Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)»

На правах рукописи

Саркисян Карина Тархановна

Судебные экспертизы объектов в цифровой форме в компьютерных сетях при расследовании незаконного оборота наркотических средств

Специальность 5.1.4. Уголовно-правовые науки

диссертация на соискание
ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Россинская Елена Рафаиловна

Москва – 2025

Оглавление

Введение 3

ГЛАВА 1. Современное состояние судебных экспертиз цифровых следов в компьютерных сетях при расследовании незаконного оборота наркотических средств 18

§ 1.1. Характеристика преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях 18

§ 1.2. Классификация объектов судебных экспертиз (цифровых следов) при расследовании незаконного оборота наркотических средств в компьютерных сетях..... 44

§ 1.3. Собирание цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях..... 62

ГЛАВА 2. Производство судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях..... 92

§ 2.1 Особенности назначения судебных экспертиз при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях..... 92

§ 2.2 Судебно-экспертные технологии производства экспертиз по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях..... 120

§ 2.3 Оценка и использование результатов судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях..... 149

Заключение..... 168

Список использованных источников и литературы..... 174

Приложение № 1. Форма анкеты для проведения опроса сотрудников правоохранительных органов по актуальным вопросам, связанным с назначением судебных экспертиз в рамках расследования незаконного оборота наркотических средств в компьютерных сетях 196

Приложение № 2. Результаты анкетирования сотрудников правоохранительных органов по актуальным вопросам, связанным с назначением судебных экспертиз в рамках расследования незаконного оборота наркотических средств в компьютерных сетях 201

Введение

Актуальность темы диссертационного исследования

В последние годы наблюдается рост незаконного оборота наркотических средств с использованием компьютерных сетей. Такая тенденция обусловлена цифровизацией всех сфер жизни общества и активным внедрением компьютерных технологий. В результате преступления, в частности их криминалистическая характеристика, претерпели значительные изменения. При этом появление новых способов, новых участников преступления естественным образом определило необходимость трансформации отдельных положений уголовно-правовых наук.

Традиционные методы расследования незаконного оборота наркотических средств, которые успешно применялись ранее, уже оказываются недостаточно эффективными. Этим подтверждается необходимость разработки и внедрения иных подходов к раскрытию таких преступлений.

Незаконный оборот наркотических средств, совершаемый с использованием компьютерных сетей, отличается особой сложностью и комплексностью, что обуславливает необходимость использования более глубокого подхода в процессе расследования таких дел. Ввиду того, что большинство преступной деятельности в сфере незаконного оборота наркотических средств осуществляется в теневом сегменте Даркнет, который обеспечивает высокий уровень конфиденциальности, криминалистически значимая информация представлена в цифровой форме в виде цифровых следов. Факт роста преступности указывает на необходимость разработки рекомендаций работы с цифровыми следами (начиная от их собирания заканчивая передачей их для производства судебной экспертизы) для рассматриваемой категории дела.

Существенное значение при расследовании незаконного оборота наркотических средств в компьютерных сетях имеют судебные экспертизы. В особенности, если учитывать тот факт, что использование компьютерных технологий привело к появлению цифровых следов, которые как раз являются

объектом исследования многих родов и видов судебных экспертиз. Заключение эксперта, будучи одним из видов доказательств, в отдельных случаях является исключительным способом получения криминалистически значимой информации, связанной с цифровыми следами.

Понимание цифровых следов уже сформировалось, хотя все еще ведутся активные дискуссии по данной проблематике среди ученых. Вместе с тем потребность в урегулировании стоит остро, так как от степени разработанности теоретических положений зависит практическая деятельность участников процесса.

То же касается и судебных экспертиз. Теория цифровизации судебно-экспертной деятельности раскрывает общие аспекты цифровых следов как объектов для всех родов и видов судебных экспертиз. Но каждому роду и виду присущи свои особенности, которые должны быть учтены и отражены впоследствии в методическом обеспечении.

Таким образом прослеживается актуальность совершенствования теоретических, правовых, организационных и методических основ цифровизации судебно-экспертной деятельности, а также различных родов судебных экспертиз, назначаемых при расследовании преступлений в области незаконного оборота наркотических средств.

Степень разработанности темы исследования

Необходимость противодействия незаконному обороту наркотических средств обусловила значительное количество научных исследований, посвященных данной проблематике. В этом контексте можно выделить труды таких ученых, как Х. Д. Аликперов, Т. А. Боголюбова, В. И. Брылев, Ю. П. Гармаев, Э. Г. Гасанов, В. Н. Гуляев, С. П. Евтеев, О. А. Есина, Л. В Иногамова-Хегай, П. В. Кривошеин, К. С. Кузьминых, Г. М. Меретуков, В. И. Пархоменко, В. П. Приказчиков, С. А. Роганова, Г. В. Середа, А. Н Сергеев, Е. В. Тарасова, А. В. Федоров, А. Е. Шалагин, Р. Д. Шарапов, Н. Н. Щелочков и другие.

Аспекты использования специальных знаний при расследовании дел незаконного оборота наркотических средств были рассмотрены в работах Е. В. Ивановой, Л. В. Лазаревой, В. В. Клевцова, А. П. Когосова, В. Н. Курченко. В их трудах подчеркивается значимость комплексного подхода к использованию экспертных знаний в рамках уголовного процесса, а также необходимость интеграции новых технологий в практику расследования.

Тем не менее вопросы, касающиеся производства в рамках данной категории дел судебных экспертиз цифровых следов, не были полноценно затронуты в науке.

Вместе с тем цифровизации судебно-экспертной деятельности (и в частности, цифровым следам как объектам судебной экспертизы) посвящены работы В. Б. Вехова, Ю. В. Гаврилина, С. В. Зуева, В. А. Мещерякова, Н. С. Неретиной, Г. Г. Омельянюка, В. В. Полякова, Е. Р. Россинской, И. А. Рядовского, А. И. Семикаленовой, А. И. Усова.

Анализ научной литературы продемонстрировал, что ряд положений, связанных с использованием специальных знаний, в частности производства судебных экспертиз цифровых следов, изменением задач, методов, методик судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях, а также изменением способов самого преступления в условиях цифровизации, ранее целостно и концептуально не рассматривались.

Объектом исследования является следственная, экспертная и судебная практика, сформировавшаяся при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях.

Предметом настоящего исследования являются закономерности формирования теоретических, организационных и методических основ цифровизации судебно-экспертной деятельности, применяемых в рамках расследования незаконного оборота наркотических средств, а также различных родов судебных экспертиз, назначаемых при расследовании преступлений в области незаконного оборота наркотических средств.

Цель диссертационного исследования заключается в изучении и последующем совершенствовании теоретических, правовых, организационных и

методических основ цифровизации судебно-экспертной деятельности в рамках расследования незаконного оборота наркотических средств, а также различных родов судебных экспертиз, назначаемых при расследовании преступлений в области незаконного оборота наркотических средств.

Для достижения указанной цели исследования последовательно решались следующие **задачи**:

– определение произошедших изменений криминалистической характеристики преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях;

– разработка классификации цифровых следов, встречающихся при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях;

– выделение особенностей собирания цифровых следов при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях;

– исследование трансформации компетенций следователя, специалиста и судебного эксперта в эпоху цифровизации;

– выделение особенностей назначения судебной экспертизы при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях;

– анализ трансформации судебных экспертиз с появлением цифровых следов на примере отдельных родов судебных экспертиз;

– рассмотрение возможностей судебных экспертиз для получения криминалистически значимой информации при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях;

– установление критериев оценки заключения эксперта.

Методология и методы научного исследования основаны на диалектическом подходе к познанию, который предполагает рассмотрение явлений в их взаимосвязи и развитии и который позволил рассмотреть различные точки

зрения о понятии, особенностях цифровых следов, образованных в ходе незаконного оборота наркотических средств.

В исследовании применялись также общенаучные методы (наблюдение, описание, сравнение, моделирование и другие), частнонаучные методы (формально-юридический, сравнительно-правовой, статистический и другие). В работе были использованы методы судебной экспертологии (общеэкспертные методы), а также методы частной теории судебных экспертиз (частноэкспертные методы).

Перечисленные методы использовались при написании работы как в совокупности, так и при решении отдельных задач исследования. На основании анализа и синтеза в исследовании были сформулированы закономерности, связанные с осуществлением следственной и экспертной деятельности в рамках расследования незаконного оборота наркотических средств в компьютерных сетях.

С помощью формально-юридического метода было проанализировано действующее уголовное в части состава преступления, связанного с рассматриваемой категорией дел) и уголовно-процессуальное законодательство (анализ норм, регламентирующих следственные действия в части собирания цифровых следов, назначение и производство судебных экспертиз, привлечение к участию специалиста), а также нормы, регулирующие судебно-экспертную деятельность.

Сравнительно-правовой метод позволил проанализировать зарубежные подходы к классификации цифровых следов, судебных экспертиз, на основании чего были сделаны соответствующие выводы и рекомендации.

Статистический метод использован при анкетировании сотрудников правоохранительных органов, обработке полученных результатов, а также при анализе судебной, следственной и экспертной статистике, связанной с незаконным оборотом наркотических средств в компьютерных сетях.

Применение общеэкспертных и частноэкспертных методов было необходимо для изучения судебно-экспертных технологий в рамках производства судебных экспертиз по делам о незаконном обороте наркотических средств в компьютерных

сетях. В результате данные методы дали возможность выявить и обозначить аспекты судебно-экспертных технологий, нуждающихся в совершенствовании.

Использование всех методов в совокупности позволило достигнуть цели исследования и решить поставленные задачи.

Теоретическая основа исследования состоит из трудов таких ученых в области судебной экспертологии и криминалистики, как Т. В. Аверьянова, Р. С. Белкин, Л. В. Бертовский, А. И. Винберг, А. М. Зинин, Е. П. Ищенко, Ю. Г. Корухов, Н. П. Майлис, Т. Ф. Моисеева, Ю. К. Орлов, Е. Р. Россинская, М. Я. Сегай и другие.

Диссертационное исследование основано также на специальной литературе, затрагивающей аспекты различных родов и видов судебных экспертиз, среди которых работы С. М. Вула, Е. И. Галяшиной, Т. И. Голощаповой, Е. И. Ермоловой, Т. А. Литвиновой, П. А. Манянина, И. И. Рубцовой, Т. А. Саакова, Г. В. Саенко, Т. П. Соколовой, Ю. А. Сорокина, Е. А. Чубиной, Л. Г. Эджубова и другие.

Нормативную основу исследования составляют Конституция Российской Федерации, Уголовный кодекс Российской Федерации (далее — УК РФ), Уголовно-процессуальный кодекс Российской Федерации (далее — УПК РФ), Федеральный закон от 31 мая 2001 г. № 73- ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В исследовании также были использованы постановления Пленума Верховного Суда Российской Федерации и постановления Пленума Высшего Арбитражного суда Российской Федерации, приказы Федеральной службы безопасности Российской Федерации, Министерства юстиции Российской Федерации и Министерства внутренних дел Российской Федерации и другие.

Эмпирическая база научного исследования представлена судебной практикой за 2020-2024 гг., размещенной в справочно-правовых системах ГАС РФ «Правосудие», «КонсультантПлюс», «Гарант», «Право.ru», базах данных «Судебные и нормативные акты (СудАкт)», 247 материалами уголовных дел,

предоставленных межрайонными прокуратурами г. Москвы (за период с 2020 по 2024 г.), 52 материалами экспертной практики (заключения эксперта назначенные в рамках расследования незаконного оборота наркотических средств в компьютерных сетях с 2020 по 2024 г.), результатами и информацией проведенного анкетирования 111 следователей, специализирующихся на преступлениях в области незаконного оборота наркотических средств, данные которого в совокупности послужили обоснованием ряда теоретических и практических положений проведенного исследования.

Кроме того, использован личный опыт автора (более двух лет работы) в негосударственной судебно-экспертной организации при производстве судебных лингвистических экспертиз.

Научная новизна исследования определяется тем, что данная работа посвящена комплексному исследованию возможностей применения специальных знаний при расследовании преступлений, связанных с незаконным оборотом наркотических средств, совершаемых в информационно-телекоммуникационных сетях. Определены организационные основы собирания цифровых следов, выработаны рекомендации по совершенствованию методического обеспечения отдельных родов судебных экспертиз, которые в результате их практического внедрения поспособствуют эффективности расследования преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях.

