через них устанавливаются другие звенья организованной группы, вплоть до организаторов криминального наркобизнеса, в том числе и в зарубежных государствах. При этом выявление указанных лиц должно осуществляться от первоначальных финансовых операций по расчёту за наркотические средства до конечных денежных активов организаторов противоправной деятельности.

Ключевую роль в повышении результативности взаимодействия играет уровень профессиональной квалификации персонала. Необходимо укреплять профильные структурные единицы, а также активно применять передовые технологические разработки. Особое внимание следует уделить внедрению решений, использующих машинное обучение и контекстный анализ, что позволит эффективно обнаруживать и изучать противоправную деятельность в цифровой среде.

Таким образом, результативное раскрытие дел, связанных с бесконтактным оборотом наркотиков, обусловлено комплексным подходом к налаживанию сотрудничества между следователем, оперативниками и экспертными организациями. Лишь благодаря строгому разделению полномочий, оперативному обмену данными и совместному стратегическому планированию можно успешно противостоять высокоинтеллектуальным наркопреступным структурам.

§ 3.2. Роль судебных экспертиз в доказывании по делам о наркопреступлениях, совершенных через ИТС

Эффективность доказывания по уголовным делам о незаконном обороте наркотических средств, совершаемом с использованием телекоммуникационных сетей, во многом определяется комплексным применением различных видов судебных экспертиз. Цифровой характер преступной деятельности порождает специфические объекты исследования, требующие специальных познаний в области компьютерных технологий, лингвистики, а также традиционных методов химического анализа. Как обоснованно отмечается в научной литературе, заключение эксперта в отдельных случаях выступает исключительным способом получения криминалистически значимой информации, связанной с цифровыми следами¹, что обуславливает необходимость совершенствования теоретических и методических основ судебно-экспертной деятельности.

Судебная компьютерно-техническая экспертиза занимает центральное место в системе экспертных исследований по рассматриваемой категории дел. Объектами данной экспертизы выступают компьютеры, ноутбуки, мобильные телефоны, планшеты, сим-карты, флеш-карты и иные носители цифровой информации. Посредством производства компьютерной экспертизы в процессе доказывания может быть обнаружена переписка в мессенджерах с контактами по поводу приобретения наркотических средств, сведения об их цене и фотографии с местами закладок.

Для извлечения криминалистически значимой информации экспертные подразделения МВД применяют различные аппаратно-программные комплексы. Наиболее распространённым является UFED (Universal Forensic Extraction Device), позволяющий выполнять извлечение данных на

¹ Саркисян, К.Т. Судебные экспертизы объектов в цифровой форме в компьютерных сетях при расследовании незаконного оборота наркотических средств : автореф. дис. ... канд. юрид. наук / К. Т. Саркисян. — М., 2025. — С. 15.

физическом, логическом и файловом уровне, а также восстанавливать пароли с различных устройств. Кроме того, используется программный комплекс «Мобильный криминалист», с помощью которого эксперт может обходить блокировку мобильного устройства, восстанавливать удалённую информацию, в том числе удалённые переписки в мессенджерах. Как отмечает начальник ЭКЦ МВД России генерал-лейтенант Вадим Казьмин, идентифицировать организаторов крупнейшей платформы наркоторговли Hydra помогло изучение переписки в мессенджерах — «речь злоумышленников как криминалистически значимый след анализируют при автороведческих, лингвистических и фоноскопических экспертизах».¹

Круг вопросов, разрешаемых компьютерной экспертизой по делам о наркопреступлениях, охватывает как общие технические характеристики устройства, так и содержание хранящейся на нём информации: установлены ли в памяти устройства программы персональной связи, имеется ли в архивах переписки наименований наркотических средств, адреса тайников, информация о денежных переводах, стоимости единиц весов, счетах электронных платёжных систем. Однако одной из проблем остаётся недостаточная оснащённость отдельных подразделений необходимыми техническими средствами и кадрами, имеющими специальные познания в информационно-технической области.

