

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 подразделений по контролю за оборотом наркотиков»), форма обучения очная, набор 2021

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:
МЕТОДИКА РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА
НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШЕННОГО С
ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Выполнил:

Слушатель группы П 2101-КОН
младший лейтенант полиции
Воронько Роман Игоревич

Руководитель:

Профессор кафедры криминалистики
д.ю.н., профессор
Гармаев Юрий Петрович

Дата защиты:

« 10 » июня 2026 г.

Оценка: отлично

Председатель ГЭК

Иванович Иван Иванович
(специальное звание)


(подпись)

А.Г. Гармаев

(инициалы, фамилия)

Красноярск 2026

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

Кафедра _____
Направление подготовки (специальность) _____

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

Выполнил:

Слушатель

(№ учебной группы, специальное звание)

(фамилия, имя, отчество)

Руководитель

(должность)

(ученая степень, ученое звание)

(специальное звание)

(фамилия, имя, отчество)

Консультант

(должность)

(ученая степень, ученое звание)

(специальное звание)

(фамилия, имя, отчество)

Дата защиты:

«__» _____ 20__ г.

Оценка: _____

Председатель ГЭК

(специальное звание)

(подпись)

(инициалы, фамилия)

Красноярск 20__

Оглавление

Введение.....	3
Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ КРИМИНАЛИСТИЧЕСКОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ .	12
1.1. Незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий как объект криминалистического исследования.....	12
1.2. Особенности формирования криминалистической методики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий	18
Глава 2. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ .	23
2.1. Типичные способы и обстановка незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	23
2.2. Личность типичного преступника незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	25
2.3. Типичная следовая картина незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий.	29
Глава 3. РАССЛЕДОВАНИЕ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ .	32
3.1. Особенности доследственной проверки и первоначальный этап расследования незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	32
3.2. Типичные следственные ситуации и версии расследования незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	36
3.3. Тактика проведения отдельных следственных действий при расследовании незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	39
3.4. Использование специальных знаний при расследовании незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	52
3.5. Проблемы криминалистической профилактики незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий	57
Заключение	63
Список использованной литературы.....	66

Введение

Актуальность темы исследования. Наркомания остаётся одной из наиболее значимых угроз обществу: постоянное появление новых видов наркотических средств и психоактивных веществ, расширение численности вовлечённых в их изготовление, сбыт и потребление групп усиливают негативное влияние на здоровье населения, экономику и безопасность государства. Из всех форм незаконного оборота именно сбыт представляет наибольшую общественную опасность, поскольку удовлетворение устойчивого спроса способствует дальнейшей наркотизации социума.

Современные преступные структуры непрерывно совершенствуют технологии торговли наркотиками, внедряя технические новшества. Широкое применение информационно-телекоммуникационных технологий резко повысило эффективность противоправной деятельности, в результате чего преступления в киберпространстве признаны одной из приоритетных угроз в настоящем и перспективном периодах. Это отражено и в стратегических документах национальной безопасности, которые ставят задачей предупреждение и пресечение правонарушений, совершаемых с использованием ИКТ, в том числе незаконного распространения наркотиков и психотропных веществ.

Открытость, трансграничность, высокая скорость обмена данными, условная анонимность и децентрализация сети Интернет делают её удобной средой для множества законных действий (коммуникация, торговля, финансовые операции), но одновременно создают благоприятную платформу для преступной деятельности. Особенно это проявляется в зонах сети с повышенной криминогенностью - в том числе в Даркнете - где сконцентрированы современные схемы сбыта наркотических средств.

Криминалистическая наука обязана оперативно реагировать на появление новых форм преступлений и специфических сред их совершения. Понимание способов совершения, механизмов слеодообразования и характерных признаков цифрового следа преступной деятельности позволяет расширять методический инструментарий, предлагать практические меры по расследованию и профилактике правонарушений и повышать эффективность работы правоохранительных органов.

Тем не менее анонимность пользователей, скорость информационных потоков и технологическое отставание правоохранительных подразделений - как в аппаратном, так и в нормативно-правовом обеспечении - существенно осложняют противодействие преступлениям в ИТ-среде. Наблюдается дефицит квалифицированных специалистов в области кибербезопасности и недостаточная оснащённость современными программно-аппаратными средствами, что создаёт разрыв между возможностями правоохранительных органов и техническим потенциалом преступных сообществ.

Если традиционная модель сбыта подразумевает непосредственную передачу товара продавцом покупателю, то с начала XXI века получили распространение скрытые способы размещения наркотиков с информационным сопровождением: через сети и мессенджеры распространяются сведения о возможности покупки, цене, объёме, месте и времени «закладок», условиях получения и т. п. В настоящее время именно такие схемы, подкреплённые средствами ИКТ, доминируют в структуре наркопреступности, что делает разработку целевых криминалистических методик расследования этой категории преступлений крайне востребованной и практически значимой.

Степень разработанности темы исследования. Вопросы уголовно-правовой, криминологической и криминалистической противодействия преступлениям с использованием телекоммуникационных технологий освещены в работах ряда отечественных исследователей, среди которых Н. А. Архипова, Р. С. Атаманов, Ю. В. Гаврилин, Н. Ю. Дусева,

Е. П. Ищенко, А. Н. Колычева, В. С. Овчинский, А. Л. Осипенко, Е. Р. Россинская, А. А. Рудых, Д. А. Степаненко, Б. П. Смагоринский и другие. Практические рекомендации по расследованию подобных преступлений представлены в трудах Р. С. Атаманова, А. В. Варданяна, В. Б. Вехова, А. С. Егорышева, Д. А. Илюшина, С. А. Ковалёва, И. Е. Мазурова, В. А. Мещерякова и др. Проблематика незаконного оборота наркотических средств и его сбыта также подробно рассматривается в работах Е. С. Безруких, В. Ф. Васюкова, С. И. Земцовой, Е. А. Ошлыковой, А. С. Щуровой и других авторов.

Особое внимание уделяется недавно опубликованным статьям, посвящённым незаконному сбыту наркотиков с применением информационно-телекоммуникационных технологий (среди авторов - Е. Л. Глушков, А. В. Климачков, А. Л. Осипенко, П. В. Миненко, А. В. Шебалин и др.), которые расширяют понимание цифровых каналов распространения и практик злоумышленников. Собранный корпус работ заложил важную теоретическую и практическую базу для противодействия наркопреступности в ИТ-среде, описал типичные схемы, нормативно-правовые проблемы и основные направления технической экспертизы.

Вместе с тем большинство исследовательских материалов носят относительно общий характер и сфокусированы либо на общих принципах расследования киберпреступлений, либо на отдельных технологических аспектах нелегальной торговли наркотиками. При этом недостаточно разработан криминалистический аспект, связанный с получением и оценкой первоначальной информации о преступлениях такого типа, а также с организацией и методикой проведения начального этапа расследования - доследственной проверки и формулирования рабочих версий. Этот пробел особенно остро проявляется в условиях быстрого развития ИТ-инструментов преступников и требует создания комплексных криминалистических методик,

интегрирующих цифровую криминалистику, оперативные приёмы и процессуальные гарантии.

Таким образом, существующая научная база предоставляет прочную отправную точку, но предъявляет потребность в целенаправленном исследовании методики расследования незаконного сбыта наркотических средств, совершённого с использованием информационно-телекоммуникационных технологий, с акцентом на практико-ориентированные алгоритмы действий, стандарты документирования цифровых следов и организацию взаимодействия между криминалистами, экспертами и оперативными подразделениями.

Объект исследования - общественные отношения, возникающие в процессе подготовки, совершения и сокрытия преступлений, а также отношения, складывающиеся на этапах предварительного и первоначального расследования дел, связанных с незаконным сбытом наркотических средств, осуществляемым с использованием информационно-телекоммуникационных технологий.

Предмет исследования - закономерности подготовки, совершения и сокрытия указанных преступлений; условия и особенности образования криминалистически значимой информации об обстоятельствах их совершения; а также организационно-методические и практические аспекты деятельности правоохранительных органов по обнаружению, фиксации и изъятию следов преступной деятельности с целью формирования доказательственной базы по таким уголовным делам.

Цель работы заключается в разработке комплексной методики расследования преступлений, связанных с незаконным сбытом наркотических средств с применением информационно-телекоммуникационных технологий, ориентированной на предварительный и первоначальный этапы уголовного преследования. Методика должна предусматривать алгоритмы получения и оценки первичной информации, тактику следственных и

оперативно-разыскных действий, порядок взаимодействия специалистов и подразделений, а также стандарты документирования цифровых следов.

Задачи исследования:

1. Проанализировать нормативно-правовую базу противодействия незаконному сбыту наркотических средств с использованием ИКТ.
2. Изучить и систематизировать типичные способы совершения преступлений данного вида.
3. Выявить особенности формирования криминалистической характеристики незаконного сбыта наркотиков с использованием ИКТ.
4. Исследовать типичную следовую картину преступлений и методы её фиксации.
5. Разработать алгоритмы действий правоохранительных органов на этапе доследственной проверки.
6. Сформулировать рекомендации по тактике проведения следственных действий и использованию специальных знаний.
7. Определить основные проблемы криминалистической профилактики данных преступлений и предложить пути их решения.

Практическая значимость исследования заключается в том, что разработанные рекомендации могут быть непосредственно внедрены в деятельность правоохранительных органов для повышения эффективности расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий. Предложенные алгоритмы действий позволят:

- сократить время доследственной проверки;
- повысить качество сбора и фиксации цифровых доказательств;
- оптимизировать взаимодействие между подразделениями;
- снизить количество ошибок при планировании расследования.

Методология исследования основывалась на материалистической диалектике как общенаучном методе познания, используемом для изучения социально-правовых процессов и явлений. Содержание и особенности

незаконного сбыта наркотических средств, совершаемого с использованием информационно-телекоммуникационных технологий, исследовались с применением методов эмпирического познания, логического анализа и синтеза, а также криминалистического прогнозирования.

Для описания основных элементов криминалистической характеристики рассматриваемых преступлений и выявления наиболее значимых связей между ними были использованы социологические методы, системно-структурный, формально-логический, а также методы криминалистического моделирования явлений и процессов.

Для исследования практической деятельности по получению первоначальной криминалистически значимой информации, её проверке и оценке, организации первоначального этапа расследования и его отдельных элементов был проведён опрос сотрудников следственных органов, а также использовались методы описания отдельных явлений и процессов, сравнения, анализа и синтеза, специальные методы: системно-структурный, формально-логический и др.

Нормативно-правовая база исследования составила Конституция Российской Федерации, общепризнанные принципы и нормы международного права, уголовное и уголовно-процессуальное законодательство Российской Федерации, федеральные законы, ведомственные и межведомственные нормативные правовые акты, регулирующие общественные отношения в рассматриваемой сфере.

Теоретическая основа исследования - труды учёных в области криминалистики, уголовного процесса, уголовного права, криминологии, информатики и других отраслей науки. Среди них фундаментальные труды Т. В. Аверьяновой, О. Я. Баева, Р. С. Белкина, В. Ф. Васюкова, В. Б. Вехова, А. Ф. Волынского, Ю. В. Гаврилина, Е. П. Ищенко, М. К. Каминского, В. А. Мещерякова, А. Л. Осипенко, Е. Р. Россинской, Д. А. Степаненко, А. Г. Филиппова, Н. Г. Шурухнова, Н. П. Яблокова и др. Изучены материалы периодических изданий, научных и научно-практических конференций,

посвящённых борьбе с преступлениями, связанными с незаконным оборотом наркотических средств, в том числе осуществляемым с использованием информационно-телекоммуникационных технологий.

Эмпирическая база исследования - результаты изучения материалов следственной и судебной практики за 2016–2025 гг. о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий: в соответствии со специальной анкетой были изучены материалы 174 уголовных дел (как направленных в суд с обвинительными заключениями, так и находящихся в производстве следователей) и обвинительные приговоры судов 15 субъектов Российской Федерации, результаты опроса 167 сотрудников органов предварительного расследования МВД России из 30 регионов страны.

Структура работы обусловлена целью и задачами исследования и включает введение, три главы, заключение, список использованной литературы.

- Введение содержит обоснование актуальности темы, степень научной разработанности проблемы, определение объекта и предмета исследования, формулировку цели и задач работы, описание методологии, теоретической, нормативной и эмпирической базы, практической значимости, а также структуру ВКР.

- Глава 1 «Теоретические основы формирования криминалистической методики расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» состоит из двух параграфов:

- 1.1. «Незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий как объект криминалистического исследования» - анализируются правовые и криминалистические аспекты явления, его место в системе преступлений против здоровья населения.

- 1.2. «Особенности формирования криминалистической методики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - рассматриваются принципы построения методики, её элементы и специфика применительно к ИКТ-среде.

- Глава 2 «Криминалистическая характеристика незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» включает три параграфа:

- 2.1. «Типичные способы и обстановка незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - систематизируются схемы совершения преступлений, каналы коммуникации, методы оплаты и доставки.

- 2.2. «Личность типичного преступника незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - анализируются социально-демографические и психологические черты участников преступных групп.

- 2.3. «Типичная следовая картина незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - описываются виды цифровых следов, их локализация и особенности фиксации.

- Глава 3 «Расследование незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» содержит пять параграфов:

- 3.1. «Особенности доследственной проверки и первоначальный этап расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» -

раскрываются алгоритмы действий правоохранительных органов на начальном этапе.

- 3.2. «Типичные следственные ситуации и версии расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - классифицируются ситуации и предлагаются типовые версии.

- 3.3. «Тактика проведения отдельных следственных действий при расследовании незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - даются рекомендации по проведению осмотра места происшествия, обыска, допроса и других действий с учётом ИКТ-специфики.

- 3.4. «Использование специальных знаний при расследовании незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - освещаются вопросы назначения экспертиз, привлечения специалистов, работы с цифровыми доказательствами.