Основные положения, выносимые на защиту

1. Выявлены новые способы незаконного оборота наркотических средств в компьютерных сетях, включающие в себя:

– распространение информации о наркотических средствах в социальных сетях и мессенджерах;

– использование мессенджера Телеграм для приискания соучастников преступления, для поиска самих наркотических средств, привлечения покупателей, планирования преступления;

– создание торговых площадок в теневом сегменте Даркнет, а также использование Даркнета с целью реализации приватной коммуникации;

– использование маркетплейсов с целью сбыта наркотических средств;

– использование криптовалют, виртуальных валют для оплаты заказов наркотических средств;

– использование технологий шифрования, обеспечивающих высокий уровень конфиденциальности при незаконном обороте наркотических средств в компьютерных сетях.

2. Установлены и систематизированы участники преступлений, выполняющие новые функции в рамках незаконного оборота наркотических средств в компьютерных в сетях:

– кадровики – лица, деятельность которых связана с поиском и подбором кандидатов для участия в незаконном обороте наркотических средств;

– кураторы – лица, деятельность которых связана с оказанием помощи закладчикам в организации их деятельности;

– диспетчеры – лица, деятельность которых связана с получением заказов на наркотические средства, а также контролем поступления денежных средств за проданные наркотические средства;

– дропы (дропперы) – лица, деятельность которых связана с выводом денежных средств и их дальнейшей передачей наркопреступникам;

– коллекторы – лица, деятельность которых связана с применением насильственных действий в отношении закладчиков при наличии угрозы деятельности с их стороны.

Совершение незаконного оборота наркотических средств с использованием информационно-телекоммуникационных сетей требует определенного уровня владения компьютерными технологиями, который зависит от следующих факторов: возраст преступника; уровень образования преступника; профессия преступника; преступление совершается единолично или организованной группой; роль преступника при совершении преступления; конечная цель совершаемого

преступления. Анализ компьютерных навыков позволяет составить портрет личности преступника, а также способствует выявлению участников организованной группы.

3. Отмечается трансформация механизма следообразования вследствие появления цифровых следов в рамках дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях.

Представлена авторская классификация цифровых следов, образованных в ходе совершения преступлений, связанных с незаконным оборотом наркотических средств, по направленности действий лиц в компьютерных сетях:

– *активные цифровые следы (криминалистически значимая информация, фактические данные, находящиеся в причинно-следственной связи с осуществлением незаконного оборота наркотических средств и характеризующие способ его совершения):* сообщения в социальных сетях и мессенджерах; публикации в социальных сетях и Телеграм-каналах; комментарии в социальных сетях, Телеграм-каналах, онлайн-форумах; поисковые запросы в сети Интернет и теневом сегменте Даркнет; данные о совершенных транзакциях; фото- , видео-, аудиоматериалы; электронные документы; активность в приложениях и программах; облачное хранилище данных;

– *пассивные цифровые следы (потенциально криминалистически значимая информация, которая может актуализироваться в ходе производства следственных действия и в ходе производства судебной экспертизы в рамках расследования незаконного оборота наркотических средств):* GPS-данные; история браузера; куки-файлы; кэш браузера; метаданные файлов; данные IP-адреса.

4. При собирании цифровых следов в рамках расследования незаконного оборота наркотических средств необходимо:

– учитывать общие особенности цифровых следов, особенности отдельных видов цифровых следов, характерных для незаконного оборота наркотических средств, особенности носителей цифровых следов, особенности

конкретного проводимого следственного действия при расследовании незаконного оборота наркотических средств;

– соблюдать порядок действий, направленных на обнаружение цифровых следов при расследовании незаконного оборота наркотических средств: установление IP-адреса; проверка содержимого мессенджеров; поиск информации и анализ активности в социальных сетях; проверка содержимого истории браузера; анализ открытых ссылок в сети Интернет; анализ имеющихся на устройстве приложений (в особенности приложений VPN и Tor); анализ активности и совершенных действий в данных приложениях; проверка на наличие/отсутствие аккаунтов в облачных серверах; анализ данных карты памяти устройства; проверка медиатеки устройства (фотогалерея, аудиофайлы, электронные документы и т.д.);

– для обеспечения неизменности и сохранности цифровых следов при фиксации цифровых следов в рамках расследования незаконного оборота наркотических средств применять технологии Блокчейн, а также указывать в протоколе сведения об использованных технических средствах, о порядке совершенных действий, направленных на обнаружение цифровых следов, о способе и порядке изъятия цифровых следов, о внешнем состоянии и внутренних свойствах изъятого устройства, о содержимом изъятого устройства, о сим-карте (при ее наличии), приложение к самому протоколу в виде фотофиксации, скриншотов, выписок и др.;

– привлекать специалиста для участия в собирании цифровых следов ввиду того, что работа с такой информацией невозможна без владения высоким уровнем специальных знаний в области IT-технологий. При этом к участию в собирании цифровых следов не может быть привлечено любое лицо, чьим основным видом деятельности является IT-сфера. Специалист должен понимать особенности цифровых следов, механизм их следообразования, а также специфику дел незаконного оборота наркотических средств.

5. Особенности назначения судебной экспертизы в рамках расследования преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях:

– *обусловленные объектами исследования, их материальными носителями и экспертными задачами, характерными для незаконного оборота наркотических средств:* следует подробно описывать вид материального носителя и информацию, которая содержится на нем; предоставлять эксперту информацию о способах и технологиях изъятия цифровых следов; учитывать род назначаемой экспертизы при определении способа и формата предоставления объектов исследования эксперту;

– *обусловленные необходимостью назначения комплекса экспертиз, комплексной экспертизы, комиссионной экспертизы с учетом потребностей, возникающих при расследовании незаконного оборота наркотических средств:* следует определять необходимость назначения комплексной/комиссионной экспертизы или комплекса экспертиз; определять очередность производства судебных экспертиз при назначении комплекса экспертиз.

6. Судебно-экспертные технологии при производстве экспертиз по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, требуют совершенствования, а в некоторых случаях изменений путем:

– обобщения экспертной практики в результате совместной деятельности экспертов как государственных, так и негосударственных экспертных учреждений (создание общих баз данных по каждому роду/виду судебных экспертиз, проводящих исследования в рамках расследования незаконного оборота наркотических средств в компьютерных сетях);

– внедрения современных технологий и методов в экспертные исследования (адаптация технологий по деанонимизации пользователей Tor в исследования судебной компьютерно-технической экспертизы);

– обновления экспертных методик; создание общих стандартов для всего экспертного сообщества в части внесения положений об особенностях механизма

следообразования цифровых следов и особенностях исследования конкретных видов цифровых следов, образованных в ходе незаконного оборота наркотических средств;

– мониторинга изменений в способах преступлений, связанных с незаконным оборотом наркотических средств, и анализ их влияния на технологии экспертного исследования.

7. Компетенция судебного эксперта при производстве различных родов/видов судебных экспертиз в рамках дел незаконного оборота наркотических средств должна включать в себя: знание судебной экспертологии, теории цифровизации судебно-экспертной деятельности, знание о специфике конкретных видов цифровых следов, знание о механизме следообразования цифровых следов, умение применять в исследовании и интегрировать в экспертные методики компьютерные технологии, IT-технологии, владение современными базами данных, а также знание методик, решающих задачи, возникающие в рамках расследования незаконного оборота наркотических средств в компьютерных сетях.

Расширение компетенции судебного эксперта возможно за счет внедрения разделов, посвященных цифровым следам как объектам экспертного исследования. в программы профильных дисциплин, направленных на изучение конкретных родов/видов экспертиз:

– механизмы следообразования цифровых следов;

– особенности исследования цифровых следов, образованных в ходе незаконного оборота наркотических средств;

– возможности использования IT-технологий и их интеграция в экспертные методики в рамках расследования незаконного оборота наркотических средств;

– особенности представления результатов судебной экспертизы, назначенной в рамках расследования незаконного оборота наркотических средств.

8. Эффективное использование результатов судебных экспертиз при рассмотрении дел о незаконном обороте наркотических средств в компьютерных

сетях обеспечивается обоснованной оценкой заключения эксперта, для реализации которой необходимо повышение уровня квалификации и расширение компетенции правоприменителя в следующих вопросах:

– общие положения о цифровых следах как об объектах судебной экспертизы;

– виды цифровых следов, образованных в ходе незаконного оборота наркотических средств, а также особенности и порядок их собирания;

– возможности судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях;

– особенности и порядок назначения судебной экспертизы при расследовании незаконного оборота наркотических средств, а также оценка заключения эксперта и использование результатов судебной экспертизы, назначенной в рамках расследования незаконного оборота наркотических средств.

Теоретическая значимость результатов научного исследования определяется совершенствованием и развитием общей теории судебной экспертологии, теории цифровизации судебно-экспертной деятельности, в частности, разработана авторская классификация цифровых следов, образованных в ходе совершения незаконного оборота наркотических средств в компьютерных сетях, определена компетенция судебного эксперта, выделена специфика собирания цифровых следов. Теоретические положения позволяют использовать данное научное исследование в целях развития судебно-экспертных технологий при производстве экспертиз по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, а также в целях совершенствования применения специальных знаний в ходе расследования рассматриваемой категории дел.

Практическая значимость результатов научного исследования заключается в выработке научно обоснованного подхода к вопросам производства судебных экспертиз при расследовании незаконного оборота наркотических средств, совершенного с использованием компьютерных сетей, и разработке

практических рекомендаций для экспертов по наиболее актуальным для данной категории дел судебным экспертизам. В то же время выявленные в рамках настоящего научного исследования особенности цифровых следов, образованных в ходе незаконного оборота наркотических средств, должны позволить следователям актуализировать методические рекомендации по собиранию цифровых следов, а также обеспечить эффективное применение специальных знаний в ходе всего расследования незаконного оборота наркотических средств в компьютерных сетях.

Теоретические и прикладные аспекты диссертации могут быть использованы правоприменителем также на этапе назначения судебной экспертизы (в части определения рода/вида экспертиз, необходимости назначения комплексной или комиссионной экспертизы, формулирования вопросов к эксперту) и в дальнейшем при оценке заключения эксперта.

Апробация результатов исследования. Диссертационное исследование было подготовлено и обсуждено на кафедре судебных экспертиз ФГАОУ ВО «Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)». Основные теоретические положения и практические рекомендации диссертационного исследования отражены в 5 научных публикациях, 3 из которых опубликованы в изданиях, входящих в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации (ВАК при Минобрнауки России), в которых должны быть опубликованы основные результаты диссертации на соискание ученой степени кандидата наук.

Основные теоретические положения и практические рекомендации докладывались на международных и всероссийских конференциях, среди которых: XXII Международная научно-практическая конференция «Кутафинские чтения» «Труды профессора Р. С. Белкина как вектор развития теории и практики судебной экспертизы. К 100-летию со дня рождения ученого и педагога» (Москва, 24 ноября 2022 г.), IX Международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях» (Москва, 26-27 января 2023 г.),

Международная научно-практическая конференция — «Экспертные ошибки: современные проблемы возникновения, выявления и профилактики» (Москва, 19 января 2024 г.), Научно-практическая конференция с международным участием «Правовое и судебно-экспертное обеспечение безопасности логистических потоков материальных ценностей» (Москва, 5 апреля 2024 г.), Научно-практическая конференция с международным участием «Современные проблемы правовой и технологической регламентации использования ИИ в судебно-экспертной деятельности» (Москва, 28 ноября 2024 г.), X Международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях» (Москва, 30 января 2025 г.).

Достоверность результатов исследования обеспечивается использованием методов научного познания, достаточным объемом эмпирического материала по тематике исследования, анализом нормативно-правовой базы и научных работ по исследуемой тематике.

Объем и структура диссертации. Диссертация состоит из введения, двух глав, включающих шесть параграфов, заключения, списка использованных источников и литературы, приложений.

ГЛАВА 1. Современное состояние судебных экспертиз цифровых следов в компьютерных сетях при расследовании незаконного оборота наркотических средств

§ 1.1. Характеристика преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях

Доступность информации, быстрота ее получения, неограниченность использования во времени и пространстве влекут за собой как положительные, так и отрицательные последствия. С одной стороны, это способствует развитию всех сфер общества, с другой стороны, внедрение новых технологий в жизнь активно используется для совершения преступлений.