Судебная лингвистическая экспертиза приобретает особое значение в связи с активным использованием участниками наркогрупп зашифрованных систем коммуникации. В целях конспирации своей незаконной деятельности они используют сленговые слова и выражения, «разовые коды», расшифровать которые, а значит, установить смысловое содержание текста, нередко возможно только с помощью применения специальных лингвистических знаний. Как показывают исследования, участники

¹ Казьмин, В. Интервью «Российской газете» / В. Казьмин // Российская газета. — 2024. — URL: <https://rg.ru>

наркогрупп нередко используют в общении зашифрованную систему коммуникации, которую составляют сленговые и стилистически нейтральные слова и фразы с особыми значениями — так называемые «разовые коды». Смысловое содержание сформированных с её помощью текстов можно установить, в частности, путём применения метода контекстологического анализа, когда слово исследуется с учётом его вербального и невербального окружения.

Значимость лингвистической экспертизы подтверждается практикой раскрытия крупных наркоплатформ. Как заявил начальник ЭКЦ МВД России, новейшие методики исследования текстов в переписках в мессенджерах позволили найти и привлечь к ответственности организаторов и участников крупнейшей платформы наркоторговли Hydra. Данный пример демонстрирует, что анализ коммуникативной активности подэкспертного позволяет составить целостный психологический портрет правонарушителя, установить его индивидуально-психологические особенности и регулятивные аспекты психической деятельности в юридически значимых ситуациях.

Традиционные химические и криминалистические экспертизы сохраняют своё значение при исследовании изъятых веществ и предметов-носителей. Согласно разъяснениям Верховного Суда РФ, для определения вида средств и веществ (наркотическое, психотропное, сильнодействующее), их названий и свойств, происхождения, способа изготовления, а также для установления принадлежности растений к культурам, содержащим наркотические вещества, требуются специальные познания. Суды при рассмотрении дел данной категории должны располагать соответствующими экспертными заключениями, полученными в соответствии с методиками, утверждёнными Постоянным комитетом по контролю наркотиков.

Объектами экспертного исследования являются сами наркотические средства, их следы на предметах-носителях, упаковочные материалы. Целями экспертизы выступают определение принадлежности исследуемого материала

к наркотическим веществам, выявление их следов, установление методов изготовления. К диагностическим вопросам относятся: принадлежит ли вещество к наркотическим средствам с конкретизацией группы и наименования; присутствуют ли на объектах следы наркотических средств; каково количество наркотического вещества и число активных компонентов; установить способ получения представленных наркотических средств. Идентификационные вопросы включают определение общей групповой принадлежности по использованному сырью, установление изготовления на конкретном предприятии, отождествление веществ, конфискованных у разных лиц.

Комплексный подход к использованию экспертных знаний является необходимым условием эффективного доказывания по делам о наркопреступлениях, совершаемых через ИТС. Цифровые следы становятся объектами исследования не только в судебной компьютерно-технической экспертизе, но и в других родах и видах судебных экспертиз, что сопряжено с возникновением ряда теоретических, правовых и организационных проблем, влияющих на их методологию и методики. Как отмечается в диссертационном исследовании К. Т. Саркисян, трансформация судебных экспертиз с появлением цифровых следов требует переосмысления задач, методов и методик экспертного исследования при расследовании незаконного оборота наркотических средств в компьютерных сетях.

Проблемным аспектом остаётся оценка и использование результатов судебных экспертиз. Следовательно необходимо не только назначить соответствующие экспертизы, но и правильно интерпретировать полученные заключения в совокупности с иными доказательствами. Заключение эксперта, будучи одним из видов доказательств, может стать основой для выдвижения и проверки следственных версий, а также для принятия процессуальных решений.

Таким образом, система судебных экспертиз по делам о наркопреступлениях, совершаемых через информационно-телекоммуникационные сети, представляет собой сложный комплекс, объединяющий компьютерно-технические, лингвистические и традиционные химические исследования. Каждый из указанных видов экспертиз решает специфический круг задач, а их совокупность обеспечивает полноту доказывания. Дальнейшее совершенствование методического обеспечения и устранение технических проблем в экспертных подразделениях являются необходимыми условиями повышения эффективности расследования указанной категории уголовных дел.