- 3.5. «Проблемы криминалистической профилактики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий» - выявляются пробелы в профилактике и предлагаются меры по их устранению.

- Заключение содержит обобщение результатов исследования, выводы по каждой главе, предложения по совершенствованию методики расследования и перспективы дальнейшего изучения темы.

- Список использованной литературы включает нормативные акты, монографии, научные статьи, материалы судебной практики и иные источники, использованные при подготовке ВКР.

Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ
КРИМИНАЛИСТИЧЕСКОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ
НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С
ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Незаконный сбыт наркотических средств с использованием
информационно-телекоммуникационных технологий как объект
криминалистического исследования

Незаконный сбыт наркотических средств с применением информационно-телекоммуникационных технологий представляет собой сложный комплекс противоправных действий, при которых передача, продажа или иное отчуждение наркотических и психотропных веществ осуществляется через цифровые каналы, сервисы и устройства. В отличие от традиционных форм сбыта, здесь ключевые этапы преступного процесса - от привлечения клиентов до логистического сопровождения - реализуются в информационно-цифровой среде.

Суть явления проявляется через многогранность его объекта исследования. Криминалистический анализ затрагивает не только сами преступления, связанные со сбытом наркотиков, но и сопутствующие организационно-технические процессы, модели поведения участников схемы, способы маскировки следов противоправных действий, а также весь комплекс возникающих цифровых и материальных следов. Лишь изучая эти элементы в комплексе, можно составить полное представление о механизме преступления.¹

¹ Введенская Ольга Юрьевна КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ // Вестник КРУ МВД России. 2022. №1 (55). URL: <https://cyberleninka.ru/article/n/kriminalisticheskaya->

Расследование осложняется многообразием форм и каналов сбыта в ИКТ-среде. Преступники задействуют разные уровни доступности: от открытых платформ - публичных сайтов и соцсетей - до полузакрытых сообществ с модерацией и полностью скрытых площадок Даркнета. Взаимодействие выстраивается по-разному: где-то идут прямые продажи через мессенджеры, где-то работают виртуальные витрины магазинов или посреднические агрегаторы. В платёжных схемах встречаются и обычные банковские переводы, и электронные кошельки, и куда более сложные криптовалютные транзакции с технологиями микширования. Логистика тоже разнообразна: личная передача, система закладок, курьерские доставки или использование легальных логистических каналов в качестве прикрытия. Каждое такое направление создаёт свою следовую картину - и требует особых оперативно-тактических подходов к расследованию.

Ещё больше усложняет дело транснациональный характер таких преступлений. Инфраструктура, участники и каналы распространения нередко раскиданы по разным юрисдикциям. Из-за этого приходится координировать международное правовое взаимодействие и адаптировать процессуальные механизмы. В техническом плане расследование подразумевает анализ платформ и протоколов, типов данных (от текстовых сообщений и логов до финансовых транзакций и файлов), а также механизмов анонимизации - они серьёзно влияют на доступность и устойчивость доказательной базы. При этом процессуальные рамки исследования охватывают весь путь: от первичного обнаружения информации до назначения экспертиз и изъятия материальных носителей. На каждом этапе критически важно строго соблюдать законность и детально фиксировать все действия.²

harakteristika-nezakonnogo-sbyta-narkoticheskikh-sredstv-s-ispolzovaniem-informatsionno-telekommunikatsionnyh (дата обращения: 03.06.2026).

² Давыдов Сергей Иванович, Кондратьев Максим Валерьевич, Поляков Виталий Викторович ПРОТИВОДЕЙСТВИЕ ТРАНСНАЦИОНАЛЬНЫМ ОРГАНИЗОВАННЫМ ГРУППАМ, ИСПОЛЬЗУЮЩИМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ // Правоприменение. 2024. №1. URL: [https://cyberleninka.ru/article/n/protivodeystvie-](https://cyberleninka.ru/article/n/protivodeystvie)

Методологическая основа исследования опирается на сочетание классических криминалистических методов с современными подходами цифровой криминалистики. Ключевые принципы здесь - комплементарность, системность, форензическая бережность, законность и междисциплинарность. Чтобы реализовать их на практике, нужно одновременно применять традиционные приёмы осмотра и фиксации материальных следов и современные методы анализа цифровых данных. Крайне важно соблюдать цепочку хранения (chain of custody), беречь метаданные и добиваться максимальной прозрачности всех процедур: именно от этого зависит, признают ли доказательства допустимыми в суде. Если вовремя привлечь квалифицированных цифровых экспертов, получится и выстроить оптимальную тактику расследования, и не допустить потери критически важной информации.

Исследование следовой картины в ИКТ-среде - процесс многоэтапный. Сначала идентифицируют источники следов: это могут быть публичные открытые данные, сведения от провайдеров, платёжные и блокчейн-записи. Затем следы тщательно классифицируют - на цифровые, физические и поведенческие, - после чего коррелируют и привязывают к хронологии: это нужно, чтобы достоверно реконструировать сценарии преступных действий. При этом всю следовую информацию обязательно стратифицируют по критериям доступности и значимости: от данных в открытом доступе до сведений, для получения которых нужны специальные процессуальные запросы, и узкоспециализированных технических данных - их могут интерпретировать только профильные эксперты.³

transnatsionalnym-organizovannym-grupparam-ispolzuyuschim-informatsionno-kommunikatsionnye-tehnologii-dlya (дата обращения: 03.06.2026).

³ Решняк О. А., Алексеева А. П. ИСПОЛЬЗОВАНИЕ ИТ-ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОГО СОВРЕМЕННЫМИ СПОСОБАМИ // Вестник Волгоградской академии МВД России. 2021. №4 (59). URL: <https://cyberleninka.ru/article/n/ispolzovanie-it-tehnologiy-v-raskrytii-i-rassledovanii-nezakonnogo-sbyta-narkoticheskikh-sredstv-sovershaemogo-sovremennymi> (дата обращения: 03.06.2026).

Оценивать значимость и достоверность обнаруженных следов помогают ключевые критерии. Прежде всего смотрят на происхождение доказательств - откуда они взялись и как были получены. Не менее важна целостность: должны сохраниться метаданные и контрольные суммы. Контекстуальная релевантность показывает, насколько следы соответствуют фактическим обстоятельствам дела. Окончательную доказательственную базу формируют корреляция с другими доказательствами и возможность проверить их через независимые источники. Для верификации используют кросс-проверку данных, сопоставляют логи с сетевыми и материальными индикаторами, детально анализируют транзакции. Если нужно, к работе подключают профильных экспертов - криптоаналитиков, специалистов по реверс-инжинирингу, химиков. Их заключения обязательно документируют: чётко указывают применённые методы, возможные погрешности и ограничения.

Эффективность расследования во многом определяется грамотной организацией взаимодействия всех участников процесса. Чёткое распределение ролей между следователем, криминалистом, цифровым экспертом и оперативными подразделениями создаёт прочную основу для слаженной работы. Следователь отвечает за формулирование процессуальных задач и обеспечение законности всех действий. Криминалист координирует осмотры и фиксацию материальных следов. Цифровой эксперт занимается извлечением и анализом цифровых данных. Оперативные подразделения обеспечивают информационно-поисковую поддержку. Для максимальной результативности необходимо внедрение формализованных процедур: чётких регламентов обмена информацией, единых протоколов документирования, регулярных совместных оперативно-аналитических совещаний.⁴

⁴ Давыдов Сергей Иванович, Кондратьев Максим Валерьевич, Поляков Виталий Викторович ПРОТИВОДЕЙСТВИЕ ТРАНСНАЦИОНАЛЬНЫМ ОРГАНИЗОВАННЫМ ГРУППАМ, ИСПОЛЬЗУЮЩИМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ // Правоприменение. 2024. №1. URL: [https://cyberleninka.ru/article/n/protivodeystvie-](https://cyberleninka.ru/article/n/protivodeystvie)

Взаимодействие с внешними структурами - провайдерами, платёжными системами, международными партнёрами - осуществляется строго в рамках правового поля через мотивированные запросы, судебные решения и процедуры взаимного правового сотрудничества в случае трансграничных дел. При составлении запросов следует придерживаться принципа минимальности объёма информации при максимальной чёткости формулировок. Полученные от провайдеров ответы подлежат обязательному документированию и тщательной проверке на целостность.

Специалисты, занимающиеся расследованием, должны обладать широким набором компетенций: знать основы цифровой криминалистики и сетевых технологий, разбираться в криптографии, уметь анализировать логи и транзакции - и при этом не терять традиционных криминалистических навыков. Чтобы наращивать кадровый потенциал, нужно принимать комплексные меры: запускать профильные образовательные программы, регулярно организовывать курсы повышения квалификации, проводить практические тренинги и отрабатывать симуляционные кейсы. Немаловажно развивать системы сертификации экспертов, собирать междисциплинарные команды и давать доступ к современному специализированному ПО.

Сбор и оценка информации строятся как чёткая последовательность шагов. Всё начинается с обнаружения сигнала - это может быть жалоба, данные мониторинга или обращение граждан. Далее идёт первичная оценка: проверяют релевантность и риски, фиксируют публично доступную информацию, решают, какие процессуальные меры нужны дальше - например, запросы к провайдерам или назначение экспертиз. Одновременно данные из разных источников сопоставляют с физическими следами, на этой основе формируют базу для рабочих версий. Каждый этап обязательно документируют, а в приоритете - меры, которые максимально сохраняют доказательства и минимально затрагивают права третьих лиц.

Планируя следственные действия, опираются на детальный анализ проверенных фактов, учитывают иерархию вероятностей и комплексно оценивают риски. В первую очередь закрепляют цифровые данные: законно фиксируют и экспортируют метаданные, осматривают объекты с учётом цифровых указаний, назначают профильные экспертизы, ставят оперативные задачи. По ходу расследования, когда поступает новая информация, рабочие версии и тактику регулярно корректируют.

Чтобы доказательства нормально представляли в суде, нужен системный подход. Следует внедрить единые формы протоколирования действий с цифровыми данными, прописать чёткие требования к цепочке хранения, разработать стандартизированные формы экспертных заключений - с описанием применённых методов, выявленных ограничений и уровня уверенности выводов. Важно грамотно визуализировать связи между цифровыми и материальными следами и готовить понятные пояснения о процедурах верификации - так, чтобы их могла воспринять даже непрофессиональная аудитория.

Объект исследования сложен из-за своей многокомпонентности. Цифровая и материальная плоскости переплетаются, активно применяются технологии анонимизации, преступления носят транснациональный характер, а технологии меняются очень быстро - всё это бросает криминалистике уникальные вызовы. Из-за этого приходится постоянно обновлять методологическую базу, соединять цифровые и традиционные подходы, развивать междисциплинарное взаимодействие и укреплять правовую основу сотрудничества всех, кто участвует в расследовании.

Польза таких исследований видна в нескольких аспектах. Они помогают создавать интегрированные методики расследования с учётом специфики ИКТ-среды, упорядочивают взаимодействие с провайдерами и международными партнёрами - за счёт этого ускоряется получение критически важной информации. Ещё они способствуют стандартизации учёта цифровых доказательств, из-за чего те обретают большую силу в суде.

И наконец, на их основе совершенствуют программы подготовки кадров - так специалисты получают нужный уровень квалификации.

Если систематически мониторить и глубоко анализировать сетевую активность, можно заранее замечать устойчивые схемы сбыта. Это даёт шанс разрабатывать эффективные превентивные меры: они сокращают масштабы правонарушений и ограничивают доступность наркотических веществ через цифровые каналы. Получается, что комплексное изучение незаконного сбыта наркотиков с использованием ИКТ не просто улучшает методы расследования - оно ещё и укрепляет общественную безопасность в цифровой среде.

1.2. Особенности формирования криминалистической методики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Создать криминалистическую методику расследования незаконного сбыта наркотиков с использованием информационно-телекоммуникационных технологий - задача непростая, многоуровневая. Всё из-за специфики объекта исследования: цифровая и материальная составляющие преступной деятельности здесь тесно переплетены. При этом цифровые следы не заменяют традиционные материальные доказательства, а дополняют их - благодаря этому удаётся восстановить полную картину преступления: от структуры преступных связей до маршрутов логистики и финансовых потоков.

В основе методики - принцип форензической бережности. Он требует предельно аккуратно обращаться с цифровыми носителями информации. Любые действия с электронными данными обязаны соответствовать нормам уголовно-процессуального законодательства РФ: только так доказательства

потом примут в суде. Значит, нужно неукоснительно соблюдать процедуры изъятия, копирования и хранения цифровой информации - те, что прописаны в УПК РФ.⁵

Лучше всего методика работает в модульном формате: он даёт возможность сочетать стандартизированные процедуры с гибкостью - подстраиваться под быстро меняющиеся технологии. Внутри такой структуры складываются отдельные блоки, которые охватывают разные аспекты расследования. К примеру, протоколы первичной фиксации цифровой информации предусматривают законные способы сохранить скриншоты, экспортировать переписку из мессенджеров и захватить сетевой трафик - разумеется, в рамках действующего законодательства. Не менее критично грамотно работать с физическими носителями данных, облачными сервисами и удалёнными хранилищами: тут важно чётко понимать их правовую природу и порядок доступа к информации.⁶

Методы разведки по открытым источникам (OSINT) и автоматизированный мониторинг играют особую роль. Если систематически анализировать публичную информацию - скажем, объявления на интернет-площадках или обсуждения в тематических сообществах, - можно выдвинуть обоснованные гипотезы и наметить приоритетные направления расследования. А вот работа с закрытыми каналами коммуникации - мессенджерами, приватными группами и даркнет-маркетплейсами - требует особой тактической осторожности. Тут крайне важно найти баланс: с одной

⁵ Шуваева М. С., Николаева А. В. РОЛЬ ФОРЕНЗИКИ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПНОСТИ. КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ // Международный журнал гуманитарных и естественных наук. 2021. №6-2. URL: <https://cyberleninka.ru/article/n/rol-forenziki-v-rassledovanii-kiberprestupnosti-kriminalisticheskiiy-aspekt> (дата обращения: 03.06.2026).