Проблема наркопреступности сохраняет свою актуальность в современном обществе. Несмотря на все направленные усилия в борьбе с этим явлением, число наркопреступлений по-прежнему растет. Согласно статистическим данным МВД за 2022 г., из незаконного оборота изъято 23 тонны наркотических средств, психотропных веществ и их аналогов, а также сильнодействующих веществ[1]. А уже по данным за 2023 г. по расследованным уголовным делам из незаконного оборота изъято 18,3 тонны наркотических средств и психотропных веществ[2].

Государство защищает общественный порядок и общественную безопасность, прежде всего, криминализируя деяния, направленные на незаконный оборот наркотических средств.

Перемещение наркопреступности в онлайн-пространство естественным образом меняет сущность данной категории преступлений как с практической, так и с теоретической стороны.

---

[1] Характеристика состояния преступности в Российской Федерации за январь-август 2022 года // URL: https://xn--b1aew.xn--p1ai/reports/item/32515852/ (дата обращения: 23.08.2023).

[2] Характеристика состояния преступности в Российской Федерации за январь-август 2023 года // URL: https://xn--b1aew.xn--p1ai/reCports/item/44036297/?ysclid=ls8zlzbdh0573477495 (дата обращения: 01.02.2024).

В частности, проследить такое влияние можно через анализ уголовно-правовой характеристики, а также криминалистической характеристики и сравнения ее с той характеристикой, которая была присуща наркопреступлениям без использования информационно-телекоммуникационных сетей.

В УК РФ закреплены несколько составов преступлений в области незаконного оборота наркотических средств, за совершение которых наступает уголовная ответственность. Составы, что логично, отличаются друг от друга отдельными элементами уголовно-правовой характеристики. Однако между ними всеми есть кое-что объединяющее: родовой и видовой объекты, а также субъект.

Родовым объектом для данной категории преступлений выступает «совокупность общественных отношений, обеспечивающих общественную безопасность и общественный порядок»[3].

Определение видового объекта является предметом дискуссий ученых, поскольку глава, включающая рассматриваемые преступления, посвящена преступлениям против здоровья населения и общественной нравственности. По общему правилу видовым объектом преступного посягательства как раз должны выступать и здоровье населения, и общественная нравственность. Однако теоретики склоняются к тому, что для при совершении преступлений по ст. 228, 228.1 УК РФ вред наносится исключительно здоровью человека[4].

Субъектом преступления может быть вменяемое физическое лицо, достигшее шестнадцатилетнего возраста на момент совершения общественно опасного деяния.

Поскольку в ст. 228.1 УК РФ содержится такой квалифицирующий признак, как использование средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), все

---

[3] Николаев К. Д. Объект и предмет преступлений, связанных с незаконным оборотом наркотиков // Вестник Воронежского института МВД, 2009, №4. С. 42-46.

[4] Чудинов А. М. Проблемы уголовно-правовой характеристики состава преступления, предусмотренного статьей 228.1 Уголовного кодекса Российской Федерации (сбыт наркотических средств, психотропных веществ или их аналогов) // Вестник Прикамского социального института. 2023. №3 (96). С. 61.

остальные элементы уголовно-правовой характеристики будут рассмотрены именно по п. б ч.2 ст. 228.1 УК РФ.

Исходя из дефиниции статьи, объективную сторону составляют производство, сбыт или пересылка наркотических средств и их аналогов (в широком смысле).

Постановление Пленума Верховного Суда РФ от 15.06.2006 №14 (ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» дает характеристику каждому из действий[5]:

Под незаконным производством наркотических средств следует понимать умышленные действия, направленные на серийное получение таких средств или веществ из растений, химических и иных веществ.

Незаконный сбыт наркотических средств предполагает незаконную деятельность лица, направленную на их возмездную либо безвозмездную реализацию (продажа, дарение, обмен, уплата долга, дача взаймы и т.д.) другому лицу.

В разрезе использования информационно-телекоммуникационных сетей при совершении преступления крайне важно отметить, что предоставление покупателю наркотических средств информации о месте их нахождения (закладке) некорректно считать покушением на сбыт, так как сбыт наркотических средств невозможен без передачи информации покупателю о месте тайников[6]. Такая же позиция отражена в упомянутом Постановлении Пленума Верховного суда РФ № 14 от 15.06.2006 г.

Незаконная пересылка означает действия лица, направленные на перемещение наркотических средств (например, в почтовых отправлениях, посылках, багаже с использованием средств почтовой связи, воздушного или другого вида транспорта, а также с нарочным при отсутствии осведомленности

---

[5] Постановление Пленума Верховного Суда РФ от 15.06.2006 N 14 (ред. от 16.05.2017) "О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами"// СПС «Консультант Плюс».

[6] Чудинов А. М. Проблемы уголовно-правовой характеристики… С. 63.

последнего о реально перемещаемом объекте или его сговора с отправителем), когда эти действия по перемещению осуществляются без непосредственного участия отправителя.

Субъективная сторона общественно опасного деяния, предусмотренного ст. 228.1 УК РФ, характеризуется прямым умыслом. Как отмечает Л. Н. Ключенко, виновный осознает, что его действия по производству, сбыту или пересылке наркотических средств, психотропных веществ или их аналогов, а также по сбыту или пересылке растений или их частей, содержащих такие средства или вещества, противоречат законодательству РФ, и желает совершить именно эти действия[7].

Особенности, связанные с совершением преступления путем использования информационно-телекоммуникационных сетей, хорошо отслеживаются при анализе криминалистической характеристики преступления. Ученые отмечают, что криминалистическая характеристика представляет собой одно из информационных средств расследования[8].

Криминалистическая характеристика позволяет отследить типовые особенности конкретного вида преступлений, но, что важно, не самого конкретного преступления. Каждое совершенное преступление, несмотря на внешнее сходство с иными, уникально по своей сути.

В подтверждение данной точки зрения можно обратиться к трудам Г. В. Лейбница, в которых ученый писал о том, что «хотя существует много вещей одного и того же рода, однако никогда не бывает совершенно одинаковых вещей»[9].

Понятие криминалистической характеристики в отечественной науке начало формироваться в 60-х гг. прошлого столетия. А. Н. Колесниченко в своей работе, говоря об общих положениях методики расследования, одним из первых употребил

---

[7] Клоченко Л. Н. К вопросу об унификации терминологии, обозначающей психическое насилие, в уголовном праве // Российский следователь. 2013. № 9. С. 24 - 27.

[8] Яблоков Н. П. Криминалистическая характеристика преступлений как составная часть общей теории криминалистической теории// Вестник МГУ. Серия «Право».2000, № 2. С.8.

[9] Лейбниц Г. Новые опыты о человеческом разумении автора системы предустановленной гармонии // Лейбниц Г. Сочинения. В 4 т. М., 1983. Т. 2. С. 230.

термин «криминалистическая характеристика преступлений», однако понятие на тот момент им не было в достаточной степени раскрыто[10].

Л. А. Сергеев в диссертационном исследовании уже более подробно остановился на данном понятии, перечислив входящие, по его мнению, в содержание криминалистической характеристики[11].

Л. А. Сергеев таким образом также задал тенденцию определения сущности криминалистической характеристики именно через ее элементный состав. На это указывал Р. С. Белкин, который обобщив точки зрения Л. А. Сергеева, С. П. Митричева, В. А. Образцова, Н. А. Селиванова и др., включил в криминалистическую характеристику преступлений следующие элементы: характеристика исходной информации, система данных о способе совершения и сокрытия преступления и типичных последствиях его применения, личности вероятного преступника и вероятных мотивах и целях преступления, данные о некоторых типичных обстоятельствах совершения преступления (место, время, обстановка), данные о типичных обстоятельствах, способствовавших совершению конкретного вида, рода преступлений[12].

Среди всех элементов криминалистической характеристики преступления наиболее ярко и отчетливо можно проследить качественные изменения наркопреступлений с использованием компьютерных сетей через анализ способа преступления.

Важно понимать, что понятие «способ преступления» нельзя приравнивать к понятию «способ совершения преступления», поскольку первое по своей сути шире и включает в себя не только способ совершения преступления, но и способ сокрытия преступления.

---

[10] Колесниченко А. Н. Научные и правовые основы расследования отдельных видов преступлений: Автореф. дисс.... док. юрид. наук. Харьков, 1967. С. 9.

[11] Сергеев Л. А. Расследование и предупреждение хищений, совершаемых при производстве строительных работ: автореф. дис. ... канд. юрид. наук. Москва. 1966. С. 4-12.

[12] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика.- М, 1999. С. 700.

При этом даже в науке учеными нередко используются эти слова в качестве синонимичных.

Например, И. А. Возгрин понимает под способом совершения преступления систему взаимосвязанных и взаимообусловленных действий, с помощью которых преступник достигает своей цели[13].

Схожей позиции придерживается В. Ф. Ермолович, который рассматривает способ совершения преступления в качестве системы умышленных действий по подготовке, совершению и сокрытию преступления, охватываемую единым преступным замыслом, детерминированную психофизическими качествами личности преступника (его соучастников) и избирательным использованием им (ими) соответствующих условий, места, времени, а также учетом возможных действий (бездействия) со стороны потерпевшего, иных лиц[14].

По мнению Г. Г. Зуйкова, способ совершения преступлений представляет собой «систему действий по подготовке, совершению и сокрытию преступления, детерминированных условиями внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий или средств и условий места и времени»[15].

Говоря о значении способа совершения преступления, Л. В. Лазарева отмечает, что он «служит источником сведений, необходимых для разработки средств, приемов и методов раскрытия, расследования и предупреждения преступлений. Данные о способе совершения и сокрытия преступления – центральная часть криминалистической характеристики, поскольку именно они выражают функциональную сторону преступной деятельности. Без их знания, без

---

[13] Возгрин И. А. Научные основы криминалистической методики расследования преступлений. Часть IV. СПб: Санкт-Петербургский юридический институт МВД России, 1993. С. 26.

[14] Ермолович В. Ф. Криминалистическая характеристика преступления. Минск: «АМАЛФЕЯ», 2001, С.54-55.

[15] Зуйков Г. Г. Криминалистическое учение о способе совершения преступления: автореф.дис. … д-ра юрид.наук. М., 1970. С. 10.

знания тех признаков, которые указывают на их использование, невозможно расследовать преступление»[16].

Представляется, что все же необходимо четко разграничивать термины «способ преступления» и «способ совершения преступления», так как даже сами ученые последнее понятие включают в качестве одного из элементов способа преступления.

Слово *совершение* определяется в словарях через глагол совершенного вида *совершить* и используется в смысле «сделать, осуществить»[17]. Иначе говоря, это означает, что совершение преступления – это уже осуществленный акт преступного замысла. В связи с этим некорректно включать в термин «способ совершения преступления» самостоятельный этап подготовки преступления.

Б. Н. Коврижных придерживается такой точки зрения и предлагает рассматривать способ подготовки, способ совершения и способ сокрытия в качестве составляющих интегрального понятия «способ преступления»[18].

Однако в разрезе компьютерных преступлений понятие криминалистической характеристики является не столь актуальным. В последние годы ученые стали говорить о необходимости создания типовой информационной модели преступления[19].

Профессор Е. П. Ищенко понимает под типовой информационной моделью «информационную систему, построенную на основе статистической обработки репрезентативной выборки уголовных дел определенной категории, отражающая закономерные связи между элементами события преступления, используемая для

---

[16] Лазарева Л. В. Особенности первоначального этапа расследования незаконного оборота синтетических наркотических средств: дис. ... канд. юрид. наук. М., 2001. С. 21.

[17] Ожегов С. И. Толковый словарь русского языка: 80000 слов и фразеол. выражений / С. И. Ожегов, Н. Ю. Шведова. Ин-т рус. яз. им. В. В. Виноградова. – 4-е изд., доп. – Москва: Азбуковник, 2003 г. URL: https://gufo.me/dict/ozhegov/совершить (дата обращения: 07.02.2024).

[18] Коврижных Б. Н. Деятельность органов прокуратуры по делам о нераскрытых убийствах: автореф. дис. на соиск. учен. степ. канд. юрид. наук / Б. Н. Коврижных; Харьк. юрид. ин-т.– Х., 1969. С. 14.