§ 3.3. Криминалистическое прогнозирование и меры профилактики с учетом развития цифровых технологий

Стремительное развитие информационных технологий и их активное использование в наркобизнесе обуславливают необходимость пересмотра не только тактики расследования, но и подходов к прогнозированию преступной активности и профилактике наркопреступлений. Как свидетельствует анализ правоприменительной практики, традиционные методы предупреждения преступлений в сфере незаконного оборота наркотиков оказываются недостаточно эффективными перед лицом высокотехнологичных и транснациональных криминальных сетей. Это диктует необходимость

внедрения современных технологических решений и совершенствования организационных механизмов противодействия.

Использование искусственного интеллекта в прогнозировании преступности. Искусственный интеллект открывает широкие перспективы для прогнозирования преступной активности в сфере наркотрафика. Как отмечается в исследованиях, алгоритмы машинного обучения способны обрабатывать данные о предыдущих преступлениях, выявляя закономерности, которые могут указывать на будущую преступную активность. В социальных сетях наиболее эффективен анализ текстовой информации для выявления ключевых слов и фраз, связанных с незаконным оборотом наркотических средств, заранее заданных программе.

Геопространственный анализ позволяет использовать географические информационные системы, интегрируя их с технологиями искусственного интеллекта для выявления и анализа «горячих точек» наркоторговли. Такой подход даёт возможность прогнозировать вероятные места и время совершения преступлений и оптимизировать маршруты патрулирования. В Российской Федерации в настоящее время проводятся эксперименты по созданию и испытанию проектов по распознаванию *émotions* и поведения человека для прогнозирования вероятности совершения ими преступлений, что свидетельствует о поиске новых эффективных инструментов профилактики.

Важным направлением является использование алгоритмов искусственного интеллекта для анализа социальных сетей и формирования карт преступных сетей. Согласно отчётам, число пользователей социальных сетей в Российской Федерации достигает значительных значений, что делает данное направление наиболее актуальным. Алгоритмы могут создавать на основе мониторинга записей и анализа изображений графы, отображающие связи между возможными кураторами, сбытчиками и клиентами.

Технические средства мониторинга интернет-пространства. В Российской Федерации уже функционирует эксплуатационная интеллектуальная система отслеживания незаконного контента в сети Интернет «Окулус». В мониторинговой деятельности используются разработки отечественных компаний: поисковая система «СЕУС» (ООО «СЕУСЛАБ»), поисковые системы противоправного контента среди открытых источников «Октонус» и «Следопыт» (ООО «БалтИнфоКом»). Эти системы позволяют выявлять противоправный контент, однако, как обоснованно отмечается, поиск незаконной информации является средством пресечения, а не профилактики, и направлен на выявление фактов нарушения законодательства.

Для профилактики преступлений в сфере незаконного оборота наркотических средств более эффективным представляется использование алгоритмов, основанных на искусственном интеллекте, целью которых является выявление сообщений, рекламных роликов и записей, содержащих информацию, связанную с наркотическими средствами. Такая система может также *automatisch* направлять запросы на блокировку выявленных записей или рекламы. Актуальность данного подхода обусловлена тем, что онлайн-продажи приобрели особую популярность, а наркоторговцы нередко маскируют свой товар под видом другого.

Профилактика через ограничение доступа к нарконтенту. Одним из направлений профилактики является ограничение доступа к интернет-ресурсам, содержащим информацию о наркотиках. Как отмечается на заседании Общественного совета при УМВД России по Архангельской области, сотрудниками полиции принимаются меры по выявлению и блокировке интернет-ресурсов с противоправным контентом, направленным на пропаганду запрещённых веществ. Однако данный подход требует постоянного совершенствования, поскольку злоумышленники оперативно создают новые площадки взамен заблокированных.

Выявление и предупреждение вовлечения несовершеннолетних. Особого внимания заслуживает профилактика вовлечения несовершеннолетних в наркоторговлю через интернет. Как свидетельствует практика, преступные группы активно используют интернет-площадки в даркнете и зашифрованные мессенджеры, вербуя курьеров без возрастных ограничений. По данным УМВД, за 8 месяцев 2025 года в Ставропольском крае зарегистрировано 85 подростковых преступлений, а основная причина вовлечения — «лёгкие деньги» через мессенджеры. В этой связи предлагается ужесточение наказания за вовлечение несовершеннолетних в наркобизнес.