⁶ Введенская Ольга Юрьевна О криминалистическом обеспечении расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий // Вестник КРУ МВД России. 2024. №2 (64). URL: <https://cyberleninka.ru/article/n/o-kriminalisticheskom-obespechenii-rassledovaniya-nezakonnogo-sbyta-narkoticheskikh-sredstv-s-ispolzovaniem-informatsionno> (дата обращения: 03.06.2026).

стороны, собрать доказательства, с другой - не скомпрометировать оперативную линию раньше времени.⁷

Технологическая часть методики опирается на современные инструменты анализа. Среди них - средства исследования сетевого трафика, программные решения для блокчейн-аналитики, законные методы дешифровки данных, инструменты реверс-инжиниринга приложений и платформы для корреляции разнородных данных. Выбирая такие инструменты, надо учитывать требования законодательства: ПО должно быть надёжным и подтверждённым, а если сертификации нет - нужны экспертные оценки его возможностей и ограничений. Это особенно важно с учётом положений Федерального закона «Об информации, информационных технологиях и о защите информации»: он регулирует порядок получения и использования цифровых данных.

Правовую основу методики определяют нормы УПК РФ, Федерального закона «О связи» и международные договоры РФ в сфере противодействия наркопреступности. Если нужно получить информацию от провайдеров, платёжных систем или зарубежных партнёров, без процессуальных документов не обойтись: потребуются судебные решения, мотивированные запросы, поручения о правовой помощи. При этом запрашивать стоит минимум данных - только то, что имеет прямое отношение к расследуемому делу. Отдельно контролируют защиту персональных данных и соблюдение конституционных гарантий тайны переписки. Всё это соответствует статье 23 Конституции РФ и нормам Федерального закона «О персональных данных».

Организовать работу помогают междисциплинарные группы. В них собирают специалистов разного профиля: криминалистов, цифровых форензик-экспертов, аналитиков блокчейна, химиков-криминалистов,

⁷ Дерюгин Роман Александрович КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОГО БЕСКОНТАКТНЫМ СПОСОБОМ // Известия ТулГУ. Экономические и юридические науки. 2023. №2. URL: <https://cyberleninka.ru/article/n/kriminalisticheskaya-harakteristika-sbyta-narkoticheskikh-sredstv-sovershaemogo-beskontaktnym-sposobom> (дата обращения: 03.06.2026).

специалистов по логистике и финансам, а также оперативных сотрудников. Чтобы группа работала слаженно, роли распределяют чётко - это фиксируют во внутренних приказах и межведомственных соглашениях. Ещё одна важная составляющая - непрерывное обучение: специалисты проходят тренинги, подтверждают компетенции через сертификацию, ротируются между подразделениями. В сложных технических вопросах привлекают внешних экспертов и научные организации - так удаётся решать задачи, не выходя за рамки закона.

Ключевой принцип организации - форензическая готовность (forensic readiness). Суть в том, чтобы заранее определить данные, критически важные для расследования, продумать, как их сохранить и получить к ним доступ, согласовать правила взаимодействия с коммерческими провайдерами и инфраструктурными организациями. Благодаря этому удаётся быстрее получать доказательства и снижать риск их утраты - особенно актуально, когда цифровые следы могут стереть в любой момент.

Проверять и подтверждать доказательства нужно комплексно: цифровые следы сопоставляют с материальными уликами. Смотрят на источник данных, следят за целостностью цепочки хранения, сверяют с независимыми индикаторами, проверяют, можно ли воспроизвести результаты. Для прозрачности используют стандартизированные формы отчётности и экспертных заключений: в них детально расписывают методы, итоги работы и возможные ограничения. Так выполняют требования статьи 204 УПК РФ к оформлению экспертных заключений.

Тактика строится на постепенном наращивании доказательственной базы. К примеру, если обнаружили цифровой след, указывающий на возможное место производства наркотиков, сначала проводят проверочные мероприятия. Анализируют энергопотребление, отслеживают транспортный трафик, изучают спутниковые снимки, организуют экологический мониторинг. Одновременно собирают цифровые доказательства, готовят основания для обысков и изъятий. Когда ресурсов не хватает, действуют по

алгоритмам приоритезации расследований: учитывают степень общественной опасности деяния, объёмы незаконного оборота и наличие международных связей у преступной группы.

Качество методики проверяют регулярно: проводят аудиты инструментов, сравнивают результаты между лабораториями, отрабатывают сценарии на учениях, анализируют, насколько воспроизводимы кейсы. Обмен опытом на национальном и международном уровнях тоже даёт эффект: накапливают банки типовых ситуаций, создают унифицированные шаблоны доказательств. Благодаря этому подходы выравниваются, а расследования становятся эффективнее.

Этические и правовые риски требуют отдельного внимания. В методике должны быть чёткие правила: как минимизировать вмешательство в права непричастных, по каким критериям оценивать законность превентивных мер, как учитывать ошибки автоматизированных систем. Если внедряют решения на основе искусственного интеллекта, алгоритмы обязаны быть прозрачными, а все решения, влияющие на ход расследования, - задокументированы. Это отвечает принципам законности из статьи 7 УПК РФ и требованиям к соблюдению прав человека в цифровой среде.

В итоге формирование криминалистической методики - процесс непрерывный. Он объединяет технические инновации, проработку правовых аспектов, подготовку кадров и практическую проверку на деле. Только такой подход - комплексный, регламентированный и способный адаптироваться - помогает эффективно противостоять современным формам незаконного сбыта наркотиков. При этом учитываются и динамика цифровизации преступной деятельности, и требования законодательства Российской Федерации.

Глава 2. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. Типичные способы и обстановка незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Незаконный сбыт наркотиков с применением информационно-телекоммуникационных технологий сегодня строится на стыке цифрового и физического: виртуальные витрины, мессенджеры и соцсети используют для общения, а для доставки задействуют тайники, почту и курьерские маршруты. Интернет-витрины и закрытые площадки, по сути, копируют схему обычной электронной торговли - там есть карточки товаров, фотоотчёты, отзывы, инструкции по оплате и получению. При этом расчёты зачастую идут через электронные кошельки, платёжные системы и криптовалюты, из-за чего отследить финансовые потоки становится сложнее.

Продавцы и покупатели в таких схемах обычно распределяют роли: администраторы площадок и операторы переписок занимаются предложениями и общением, логисты с курьерами отвечают за доставку, а покупатели дистанционно платят и получают координаты «закладок» либо инструкции к получению.⁸

Способ сбыта преступники подбирают с оглядкой на обстановку. На выбор между уличными «закладками», контактными передачами или использованием жилых помещений влияют время суток, погода, плотность людского потока и присутствие посторонних. В непогоду и по ночам чаще

⁸ Чистанов Т. О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // МНИЖ. 2016. №11-1 (53). URL: <https://cyberleninka.ru/article/n/nezakonnyy-sbyt-narkoticheskikh-sredstv-s-ispolzovaniem-telekommunikatsionnyh-setey-i-ustroystv> (дата обращения: 03.06.2026).

задействуют закрытые и бытовые точки сбыта, а в тёплую и спокойную погоду активнее пользуются уличными тайниками в общественных местах. Погода сказывается и на сохранности улики: осадки и сильный ветер быстрее уничтожают материальные следы, зато мороз способен дольше сохранять биологические маркеры - это надо учитывать, оценивая, сколько времени прошло между совершением преступления и его обнаружением.

Чтобы замести следы, преступники прибегают к разным уловкам: используют анонимизирующие сервисы и временные идентификаторы, берут подставные сим-карты и аккаунты, регистрируют электронные кошельки на третьих лиц, гоняют деньги через цепочки обменников и конвертаций, в том числе с криптовалютой. Выявить такие схемы помогают характерные маркеры: массовая синхронная активация анонимных профилей, повторяющаяся лексика и фотошаблоны, однотипная упаковка закладок, а также типичные платёжные паттерны. По ним можно выделить высокорисковые каналы и выдвинуть оперативные версии, не вникая в технические хитрости злоумышленников.

Чтобы выявлять и пресекать подобные схемы, важно грамотно соединять цифровую и полевую аналитику: мониторить контент и финансовые следы, а параллельно проверять всё на местности. Не менее критично наладить межведомственную координацию. Нужно чётко регламентировать взаимодействие с хостинг-провайдерами, площадками и платёжными операторами - в том числе оформлять запросы в зарубежные юрисдикции. Пригождаются и специализированные инструменты: блокчейн-аналитика и средства сетевого анализа, которые помогают найти точки входа и выхода денежных потоков. При этом любые действия, затрагивающие тайну переписки и другие конституционные права, обязаны укладываться в процессуальные нормы и сопровождаться должной документацией - только так собранные материалы получают правовую допустимость.⁹

⁹ Введенская Ольга Юрьевна Способ незаконного сбыта наркотических средств с использованием сети Интернет и телекоммуникационных технологий // Вестник КРУ МВД

На уровне приоритизации оперативных усилий целесообразно ориентироваться на признаки массовости и организованности, наличие прямой связи цифровых следов с физическими координатами, и на финансовые индикаторы аномальной активности. Профилактическая работа, сотрудничество с платформами объявлений и платёжными системами, а также повышение цифровой компетенции сотрудников и регулярное обновление базы маркеров позволяют снижать латентность и оперативно реагировать на изменения в методах сбыта. Комплексный подход, сочетающий аналитическую экспертизу, правовое сопровождение и оперативные меры на местности, повышает вероятность выявления не только исполнителей, но и организаторов преступных сетей, при соблюдении баланса между эффективностью и защитой прав граждан.

2.2. Личность типичного преступника незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Личность преступника, занимающегося незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий, не поддаётся однозначной типологизации, однако анализ следственной практики позволяет выделить ряд устойчивых характеристик, формирующих обобщённый портрет такого правонарушителя.

Как правило, это мужчина в возрасте от 18 до 40 лет, хотя в преступных схемах участвуют и лица других возрастных категорий, а также женщины - их доля и роль варьируются в зависимости от региональной специфики и структуры конкретной преступной группы. Социально-экономический статус большинства таких лиц отличается нестабильностью: значительная часть не имеет постоянного официального трудоустройства либо занята в неформальном секторе экономики. Это зачастую сопряжено с материальной нуждой, стремлением к быстрому получению дохода, а нередко - с собственной зависимостью от психоактивных веществ.¹⁰

Уровень образования неоднороден и коррелирует с выполняемой функцией в преступной схеме. Организаторы и администраторы онлайн-площадок нередко обладают средним техническим или высшим образованием, в том числе в сфере информационных технологий. Среди лиц, занимающихся изготовлением наркотических средств, встречаются те, кто имеет профильные знания в области химии, биологии или фармакологии. Курьеры и так называемые закладчики, как правило, демонстрируют более низкий уровень квалификации и образования.

Мотивация участников подобных преступлений многообразна. На первом плане - экономическая составляющая: желание получить доход, покрыть долги, оплатить лечение или поддерживать привычный образ жизни. Наряду с этим значимы психологические факторы - зависимость от наркотиков, стремление к групповой идентификации, ощущение причастности к «закрытому кругу». Нередко участие в незаконном сбыте стимулируется наличием долговых обязательств перед организаторами либо предшествующим криминальным опытом: лица с судимостями за

¹⁰ Куашев Алим Ауесович Характеристика личности преступника, совершающего преступления с использованием информационно-коммуникативных технологий в сфере незаконного оборота наркотических средств // Пробелы в российском законодательстве. 2018. №4. URL: <https://cyberleninka.ru/article/n/harakteristika-lichnosti-prestupnika-sovershayuschego-prestupleniya-s-ispolzovaniem-informatsionno-kommunikativnyh-tehnologiy-v> (дата обращения: 03.06.2026).

имущественные преступления или незаконный оборот наркотиков чаще вовлекаются в подобную деятельность повторно.

Поведенческие и коммуникативные особенности таких лиц обусловлены спецификой преступной деятельности. Они привыкают к дискретной коммуникации, используя мессенджеры, закрытые каналы и анонимные учётные записи. В их действиях прослеживается стандартизация: шаблонные формулировки сообщений, унифицированные фотографии, регулярность активности в определённые временные промежутки. В офлайн-взаимодействиях они стремятся выбирать нейтральные, малозаметные места для встреч, прибегают к использованию подставных лиц для хранения и транспортировки запрещённых веществ, комбинируют личные контакты с дистанционными инструментами координации.

Техническая компетентность варьируется в зависимости от роли в преступной цепочке. Организаторы и администраторы площадок обычно владеют продвинутыми навыками работы с интернет-ресурсами, методами шифрования и анонимизации. Изготовители демонстрируют знания химических процессов и умение обращаться с соответствующим оборудованием. Курьеры и исполнители, как правило, ограничиваются базовыми умениями в области скрытной логистики и упаковки. Тем не менее даже менее технически подготовленные участники зачастую осведомлены о элементарных способах сокрытия цифровых следов: использовании временных сим-карт, создании одноразовых учётных записей, методах уклонения от мониторинга.

Медицинские и психофизиологические аспекты также играют существенную роль. Среди участников незаконного сбыта нередко выявляются лица с длительной историей употребления наркотиков, состоящие на учёте в наркологических учреждениях, имеющие хронические заболевания, связанные с образом жизни. Наличие зависимости способно усиливать рискованность поведения, влиять на мотивацию и характер взаимодействия внутри группы. При инъекционном употреблении наркотиков у таких лиц

могут обнаруживаться специфические следы, которые в совокупности с данными токсикологических исследований предоставляют дополнительную информацию для расследования.