[19] Колдин В. Я., Ищенко Е. П. Типовая информационная модель преступления как основа методики расследования // Известия высших учебных заведений. Правоведение. № 6 (269). 2006. С. 128–144.

построения типовых версий и формирования методики расследования данной категории преступлений»[20].

По мнению А. А. Бессонова, «Криминалистическая характеристика преступлений – информационная модель, которая отражает криминалистическую сущность преступлений определенного вида (подвида, криминалистически схожих групп), заключающуюся в сведениях о его криминалистически значимых признаках и их закономерных связях между собой, построенная на основе анализа и обобщения практики их расследования и судебного рассмотрения, и имеющая значение для формирования частных методик расследования и решения задач деятельности по расследованию и предупреждению преступлений[21].

Авторы монографии, в свою очередь, пишут о том, что объединение информационных моделей по видам преступлений не является результативным, так как способы совершения компьютерных преступлений могут быть идентичными[22].

Ученые считают, что в основе информационно-компьютерных моделей должно лежать «ранжирование их по сложности способов реализации противоправных действий, включая используемые IT-технологии и корреляции с этими способами уровня компетенции преступников, состава преступной группы или сообщества»[23].

Для рассмотрения компьютерных преступлений, действительно, нужен несколько иной теоретический подход, поскольку сущностно они отличаются от «традиционных» преступлений.

---

[20] Ищенко Е. П. Как наполнить фантом криминалистической характеристики преступлений реальным содержанием // Информационный бюллетень № 17 по материалам Криминалистических чтений «Научная состоятельность криминалистической характеристики преступлений». М., 2002. С. 8–14.

[21] Бессонов А. А. Частная теория криминалистической характеристики преступлений. Автореф. дисс. доктора юрид. наук. М., 2017. 46 с.

[22] Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е. Р. Россинской — Москва: Проспект, 2023. С. 137.

[23] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 139.

Эти отличия обуславливают, в частности, все особенности преступлений, связанных с незаконным оборотом наркотических средств.

В российском законодательстве при обозначении квалифицирующего признака употребляются такие понятия, как «электронные сети», «информационно-телекоммуникационные сети, в том числе сеть Интернет, «преступления, совершаемые с использованием средств массовой информации».

Понятие информационно-телекоммуникационной сети раскрывается в Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации». Под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[24].

При этом, что следует понимать под электронной сетью, законодатель не уточняет. Рассматривая вопрос разграничения понятий «электронная сеть» и «информационно-телекоммуникационная сеть», ряд ученых приходят к выводу, что это совпадающие понятия[25].

Так, В. Н. Винокуров, А. В. Агафонов, давая определение электронной сети, дословно повторяют определение информационно-телекоммуникационной сети и говорят о том, что указание в законе на электронную сеть является избыточным[26].

Говорить о том, что рассматриваемые понятия являются полностью идентичными, представляется нецелесообразным ввиду их различий в основах принципа действия.

---

[24] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) "Об информации, информационных технологиях и о защите информации". URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 07.02.2024).

[25] Литвяк Л. Г., Пирогова Е. Н. К вопросу о понятии электронных или информационно-телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. №11-2. URL: https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-elektronnyh-ili-informatsionno-telekommunikatsionnyh-setey-dlya-tseley-ugolovnogo-zakona (дата обращения: 26.03.2024).

[26] Винокуров В. Н., Агафонов А. В. Особенности квалификации сбыта наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право. 2023. № 1.

«Электронный» означает то, что связано с применением свойств электрона, основано на использовании свойств электронов[27]. То есть в основе действия электронной сети должен лежать электрон. Информационно-телекоммуникационная сеть работает иначе, на основе программного и аппаратного обеспечения, позволяющего передавать по линиям связи информацию.

Соответственно понятие «электронная сеть» не учитывает в полной мере всех возможных способов использования современных технологий и более того, отчасти является не самым актуальным.

При рассуждении на данную тему возникает вопрос, к чему относить тогда облачное хранилище, маркетплейсы или тот же Даркнет. Корректно ли относить их к информационно-телекоммуникационным сетям?

На наш взгляд, информационно-телекоммуникационные сети необходимо рассматривать несколько шире, чем передачу информации в буквальном смысле. По своей сути, те же маркетплейсы, облачные хранилища и т.д. также содержат сведения, которые принимает потребитель. Просто сама технология передачи информации происходит иным образом.

Нами в диссертационном исследовании также был употреблен термин «компьютерные сети». Оговоримся, что, во-первых, понятие «компьютерные сети» в данном контексте мы рассматриваем не в узком смысле (как систему, состоящую из компьютеров и компьютерных устройств), а во-вторых, используем в качестве синонима информационно-телекоммуникационным сетям.

Информационно-телекоммуникационные сети активно используются в наркопреступлениях при подготовке, совершении и сокрытии преступления. Конкретный способ преступления зависит, во-первых, от уровня компетенций преступника в области IT-технологий, и, во-вторых, от того, каким составом лиц совершается преступление: единолично или, например, организованной группой.

---

[27] Большой толковый словарь русского языка / гл. ред. С. А. Кузнецов. - Санкт-Петербург: Норинт; Москва: Рипол классик, 2008. URL: https://gufo.me/dict/kuznetsov/электронный (дата обращения: 07.03.2024).

Анализ судебной практики демонстрирует, что преступники для осуществления умысла прибегают к использованию социальных сетей Одноклассники, ВКонтакте и мессенджеров Viber, WhatsApp и Telegram.

Если раньше можно было четко проследить отличия между социальными сетями и мессенджерами, то сейчас эти различия размываются. В мессенджерах появились функции публикаций постов, сторис, оставления комментариев.

Однако, чтобы увидеть пост в мессенджере, пользователь должен быть подписан на соответствующий канал, в социальных сетях такого условия нет. Поэтому информация о наркотических средствах в таких социальных сетях, как Одноклассники, ВКонтакте, в основном распространяется через посты, содержащие предложения приобретения наркотических средств, а также ссылки на торговые площадки в комментариях, в постах групп, реже – через личные сообщения.

В мессенджерах Viber, WhatsApp основным способом поиска соучастников выступает реклама и ее распространение в чатах с пользователями. Через Даркнет (принцип работы Даркнета будет раскрыт далее) приобретаются номера телефонов, с которых дальше осуществляется рассылка. В Даркнете наркопреступники покупают базу данных с телефонами различных операторов. Например, таким способом на номера российских абонентов в ноябре 2023 г. в мессенджеры Viber, WhatsApp приходили сообщения с информацией о возможности покупки наркотических средств со ссылками на интернет-магазины, в которых можно их приобрести. Стоит отметить, что такое распространение происходит не только через личные чаты, но и через групповые беседы.

Но этот способ преступления характерен не только для Viber, WhatsApp, но и в принципе для всех социальных сетей и мессенджеров.

Самым большим функционалом, отличным от всех, обладает Телеграм, в связи с чем данный мессенджер наиболее популярен в среде наркопреступников.

Структурно в Телеграме можно выделить следующие компоненты: чаты, которые в свою очередь делятся на личные, групповые и секретные; каналы – открытые и закрытые; Телеграм-боты.

Принцип работы Телеграм-ботов основан на использовании API мессенджера Телеграм для обмена сообщениями между ботом и пользователями. Боты представляют собой автоматизированные программы, которые могут выполнять различные задачи: от предоставления информации до выполнения команд.

Важной способностью ботов является возможность интеграции с различными внешними сервисами и API для получения данных или выполнения дополнительных функций.

Именно таким образом часто происходит подбор курьеров-закладчиков. При нажатии в боте на кнопку «Начать» пользователь должен указать свой возраст и город проживания, после чего ему предоставляются контакты лиц, которые дают соответствующие инструкции.

В Телеграме по таким ключевым словам, как «курьер», «трудоустройство», «кладмен» также можно найти каналы, занимающиеся незаконным оборотом наркотических средств. В данных каналах можно ознакомиться с подробной инструкцией приобретения наркотических средств.

При этом сама информация может быть замаскирована. В канале может быть опубликован текст, не относящийся к наркотическому дискурсу, но отдельные слова в тексте могут оказаться гиперссылками, при нажатии на которые пользователь переходит, например, на каталог наркотических средств.

При поиске по слову «работа» Телеграм выдает множество результатов разной направленности, но так или иначе связанных с поиском работы. При переходе на один из таких каналов «RABOTA» видим два креолизованных текста: «ССЫЛКА В ШАПКЕ» и «ПЛАТИМ БОЛЬШЕ ВСЕХ». Иная информация в самом канале отсутствует. Однако, заходя в раздел описания канала, находим две ссылки. Первая ссылка https://t.me/Kurercc_zakladchikcf_kladmenomvv направляет, собственно, на данный Телеграм-канал. Вторая ссылка @RABOTA_KURERY перенаправляет в чат ТОЛЬКО РФ 17+.

Текст ссылок выполнен буквами латинского алфавита. Поэтому в такой ситуации нужно ориентироваться на ГОСТ 7.79-2000 Система стандартов по

информации, библиотечному и издательскому делу. Правила транслитерации кирилловского письма латинским алфавитом.

С опорой на ГОСТ можно перевести текст ссылок, выполненный латиницей, на кириллицу. Стоит учитывать, что в ссылках в слова внедряются лишние символы, не относящиеся к слову и не имеющие никакого значения. Без учета таких буквенных и знаковых символов первая ссылка состоит из трех слов «курьер», «закладчик», «кладмен», вторая ссылка – из двух слов «работа» и «курьеры». Данные лексемы относятся к семантическому полю «наркотические средства». Принимая во внимание использование лексемы «работа» в обеих ссылках, делаем вывод о том, что канал RABOTA предоставляет работу закладчика.

Личные и групповые чаты не обладают отличительными чертами, информация в них распространяется по тому же принципу, как и в других мессенджерах.

Среди особенностей секретных чатов можно выделить следующие:

– оконченное шифрование;
– отсутствие следов на серверах;
– запрет на пересылку сообщений;
– автоудаление сообщений по таймеру.

Оконченное шифрование – это метод шифрования, при котором сообщения между отправителем и получателем зашифрованы на устройстве отправителя и расшифровываются только на устройстве получателя. Даже сам сервис (в данном случае Телеграм) не имеет доступа к содержимому сообщений, так как данные шифруются и дешифруются локально на устройствах пользователей.

Это означает, что даже если данные перехватываются в процессе передачи через серверы Телеграм, они остаются зашифрованными и недоступны для просмотра третьим лицам, включая компанию-провайдера. Таким образом, конфиденциальность сообщений обеспечивается оконченным шифрованием в Телеграм.

А с учетом того факта, что использование секретного чата обеспечивает отсутствие следов на серверах, то есть в цифровой среде не остается никаких следов о проделанных действиях в рамках чата, перехват данных таким образом исключается, пользователи получают полную анонимность и конфиденциальность.

Конфиденциальность обеспечивается также за счет того, что сообщения секретного чата нельзя пересылать в иные чаты, а также возможности настройки таймера автоматического удаления сообщений (от 1 секунды до 1 недели). В совокупности данные функции уберегают пользователя от возможной утечки информации.

О возможности использования секретных чатов знают не все пользователи Телеграма, что опять же свидетельствует о различном уровне знаний лиц в области компьютерных технологий.

Нередко при задержании закладчиков и при дальнейшем осмотре их телефонов у них обнаруживают переписки, содержащие информацию о распространении наркотических средств, фотоснимки местоположения сделанных закладок или данные о геопозиции. Подробнее об этом будет сказано в третьем параграфе настоящей главы.

Наиболее продвинутые пользователи используют Даркнет. Даркнет – это теневой сегмент Интернета, который изначально был разработан для военных целей. На данный момент Даркнет стал основным местом осуществления незаконной деятельности.

Отсутствие ограничений во времени и пространстве способствует быстрому распространению по всему миру не только наркотических средств, но и инструкций относительно их использования и производства.

На рынках, расположенных в Даркнете, наркотики продаются открыто, но личности и местонахождение участников, а также сам рынок замаскированы. Технологии же, с помощью которых функционируют онлайн-рынки, постоянно совершенствуются.

Одной их таких технологий является Tor. Разработка сетевых технологий Tor началась в 1995 г. как проект Военно-морских сил США, целью которого было создание более безопасных сетей связи[28].

Однако впоследствии такая технология стала доступна для более широкого круга лиц, что привело к использованию Tor в преступных целях.