Совершенствование законодательной базы. Существенным направлением профилактики является совершенствование уголовного законодательства. В научной литературе отмечается терминологическая непоследовательность законодателя в описании использования различных сетей как способа совершения преступления. Так, в одних нормах установлена ответственность за совершение преступления с использованием только информационно-телекоммуникационных сетей, а в других — с использованием электронных и информационно-телекоммуникационных сетей. Это создаёт правовую неопределённость при квалификации деяний.

Проблемы безопасности информационных систем. При внедрении технологий искусственного интеллекта необходимо усилить защиту в соответствии с современными тенденциями и угрозами. Как отмечается в исследованиях, применение искусственного интеллекта делает информационную инфраструктуру правоохранительных органов более уязвимой — появляется риск утраты, искажения, передачи служебной информации. Предлагается реализация механизма повышения безопасности данных, включающего авторизацию и аутентификацию сотрудников посредством электронной цифровой подписи, персонального идентификационного номера и идентификации с использованием биометрических считывателей.

Таким образом, криминалистическое прогнозирование и профилактика преступлений в сфере наркотрафика, совершаемых через информационно-телекоммуникационные сети, требуют комплексного подхода, объединяющего использование современных технологических решений (искусственный интеллект, системы мониторинга), совершенствование законодательной базы, усиление мер безопасности информационных систем и активизацию профилактической работы, особенно среди несовершеннолетних. Только сочетание указанных мер способно обеспечить эффективное противодействие высокотехнологичной наркопреступности.

Заключение

Проведённое исследование организационно-тактических особенностей расследования преступлений, связанных с незаконным оборотом наркотических средств, совершаемых с использованием информационно-телекоммуникационных сетей, позволяет сформулировать ряд выводов, имеющих как теоретическое, так и прикладное значение.

Основные результаты исследования. В ходе работы установлено, что современный наркобизнес представляет собой сложную многоуровневую систему, интегрированную в цифровую среду. Выявлено, что структурно-криминалистическая характеристика рассматриваемых преступлений включает качественно новый элемент — цифровые следы, которые занимают промежуточное положение между материальными и идеальными следами, но по своей природе относятся к материальным, поскольку неотделимы от своих носителей. На основе анализа эмпирических материалов разработана классификация цифровых следов, встречающихся по делам о наркопреступлениях, совершаемых через ИТС: IP-адреса, геолокационные данные, переписки в мессенджерах, криптовалютные транзакции, метаданные мультимедийных файлов. Определено, что наиболее информативными являются данные мессенджеров (Telegram, WhatsApp) и приложений для заметок, содержащие координаты тайников и переписку с кураторами.

Систематизированы типичные исходные следственные ситуации, возникающие на первоначальном этапе расследования: задержание курьера-закладчика с поличным; обнаружение наркотических средств без установления лица, их оставившего; поступление оперативной информации о готовящемся сбыте при известной личности предполагаемого участника;

задержание лица после приобретения наркотического средства (потребителя). Для каждой ситуации разработаны алгоритмы действий следователя, учитывающие специфику цифровой среды и необходимость оперативного процессуального закрепления электронных доказательств.

В тактическом аспекте сформулированы практические рекомендации по производству осмотра цифровых носителей с акцентом на необходимость изоляции устройств от внешних сетей (режим «полёта», пакет Фарадея) до момента их процессуального закрепления. Обосновано, что нарушение данного требования влечёт утрату доказательственной информации в результате дистанционной блокировки или удаления данных. Определён перечень объектов, подлежащих изъятию при обыске у лиц, осуществляющих дистанционное управление наркотрафиком, включающий не только традиционные носители, но и аппаратные криптокошельки, файлы с закрытыми ключами, записи с паролями доступа к криптобиржам. Разработаны тактические приёмы допроса дифференцированно для каждой категории участников преступной группы (организатор, оператор, закладчик, свидетель), учитывающие их функциональную роль и степень осведомлённости о деятельности организации.