В структуре преступных групп обычно наблюдается чёткое распределение функций. Организаторы координируют деятельность, управляют финансами и разрабатывают схемы сбыта. Диспетчеры (операторы) принимают и оформляют заказы, распределяют задачи между исполнителями. Закладчики размещают запрещённые вещества в тайниках, курьеры осуществляют транспортировку крупных партий, а кассиры контролируют денежные потоки. При этом один и тот же человек в разное время может выполнять различные роли, а преступные схемы адаптируются к мерам правоохранительных органов.¹¹

Важно подчеркнуть, что описанный портрет является не жёсткой классификацией, а инструментом для приоритезации проверок и формирования следственных версий. Интеграция данных о социально-биографических характеристиках, состоянии здоровья, цифровых следах и финансовых операциях позволяет составить наиболее полное представление о фигуранте и выстроить законные, этически обоснованные следственные действия в рамках действующего законодательства Российской Федерации. Все мероприятия, затрагивающие конституционные права граждан, должны проводиться исключительно на основании процессуальных норм с надлежащим документальным оформлением, что обеспечивает правовую допустимость собранных доказательств.

¹¹ Г. Х. Афзалетдинова К ВОПРОСУ ОБ ОСОБЕННОСТЯХ СОВЕРШЕНИЯ СБЫТОВ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ ОРГАНИЗОВАННОЙ ГРУППОЙ // Общество, право, государственность: ретроспектива и перспектива. 2020. №1 (1). URL: <https://cyberleninka.ru/article/n/k-voprosu-ob-osobennostyah-soversheniya-sbytov-narkoticheskikh-sredstv-i-psihotropnyh-veschestv-organizovannoy-gruppy> (дата обращения: 03.06.2026).

2.3. Типичная следовая картина незаконного сбыта наркотических средств с использованием информационно- телекоммуникационных технологий

Типичная следовая картина незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий представляет собой совокупность электронно-цифровых, материальных и оперативно-розыскных данных, отражающих все этапы преступной деятельности - от привлечения клиентов до получения оплаты и размещения «закладок».¹²

В первую очередь следует выделить электронно-цифровые следы, которые подразделяются на пассивные и активные. Пассивные следы образуются в результате обычного использования интернет-ресурсов: это IP-адреса устройств, история посещений сайтов, сведения о времени подключения к сети. Несмотря на попытки преступников скрыть такие данные с помощью анонимайзеров, при законном взаимодействии с провайдерами и операторами связи возможно установление реального IP-адреса и сведений о лице, на которое оформлен договор об оказании услуг связи.

Активные следы формируются в процессе целенаправленной коммуникации и включают: переписку в мессенджерах и социальных сетях, сообщения с координатами мест размещения «закладок», данные о переводах денежных средств через электронные платёжные системы или криптовалютные кошельки, инструкции по фасовке и транспортировке наркотиков, информацию о лицах, чьи персональные данные используются для сокрытия преступной деятельности. Для фиксации подобных следов проводится осмотр технических устройств (смартфонов, компьютеров,

¹² Меняйло Д. В., Малыгина Е. А. ЦИФРОВЫЕ СЛЕДЫ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ // ППД. 2022. №4. URL: <https://cyberleninka.ru/article/n/tsifrovyye-sledy-v-sfere-nezakonnogo-oborota-narkoticheskikh-sredstv> (дата обращения: 03.06.2026).

планшетов) с применением специализированного программного обеспечения, позволяющего извлекать информацию даже при блокировке или физическом повреждении устройств.

Материальные следы представлены непосредственно наркотическими средствами и предметами, контактировавшими с ними (упаковки, инструменты для фасовки - электронные весы, пластиковые пакеты, изоленга для маркировки), а также следами на местах размещения «закладок» (остатки упаковки в подъездах, на детских площадках, в гаражных кооперативах). Кроме того, к материальным следам относятся документы или носители информации, содержащие данные о маршрутах, «дропках» и иных аспектах преступной деятельности.

Значимую часть следовой картины составляют данные, получаемые в рамках оперативно-розыскной деятельности при соблюдении требований Федерального закона «Об оперативно-розыскной деятельности». К ним относятся: детализация телефонных соединений от операторов связи, позволяющая установить привязку к базовым станциям и отследить перемещения участников преступления; сведения от интернет-провайдеров о зарегистрированных IP-адресах и используемых ресурсах; информация от электронных платёжных систем и криптовалютных бирж, раскрывающая цепочки финансовых операций; данные от владельцев сервисов анонимизации, способствующие выявлению реальных IP-адресов пользователей.

Современные преступники активно применяют меры конспирации, усложняющие расследование. Они используют мессенджеры со сквозным шифрованием и функцией автоматического удаления сообщений, временные сим-карты, одноразовые учётные записи. Нередко вовлекаются лица, находящиеся в уязвимом положении (в том числе несовершеннолетние или лица с зависимостью), чьи персональные данные (сканы паспортов, геолокационные сведения) используются для подтверждения «лояльности» и впоследствии могут стать инструментом шантажа. Финансовые операции

маскируются посредством переводов через счета подставных лиц или юридических организаций перед обналичиванием.¹³

При расследовании подобных преступлений возникают определённые сложности. Ключевой проблемой является стремление преступников к максимальной анонимности. Особую трудность представляет отслеживание транзакций в криптовалютах, особенно при использовании бирж или специальных сервисов-миксеров. Быстрое удаление цифровых следов требует незамедлительного изъятия технических средств и проведения экспертиз. Кроме того, расследование нуждается в привлечении высококвалифицированных специалистов в области информационных технологий и современного программного обеспечения для анализа данных.

Для эффективного раскрытия преступлений в данной сфере необходимо тесное взаимодействие следователей с оперативными подразделениями, применение современных технических средств и методов, а также соблюдение всех процессуальных норм, предусмотренных законодательством Российской Федерации. При трансграничном характере преступной деятельности особую роль играет международное сотрудничество правоохранительных органов. Все следственные и оперативно-розыскные мероприятия должны проводиться строго в рамках закона с надлежащим документальным оформлением, что обеспечивает правовую допустимость получаемых доказательств.

¹³ Саркисян Карина Тархановна Проблемы собирания цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях // Актуальные проблемы российского права. 2025. №1 (170). URL: <https://cyberleninka.ru/article/n/problemy-sobiraniya-tsifrovyyh-sledov-pri-proizvodstve-sledstvennyh-deystviy-po-delam-svyazannym-s-nezakonnym-oborotom> (дата обращения: 03.06.2026).

Глава 3. РАССЛЕДОВАНИЕ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

3.1. Особенности доследственной проверки и первоначальный этап расследования незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Активное внедрение информационно-телекоммуникационных технологий в сферу незаконного оборота наркотиков существенно изменяет характер преступной деятельности. Это предъявляет особые требования к организации доследственной проверки и первоначальным следственным действиям. Использование онлайн-площадок, мессенджеров со сквозным шифрованием, сегментов darknet и динамичных платёжных схем создаёт высокий риск утраты цифровых следов. В связи с этим критически важны как оперативность реагирования, так и неукоснительное соблюдение процессуальных норм.

Правовая основа проводимых мероприятий базируется на положениях Уголовно-процессуального кодекса РФ. Ключевое значение имеет статья 144 УПК РФ, регламентирующая порядок проверки сообщений о преступлении. Вопросы изъятия и получения цифровых сведений регулируются статьями 182–186.1 УПК РФ. При этом необходимо учитывать требования профильных федеральных законов: «Об оперативно-розыскной деятельности», «О связи», «Об информации, информационных технологиях и о защите информации», «О персональных данных», а также законодательства о противодействии легализации доходов, полученных преступным путём.¹⁴

¹⁴ Бушуев И. В., Гончарова С. В., Полунина Е. Н. Проблемные вопросы доследственной проверки по материалам о преступлениях в сфере незаконного оборота наркотиков // Вестник ВУиТ. 2019. №3. URL: <https://cyberleninka.ru/article/n/problemnye-voprosy-dosledstvennoy-proverki-po-materialam-o-prestupleniyah-v-sfere-nezakonnogo-oborota-narkotikov> (дата обращения: 03.06.2026).

При поступлении сообщения о возможном интернет-сбыте наркотиков уполномоченное лицо обязано оперативно и всесторонне оценить поступившие сведения. На этапе доследственной проверки первостепенное значение приобретает фиксация источника информации с последующей оценкой её достоверности и степени срочности. Одновременно осуществляется сбор первичных материалов - скриншотов, ссылок, скриншотов чатов, платёжных уведомлений. Если существует риск быстрой утраты доказательств (например, удаление сообщений или истечение срока хранения логов), необходимо своевременно обосновать необходимость безотлагательных действий с учётом требований судебного контроля.

Вся первичная фиксация должна сопровождаться тщательным документированием. В материалах отражаются источник и время получения данных, подробно описываются проведённые операции по их сохранению - будь то фотосъёмка экрана или архивирование ссылок. Обязательно указываются лица, участвовавшие в фиксации информации. При этом следует избегать опоры исключительно на распечатки и скриншоты как на единственные доказательства. Хотя они полезны для оперативной ориентировки, для последующего допуска в суде требуются форензик-копии и документальное подтверждение целостности данных.

На стадии проверки целесообразно заблаговременно сформировать перечень организаций, от которых может потребоваться получение логов, резервных копий и платёжных сведений. К ним относятся операторы связи, интернет-платформы, банки и платёжные агрегаторы. Взаимодействие с этими субъектами должно осуществляться строго в рамках закона с соблюдением установленных процедур.¹⁵

¹⁵ Инна Валериевна Тишутина Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: актуальные вопросы правового обеспечения // Вестник Московского университета МВД России. 2025. №3. URL: <https://cyberleninka.ru/article/n/rassledovanie-prestupleniy-sovershennyh-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy-aktualnye-voprosy-pravovogo> (дата обращения: 03.06.2026).

Получение доступа к содержимому переписок, электронной почты и резервных копий осуществляется в строгом соответствии с требованиями уголовно-процессуального законодательства. Запросы к провайдерам оформляются только на основании процессуального решения - судебного разрешения или иного законного основания. В них чётко указываются период, виды запрашиваемых данных и правовые основания для их получения. При взаимодействии с иностранными сервисами необходимо учитывать длительность процедур взаимной правовой помощи и по возможности задействовать международные каналы взаимодействия для ускорения процесса.

Блокировать аккаунты и накладывать арест на сообщения можно только на законных основаниях - для этого нужны документы: судебное решение, протоколы о выемке, соответствующие акты. Если действия затрагивают конституционные права граждан, важно соблюдать принцип пропорциональности и вмешиваться в частную жизнь минимально.

Оперативно-розыскные мероприятия помогают подтвердить каналы сбыта и разобраться, кто какую роль играет в преступной схеме. Особенно важны проверочные закупки: их планируют вместе со следователем и обязательно фиксируют на аудио и видео. Во время таких операций строго соблюдают правила безопасности и стараются не затрагивать права третьих лиц. В итоге должны получить вещественные образцы для судебной химической экспертизы и собрать достаточно оперативной информации, чтобы начать следственные действия - например, провести обыски и выемки.

Обыск и изъятие электронных устройств проводят по процессуальным нормам. При этом детально протоколируют каждое действие: записывают марку, модель, серийный номер и IMEI каждого устройства, фиксируют его состояние на момент изъятия, отмечают, есть ли SIM- и SD-карты. Устройства сразу изолируют от сети, оформляют акты приёма-передачи. Если при изъятии и последующем исследовании устройств участвует специалист по цифровой

криминалистике, проще соблюсти методики форензик-копирования и хеш-контроля - а значит, материалы будут весомее в суде.

На этапе доследственной проверки нельзя самостоятельно изучать содержимое устройств - без экспертизы и решения следователя или суда это запрещено. Такие действия не просто нарушают процессуальные нормы, но и могут привести к утрате доказательств.

В начале расследования анализ платёжных операций помогает выявить, откуда поступают деньги: будь то банковские карты, счета, электронные кошельки или платёжные агрегаторы. Одновременно выясняют схемы обналичивания и ищут возможных посредников. Запросы к банкам и платёжным системам составляют с учётом законодательства о банковской тайне и норм по противодействию легализации преступных доходов. Расследование идёт эффективнее, если сочетать финансовую аналитику с цифровыми логами и данными от провайдеров: так проще установить причинно-следственные связи и понять, кто за что отвечал в преступной схеме.

Ошибки на начальном этапе расследования порой приводят к тому, что доказательства признают недопустимыми. Чаще всего встречаются такие промахи: нет должной мотивации для срочных действий, запросы к провайдерам оформлены некорректно, данные изъяли без судебного решения, не сохранили доказательства должным образом. Чтобы снизить риски, нужно скрупулёзно документировать каждое действие, привлекать квалифицированных специалистов для форензик-копирования, грамотно составлять судебные ходатайства - чётко указывать, какие данные нужны и в какие сроки их надо предоставить.

Успешная доследственная проверка и начальный этап расследования держатся на балансе между оперативностью и строгим соблюдением процессуальных норм. Если грамотно организовать первичные действия, получится сформировать надёжную доказательственную базу из цифровых и финансовых доказательств. Это заложит прочный фундамент для дальнейших

следственных мероприятий и повысит шансы на успешное судебное преследование по статьям Уголовного кодекса РФ.

Чтобы расследование шло результативнее, стоит заранее подготовить шаблоны процессуальных документов, прописать чёткие регламенты взаимодействия с банками и провайдерами, обеспечить быстрый доступ к услугам региональных форензик-лабораторий. Так получится сократить разрыв между фиксацией оперативной информации и созданием надёжных доказательств, которые отвечают всем требованиям закона.