Доступ к сети Tor можно получить с помощью специального программного обеспечения известного, как Tor Browser Bundle, или клиента Tor. Пользователи Tor образуют виртуальные цепи из двух или более узлов, которые передают трафик пользователя на сервер назначения. Данные многократно шифруются перед передачей по сети Tor, что позволяет сохранить конфиденциальность исходных данных только на выходном узле, последнем узле в цепи. Аналогичным образом работает виртуальная частная сеть (VPN)[29].

С помощью данных сервисов пользователи скрывают свой реальный IP-адрес, тем самым обеспечивают себе определенный уровень безопасности.

Таким образом, использовав анонимайзеры, пользователи переходят на сайты Даркнета, специализирующиеся на незаконном обороте наркотических средств.

Сами ссылки на сайты Даркнета часто публикуют именно в Телеграм-каналах или в социальных сетях.

В России одной из самых популярных торговых площадок являлась «Гидра», действовавшая с 2015 г. до 2022 г. В рамках данной площадки действовало более 19 тысяч виртуальных магазинов.

Однако закрытие «Гидры» не повлияло на снижение наркопреступности, так как данную нишу заняли другие рынки Даркнета. В частности, к таковым можно отнести White House Market, Empire Market, DarkMarket, Berlusconi Market, Solaris, Kraken. Последний в данный момент используется наиболее активно. Рекламу

---

[28] Информация об истории и работе Tor. URL: http://torproject.org/ (дата обращения: 16.01.2024).

[29] Дык Буй Минь, Хуи Нгуен Нгок, Линь Лай Тхи, Хю Нгуен Ба, Чыонг Нгуен Динь Принцип работы tor-браузера // Проблемы Науки. 2017. №1 (83). С. 52-55.

Kraken можно найти в социальных сетях, мессенджерах, QR-коды на данный сайт распространители оставляют на стенах зданий, на асфальте.

На таких торговых площадках действует усовершенствованная система обратной связи, целью которой является укрепление доверия между покупателями и продавцами. Рейтинги продавцов являются открытыми для пользователей. Существуют также «скрытые списки» каталога товаров, доступ к которым предоставляется только по прямым URL-адресам. Как правило, ссылки на такие товары есть у тех покупателей, у которых уже установлены определенные доверительные деловые отношения с продавцами. Такая система обеспечивает дополнительную безопасность как для продавцов, так и для покупателей.

Обнаружить местоположение лиц, ориентируясь исключительно на их действия, аккаунты в Даркнете, на данный момент не представляется возможным. В рамках оперативно-разыскной деятельности используются иные способы поиска преступников, о чем будет сказано позднее.

Правоохранительные органы проводят мероприятия, в результате которых блокируются такие сайты. И все же информационно-коммуникационные технологии развиваются настолько быстро, что правовые, организационные средства не успевают за ними. В результате чего количество онлайн-рынков постоянно увеличивается.

Еще одним инструментом, обеспечивающим безопасность при купле-продаже наркотических средств, является способ оплаты. Оплата товаров в Даркнете проходит несколько иначе, чем в Интернете, а именно с помощью криптовалют и виртуальных валют.

Одним из наиболее популярных видов криптовалюты является биткоин. Биткоины – это виртуальная валюта, которая работает на основе технологии блокчейн. Блокчейн – это распределенная база данных, которая хранит информацию в блоках, каждый из которых содержит информацию о предыдущем блоке. Каждый блок в блокчейне связан с предыдущим блоком с помощью

криптографической хэш-функции, что обеспечивает целостность и надежность цепочки блоков[30].

Биткоины создаются через процесс, называемый майнингом. Майнеры используют свои компьютеры для решения сложных математических задач, которые подтверждают транзакции с биткоинами и добавляют их в блокчейн. За каждый блок, который майнер добавляет в блокчейн, он получает вознаграждение в виде новых биткоинов.

В. А. Перов в своем исследовании выделяет следующие принципы, которые составляют основу создания (майнинга) и последующего использования полученной криптовалюты:

– «децентрализация выпуска криптовалют. Отсутствует единый эмитент, который может оказать влияние на количество генерируемых криптомонет, уменьшать или увеличивать процесс их генерации, оказывая тем самым искусственное влияние на их стоимость (манипулируя рынком криптовалют);

– отсутствие возможности регулирования и контроля, в том числе со стороны государства, за выпуском и обращением криптовалюты;

– анонимность лиц, использующих криптовалюту, при полной открытости ее обращения и в то же время возможность проследить оборот (транзакции) каждой из созданных криптомонет любым лицом, имеющим такое желание;

– отсутствие административных, территориальных и политических барьеров для создания и использования криптовалюты;

– возможность анонимного совершения любых сделок вне зависимости от того, разрешены они или нет действующим национальным законодательством определенной страны»[31].

---

[30] Канатьев К. Н., Большаков В. Н., Анисимов А. Р., Скоморохина Е. Р., Чикенев С. Д. Анализ возможностей технологии блокчейн в управлении данными, Инновации и инвестиции, № 5, 2023, С. 175.

[31] Перов В. А. Криптовалюта как объект гражданского права // Гражданское право. 2017. № 5. С. 7.

Соответственно, транзакции с биткоинами происходят без посредников и без необходимости раскрывать личную информацию. Каждая транзакция записывается в блокчейн и подтверждается другими участниками сети. Это делает систему безопасной и защищенной.

Ю. В. Попова под виртуальной валютой понимает «средство выражения стоимости, представленное в цифровом формате и выступающее в качестве средства обмена, либо расчетной денежной единицы, либо средства хранения стоимости и при этом не подпадающее под понятие законного платежного средства, т. е. не являющееся официально действующим законным средством платежа при расчетах с кредиторами»[32].

В совокупности все данные факты влияют на неурегулированность вопроса криптовалют и виртуальных валют, в результате чего и допускается их использование в преступных целях.

После того как покупатель оплачивает заказанные наркотические средства, продавец организует отправку товара. Продукция отправляется почтой или курьерской службой по адресу, указанному покупателем. Продукция обычно доставляется в вакуумных пакетах, что затрудняет ее обнаружение по запаху. Доставка часто маскируется под обычную посылку.

На каждом этапе, начиная от способа распространения информации о наркотических средствах, заканчивая способами доставки наркотических средств, лица, являющиеся участниками незаконного оборота наркотических средств, создают максимально безопасные для реализации преступного умысла.

Даркнет в качестве площадки для совершения преступлений, как уже было сказано, используется достаточно давно. В последние годы появился еще один способ преступления, а именно сбыт наркотических средств через маркетплейсы.

Уже известны случаи сбыта наркотических средств через посылки Почты РФ, сервисы Озон и Вайлдбериз.

---

[32] Попова Ю. В. Организация деятельности криптоказино: проблемы привлечения к уголовной ответственности (статья 171.2 Уголовного кодекса РФ) // Молодой ученый. — 2019. № 47 (285). С. 359.

В марте 2024 г. возбуждено уголовное дело по ч. 5 ст. 228.1 УК РФ в отношении женщины, продававшей наркотические средства через маркетплейс Озон. По данным правоохранительных органов женщина продавала товары в Озоне, а в упаковку вкладывала наркотические средства. Сотрудниками были изъяты из сортировочного склада 123 коробки с наркотическими средствами, часть из которых уже были адресованы для доставки получателям в Москве, Пскове, Казани и Краснодаре.

Ярким примером совершения преступления с использованием компьютерных сетей является дело в отношении главы отделения Почты России в Московской области Юрова А. Н., виновного в совершении преступлений, предусмотренных п. «б» ч.4 ст.229.1, ч.3 ст.30, ч.5 ст.228.1, п. «б» ч.4 ст.229.1, ч.5 ст.228.1, ч.3 ст.30, ч.5 ст.228.1, ч.2 ст.228 УК РФ.

Гражданин Юров А. Н. приобрел наркотические средства через приватный чат зарубежного интернет-магазина «Empiremarket», располагающегося в теневом сегменте Даркнет, доступ к которому получил с помощью браузера-анонимайзера То». Оплатил сделанный заказ Юров А. Н. в криптовалюте биткоин. Движение международного почтового отправления, содержащего наркотические средства, отслеживал путем удаленного наблюдения посредством мобильного телефона марки «IPhone 12 Pro».

С целью дальнейшего сбыта наркотических средств Юров А. Н. создал свой интернет-магазин по продаже наркотических средств на торговой площадке Hydra. На сайте были опубликованы фотоизображения «ЛСД, нанесенного на муляж купюры номиналом в 100 долларов США, перфорированной для разделения на части». В дальнейшем в фотогалерее изъятого мобильного телефона были обнаружены данные фотоизображения[33].

[33] Приговор Московского областного суда по делу № 2-102/2022. – URL: https://oblsud--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=34472938&delo_id=1540006&new=0&text_number=1 (дата обращения: 20.03.2024).

При совершении преступления были Юровым А. Н. использованы: браузер-анонимайзер Tor, Даркнет, приватные чаты, приложение удаленного отслеживания товара, фотокамера мобильного телефона.

Данный кейс из судебной практики также демонстрирует, как личность преступника влияет на способ преступления. В рассматриваемом деле обвиняемый имел особое служебное положение (глава отделения почты России Московской области), что позволило ему получать и направлять посылки со своего почтового отделения скрытно, а также владел определенным уровнем использования компьютерных технологий.

Можно заметить, что все рассмотренные выше способы преступления так или иначе направлены на обеспечение анонимности, конфиденциальности, что по итогу способствует сокрытию следов преступления. Эти обстоятельства являются характерными именно для преступлений, совершенных с использованием компьютерных сетей.

Для сокрытия осуществления преступной деятельности преступники прибегают к применению метода стеганографии. Сущность метода стеганографии сводится к сокрытию не самой информации, а факта ее передачи. Лицо, чьи действия имеют умысел на совершение преступления, используя данный метод, имеет возможность направлять через открытые каналы связи любые, даже секретные сведения.

Для обеспечения еще более высокого уровня конфиденциальности стеганография применяется в комбинации с шифрованием. Такой способ позволяет скрытую (закодированную) информацию передать безопасным образом без возможности ее перехвата.

Существуют разнообразные методы стеганографии, позволяющие скрыть послание или файл, но наиболее популярным в настоящее время является метод, скрывающий сообщения в компьютерных файлах (контейнерах). Секретная

информация вставляется, например, в текстовый файл, в файлы изображения или даже в часть IP-пакетов[34].

Соответственно, качественным образом изменились и способы сокрытия преступления.

Анализ судебной практики, материалов уголовных дел позволяет отметить, что преступления, связанные с незаконным оборотом наркотических средств в компьютерных сетях, совершаются следующими способами:

– распространение информации о наркотических средствах в социальных сетях и мессенджерах;

– использование мессенджера Телеграм с целью приискания соучастников преступления, с целью поиска самих наркотических средств, привлечения покупателей, планирования хода совершения преступления;

– создание торговых площадок в теневом сегменте Даркнет;

– использование теневого сегмента Даркнет с целью реализации приватной коммуникации;

– использование маркетплейсов с целью сбыта наркотических средств;

– использование криптовалют, виртуальных валют для оплаты заказа наркотических средств.

Внедрение компьютерных сетей для совершения преступлений, связанных с незаконным оборотом наркотических средств, изменило главным образом не только способы преступления, но также понимание места их совершения.

Ряд теоретиков отмечают, что с появлением преступлений в онлайн-пространстве традиционное представление о месте совершения преступления стало нуждаться в пересмотре и обновлении знания. В частности, на это указывает в своей работе М. М. Долгиева[35].

---

[34] Зиновьева Н. С. К вопросу о месте криптографии и стеганографии в криминалистической науке // Гуманитарные, социально-экономические и общественные науки. 2019. №2. С. 89.

[35] Долгиева М. М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. N 10. С. 109 - 115.

С. А. Евсеева пишет о том, что место происшествия киберпреступления вовсе отсутствует в реальности[36]. Продолжая ее идею, С. В. Глазатова, Е. В. Бурцева и С. В. Медведева отмечают, что место совершения преступлений такого рода представляет собой сложную систему киберпространства[37].

Другие ученые, например, А. Г. Волеводз, предлагают рассматривать Интернет (в широком смысле) по аналогии с так называемыми открытыми пространствами (космическое пространство, открытое море)[38].