Новизна полученных результатов. Отличие настоящего исследования от существующих подходов состоит в следующем. Во-первых, в отличие от традиционных криминалистических методик, ориентированных на «контактные» способы совершения преступлений, разработанный комплекс рекомендаций адаптирован к бесконтактной модели наркотрафика, где ключевым объектом исследования выступает не физическое взаимодействие субъектов, а их цифровая активность. Во-вторых, предложена не просто классификация цифровых следов, а алгоритмизированная последовательность действий следователя на каждом этапе расследования с учётом конкретной следственной ситуации, что позволяет минимизировать риск утраты доказательств. В-третьих, в отличие от существующих работ, акцентирующих

внимание на технических аспектах изъятия цифровой информации, разработаны тактические приёмы допроса, учитывающие психологические особенности участников бесконтактного наркотрафика и возможность использования цифровых доказательств для изобличения во лжи. В-четвёртых, обоснована необходимость комплексного применения судебных экспертиз (компьютерно-технической, лингвистической, химической) в их взаимосвязи, а не изолированно, что позволяет формировать целостную доказательственную базу.

Практическая значимость и направления применения. Результаты исследования могут быть применены в следующих направлениях:

1. В следственной практике — разработанные алгоритмы действий в типичных следственных ситуациях и тактические рекомендации по производству осмотра, обыска и допроса могут быть использованы следователями и дознавателями при расследовании уголовных дел о наркопреступлениях, совершаемых через ИТС. Особую ценность представляют рекомендации по изоляции мобильных устройств от внешних сетей и перечень объектов, подлежащих изъятию при обыске у лиц, использующих криптовалюту.

2. В экспертной практике — систематизация объектов экспертного исследования и круга разрешаемых вопросов по каждому виду экспертиз (компьютерно-технической, лингвистической, химической) позволяет оптимизировать взаимодействие следователя с экспертными подразделениями при назначении и производстве экспертиз.

3. В учебном процессе — материал исследования может быть использован при подготовке учебных пособий и методических рекомендаций по курсу «Криминалистика» (раздел «Методика расследования преступлений в сфере незаконного оборота

наркотических средств»), а также в программах повышения квалификации следователей и оперативных сотрудников.

Таким образом, проведенное исследование позволяет констатировать, что эффективное расследование преступлений в сфере незаконного оборота наркотических средств, совершаемых с использованием информационно-телекоммуникационных сетей, возможно только при условии системного применения разработанных тактических рекомендаций, организационных мер и современных технических средств, что обеспечивает формирование допустимой и достоверной доказательственной базы по уголовным делам данной категории.

Список использованной литературы

Нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации: принята референдумом Российской Федерации 12 декабря 1993 г. // Российская газета. – 1993. – 25 декабря.
2. О наркотических средствах и психотропных веществах: Федеральный закон от 8 января 1998 г. № 3-ФЗ (ред. от 26.07.2019) // Собрание законодательства Российской Федерации. – 1998. – № 2, ст. 219.
3. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (ред. от 02.12.2019) // Собрание законодательства Российской Федерации. – 1995. – № 33, ст. 3349.
4. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ (ред. от 27.12.2019) // Собрание законодательства Российской Федерации. – 1996. – № 25, ст. 2954.
5. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 02.08.2019) // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. 1), ст. 4921.
6. О применении судами законодательства о мерах ответственности за незаконный оборот наркотических средств, психотропных веществ и их аналогов: постановление Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 (ред. от 16.05.2017). – URL: <https://vsrf.ru> (дата обращения: 20.07.2026).

Научная и учебная литература:

7. Асташкина, Е.Н. Квартирные кражи: проблемы оптимизации и алгоритмизации первоначального этапа расследования : монография / Е.Н. Асташкина, Н.А. Марочкин. – М. : Юрлитинформ, 2005. – 184 с.
8. Введенская, О.Ю. Первоначальный этап расследования незаконного сбыта наркотических средств с использованием информационно-

- телекоммуникационных технологий : учебное пособие / О.Ю. Введенская. – Краснодар: Краснодарский университет МВД России, 2023. – 112 с.
9. Криминалистика: учебник / под ред. Н. П. Яблокова. – М. : Юристъ, 2021. – 672 с.
10. Криминалистика: учебник / под ред. А. Г. Филиппова. – М. : Спарк, 2022. – 688 с.
11. Криминалистика : учебник / под ред. Е.Р. Россинской. – М. : Норма, 2023. – 704 с.