3.2. Типичные следственные ситуации и версии расследования незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Р. С. Белкин определял следственную ситуацию как совокупность условий, в которых идёт расследование, - иными словами, как обстановку, в которой разворачивается процесс. На практике чаще всего попадают несколько типовых ситуаций. Бывает, что человека задерживают при передаче или получении наркотика: тогда цифровые следы - переписка, платежи, скриншоты - сочетаются с вещественными уликами. Иногда обнаруживают тайник или посылку с цифровыми маркерами: треками доставки, уведомлениями, - но исполнителя при этом нет. Встречается и так: каналы сбыта выявляют в соцсетях, мессенджерах или даркнете, а администраторы и продавцы остаются неустановленными. Порой в распоряжении следствия - лишь разрозненные цифровые данные: логи, IP-адреса, криптовалютные транзакции, - без сопоставимых материальных улик. Наконец, бывают аналитические

сценарии с распределёнными ролями участников: транзакции там небольшие, активно задействуются миксеры и замысловатые маршруты вывода средств.¹⁶

Для каждой такой ситуации стоит выдвигать и проверять несколько рабочих гипотез. Например, предположить, что перед нами непосредственный продавец, курьер или исполнитель, администратор площадки, финансовый посредник (мани-мул), технический помощник (тот, кто обслуживает ботов или хостинг) либо что всё это провокация или «площадка-ловушка».

Чтобы верифицировать версии, приходится комплексно сопоставлять цифровые и материальные следы. Для этого делают форенз-копирование и сохраняют устройства с соблюдением chain of custody. Отправляют запросы к провайдерам и хостерам за логами и метаданными - разумеется, с судебным оформлением. Оперативно запрашивают данные в банках, платёжных системах, а если нужно - у криптобирж и аналитических сервисов. Анализируют сообщения и объявления: и по содержанию, и с лингвистической точки зрения. Сопоставляют тайм-штампы сообщений с трек-данными отправок, видеозаписями и показаниями свидетелей. Идентифицируют уникальную маркировку упаковки и микрочастицы на изъятых партиях. Не обойтись и без оперативных мероприятий - наблюдения, контрольных закупок, - но их надо тщательно обосновывать с точки зрения закона и процессуальных норм: иначе доказательства могут признать недопустимыми.

Есть и особые риски. Преступники анонимизируются через TOR или VPN, мгновенно удаляют сообщения, пользуются ephemeral-сообщениями и шифрованием, пускают деньги через криптовалютные миксеры и обменники. Чтобы нейтрализовать эти угрозы, в первую очередь надо сохранять логи и образы, быстро блокировать финансовые каналы, привлекать сетевых экспертов и комбинировать улики: цифровые и материальные должны

¹⁶ Чистова Любовь Евгеньевна К вопросу о типичных следственных ситуациях при расследовании незаконного оборота наркотиков // IN SITU. 2016. №11. URL: <https://cyberleninka.ru/article/n/k-voprosu-o-tipichnyh-sledstvennyh-situatsiyah-pri-rassledovanii-nezakonnogo-oborota-narkotikov> (дата обращения: 03.06.2026).

подтверждать роли участников. Нередко приходится взаимодействовать с зарубежными партнёрами: данные от хостеров и обменников за границей получить без международного сотрудничества почти нереально. При этом нужно учитывать сроки MLAT и особенности юрисдикций - и заранее продумывать запасные варианты, чтобы не терять время.¹⁷

Межведомственная координация тут критически важна. Следственные подразделения, оперативные службы, эксперты по цифровой криминалистике, финансовые аналитики и, если требуется, международные партнёры должны действовать слаженно. Не менее значима и экспертиза: не только судебно-химическая и биологическая, но и цифровая. Надо уметь восстанавливать удалённые данные, анализировать сетевую активность, трассировать криптопотoki. А процессуальная строгость - грамотное оформление ходатайств и протоколов изъятий, пломбирование, хеш-контроль - напрямую влияет на то, примут ли материалы в суде.

Бороться с цифровым наркотрафиком можно лишь при системном обновлении подходов. Тут мало тактической гибкости - нужны институциональные изменения. Правоохранительным органам стоит вкладываться в специализированные цифровые лаборатории и непрерывно обучать экспертов, оттачивать практику оперативной правовой подготовки запросов к провайдерам и финансовым институтам, выстраивать прозрачные протоколы взаимодействия с IT-компаниями. При этом нельзя терять баланс между оперативной эффективностью и защитой гражданских прав: ускоренное форенз-копирование и оперативные меры не должны подменять судебный контроль и соблюдение процедур. Иначе доказательства потеряют силу, а доверие общества будет подорвано. Учитывая, что многие платформы и платёжные схемы работают на трансграничном уровне, нужно активнее

¹⁷ Саркисян Карина Тархановна Проблемы собирания цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях // Актуальные проблемы российского права. 2025. №1 (170). URL: <https://cyberleninka.ru/article/n/problemy-sobiraniya-tsifrovyyh-sledov-pri-proizvodstve-sledstvennyh-deystviy-po-delam-svyazannym-s-nezakonnym-oborotom> (дата обращения: 03.06.2026).

налаживать международную кооперацию и обмениваться опытом. И параллельно адаптировать национальное законодательство к быстрому развитию технологий - чтобы следствие действовало и оперативно, и легитимно.

3.3. Тактика проведения отдельных следственных действий при расследовании незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Каждый вид преступлений обладает собственной спецификой, которая особенно заметна в приёмной технологии проведения следственных действий. Это полностью относится и к делам об незаконном обороте наркотиков. На наш взгляд наиболее трудоёмкими и тактически значимыми являются допрос и обыск - им и следует уделять повышенное внимание при планировании расследования.

Правовой статус допрашиваемого (свидетель, подозреваемый и т.д.) имеет ключевое значение для тактики. Это особенно важно уже на стадии проверки сообщения о преступлении, когда объяснения получают сразу после обнаружения факта. При этом практика показывает системные недостатки: в значительной доле случаев должностные лица ограничиваются поверхностным сбором объяснений, в трети протоколы оформляются трудночитаемым почерком, и лишь в примерно каждом десятом случае формулируются наводящие вопросы. Часто это связано с тем, что участковые уполномоченные, ожидая передачи материала в другие органы по подследственности, фиксируют лишь формальные основания для такой передачи, что в дальнейшем серьёзно осложняет работу следователя. Лица,

давшие поверхностные объяснения, получают время для подготовки к полноценному допросу, а следователь, не уточнив ключевые моменты (например, точное время совершения деяния), вынужден затрачивать значительные ресурсы на перебор видеозаписей и иных материалов за крупные промежутки времени.

Допросы - как свидетелей, так и подозреваемых - должны проводиться по заранее разработанному следователем алгоритму, который учитывает текущую следственную ситуацию, характер и объём уже имеющихся доказательств, выдвинутые версии и ожидаемую линию защиты. Подготовительный этап включает решение организационных вопросов: изучение материалов дела или материалов проверки, детальное изучение личности допрашиваемого для установления психологического контакта, выбор способа вызова (по телефону, повесткой и пр.), обеспечение участия защитника, определение времени и места проведения допроса (в следственном отделе, по месту жительства и т.д.), тактическую подготовку (подготовка вещественных доказательств и материалов дела), техническое обеспечение (включая видеосъёмку), сам допрос и последующую фиксацию его результатов. В отношении несовершеннолетних при допросе видеозапись является обязательной, если на неё не возражают сам несовершеннолетний или его законный представитель.

В соответствии с частью 1 статьи 56 УПК РФ свидетелем признаётся лицо, которому могут быть известны обстоятельства, имеющие значение для расследования, и которое вызвано для дачи показаний. По делам, предусмотренным статьёй 228 УК РФ, такими лицами могут выступать самые разные граждане - очевидцы, понятые, работники бригад скорой помощи и т.д. Особую информационную ценность обычно представляют близкие лица подозреваемого (родственники, сожители, друзья), а также коллеги, соседи и сослуживцы. Вместе с тем следует учитывать, что личные взаимоотношения с подозреваемым часто затрудняют получение объективных сведений.

Указанных лиц целесообразно разделять по функциональному признаку. В первую группу входят свидетели, способные сообщить о подготовке, совершении или сокрытии преступления и предоставить иные фактические данные: наличие или отсутствие у подозреваемого умысла на сбыт, сведения о потреблении наркотиков и его частоте, сведения о предыдущем опыте приобретения или изготовления наркотиков, а также сведения о лицах, оказывавших на него влияние. Во вторую группу включаются лица, чьи показания в дальнейшем могут быть верифицированы или опровергнуты - те, кто даёт правдивые показания, сознательно лжёт либо утаивает известные ему факты.

Необходимо помнить, что свидетель может стать и подозреваемым, особенно когда отсутствуют данные о другом очевидном лице, либо имеются основания полагать причастность группы лиц. Поэтому перед допросом важно собрать максимум предварительной информации о свидетеле. Если же есть серьезные основания полагать, что сам свидетель причастен к преступлению, начинать с него допрос не всегда целесообразно. В то же время промедление также недопустимо в случаях, например, задержания лица с поличным: узнав о результатах оперативных мероприятий, задержанный может испытывать страх и растерянность, что порой способствует получению более правдивых показаний, нежели опрошенный спустя длительное время.

В тактическом плане целесообразна очередность и выбор первых допрашиваемых. При наличии времени логично сначала опросить понятых, сотрудников правоохранительных органов, прибывших на место, и других очевидцев - из них можно получить сведения о том, при каких обстоятельствах обнаружен факт незаконного приобретения, хранения, перевозки или изготовления наркотиков, где именно это произошло, какие технико-криминалистические средства применялись, какие признаки имели изъятые вещества или предметы. От этих лиц выясняется поведение подозреваемого во время процессуальных действий, его объяснения при задержании или обыске, а также кем, куда и каким образом изъяты и

упакованы вещественные доказательства и обеспечивалась ли при этом достаточная видимость действий сотрудников.¹⁸

Практика привлечения в качестве понятых так называемых «общественных помощников» заслуживает осторожности: хотя закон не вводит жёстких ограничений, ведомственные акты и следственные стандарты могут установить запреты или ограничить такую практику. Считаем привлечение неподготовленных лиц в качестве понятых нежелательным в большинстве случаев, поскольку это может повлиять на надёжность фиксации действий и их оценку в дальнейшем.

Допрос каждого из участников следует планировать с учётом той информации, которая могла быть ему доступна. Протоколирование, детальная фиксация показаний и сопоставление рассказов между собой позволяют выявить противоречия и уточнить хронологию событий. Тактическое мастерство следователя проявляется в умении выстраивать последовательность действий так, чтобы не дать обвиняемым и заинтересованным лицам времени для согласования позиций и подготовки противоречащих показаний.

При опросе близких родственников, друзей, сожителей и других лиц, находившихся в тесных отношениях с подозреваемым, важно системно прояснить весь круг обстоятельств, которые могут свидетельствовать о его причастности к незаконному обороту наркотиков или указывать на источники и способы их получения. Содержание такого опроса должно охватывать следующие тематические блоки.

Употребление и наличие веществ: имел ли место приём наркотиков у подозреваемого раньше, кому об этом могло быть известно, замечал ли допрашиваемый у него сами вещества, части растений или приспособления,

¹⁸ Удовиченко Виктор Сергеевич Тактико-ситуационное обеспечение допроса подозреваемого в сбыте наркотических средств посредством глобальной сети Интернет // Известия АлтГУ. 2015. №2 (86). URL: <https://cyberleninka.ru/article/n/taktiko-situatsionnoe-obespechenie-doprosa-podozrevaemogo-v-sbyte-narkoticheskikh-sredstv-posredstvom-globalnoy-seti-internet> (дата обращения: 03.06.2026).

свидетельствующие о хранении или изготовлении. Важно установить частоту и характер потребления, наличие ранее приобретённого опыта в приобретении или изготовлении, а также изменения в этом поведении во времени.

Бытовые и социальные связи: чем подозреваемый обычно занимается в свободное время, как проводит выходные и праздники, с кем чаще общается; характер и круг его друзей, коллег и знакомых, род их занятий. Выясняются источники его доходов, любые необычные финансовые поступления или расходы, а также наличие близких интимных связей, которые могли бы быть связаны с оборотом наркотиков.

Профессиональные и образовательные навыки: есть ли у подозреваемого образование или навыки в смежных областях (например, химия, ботаника, растениеводство), которые могли бы пригодиться при изготовлении веществ; отмечались ли успехи в соответствующих дисциплинах или работа, связанная с обращением с химическими веществами (например, на химическом предприятии).

Изменение поведения и режима: отмечались ли в поведении подозреваемого недавние изменения - чаще ли он стал отсутствовать дома, позже возвращаться с работы, уезжать в командировки; увеличилось ли общение с какими-то новыми лицами; появлялись ли признаки скрытности или стремления ограничить доступ посторонних к жилому помещению.

Намерения и предыдущая деятельность: были ли у допрошенного сведения о намерениях подозреваемого сбыть или передать обнаруженные вещества, имелись ли ранее факты сбыта или попыток сбыта; если известны сведения об изготовлении, важно уточнить объёмы, периодичность, места хранения и перевозки, а также участие третьих лиц - действовал ли подозреваемый один или совместно с кем-то.

Когда есть подозрение на изготовление наркотиков, нужно разобраться, могла ли такая деятельность вестись в лабораторных или полулегальных условиях. Для этого изучают бытовые и инженерные особенности места - где оно находится, как устроено. Смотрят, сколько этажей в доме, где

расположена квартира относительно других помещений, есть ли вентиляция, газоснабжение, какие особенности у электропроводки. Выясняют, замечали ли люди странные или неприятные запахи и не было ли из-за этого каких-то изменений в самочувствии. Обращают внимание на необычную активность соседей: например, доносятся ли ночью посторонние шумы, стоит ли постоянный гул от систем водоснабжения или канализации. Ещё важно понять, кто живёт в квартире подозреваемого и кого видели входящим туда. Иногда помогают свидетельства соседей - если они слышали разговоры, которые могут указывать на изготовление или оборот наркотиков.