Представленные мнения относительно места совершения преступления в компьютерных сетях являются дискуссионными, поскольку, если мы все же рассматриваем сеть Интернет, Даркнет, социальные сети, мессенджеры и т.д. именно как место совершения преступления, то говорить об отсутствии их в реальности не представляется возможным. Доступ ко всем компьютерным сетям осуществляется через то или иное устройство (персональный компьютер, мобильный телефон, планшет), использование которых происходит в конкретном месте.

Если обратиться к ранее приведенному примеру из судебной практики по незаконному обороту наркотических средств через маркетплейс Озон и исходить из рассуждений выше представленных авторов, то выходит, что установить место совершения преступления нельзя, так как маркетплейс в виде приложения не имеет фактического адреса. Такой подход все же не соответствует ни фактической, ни правовой реальности.

---

[36] Евсеева С. А. Некоторые проблемы расследования преступлений в отношении несовершеннолетних киберпреступников // Вестник Уфимского юридического института МВД России. 2019. N 3 (85). С. 71.

[37] Евсеева С. А. Некоторые проблемы расследования… С. 70.

[38] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2009. С. 313-314.

Справедливо, в связи с этим отмечает Д. А. Овсюков, что ошибочно считать местом совершения преступления саму сеть Интернет или любое иное виртуальное пространство – они не являются ни географической территорией, ни местностью[39].

Сеть Интернет или любая иная компьютерная сеть является именно средством, способом преступления, но не местом.

Ответ на этот дискуссионный вопрос в 2022 г. был дан Пленумом Верховного суда. Согласно Постановлению, «местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления»[40].

Определение места совершения преступления при использовании компьютерных сетей возможно при применении специальных знаний в области компьютерно-технической экспертизы. Возможности судебной компьютерно-технической экспертизы будут подробно раскрыты далее.

Компьютерные сети существенно повлияли на изменение характеристики личности преступника, а как следствие на структуру организованных преступных сообществ в сфере незаконного оборота наркотиков.

В первую очередь, использование компьютерных сетей требует определенного уровня владения технологиями, о чем уже было сказано. Этот уровень зависит от следующих факторов:

- возраст преступника;
- уровень образования преступника;
- профессия преступника;
- преступление совершается единолично или организованной группой;
- какую роль выполняет преступник при совершении преступления;

---

[39] Овсюков Д. А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: монография / под науч. ред. С. М. Кочои. М.: Проспект, 2023. С. 184.

[40] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" // СПС «Консультант Плюс».

– какова конечная цель совершаемого преступления.

Все перечисленные факторы необходимо рассматривать в совокупности.

Лица молодого возраста владеют технологиями несколько лучше, чем лица пожилого возраста. Однако при этом, если профессия лица пожилого возраста связана, например, с IT-технологиями, то его навыки будут более развитыми.

Наиболее наглядно прослеживается важность учета компьютерных навыков личности преступника при анализе структуры организованной группы.

Традиционно в наркопреступлениях между участниками распределялись следующие роли: организаторы, координаторы, контрабандисты, курьеры. В ходе проведенного исследования обнаружено, что изменение способа преступления привело к появлению абсолютно новых участников, среди которых: диспетчеры, кадровики, кураторы, коллекторы, дропы (дропперы).

Деятельность кадровиков, кураторов, коллекторов связана с взаимодействием с кладменами (или как традиционно их называют «закладчиками»). Сначала кадровики занимаются поиском кладменов, затем в работу с ними вступают кураторы, которые помогают им в работе. Коллекторы же необходимы для обеспечения «безопасности» в рамках наркобизнеса путем применения насилия в отношении кладменов, например, при краже наркотических средств.

При исследовании личности кадровиков, а в особенности кураторов важно учитывать их уровень владения технологиями, поскольку такой анализ позволит выяснить, какие конкретно способы ими применяются, действуют ли они по одиночке или же группой.

Аналогичная ситуация обстоит с диспетчерами, целью которых является получение и обработка заказов на наркотические средства с передачей их кладменам, и в конечном итоге контроль поступления денежных средств за заказ.

То, каким образом они получают и обрабатывают заказы, как организовывают оплату наркотических средств, обеспечивают ли анонимность и конфиденциальность проведенных операций, все это свидетельствует об их компьютерно-технических навыках.

Нередко для обналичивания полученных денежных средств и их дальнейшей передачи соответствующим лицам привлекаются так называемые дропперы. Дропперы используются лицами, непосредственно совершающими преступления, чтобы самим остаться в тени. В связи с тем, что дропперы через свои паспортные данные обналичивают средства, полученные в ходе преступной деятельности, сотрудники правоохранительных органов, в первую очередь, в ходе проведения розыскных мероприятий выходят именно на них.

Для криминалистической характеристики наиболее важно анализировать не личность самих дропперов (хотя преуменьшать их значение тоже было бы неверным), а то, каким образом были привлечены индивиды для участия в такой деятельности. Люди, становящиеся в конечном итоге дропперами, нередко даже не подозревают о нелегальности совершаемых ими действий, так как информация подается абсолютно с иным контекстом.

Например, в Телеграм-каналах может быть осуществлена рассылка с предложением подработки в той или иной сфере. Информационно неграмотные субъекты откликаются на такое предложение, после чего собираются их персональные данные, а затем на них оформляется банковская карта, через которую впоследствии и производится обналичивание средств. Жертвами такого мошенничества становятся пенсионеры и подростки, желающие найти легкий способ заработка.

Исследование еще раз подтверждает сделанное ранее утверждение: компьютерные сети оказывают влияние на все элементы криминалистической характеристики и определенным образом изменяют сами преступления.

Сравнение «традиционного» незаконного оборота наркотических средств с незаконным оборотом в компьютерных сетях демонстрирует, как и насколько изменились способы преступления.

Если раньше поиск закладчиков происходил либо непосредственно на улице, либо через передачу разными способами телефонов для связи (например, через объявления), то на данный момент таких возможностей значительно больше. Более

того, усложнилась структура участников, повысились анонимность, доступность совершения преступления.

Все это привело к тому, что в отличие от «традиционных» способов незаконного оборота наркотических средств вероятность выявления распространителей, продавцов, покупателей и иных лиц, участвующих в данных преступлениях, значительно ниже, благодаря технологиям, обеспечивающим высокий уровень конфиденциальности. Причем это касается как общения между отдельными лицами и группами, так и работы на рынках и анонимной продажи наркотических средств.

Новые разработки ставят правоохранительные органы в ситуацию, когда они видят, что преступная деятельность осуществляется, но имеют очень мало средств, а зачастую и вовсе ограниченные ресурсы, чтобы перехватить его.

Местонахождение (физическое и виртуальное) онлайн-рынка наркотиков обычно скрыто, что делает затруднительным обнаружение лица, ведущего деятельность на торговой площадке. Местонахождение покупателей и продавцов также замаскировано, а все прямые коммуникации между ними зашифрованы. Это означает, что получить любую информацию о том, кто и где находится подозреваемые или что они покупают, практически невозможно. Более того, Интернет предоставляет анонимные способы оплаты незаконных покупок.

Это снижает риск того, что наркопреступники на рынках будут пойманы, и как следствие, повышает привлекательность участия в незаконной деятельности. Именно по этой причине новый онлайн-рынок наркотических средств обладает способностью уклоняться от вмешательства правоохранительных органов.

В связи с этим необходимо совершенствовать и развивать методику раскрытия преступлений, связанных с незаконным оборотом наркотических средств.

Е. В. Иванова в своем исследовании пишет о том, что «информационный ресурс, являясь наиболее важным аспектом в расследовании преступлений, требует дальнейшей разработки в части необходимости и достаточности информации для принятия процессуальных решений, систематизации ситуаций информационной

определенности, разработки их особенностей с криминалистической точки зрения»[41].

Необходимо учитывать, что использование информационно-телекоммуникационных сетей для совершения преступлений привело к появлению нового объекта – цифрового следа, сущность которого будет раскрыта в следующем параграфе.

При этом ряд ученых корректно замечают, что «новые средства и благоприятные возможности совершения преступлений в эпоху цифровизации, одновременно и закономерно позволяют расширить следовую картину компьютерных преступлений и увеличить диапазон тактических приемов и решений, связанных с выявлением «цифровых» следов, их фиксацией и преобразованием в судебные доказательства»[42].

§ 1.2. Классификация объектов судебных экспертиз (цифровых следов) при расследовании незаконного оборота наркотических средств в компьютерных сетях

Как уже было сказано, большое количество преступлений совершаются с использованием компьютерных средств и систем, в результате чего и появляются цифровые следы.

Понятие «след» является одним из ключевых в криминалистике. В широком смысле слова следы — это любые изменения, связанные с событием преступления,

---

[41] Иванова Е. В. Концептуальные основы использования специальных знаний при выявлении и расследовании преступлений, связанных с опасными для здоровья веществами: Теория и практика: дис. … д-ра юрид. наук. М., 2014. С. 363-364.

[42] Лубин А. Ф. Некоторые тактические проблемы выявления и оценки цифровых следов компьютерных преступлений / А. Ф. Лубин, С. А. Лубин // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 4(64). С. 124.

отражающие его сущность и специфику[43]. В узком смысле «следы» — это отображение внешнего строения одного материального объекта на другой[44].

Понятие цифрового следа естественным образом вытекает из общего понятия следа. Однако все еще данный термин является предметом научных дискуссий. Среди ученых идут споры не только относительно сущности рассматриваемых объектов, но и относительно непосредственно терминологической составляющей.

В научных работах на данную тему можно выделить следующие позиции по наименованию рассматриваемых объектов: электронные следы, виртуальные следы и цифровые следы.

В. А. Мещеряков в своих работах вводит понятие «виртуальные следы», под которыми понимает любое изменение состояния автоматизированной информационной системы, связанное с событием преступления, представленное в виде компьютерной информации и зафиксированное на материальном носителе[45].

По мнению В. А. Перова, понятие «электронный след» более широкое чем «цифровой» или «виртуальный», так как может включать в себя не только цифровую, но и некую аналоговую информацию[46].

Не согласимся с данной точкой зрения, поскольку понятие «электронный» в любом контексте предполагает то, что работает на основании электрона. В заложенном принципе действия уже есть ограничения, в связи с чем термин «электронный» априори не может включать в себя цифровую информацию.

В. Б. Вехов определяет цифровой след как любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные),

---

[43] Криминалистика в 3 т. / под ред. Р. С. Белкина, В. Г. Коломацкого, И. М. Лузгина. М.: Академия МВД России, 1995. Т. 1: История, общие и частные теории. С. 49.

[44] Конон А. В. Криминалистическое учение о следах в отечественной и зарубежной литературе // Евразийский Союз Ученых. 2016. № 5-1 (26). С. 121.

[45] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков // Издательство Воронежского государственного университета. 2002. № 3. С. 94-98.

[46] Перов В. А. Компьютерная криминалистика: электронный след понятие и виды / В. А. Перов // Уголовное судопроизводство: проблемы теории и практики. 2021. № 1. С. 95.

представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим. 1 к ст. 272 УК РФ)[47].

А. И. Усов, И. А. Лапина, Г. Г. Омельянюк вводят понятие следов цифровой трансформации (ЦТ-следов). След цифровой трансформации (ЦТ-след) — это «криминалистически значимая информация о каких-либо событиях или действиях, отраженная в материальной среде путем цифрового преобразования до (вне судебно-экспертной деятельности), в процессе (промежуточное состояние) или в результате (выводное знание) судебно-экспертного исследования[48]».

В представленном определении ученые рассматривают цифровой след через призму судебно-экспертной деятельности, тем самым существенно сужая значение цифровых следов. Далеко не всегда при обнаружении цифровых следов требуется назначение судебной экспертизы. След считается цифровым не по причине проведения того или иного рода/вида экспертизы, а исходя из своей сущности.

На наш взгляд, наиболее точно и полно отражает суть рассматриваемых объектов определение Е. Р. Россинской: «Цифровой след – криминалистически значимая компьютерная информация о событиях или действиях, отраженная в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»[49].

За рубежом вопрос понятийного аппарата является более урегулированным. Описывая объекты такого рода, все авторы используют термин *digital footprints,* что и переводится как «цифровые следы».

В зарубежных источниках акцент сделан именно на цифровой сущности рассматриваемых доказательств; электронная природа носителя учитывается,

---

[47] Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. С. 97.