Диссертации и авторефераты

12. Саркисян, К.Т. Расследование незаконного оборота наркотических средств, совершенного с использованием компьютерных сетей : дис. ... канд. юрид. наук: 12.00.12 / К. Т. Саркисян. – М., 2020. – 205 с.
13. Саркисян, К.Т. Судебные экспертизы объектов в цифровой форме в компьютерных сетях при расследовании незаконного оборота наркотических средств : автореф. дис. ... канд. юрид. наук: 5.1.4 / К. Т. Саркисян. – М., 2025. – 29 с.

Научные публикации и статьи в иных периодических изданиях:

14. Белей, А.В. Тактика применения современных технико-криминалистических средств при сборании криминалистически значимой информации, содержащейся в дампе оперативной памяти персональных компьютеров / А.В. Белей // Российский следователь. – 2022. – № 8. – С. 3–6.
15. Беляков, А.А. Тактические особенности работы с электронно-цифровыми следами на месте происшествия / А.А. Беляков, В.Ю. Иванов // Криминалистика: вчера, сегодня, завтра. – 2021. – № 4 (20). – С. 17–26.

16. Герасенков, В.М. Процессуальные аспекты изъятия электронных носителей информации / В.М. Герасенков // Российский следователь. – 2020. – № 7. – С. 34–37.
17. Залескина, А.Н. Бесконтактный сбыт наркотических средств как элемент криминалистической характеристики преступлений / А.Н. Залескина, И.А. Яцкина, В.С. Замашников // Философия права. – 2025. – № 4 (115). – С. 106–111.
18. Иванова, К.С. Расследование незаконного сбыта наркотических средств: специфика следственных действий в цифровой среде / К.С. Иванова // Молодой ученый. – 2025. – № 49 (600). – С. 335–336.
19. Карлов, А.Л. Проблемы получения электронной переписки в уголовном судопроизводстве / А.Л. Карлов // Уголовное судопроизводство. – 2018. – № 4. – С. 39–43.
20. Мещеряков, В.А. Виртуальные следы в раскрытии и расследовании преступлений / В.А. Мещеряков // Информационное право. – 2017. – № 3. – С. 22–27.
21. Моисеев, А.М. Криминалистические признаки наркосбыта посредством Интернет / А.М. Моисеев, С.В. Кондратюк // Балканско научно обозрение. – 2017. – № 1. – С. 29–33. Недосекова, Е.С. К вопросу об объектах безопасности / Е. С. Недосекова // Административное и муниципальное право. – 2011. – № 9. – С. 48–51.
22. Россинская, Е.Р. Цифровые следы как объект судебной экспертизы / Е.Р. Россинская // Теория и практика судебной экспертизы. – 2019. – № 1. – С. 8–15.
23. Рясков, А.А. Способы взлома запирающих устройств и их криминалистическое значение / А.А. Рясков, Г.Г. Жигалова // Мир науки, культуры, образования. – 2015. – № 4 (53). – С. 229–231.

24. Соколова, О.А. Цифровые следы в судебных экспертизах: теоретические и организационные проблемы / О.А. Соколова // Судебная экспертиза. – 2020. – № 1. – С. 44–49.

Электронные ресурсы

25. Всемирный доклад ООН о наркотиках 2023 года. – URL: <https://www.unodc.org> (дата обращения: 20.07.2026).
26. Доклад Генеральной прокуратуры РФ о состоянии законности в сфере противодействия наркопреступности. – 2024. – URL: <https://genproc.gov.ru> (дата обращения: 20.07.2026).
27. Доклад Управления ООН по наркотикам и преступности о транснациональной организованной преступности. – 2024. – URL: <https://www.unodc.org> (дата обращения: 20.07.2026).
28. Информация о программном комплексе «Мобильный криминалист». – URL: <https://www.oxygen-forensic.com> (дата обращения: 20.07.2026).
29. Сводка основных показателей деятельности по контролю за оборотом наркотиков за январь-декабрь 2024 года / Министерство внутренних дел Российской Федерации. – URL: <https://мвд.рф> (дата обращения: 20.07.2026).
30. Статистика наркопреступлений в России: динамика и тенденции. – URL: <https://xn--b1aew.xn--p1ai/statistics> (дата обращения: 20.07.2026).
31. Казьмин, В. Интервью «Российской газете» / В. Казьмин // Российская газета. — 2024. — URL: <https://rg.ru>