Если речь идёт о выращивании растений, используемых для изготовления наркотиков, вопросы смещаются в агротехническую и ресурсную плоскость. Тут важно выяснить, где именно происходило выращивание, откуда взялись семена и удобрения, как человек узнал о методах культивации и обработки. Надо понять, какие приёмы применялись при выращивании и с какой целью. Наконец, спрашивают, знает ли допрашиваемый о других местах, где растут подобные растения, - и может ли он их назвать.

Тщательная фиксация ответов и сопоставление сведений от разных лиц помогают выявить противоречия, уточнить хронологию и очертить круг причастных. Тактическая цель таких опросов - получить максимально подробную и проверяемую информацию, которая позволит следствию оперативно принять меры, сузить круг обстоятельств и определить дальнейший план действий.

Особый интерес представляют вопросы, адресуемые лицам, приобретавшим наркотики через интернет-магазины, а также свидетелям таких действий. В условиях, когда сбыт часто организуется через тайники, важно строить допрос так, чтобы максимально подробно восстановить схему передачи и место хранения. Рекомендуемая структура вопросов включает несколько тематических блоков.

Вопросы по факту установки тайника

- Видели ли они людей, которые устанавливали тайник; если да - каковы их приметы и поведение.

- Наблюдали ли посторонних в подъезде или около предполагаемого места тайника в последние дни/часы.

- Каким образом был сделан тайник (на магните, на скотче, зарыт, спрятан в щели/нише и т.п.).

- Были ли замечены какие-либо предметы при извлечении тайника: сами вещества, упаковочный материал, мобильные устройства, носители информации (флеш-карты), упаковочные пломбы и т. д.; описать внешний вид и любые идентифицирующие признаки (цвет, маркировка, надписи, необычные метки).

Вопросы по электронным устройствам и носителям

- Кому принадлежат найденные устройства (смартфоны, ноутбуки, планшеты), сим-карты и банковские карты; если не подозреваемому - кому именно и при каких обстоятельствах они оказались у него.

- Когда и где устройства/сим-карты/карты были приобретены; с какой целью использовались.

- Какое программное обеспечение установлено на устройствах; какие приложения, мессенджеры, анонимизирующие или шифрующие утилиты применялись, и как именно они использовались в контактах со сбытчиками.

- Откуда у лица знания и навыки по использованию соответствующих программ; приобретал ли он такое ПО, имеет ли профильное образование или опыт в IT/информационной безопасности.

- Имеют ли обнаруженные программы специальное назначение (например, для сокрытия трафика, шифрования, автоматизации заказов) и каким образом это проявляется на практике.

- Каким способом осуществлялась коммуникация со сбытчиком: через какие каналы, с использованием каких учётных записей или идентификаторов; может ли лицо назвать или предоставить известные ему идентификационные данные контрагента (логины, номера, адреса почты, псевдонимы).

- Каким образом производилась оплата заказов (электронные переводы, карточные платежи, криптовалюта, наличные через третьих лиц); есть ли у допрашиваемого сведения о платёжных реквизитах или схемах конвертации средств.

Дополнительные уточнения

- Были ли у лица знания о логистике доставки (адреса тайников, характер маркировки, частота и время закладок); может ли он указать на другие места закладок или лиц, которые этим занимаются.

- Имеются ли свидетельства использования нескольких устройств для единого канала связи (смена сим- карт, «чистых» телефонов), и мог ли допрашиваемый наблюдать такую практику.

- Есть ли информация о том, кто из контактов может быть вовлечён в сеть сбыта (посредники, курьеры, организаторы), и каким образом происходил контакт между ними.

Тщательное и поэтапное выяснение этих фактов позволяет установить технологию доставки и передачи веществ, идентифицировать контрагентов и каналы оплаты, а также подготовить обоснованные процессуальные шаги по дальнейшему сбору цифровых и материальных доказательств.

У подозреваемого необходимо выяснить следующие вопросы:

- биографические сведения, место рождения, кем воспитывался, в какой обстановке;

- его ближайшее окружение (родственники, друзья, знакомые, коллеги, сослуживцы), с кем из них поддерживает близкие отношения;

- употребляет ли наркотики, какие, в каких дозах, как долго и как часто, с кем, склонил ли его кто-либо к употреблению наркотика, состоит ли на учете в психоневрологическом или наркологическом диспансере;

- если не употребляет, то с какой целью осуществлял незаконное приобретение, хранение, перевозку, изготовление или переработку наркотика, не намеревался ли он его кому-либо передать;

- каким образом был приобретен наркотик, где, от кого, с помощью каких технических средств осуществлялась связь с продавцом, стоимость наркотика, его размер;

- входит ли химия и смежные с ней науки в круг его интересов, имел ли высокую успеваемость по данным предметам, имеет ли специальное образование по данным направлениям;

- где хранился наркотик, специально приспособленные для этого места;

- если осуществлялась перевозка, маскировалось ли перевозка особым образом в транспортном средстве, каким образом;

- где было взято сырье для изготовления или переработки наркотика, где именно, что для этого было использовано, помогал ли ему кто-либо;

- откуда получена информация о конкретных способах совершения данного преступления;

- может ли он описать стадии изготовления изъятого наркотика, с помощью каких имеющихся предметов, оборудования это осуществлялось;

- в случае, если предварительно изготовлению наркотика осуществлялось его выращивание, явившееся сырьем для его изготовления, то необходимо узнать: как, где, в каком количестве выращивались растения, каким образом, какое оборудование для этого было приспособлено, какое куплено, источники приобретения семян и т.п., если им были собраны дикорастущие растения, то где, в какое время суток, когда, в каком количестве растений, произрастает ли сейчас там указанное растение, знает ли лицо об иных местах, где произрастает данное растение.

Допрос может проходить в бесконфликтной или конфликтной обстановке, а также переходить из одного состояния в другое по мере развития следственного действия.

1. Бесконфликтная обстановка

Бесконфликтная ситуация характеризуется отсутствием враждебности к следователю и готовностью допрашиваемого содействовать установлению

истины. В таких условиях эффективны приёмы, направленные на воспоминание и упорядочивание фактов:

- разъяснить допрашиваемому, что его показания помогут раскрыть преступление и установить виновных;
- попросить изложить события последовательно, по хронологии;
- предъявить вспомогательные средства (фотографии, схемы, планы и т.п.), облегчающие воспоминание;
- задавать вопросы, стимулирующие ассоциативную память;
- знакомить с фрагментами показаний других лиц (при необходимости и в соответствии с процессуальными нормами);
- при допросе на месте события дополнительно подчеркнуть общественную опасность совершённого деяния и значимость правдивых показаний.

2. Конфликтная обстановка

Как отмечает А. В. Репин, конфликтная ситуация проявляется через: отказ от дачи показаний, дачу ложных показаний, изменение ранее данных показаний, ложное алиби, самооговор, отказ подписать протокол, попытки давления, подкупа или шантажа, симуляцию болезни, попытки уничтожить материалы и т. п. На практике наиболее часто встречаются либо полный отказ от показаний, либо частично ложные показания.

3. Практически значимые тактики поведения следователя

При работе в ситуациях сопротивления целесообразно применять следующие тактические приёмы:

- чёткое разъяснение сущности и общественной опасности преступления, указание причин, по которым важна правдивость показаний; акцентирование на положительных качествах допрашиваемого или использование известных ему мотивирующих факторов;
- напоминание о последствиях за заведомо ложные показания (с учётом правового статуса допрашиваемого);

- устранение объективных причин и мотивов, мешающих давать правдивые показания (например, гарантии безопасности при угрозах со стороны третьих лиц); демонстрация бессмысленности ложных показаний в сложившейся ситуации;

- добиваться максимально подробных и детализированных показаний, чтобы выявить и поставить перед допрашиваемым противоречия - как внутри текущих показаний, так и между ними и ранее данными сведениями; требовать пояснений по обнаруженным несоответствиям;

- грамотное использование имеющихся доказательств и фактов, избобличающих лицо, с целью склонить его к признанию; при этом вопросы следует формулировать так, чтобы не раскрывать весь объём имеющихся данных и обмануть попытки обвиняемого «прочитать» уровень осведомлённости следствия;

- применять и другие приёмы преодоления противодействия (доверительная беседа, метод «легенды» и т.д.), выбирая тактику в зависимости от конкретного человека и ситуации.

Эффективность допроса зависит от гибкости тактического подхода, умения следователя корректно сочетать убеждение, демонстрацию фактов и обеспечение прав допрашиваемого, а также от своевременного реагирования на изменения в поведении и настроении опрашиваемого.

Одно из главных мест по рассматриваемому виду преступлений, производимому только после возбуждения уголовного дела, принадлежит такому следственному действию, как обыск. Задача данного действия заключается в отыскании следов преступления, проверке выдвинутых версий, получении новых доказательств и установлении иных обстоятельств.

Не описывая законодательно урегулированный порядок проведения обыска, отметим, что обыск осуществляется:

- 1) в определенное время: его производство можно отложить и произвести в дневное время, либо существует необходимость безотлагательного его проведения (в ночное время). Представляется, что

обыск должен быть неожиданным, в целях исключения возможности сокрытия следов преступления (а так как предметом выступают наркотики, для преступника это не вызовет сложностей);

2) по месту жительства, работы, учебы, в иных местах: склады, гаражи, дачные участки, коттеджи, автомобили, иные транспортные средства, обыск подозреваемых (обвиняемых), их одежды (личный обыск);

3) с целью поиска предметов, имеющих значение для уголовного дела, подлежат поиску и изъятию следующие предметы: электронные устройства подозреваемого (сотовые телефоны, ноутбуки и т.п.), наркотики, химические вещества, реагенты, оборудование, инструменты и бытовые приборы применяемые при изготовлении наркотика, упаковке и расфасовке, а также защитные средства (противогазы, фильтры для них, резиновые перчатки); те вещества, которые применялись при переработке наркотика, либо увеличении его массы (при том же весе наркотика); предметы, в которых хранился и перевозился наркотик (стоит учитывать, что многие из них замаскированы); предметы, используемые для потребления наркотиков (иглы, шприцы, ложки, бонги, кальяны, т.н. «гриндеры», используемые для крошения растительной массы и хранения наркотика и т.п.); следы рук на предметах; различного рода документация, которая может иметь отношение к рассматриваемому преступлению (чеки, квитанции и т.п.).

При проведении обыска по месту жительства, связанного с хранением наркотиков, легко упустить сопутствующие объекты - например, мастерскую или гараж, где вещество могло изготавливаться. Если задержанный успеет связаться с родственниками или сообщниками, улики могут быть быстро уничтожены. Чтобы этого избежать, раскрытие дела и проведение обыска требуют тщательного планирования.

Основные элементы подготовки

- Перечислить все возможные места и предметы, имеющие отношение к делу (жилище, гараж, дача, автомобиль, рабочие помещения и т. п.).

- Выбрать оптимальное время для обыска с учётом цели внезапности и безопасности.

- Собрать информацию о личности подозреваемого и о самом объекте обыска, чтобы предсказать поведение лиц на месте и оценить риски.

- Определить состав группы и распределить роли: следователь, оперативные сотрудники, понятые, специалисты (химики, эксперты по электронике), кинологи и т. п.

- Подготовить технические и защитные средства, организовать каналы связи и документирование действий.

- Продумать меры по обеспечению внезапности и разработать сценарии действий на случай нестандартных ситуаций: звонки на мобильный, появление посторонних у двери, попытки «подбросить» вещи и т. д.

- Изучить возможные пути отхода и варианты вооружённого сопротивления; при признаках синтеза наркотиков предусмотреть средства защиты против химических и других угроз.

Тактика проникновения и ход обыска

- Тактика должна быть разработана целиком - от подготовки до завершения процедуры. Вход в помещение не обязательно должен быть связан с принудительным вскрытием двери: при грамотном планировании можно войти в подходящий момент (при выходе или входе лица) и избежать разрушений.

- При необходимости используются иные пути доступа (через окна, вентиляцию, крышу и т. п.) или специальные технические средства; возможны и скрытные методы проникновения, если это оправдано и законно.

- Конкретные приёмы выбираются с учётом обстановки, оперативных данных и требований безопасности.

Взаимосвязь обыска и допроса; ответственность следователя

- Тактика обыска и стратегия допроса определяются фактами и информацией, которыми располагает следователь; оба действия взаимодополняют друг друга. Допрос следует рассматривать как заранее

продуманную тактическую операцию, направленную на проверку версий и получение уточняющей информации, а не как простое свободное повествование подозреваемого.

- Обыск - это не только поиск наркотиков; главная ответственность следователя - обеспечить безопасность участников, сохранить следы и корректно оформить изъятые доказательства в рамках процессуальных норм. Профессионализм проявляется в умении учитывать специфику действий, планировать их и координировать взаимодействие с оперативными и экспертными подразделениями.

Учет всех перечисленных аспектов повышает вероятность успешного обнаружения и надёжной фиксации доказательств, снижает риски и способствует достижению целей уголовного судопроизводства.