[48] Усов А. И., Лапина И. А., Омельянюк Г. Г. Новые тенденции в сфере судебно-экспертной деятельности как ответ на вызовы современности / И. А. Лапина, Г. Г. Омельянюк, А. И. Усов // Судебная экспертиза Беларуси. 2021. № 1 (12). С. 5–13.

[49] Теория информационно-компьютерного обеспечения криминалистической деятельности... С.44.

однако интерес вызывает в первую очередь сама цифровая информация, а не ее носитель[50].

В употреблении именно такой терминологии есть логическое объяснение, нельзя сказать, что это «калька» опыта иных стран на наш. В основе действия компьютеров, смартфонов, иных технических средств и даже в основе информации лежит двоичный код, а проще говоря – цифра. Поэтому понятие «цифровой» отражает саму сущность таких следов.

Среди основных особенностей цифровых следов, в связи с которыми и выделяется самостоятельный вид объектов, можно выделить следующие:

– цифровые следы представляют собой компьютерную информацию;

– цифровым следам присуща доступность – принимая во внимание уровень и степень внедрения современных технологий, стоит учитывать, что пользователь имеет возможность без труда и достаточно оперативно управлять компьютерной информацией, проводить с ней различные процедуры в удаленном режиме;

– цифровые следы наиболее подвержены изменениям – вытекает из предыдущей особенности. Если сравнивать традиционные криминалистические следы и цифровые следы, то можно сказать, что в последние гораздо легче внести изменения более незаметно. Чтобы изменить, уничтожить, например, след пальцев рук, нужен физический доступ к следу, а для цифровых следов это требуется не всегда;

– цифровые следы неотделимы от материального носителя, на котором они располагаются – их обнаружение происходит за счет осмотра носителя, так как информация все же представляет собой нечто нематериальное, что нельзя воспринимать органами чувств непосредственно.

---

[50] Sadiku M., Tembely M., Musa S. Digital Forensics // International Journal of Advanced Research in Computer Science and Software Engineering. 2017. №. 7. P. 274–276.

Отсутствие точного, стандартизированного понятийно-терминологического аппарата приводит к тому, что в практической деятельности лица, сталкивающиеся непосредственно с цифровыми следами, совершают ряд ошибок.

Об этом свидетельствуют итоговые данные анкетирования. В ходе проведенного исследования нами было опрошено более 100 респондентов из числа сотрудников правоохранительных органов. Согласно результатам анкетирования, 55,8% сталкиваются в своей работе с цифровыми следами.

Рисунок 1. Статистические данные по результатам ответа сотрудников правоохранительных органов на вопрос «Как часто при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях, Вы сталкиваетесь с цифровыми следами?»



При этом на вопрос «Что Вы понимаете под цифровыми следами?» 12% ответили «ничего», 83% определили цифровые следы как следы, оставленные в Интернете, и только 5% дали более развернутый ответ, продемонстрировав некое понимание сущности цифровых следов, например:

– следы преступной деятельности, сохранившиеся в виде информации на электронных носителях, в т.ч. персональных коммуникационных устройствах, на серверах с возможностью доступа через сеть (либо невозможностью);

– криминалистически значимая информация, выраженная посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники;

– отдельная категория следов, компьютерная информация, то есть сведения, представленные в форме электрических сигналов.

В приведенных примерах определений прослеживается лишь частичное понимание цифровых следов, так как все респонденты ошибочно употребляют термины «электронный», «электромагнитный», «электрический».

Такое некорректное использование перечисленных терминов связано с несколькими причинами: во-первых, отсутствие единого понимания цифровых следов в теории, во-вторых, фигурирование в УК РФ и УПК РФ понятия «электронные носители», и, в-третьих, отсутствие у опрошенных респондентов, являющихся следователями, специальных компьютерно-технических знаний.

Ответы опрошенных лиц подтверждают высказанную ранее мысль, что в своем большинстве у сотрудников правоохранительных органов отсутствует понимание цифровых следов. На основании этого можно предположить, что с цифровыми следами из опрошенных работали даже более 55,8%, так как представляется, что, столкнувшись с объектами данного рода, они могли их классифицировать иначе.

Вопрос классификации цифровых следов, в особенности цифровых следов по делам, связанным с незаконным оборотом наркотических средств, также является дискуссионным.

Традиционно в криминалистике следы делят на материальные и идеальные.

По мнению В. Б. Вехова, Б. П. Смагоринского, С. А. Ковалева компьютерная информация обладает определенными фиксированными характеристиками и представляет собой «невидимые материальные следы»[51].

Включение цифровых следов в такую отдельную группу, как «невидимые материальные следы» представляется неуместным, так как не всегда и не все цифровые следы невозможно увидеть без использования специальных методов и средств. Например, скриншот переписки в мессенджере является видимым для человеческого зрения.

[51] Цифровая криминалистика: учебник для вузов... С. 17.

Р. А. Дерюгин, А. А. Жижелева считают, что цифровые следы нельзя отнести ни к материальным, ни к идеальным, поскольку они занимают промежуточное положение[52].

В связи с этим ряд авторов, в частности, уже упомянутый В. А. Мещеряков вводят еще одну категорию «виртуальные следы»[53]

Однако представляется, что такое деление будет не совсем корректным, так как цифровые следы, как уже было сказано ранее, все же содержатся на материальных носителях и, что важно, неотделимы от них.

По этой причине нельзя не согласиться с мнением Е. Р. Россинской, которая пишет о том, что «по природе цифровые следы являются следами материальными»[54].

Сами же цифровые следы можно классифицировать по нескольким основаниям.

Достаточно новаторской является классификация, предложенная А. А. Саркисян, которая делит цифровые следы по их происхождению на:

Оригинальные — это подлинные, первоначальные записи, возникшие в результате естественного цикла.

Реплицированные — это реплики записей, копии, возникшие в результате естественного цикла записи или же созданные с умыслом подражания оригиналу[55]. Причем к данному виду цифровых следов А. А. Саркисян относит также копии цифровых следов и поддельные цифровые записи.

---

[52] Дерюгин Р. А., Жижелева А. А. Технологии XXI века в юриспруденции Материалы Всероссийской научно-практической конференции // под редакцией Д. В. Бахтеева. 2019. С. 40-46.

[53] Мещеряков В. А. Преступления в сфере компьютерной информации... С. 94-98.

[54] Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. №2 (89). С. 199.

[55] Саркисян А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты: автореферат дис. ... кандидата юридических наук: 5.1.4. / Москва, 2024. С. 101.

Развивая вопрос классификации цифровых следов, Е. Р. Россинская выносит следующую классификацию цифровых следов[56]:

– могут находиться на отдельных носителях, например, на жестком магнитном диске (HDD), флеш-накопителе и др.;

– могут непосредственно содержаться в компьютерных системах и сетях, мобильных коммуникаторах, планшетах, на серверах, в облачных хранилищах;

– в качестве цифровых следов можно рассматривать электронные документы;

– образы цифровых следов – отображаются в цифровом виде с помощью различных программных продуктов, например, изображения подписей, дактилоскопических отпечатков в графических или текстовых процессорах; скриншоты переписки в социальных сетях и др.;

– образы цифровых следов – отображаются на бумажных носителях, например, распечатки скриншотов, распечатки электронных документов и др.

В контексте преступлений, рассматриваемых в рамках настоящего исследования, наиболее актуальным является исследование цифровых следов, содержащихся именно в компьютерных системах и сетях, мобильных коммуникаторах, планшетах, на серверах, в облачных хранилищах.

Д. В. Бахтеев, Е. В. Смахтин проводят классификацию по следующим основаниям[57]:

– по форме носителя: цифровые следы, расположенные на оптических носителях (CD, DVD, blu-ray диски и пр.), полупроводниковых носителях (флеш-накопители, SSD) и магнитных носителях (жесткие диски).

– по способу доступа – локальный или удаленный.

---

[56] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 46.

[57] Бахтеев Д. В. Криминалистические особенности производства процессуальных действий с цифровыми следами / Д. В. Бахтеев, Е. В. Смахтин // Российский юридический журнал. 2019. № 6(129). С. 61-68.

Такая классификация цифровых следов имеет достаточно важное значение при расследовании дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях. В зависимости от того, какой способ доступа превалирует в конкретной ситуации, в первую очередь, меняется тактика действий следователя, специалиста, эксперта при собирании, фиксации, изъятии следов, а также при производстве в дальнейшем экспертизы. Игнорирование данных обстоятельств приводит к ряду ошибок, которые будут раскрыты в дальнейшем.

– по характеру доступа: доступные (например, электронные документы), скрытые (скрытые файлы, информация, скрытая с помощью методов стеганографии) и зашифрованные.

Как и в предыдущем основании данной классификации, от характера доступа зависит выбор методов, средств и приемов при собирании цифровых следов.

– по характеру происхождения: оставленные человеком непосредственно (электронные документы, записи в социальных сетях и т. п.) и опосредованно (данные телеметрии, файлы регистрации, атрибуты создаваемых файлов и т. п.).

Схожее с последним по своей сущности основание деления цифровых следов имеет большую популярность в зарубежной научной литературе. Так, ученые в своем большинстве делят цифровые следы на активные и пассивные[58].

N. Casemajor, S. Couture, M. Delfin, M. Goerzen и A. Delfanti пишут о том, что цифровые следы появляются не только за счет активного и непосредственного участия людей в Интернете, но и за счет скрытой части сети, например, действия различного рода алгоритмов. Следовательно, цифровые следы представляют собой сумму данных, полученных как при активной, так и при пассивной форме участия[59].

---

[58] Худяков В. В., Ананьев А. А. Цифровые следы // Криминологический журнал. 2023. №4. С. 244.

[59] Casemajor N., Couture S., Delfin M., Goerzen M. and Delfanti A. (2015), «Non-participation in digital media: toward a framework of mediated political action», Media, Culture & So- ciety, Vol. 37 №. 6. PP. 856.

Активный цифровой след характеризуется тем, что пользователь лично и целенаправленно создает, делится определенной информацией, например, путем публикаций в социальных сетях, комментариев на иных онлайн-ресурсах и т.д.

Пассивные цифровые следы отличаются тем, что такие следы формируются вне зависимости от воли самого пользователя. Этим обосновывается пассивность участия субъекта в создании таких следов. В частности, такое происходит, когда веб-сайты собирают информацию о том, сколько раз пользователи посещают страницу, их месторасположение по IP-адресу посетителей. Такой процесс является теневым, при недостаточном уровне владения компьютерными технологиями субъект может не догадываться о существовании таких цифровых следов.

М. Мишель, К. Лутц, М. Бехи выделяют два типа пассивного участия: данные, генерируемые платформами как побочный продукт онлайн-деятельности пользователей, и данные, публикуемые другими пользователями, но связанные с иным лицом[60].

Участники опроса выделяет следующие виды цифровых следов, с которыми они сталкивались в своей работе:

– данные социальных сетей и мессенджеров;

– данные сайтов сети Интернет, теневого сегмента Даркнет, а также история посещения сайтов;

– данные приложений, содержащие информацию, например, о местоположении и о проведенных транзакциях;

– облачное хранилище данных;

– содержимое памяти персональных устройств – записные книжки, календари, информация в иных приложениях, фотографии, геотеги, связки ключей.

[60] Micheli M., Lutz C., Büchi M. (2018). Digital footprints: an emerging dimension of digital inequality. Journal of Information, Communication and Ethics in Society, 16(3): P. 246.

Рисунок 2. Статистические данные по результатам ответа сотрудников правоохранительных органов на вопрос «С какими видами цифровых следов Вы сталкиваетесь при расследовании дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях?»



Все перечисленные респондентами виды цифровых следов можно разделить на активные и пассивные. Так, например, поисковый запрос пользователя в сети Интернет будет являться активным цифровым следом, так как он непосредственно вводил данные и совершал активные действия, а история посещения сайтов будет уже пассивным цифровым следом, так как это сбор данных, осуществленный не лично самим пользователем, но в связи с совершением им определенных действий.

Представляется, что цифровые следы, образованные в ходе совершения преступлений, связанных с незаконным оборотом наркотических средств, можно классифицировать в соответствии с направленностью действий лиц в компьютерных сетях следующим образом:

1. Активные цифровые следы

– сообщения в социальных сетях и мессенджерах;
– публикации в социальных сетях и Телеграм-каналах;
– комментарии в социальных сетях, Телеграм-каналах, онлайн-форумах;
– поисковые запросы в сети Интернет и теневом сегменте Даркнет;
– данные о совершенных транзакциях;
– фото-, видео-, аудиоматериалы;
– электронные документы;
– активность в приложениях и программах;

– облачное хранилище данных.