3.4. Использование специальных знаний при расследовании незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий

Специальные знания и профильные специалисты в расследовании дел с ИТ- компонентом

Расследование незаконного сбыта наркотических средств с использованием информационно - телекоммуникационных технологий требует сочетания глубоких технических, криминалистических и юридических компетенций. Ключевые области знаний включают цифровую криминалистику (forensics) - методы создания хешированных образов носителей, извлечение и анализ данных из мобильных устройств, ПК и облачных хранилищ, восстановление удалённых сообщений и анализ

метаданных; OSINT- компетенции - системный мониторинг публичных источников, архивирование страниц, идентификация аккаунтов и шаблонов поведения; крипто- аналитику - понимание устройства блокчейн- систем, методы трассировки транзакций, выявление операций через обменники и миксеры; традиционные криминалистические специализации - токсикология и аналитическая химия (идентификация веществ методами GC- MS, LC- MS/MS и др.), трасология упаковочных и следовых материалов, дактилоскопия и ДНК- исследования; финансовый анализ - построение цепочек движения средств, выявление схем структурирования и отмывания; процессуальная экспертиза - знание процессуального права, правил составления постановлений и обеспечения допустимости доказательств.¹⁹

В междисциплинарной команде каждый профиль имеет чёткую роль. Следователь координирует процесс, формулирует процессуальные документы и принимает ключевые решения; цифровой эксперт отвечает за корректное извлечение, сохранение и первичный анализ электронных данных и подготовку форензик- образов; аналитик блокчейна занимается трассировкой криптовалютных потоков и их корреляцией с ретроспективными событиями; OSINT- специалист поддерживает сбор публичных материалов и построение «социальной карты» аккаунтов; токсиколог/химик проводит лабораторную идентификацию изъятых веществ и оценивает их массу/чистоту; криминалист работает с физическими следами, упаковкой и местом осмотра; юрист обеспечивает соблюдение процессуальных норм и готовит запросы к провайдерам и в органы международного сотрудничества. Для крупных дел привлекаются также специалисты по информационной безопасности, сетевые аналитики и судебные переводчики.²⁰

¹⁹ М. О. Янгаева, Н. О. Павленко OSINT. ПОЛУЧЕНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ИЗ СЕТИ ИНТЕРНЕТ // АЮВ. 2022. №2 (38). URL: <https://cyberleninka.ru/article/n/osint-poluchenie-kriminalisticheski-znachimoy-informatsii-iz-seti-internet> (дата обращения: 03.06.2026).

²⁰ Судницын Алексей Борисович, Молоков Вячеслав Витальевич Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019. №2 (89). URL: <https://cyberleninka.ru/article/n/otdelnye-vozmozhnosti>

Требования к квалификации и аккредитации экспертов включают наличие профильного высшего образования, практического опыта и документальной аттестации. В российской практической плоскости эксперты должны иметь свидетельства о допуске к судебно-экспертной деятельности в установленном порядке, проходить регулярную переподготовку и подтверждение квалификации; на цифровых компетенциях полезны международные сертификации (например, EnCE, GCFA, CCE и пр.) и опыт работы с сертифицированным криминалистическим ПО. Критично значение стандартов и протоколирования: наличие методик, SOP и возможности описать в экспертизе применяемые процедуры и их ограничения.

Процессуально-правовое обеспечение получения цифровых и иных доказательств

Правовая база расследования включает уголовный и процессуальный кодексы (в российской практике - УК РФ и УПК РФ), а также законы, регулирующие обработку персональных данных (ФЗ- 152), информационные технологии и связи (ФЗ об информации; ФЗ «О связи»), и другие профильные нормативные акты. Международная кооперация опирается на механизмы взаимной правовой помощи (MLAT), двусторонние соглашения и международные конвенции (включая, где применимо, Конвенцию Совета Европы о киберпреступности).

Практически любой доступ к содержимому аккаунтов, логам провайдеров, геолокационной информации или к облачным хранилищам должен быть оформлен процессуально корректно: постановление следователя или решение суда, с чётким указанием объёма запрашиваемых данных, периода и обоснования необходимости. При выемке физических носителей обязателен протокол осмотра, создание форензик-образов с фиксированием контрольных хешей, документирование цепочки хранения. Запросы к иностранным провайдерам и хостинговым компаниям чаще происходят через

официальные каналы MLAT или через прямое взаимодействие при наличии юридических оснований; в отдельных случаях используются механизмы экстренного предоставления информации, если это предусмотрено соглашениями с провайдерами. При всех процедурах необходимо соблюдать принципы законности, соразмерности и уважения прав подозреваемых и третьих лиц: минимизация объёма изымаемой информации, обоснование временных рамок запроса, конфиденциальность персональных данных.

Проблемы и риски при проведении расследований

Технические и организационные барьеры могут существенно осложнить расследование. Шифрование (end- to- end), временные/ephemeral- сообщения, использование VPN/Tor и даркнет- маркетов снижают доступность содержимого коммуникаций; криптовалютные миксеры и обменники затрудняют трассировку финансовых потоков. Географическая рассредоточенность сервисов и субъектов создаёт юрисдикционные сложности; международные запросы часто занимают месяцы, что позволяет уничтожить улики.

Существует риск ошибочной атрибуции: цифровые следы не всегда однозначно указывают на конкретного человека - устройства могут быть общими, аккаунты - взломаны, сообщения - подложными. Автоматические аналитические решения порождают ложные корреляции, поэтому выводы должны подтверждаться экспертной оценкой и сопоставлением с традиционными уличными доказательствами (посылки, упаковка, лабораторные результаты). Недостаток квалифицированных кадров, ограниченные технические ресурсы и отсутствие централизованных баз данных по новым психоактивным веществам и цифровым индикаторам также увеличивают риск ошибок и снижают оперативность. Процессуальные ошибки - неполные или некорректно оформленные постановления, нарушение цепочки хранения - приводят к недопустимости доказательств в суде.

Практические аспекты: организация междисциплинарной работы и алгоритм действий

Организация работы должна опираться на заранее разработанные стандарты (SOP) и четкую координацию. Типичная последовательность действий начинается с инициации: поступление оперативной информации или заявления, первичная оценка рисков и угроз (включая химико-биологическую). Следует быстро подготовить процессуальные документы - обоснование для осмотра, выемки или доступа к данным у провайдеров. На месте осмотра реализуется триаж: фиксация обстановки фото/видео, идентификация критичных объектов (устройства, упаковки, следы), изъятие в порядке, исключающем модификацию данных (при цифровых носителях - по возможности изолировать питание и создать образ), оформление протоколов и цепочки хранения.

Параллельно формируются запросы к провайдерам и иницируется лабораторный анализ изъятых веществ. Дальнейший этап - распределение экспертных задач: назначение цифровой экспертизы, химико-токсикологической, трасологической и т. д. Ключевым моментом является интеграция результатов: создание единой хронологической модели событий, сопоставление временных меток сообщений и транзакций с доставкой посылок, физическими следами и лабораторными данными. Рекомендуется применять визуализацию связей (link-analysis), таймлайны и карту геоперемещений для понятного представления фактов в суде.

Документация должна включать подробные протоколы, хеш-контролли, экспертные методики с указанием программного обеспечения и его версии, ограничения применяемых методов и оценку степени достоверности выводов. Экспертное заключение должно быть составлено доступным языком, с чётким указанием методики, результатов и выводов, подтверждённых доказательствами. При подготовке материалов для суда важно предусмотреть наглядные экспонаты, сопроводительные пояснения и подготовку свидетелей-экспертов к простому и структурированному изложению сложных технических моментов и возможных возражений защиты.

Эффективное расследование незаконного сбыта наркотиков с использованием ИТ требует скоординированного междисциплинарного подхода: цифровая криминалистика, традиционные экспертизы, крипто- и финансовый анализ, OSINT и строгая правовая фиксация должны работать как единая система. Ключевые вызовы - шифрование, анонимизация, юрисдикционная фрагментация и риск ошибочной атрибуции - устраняются сочетанием оперативной аналитики, лабораторной верификации и соблюдения процессуальных гарантий. Практические меры: подготовка кадров, унифицированные SOP, создание специализированных центров и укрепление международного сотрудничества с провайдерами и правоохранительными органами.

3.5. Проблемы криминалистической профилактики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Распространение информационно-телекоммуникационных технологий (ИТТ) кардинально изменило характер незаконного оборота наркотических средств. Появление даркнет-площадок, мессенджеров с end-to-end-шифрованием, криптовалют и платформ для мгновенных коммуникаций обеспечило преступникам новые каналы сбыта, снижающие риск личных контактов и облегчая географическую диверсификацию реализации. Для криминалистики это означает переход от традиционных инструментов профилактики и расследования к требованиям цифровой компетенции, межведомственного взаимодействия и быстрого правового реагирования. В статье систематизированы основные проблемы, которые

препятствуют эффективной криминалистической профилактике таких преступлений, и предложены направления их преодоления.

Онлайн-сбыт обладает рядом отличительных черт: высокая степень анонимности участников, использование технических средств конспирации и дешёвая масштабируемость операций. Вдобавок распространение инструктивного контента (рецепты, советы по уклонению от контроля, «как заказать и получить») выступает фактором немедленного распространения практических знаний, что представляет угрозу не только для эффективности правоохранительных органов, но и для общественного здоровья.

Техническая анонимность и шифрование серьёзно осложняют криминалистическую профилактику. Преступники всё чаще прибегают к анонимизирующим сетям - Tor, I2P, - пользуются VPN-сервисами, распределёнными инфраструктурами и мессенджерами с end-to-end-шифрованием. Из-за этого практически невозможно быстро выявить участников сделок и точно установить их личности. Ещё сложнее отследить каналы поставок: действия в сети уже не получается напрямую связать с конкретными людьми.²¹

Стандартные методы фиксации дают сбой: логирование, привязка IP-адресов и анализ трафика перестают работать как раньше. Следствию приходится искать нестандартные решения - копать глубже в метаданные, сопоставлять события на уровне конечных точек, использовать данные человеческой разведки и ловить злоумышленников на допущенных ошибках. Но тут важно не перегнуть палку: даже в погоне за новыми процедурами нельзя допускать неконтролируемого массового наблюдения. Любые технические инструменты должны применяться строго в рамках процессуальных гарантий.

²¹ Петухов Андрей Юрьевич, Куликов Кирилл Сергеевич Проблемы противодействия использованию компьютерных технологий в незаконном обороте наркотиков // Вестник КРУ МВД России. 2020. №1 (47). URL: <https://cyberleninka.ru/article/n/problems-protivodeystviya-ispolzovaniyu-kompyuternyh-tehnologiy-v-nezakonnom-oborote-narkotikov> (дата обращения: 03.06.2026).

С криптовалютами ситуация не проще - тут проблемы идут рука об руку: и технические, и правовые. Блокчейн-платформы, сервисы микширования, децентрализованные обменники и приватные монеты создают серьёзные помехи: становится почти нереально привязать транзакции к реальным людям и проследить путь средств. Да, инструменты для аналитики блокчейна и трассировки платежей постепенно совершенствуются, но на практике их эффективность часто натывается на жёсткие ограничения. Во-первых, нет доступа к данным офф-чейн-звеньев - тем же платёжным шлюзам или ОТС-брокерам. Во-вторых, при запросах к криптобиржам возникают правовые барьеры. В-третьих, на рынке хватает инструментов, специально разработанных для сокрытия следов.²²

Решить эти проблемы можно только комплексно: нужно наладить более тесное межведомственное взаимодействие с финансовыми регуляторами, доработать процедуры по KYC/AML и чётко прописать правила работы с провайдерами криптосервисов.

Юрисдикционные и процессуальные барьеры затрудняют оперативное получение доказательств и принуждение зарубежных провайдеров к сотрудничеству. Многие площадки, хостинг-операторы и платёжные сервисы работают под юрисдикцией иностранных государств или через посредников в «нейтральных» юрисдикциях, что делает MLAT-запросы медленными и формализованными. Отсутствие механизмов экстренного сохранения данных, различия в подходах к защите персональных данных и несогласованность процессуальных требований создают длительные правовые проволочки, ослабляющие профилактический потенциал мер. Необходимы ускоренные процедуры сохранения и передачи электронных данных, а также

²² Решняк Ольга Александровна ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТЫ ПРИ ПРИОБРЕТЕНИИ НАРКОТИЧЕСКИХ СРЕДСТВ: ПРОБЛЕМЫ РАССЛЕДОВАНИЯ И ПУТИ ИХ РЕШЕНИЯ // ЮП. 2024. №2 (109). URL: <https://cyberleninka.ru/article/n/ispolzovanie-kriptovalyuty-pri-priobrenenii-narkoticheskikh-sredstv-problemy-rassledovaniya-i-puti-ih-resheniya> (дата обращения: 03.06.2026).

международные соглашения, адаптированные к скоротечности онлайн-операций.

Недостаточная техническая оснащённость и кадровый дефицит в следственных и экспертных подразделениях ограничивают возможности полноценной профилактики и расследования. Для эффективной борьбы с ИТТ-сбытом требуются современные инструменты для мониторинга закрытых каналов, аналитические платформы для работы с большими данными и блокчейн-аналитиками, лаборатории цифровой криминалистики и постоянно действующие централизованные ресурсы. Одновременно необходимы программы постоянного повышения квалификации, привлечение профильных специалистов из ИТ-сектора и создание условий для их долгосрочной работы в правоохранительных органах.²³

Методологические и доказательственные проблемы включают отсутствие единых стандартов по сбору, сохранению и оформлению цифровых следов, что повышает риск непринятия материалов в судебных инстанциях. Важны четкие протоколы сохранения целостности данных (hash-образы, метаданные, временные метки), верификация используемых инструментов и стандартизированные формулировки экспертных задач, позволяющие надёжно связать цифровые следы с преступной деятельностью и намерением.

Быстрая адаптация преступников требует от профилактики высокой гибкости: миграция площадок, использование одноразовых аккаунтов, мультиканальные схемы коммуникации и новые способы доставки (комбинация курьерских, почтовых и «тайниковых» методов) делают долгосрочное наблюдение малоэффективным без оперативных вмешательств и аналитики в

²³ Пупцева Анна Викторовна НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ, СОВЕРШЕННЫХ С ПОМОЩЬЮ СЕТИ "ИНТЕРНЕТ" БЕСКОНТАКТНЫМ СПОСОБОМ // Вестник Волгоградской академии МВД России. 2018. №3 (46). URL: <https://cyberleninka.ru/article/n/nekotorye-osobennosti-vyyavleniya-raskrytiya-i-rassledovaniya-prestupleniy-v-sfere-nezakonnogo-oborota-narkotikov-sovershennyh-s> (дата обращения: 03.06.2026).

реальном времени. Для противодействия необходимы проактивные методы - мониторинг трендов, автоматизированные системы оповещения и гибкие ресурсы, способные быстро настраиваться под новые модусы.

Распространение инструктивного контента - это отдельная угроза: когда в свободном доступе появляются рецептуры, технологические схемы и советы по конспирации, преступные практики начинают быстро копироваться. Чтобы с этим бороться, нужны скоординированные подходы к модерации и удалению таких материалов. При этом важно не ущемлять академическую свободу и право на информацию - тут выручит механизм ответственного раскрытия, сотрудничество с платформами и издателями, а ещё - чёткие руководства по безопасной публикации технической информации.

Криминалистическая профилактика незаконного сбыта наркотиков с использованием информационно-телекоммуникационных технологий упирается в целый клубок взаимосвязанных проблем. Тут и техническая анонимность со шифрованием, и сложности с финансовой трассировкой из-за распространения криптовалют, и юрисдикционные с процессуальными барьерами, и нехватка оборудования и кадров, и трудности с оформлением цифровых доказательств, и быстрая адаптация преступников, и риск массового распространения инструктивного контента. Каждая из этих проблем подтачивает превентивные возможности правоохранительных органов - и к каждой нужны точечные решения.

Справиться с вызовами можно только комплексно. Надо совершенствовать правовую базу и активнее взаимодействовать на международном уровне, вкладываться в технические средства мониторинга и аналитики - в том числе в blockchain-инструменты и системы работы с большими данными. Ещё важно разработать единые методики цифровой криминалистики и стандарты сохранения целостности доказательств, создать специализированные межведомственные центры и программы подготовки кадров, наладить конструктивное сотрудничество с провайдерами и платформами. При этом не стоит забывать про этические гарантии и

прозрачные процедуры: меры профилактики не должны подрывать правовую защиту граждан.

В приоритете - опережающая аналитика и гибкие оперативные механизмы. Речь про автоматизированный мониторинг трендов, проактивные операции в рамках закона, быстрые каналы для сохранения данных и плотную координацию с международными партнёрами. Дополнительный плюс даст профилактическая работа с обществом: снизить спрос помогут образовательные и социальные программы.

Только если синхронно развивать правовые, технические, методические и кадровые компоненты - и при этом устойчиво взаимодействовать с частным сектором и международным сообществом, - получится заметно усилить криминалистическую профилактику и сократить вред от нелегального онлайн-рынка наркотиков.

Заключение

Проведённое исследование подтвердило, что незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий представляет собой качественно новый и динамично развивающийся феномен, требующий специализированной криминалистической методики, адаптированной к особенностям цифровой среды. Анализ теоретических разработок, материалов 174 уголовных дел 2016–2025 гг. и опросов 167 сотрудников органов предварительного расследования позволил выявить ключевые закономерности преступной деятельности, типичные следовые элементы и проблемные зоны практической деятельности правоохранительных органов на предварительном и первоначальном этапах расследования.

Основные выводы исследования

- Специфика преступлений: торговля наркотиками в ИКТ-среде характеризуется высоким уровнем анонимности, географической рассредоточенностью, использованием криптоплатежей и сервисов с повышенной защитой конфиденциальности (darknet, зашифрованные мессенджеры). Это обуславливает смещение акцентов в расследовании с традиционных материальных доказательств на цифровые следы и косвенные поведенческие признаки.

- Криминалистическая структура методики: эффективная методика должна базироваться на принципах системности, адаптивности к технологическим изменениям, интеграции цифровой криминалистики с оперативно-разыскной практикой и строгом соблюдении процессуальных гарантий. Парадигма «быстрой и корректной фиксации цифровых следов» оказывается ключевой для сохранения доказательной ценности.

- Практические элементы: установлены приоритетные источники первичной информации (заявления граждан, мониторинг сетевого окружения, данные платёжных систем и провайдеров, результаты оперативных мероприятий), типичные схемы совершения преступлений и модельные версии, требующие проверки на доследственной стадии.

- Методические и организационные пробелы: отмечены недостаточная унификация стандартов документирования цифровых следов, недостаток специализированной подготовки следователей, слабая координация между экспертными подразделениями и оперативными органами, а также проблемы оперативного взаимодействия с провайдерами и платёжными операторами.

Практическая значимость и рекомендации

На базе проведённого анализа предложена комплексная методика, включающая алгоритмы получения и оценки первоначальной информации, типизации следственных ситуаций и рабочих версий, набор тактик для проведения приоритетных следственных действий и стандарты документирования цифровых следов (фиксация метаданных, контроль целостности данных, Chain of Custody, шаблоны протоколов и постановлений). Для внедрения методики рекомендуется:

- внедрить единые чек-листы и шаблоны процессуальных документов для доследственной проверки и выемки цифровых носителей;

- регламентировать порядок взаимодействия с провайдерами и платёжными системами посредством типовых запросов и межведомственных соглашений;

- усилить подготовку следователей и экспертов по цифровой криминалистике (курсы, практикумы, совместные учения);

- развивать техническую оснащённость экспертных подразделений (форензик-инструменты, системы корреляции логов, аналитические платформы);

- усиливать превентивные меры: мониторинг уязвимых каналов распространения, информационные кампании и взаимодействие с платформами для блокировки противоправного контента.

Ограничения и перспективы дальнейших исследований

Исследование опирается на материалы дел и опросов, характерных для 2016–2025 гг.; быстрый темп технологических изменений требует постоянного обновления методики и верификации её элементов на новых эмпирических данных. Перспективными направлениями дальнейшей работы являются: разработка отраслевых стандартов документирования цифровых доказательств, совершенствование нормативно-правового механизма обмена данными между государственными органами и коммерческими провайдерами, создание обучающих программ на основе кейс-методики и моделирование новых схем преступной деятельности с применением ИИ и скрытых платёжных протоколов.

Предложенная в работе комплексная методика даёт практико-ориентированный и теоретически обоснованный инструментарий для повышения эффективности предварительного и первоначального этапов расследования преступлений, связанных с незаконным сбытом наркотических средств в ИКТ-среде. Её внедрение и дальнейшая адаптация с учётом технологических тенденций способны существенно повысить качество фиксации цифровых следов, сократить время реагирования и укрепить доказательственную базу уголовных дел по данной категории преступлений.

Список использованной литературы

1. Бастрыкин А.И. Преступления в сфере незаконного оборота наркотиков. – М.: Юрлитинформ, 2020.
2. Волкова А.Н. Методика расследования преступлений, связанных с незаконным оборотом наркотиков. – М.: Юрайт, 2021.
3. Гаврилов Б.Я. Криминалистика: учебник. – М.: Норма, 2022.
4. Зеленин Д.А. Использование информационно-телекоммуникационных технологий при расследовании преступлений. – СПб.: Юридический центр Пресс, 2020.
5. Кабанов П.А. Цифровая криминалистика. – Казань: Казанский юридический институт МВД России, 2021.
6. Корухов Ю.Г. Современные подходы к расследованию преступлений, совершённых с использованием сети «Интернет». – М.: Проспект, 2019.
7. Лапатников М. В. Расследование преступлений, связанных с незаконным оборотом наркотиков: учебник для вузов / М. В. Лапатников, Т. А. Николаева, И. А. Казнина. - Москва: Издательство Юрайт, 2025.
8. Введенская Ольга Юрьевна КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ // Вестник КРУ МВД России. 2022. №1 (55).
9. Ковалев, С. А. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: Монография / С. А. Ковалев, В. Б. Вехов. – Москва: КТ "Буки-Веди", 2015. – 182 с. – EDN ZXEBQZ.

10. Шмонин, А. В. Методология криминалистической методики: монография / А. В. Шмонин; А. В. Шмонин. – Москва: Юрлитинформ, 2010. – 415 с. – (Библиотека криминалиста). – ISBN 978-5-93295-646-5. – EDN QRPNWL.

11. Голубчикова, А. А. Криминалистическая характеристика незаконного сбыта наркотических средств - курительных смесей, совершенного бесконтактным способом / А. А. Голубчикова // Молодежь и XXI век - 2018 : материалы VIII Международной молодежной научной конференции, Курск, 21–22 февраля 2018 года / Юго-Западный государственный университет. Том 3. – Курск: Закрытое акционерное общество "Университетская книга", 2018. – С. 348-351. – EDN LBPEUX.

12. Дремлюга, Р. И. Интернет-преступность / Р. И. Дремлюга. – Владивосток: Дальневосточный федеральный университет, 2008. – ISBN 978-5-7444-2114-4. – EDN QQZHWN.

13. Демидова, В. Р. Особенности криминалистической методики в расследовании наркотических преступлений / В. Р. Демидова // Вестник науки. – 2023. – Т. 4, № 12(69). – С. 405-409. – EDN RNHGTU.

14. Кустов Анатолий Михайлович, Мурзагалиева Оксана Канатовна, Шимановская Кристина Евгеньевна Типичная информация о личности преступника при расследовании преступлений, совершенных в сфере оборота наркотических средств // Успехи в химии и химической технологии. 2017. №7 (188).

15. Владимир Батоевич Батоев ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИЛИ ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: СПОСОБЫ ИХ СОВЕРШЕНИЯ И КОЛИЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ // Правопорядок: история, теория, практика. 2023. №3 (38).

16. Поддубный Илья Васильевич, Кураков Денис Владимирович ОБСТАНОВКА И СПОСОБЫ СОВЕРШЕНИЯ СБЫТА НАРКОТИЧЕСКИХ

СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2025. №1 (102).

17. Меняйло Д. В., Малыхина Е. А. ЦИФРОВЫЕ СЛЕДЫ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ // ППД. 2022. №4.

18. Решняк Ольга Александровна, Резван Александр Павлович ФИКСАЦИЯ СЛЕДОВ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ В СЕТИ ИНТЕРНЕТ // Вестник Волгоградской академии МВД России. 2020. №4 (55).

19. Роганов С. А., Роганова Т. Л. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ НАРКОБИЗНЕСА // Ленинградский юридический журнал. 2019. №4 (58).

20. Бирюков А. П. Тактика первоначальных следственных действий в расследовании преступлений в сфере незаконного оборота наркотических средств // Таврический научный обозреватель. 2016. №10-2 (15).

21. Лебеденко Сергей Евгеньевич, Унжакова Светлана Владимировна, Заер Евгения Валерьевна ОСОБЕННОСТИ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ СПЕЦИАЛИСТА ПРИ РАССЛЕДОВАНИИ ФАКТОВ НЕЗАКОННОГО ПРОИЗВОДСТВА НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ ПРЕКУРСОРОВ // Сибирский юридический вестник. 2023. №3 (102).

22. Аминев Ф. Г. Актуальные вопросы использования специальных знаний при расследовании преступлений в сфере незаконного оборота наркотиков // Правовое государство: теория и практика. 2014. №4 (38).

23. Сыроегин, В. А. Вопросы квалификации незаконного сбыта наркотических и психотропных веществ, с использованием сети Интернет / В. А. Сыроегин, А. Б. Калинкина // Современное состояние, проблемы и перспективы развития специальных знаний : Материалы Всероссийской научно-практической конференции, Новосибирск, 19 ноября 2024 года. –

Москва: Московская академия следственного комитета, 2025. – С. 79-84. – EDN JLKWAV.

24. Третьяков, Г. М. Информационные технологии в структуре способа совершения преступлений, связанных с незаконным оборотом наркотических средств / Г. М. Третьяков // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. – 2021. – Т. 11, № 1. – С. 96-103. – EDN DJWCXX.

25. Соболевская, С. И. Отдельные вопросы использования специальных знаний при расследовании преступлений о фактах незаконного сбыта наркотических средств, психотропных веществ и их аналогов / С. И. Соболевская // Использование специальных знаний: теоретико-правовая парадигма и проблемы практической деятельности : Материалы международной научно-практической конференции, Владивосток, 26–27 сентября 2019 года. – Владивосток: Дальневосточный юридический институт Министерства внутренних дел Российской Федерации, 2019. – С. 269-275. – EDN LRKXHQ.

26. Гуриков, С. Р. Интернет-технологии / С. Р. Гуриков. – Изд. 2-е : ООО "Научно-издательский центр Инфра-М", 2022. – 174 с. – (Высшее образование: Бакалавриат). – ISBN 978-5-16-016517-2. – DOI 10.12737/1044018. – EDN YHGreg.

27. Земцова, С. И. Принцип "дополнительности" специальных знаний и его использование при производстве отдельных видов следственного осмотра по уголовным делам, связанным с незаконным оборотом наркотиков / С. И. Земцова // Библиотека криминалиста. Научный журнал. – 2017. – № 1(30). – С. 213-220. – EDN XQWZKX.

28. Давыдов, Е. В. К вопросу назначения и проведения отдельных видов судебных экспертиз при расследовании преступлений в сфере незаконного оборота наркотических средств, психотропных веществ или их аналогов / Е. В. Давыдов, Ю. С. Василенко // Право и управление. – 2025. – № 4. – С. 95-98. – DOI 10.24412/2224-9133-2025-4-95-98. – EDN DMBSVB.

29. Назначение многообъектных экспертиз по фактам незаконного сбыта, изготовления и хищений наркотических средств / Д. В. Кайргалиев, Д. В. Васильев, Н. А. Анчабадзе [и др.] // Современные проблемы науки и образования. – 2015. – № 2-2. – С. 699. – EDN UZJIFH.

30. Павлов Владимир Григорьевич, Роганов Сергей Александрович Криминалистическая профилактика преступлений в сфере наркобизнеса // Ленинградский юридический журнал. 2012. №1.

31. Меретуков Гайса Мосович, Лунина Евгения Станиславовна, Бирюкова Сусана Николаевна Криминалистическая профилактика по конкретному уголовному делу о незаконном обороте наркотиков // Научный журнал КубГАУ. 2017. №128.