2. Пассивные цифровые следы

– GPS-данные;

– история браузера;

– куки-файлы;

– кэш браузера;

– метаданные файлов;

– данные IP-адреса.

Когда мы говорим о киберпреступлениях либо об иных преступлениях, но совершенных с использованием компьютерных технологий, недостаточно проводить анализ исключительно следов преступления. Понятие следов тесно связано с понятиями механизма следообразования и технологиями исследования.

На это в своей работе справедливо указали А. Н. Савенков и Е. Р. Россинская. Ученые пишут о том, что классический «крест следов» необходимо несколько модернизировать, внедрив туда как раз механизм следообразования и технологии исследования[61].

Проведенное нами выше исследование лишь подтверждает данную позицию, поскольку именно с помощью анализа процесса происхождения следов, в дальнейшем удалось их классифицировать. Причем это работает и в обратную сторону. Если у нас имеется знание о самом следе, то появляется возможность определения того, как эти следы образуются.

В частности, знание о том, что существует такой вид цифровых следов, как сообщения в мессенджерах, приводит к размышлению о том, каким неочевидным образом данный след могут оставлять преступники. Вследствие чего обнаруживаются различные механизмы шифрования и сокрытия информации.

Представление о непосредственно видах следов и их механизме следообразования впоследствии позволяет выработать технологии исследования.

---

[61] Савенков А. Н., Россинская Е. Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. № 10. С. 156—168.

Соответственно, представленная классификация цифровых следов имеет, как видно, не только теоретические значение (для всех уголовно-правовых наук), но и практическое.

Для судебно-экспертной деятельности такое разделение цифровых следов позволяет четко выделить и определить те объекты, с которыми эксперты могут столкнуться при назначении экспертизы. В свою очередь, знание об объектах влияет на разработку новых методик экспертиз, новых методов и средств работы с цифровыми следами. Результатом совокупности полученных новых знаний является повышение качества проводимых экспертиз, что имеет значение для процесса доказывания.

Понимание того, что помимо «видимых» цифровых следов присутствуют еще и скрытые, значительно расширяет возможности следствия и формирования ими доказательственной базы, а, как следствие, в случае назначения судебной экспертизы, повышает и качество ее результатов.

В отдельных случаях пассивные цифровые следы могут быть даже информативнее, чем активные цифровые следы. Данные IP-адреса позволяют вычислить не только местонахождение лица, но и конкретное устройство, с которого совершались те или иные действия.

Куки-файлы позволяют отследить повторяющиеся посещения сайтов одним и тем же пользователем, определить активность и действия пользователя на каждом сайте, а также выявить предпочтения пользователя и иную информацию о конкретном лице.

Соответственно, при расследовании преступлений важным является учитывать наличие активных и пассивных цифровых следов по следующим причинам.

Во-первых, анализ в совокупности активных и пассивных цифровых следов может способствовать идентификации подозреваемых в совершенном преступления лиц. Во-вторых, после идентификации подозреваемых появляется возможность определить их связи между собой и выполняемую роль (если речь идет о совершении преступления группой лиц). Для незаконного оборота

наркотических средств очень характерна именно такая модель совершения преступления. В-третьих, таким образом следователи могут установить хронологию и последовательность событий совершенного преступления. И наконец, анализ цифровых следов одного преступления может позволить выявить закономерности и модели совершения преступлений такого рода.

Однако важно учитывать, что работа с цифровыми следами требует особых дополнительных компетенций. Можно допустить, что следователь, обладая такими компетенциями в рамках осуществляемой им деятельности, может в отдельных случаях самостоятельно собирать активные цифровые следы, например, зафиксировать переписку между лицами путем скриншота. Но собирание пассивных цифровых следов невозможно без участия специалиста.

В связи с этим необходимо расширять компетенции сотрудников правоохранительных органов в области цифровых следов. Согласны с таким мнением 63,1% опрошенных.

Рисунок 3. Статистические данные по результатам ответа сотрудников правоохранительных органов на вопрос «Считаете ли необходимым расширение Ваших компетенций в области собирания цифровых следов?»



По мнению В. Ф. Васюкова и А. К. Шеметова, «профессиональная квалификация следователя должна рассматриваться как постоянно совершенствующаяся совокупность не только специальных, но и общих знаний, способностей, на которых базируются умения и навыки выполнения

профессиональных функций в рамках раскрытия и расследования преступлений на различных этапах»[62].

Ф. К. Зиннуров, Э. Т. Хайруллова провели опрос среди следователей и выяснили, что 78% опрошенных ими респондентов в своей работе не учитывают особенностей полученной компьютерной информации или вовсе относятся скептически к возможностям получения от цифровых следов информации, имеющей значение для дела, и только 22% указанных респондентов в своих действиях и решениях в рассматриваемых ситуациях полагаются на специалистов[63].

С одной стороны, возникает вопрос: «Зачем следователям необходимо обладать минимальной компетенцией в цифровых следах, если они могут привлекать специалистов?» Но, с другой стороны, необходимо помнить, что следователь – самостоятельная процессуальная фигура в уголовном деле, и именно от действий и решений следователя зависит ход расследования, а по итогу качество полученных доказательств.

Если же следователь не знает, что представляют собой цифровые следы, каковы их отличительные признаки, каковы особенности их собирания, то он не сможет определить, какой порядок действий он лично должен совершить, специалиста в области каких специальных знаний необходимо привлечь, какую экспертизу надо назначить.

18% из числа опрошенных в рамках настоящего исследования сообщили, что им известны случаи утраты цифровых следов при производстве следственных действий по преступлениям, связанным с незаконным оборотом наркотических средств в компьютерных сетях. Для уголовных дел по данной категории преступлений эта цифра является значительной и весомой.

---

[62] Васюков В. Ф. Некоторые особенности повышения квалификации следователей правоохранительных органов / В. Ф. Васюков, А. К. Шеметов // Правовая парадигма. – 2021. – Т. 20, № 2. – С. 102.

[63] Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С. 275.

Часть ученых в качестве решения образовавшейся проблемы предлагают ввести такую специальность, как IT-следователь. Об этом пишут в своей работе С. В. Зуев и А. И. Зазулин. По мнению авторов, и «обычные следователи», и «IT-следователи» сталкиваются в осуществляемой ими деятельности с цифровыми следами. Однако принципиальное отличие состоит в том, «IT-следователь должен уметь работать с большими данными, читать экспертные заключения по результатам проведения компьютерно-технических экспертиз любой сложности, широко применять электронные документы в перспективе использовать электронного помощника»[64].

В связи с этим предлагается ввести специальные образовательные программы, которые включали бы, помимо теоретических курсов с ведущими учеными в сфере цифровизации уголовного процесса, практическую часть занятий с экспертами-программистами с целью разъяснения принципа действия и применения цифровых технологий[65].

Важность обучения следователей работе с цифровыми следами сложно переоценить, об этом ранее уже было не раз сказано. При этом целесообразность введения новой специальности «IT-следователь» подвергается сомнениям, поскольку отчасти таким образом происходит замена отдельного самостоятельного участника уголовного процесса – специалиста.

Именно в задачи специалиста входят работа с данными, требующими специальных знаний, анализ на соответствие требованиям заключений экспертов (всех видов экспертиз, не только компьютерно-технических экспертиз), а также понимание, как протекают те или иные цифровые процессы. Следователь же должен грамотно направлять и ввести ход расследования дела.

IT-следователь не может быть компетентными во всех областях специальных знаний, а цифровые следы встречаются не только в рамках компьютерно-

---

[64] Зуев С. В. IT-следователь в цифровой среде уголовного судопроизводства / С. В. Зуев, А. И. Зазулин // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 50-51.

[65] Зуев С. В. IT-следователь в цифровой среде... С. 51.

технической экспертизы. Цифровые следы так или иначе оказали и оказывают существенное влияние на все виды экспертиз.

Представляется, что наиболее рациональным решением будет являться проведение для уже действующих сотрудников правоохранительных органов повышения квалификации, а для обучающихся включение в рабочие программы разделов, посвященных цифровым следам, в той мере, которая необходима именно для их компетенции.

В своем диссертационном исследовании А. А. Саркисян представила рабочую программу дисциплины «Экспертиза в судопроизводстве», в которую включила следующие вопросы касательно цифровых следов[66]:

1. Цифровые следы как объект судебных экспертиз.

2. Признаки и свойства цифровых следов.

3. Основы обнаружения, фиксации и изъятия цифровых следов.

4. Правила упаковки и хранения цифровых следов и их материальных носителей.

5. Правила и правовая регламентация организации процессуальных действий, связанных с обнаружением, фиксацией и изъятием цифровых следов для последующего назначения судебных экспертиз.

6. Возможные ошибки при работе с цифровыми следами.

7. Участие специалиста при производстве процессуальных действий, связанных с обнаружением, фиксацией и изъятием цифровых следов для последующего назначения судебных экспертиз.

На наш взгляд, такое содержание дисциплины с сопровождением должного количества лекционных и практических занятий в полной мере обеспечит формирование у сотрудников правоохранительных органов необходимых навыков и умений в области цифровых следов.

Хотелось бы добавить к указанному перечню вопросов также аспект рассмотрения цифровых следов как цифровых доказательств.

---

[66] Саркисян А. А. Цифровизация судебно-экспертной деятельности… С. 135-136.

Зарубежные ученые, рассуждая о цифровых доказательствах, преимущественно относят к ним данные в любом виде представления, которые можно извлечь из компьютерных систем для использования в доказывании, подтверждения либо опровержения проверяемых фактов и обстоятельств[67].

Отход от аналогового понятия «доказательство» и признания в качестве самостоятельного вида «цифровое доказательство» требует переосмысления, в частности, способов собирания доказательств. Очевидно, «цифровая» составляющая рассматриваемых доказательств требует учета их специфики при получении, анализе, хранении и процессуальном закреплении собранных цифровых следов.

М. И. Воронин справедливо отмечает, что традиционные следственные действия, такие как обыск и выемка, должны быть адаптированы к особенностям цифровой информации, что приводит к размышлениям о необходимости разработки специальных видов обыска и выемки, таких как обыск (выемка) электронных (цифровых) носителей информации; выемка электронной (цифровой) информации; распоряжение провайдеру, оператору информационной системы, депозитарию о предоставлении информации об операциях с электронными (цифровыми) активами; предоставление удаленного доступа к базам данных (сбор данных в режиме реального времени)[68].

Сам по себе цифровой след еще не является доказательством. Он становится таковым после совершения определенного порядка действий. Цифровые доказательства могут являться сильными инструментами для правоохранительных органов, так как они часто содержат информацию, которая не может быть получена из других источников. Однако, чтобы грамотно использовать цифровые доказательства в суде, необходимо учитывать особенности таких объектов при их представлении в суде.

---

[67] Maras Marie-Helen. Cybercriminology: Oxford University Press, 2016. P. 44.

[68] Воронин М. И. О правовой природе электронных (цифровых) доказательств // Вестник Университета имени О. Е. Кутафина. 2020. №10 (74). URL: https://cyberleninka.ru/article/n/o-pravovoy-prirode-elektronnyh-tsifrovyh-dokazatelstv (дата обращения: 20.03.2023).

При собирании цифровых следов, а в дальнейшем использовании уже цифровых доказательств важно соблюдать все необходимые процедуры и правила, чтобы избежать нарушений прав человека или неправомерного использования данных. Для обеспечения достоверности доказательств необходимо следить за сохранностью цифровых данных и защитой их от несанкционированного доступа.

На наш взгляд, при обучении сотрудников правоохранительных органов важно акцентировать внимание на обозначенных выше вопросах.

При этом всем важно отметить, что в постоянном повышении квалификации в области цифровизации нуждаются не только сотрудники правоохранительных органов, но и сами эксперты и специалисты, так как основополагающую роль при работе с цифровыми следами играют именно данные участники уголовного судопроизводства.

Обучение экспертов существенным образом отличается и должно отличаться от обучения юристов (в широком смысле), так как требует более глубокого погружения в тему цифровых следов. Более такого для экспертов важно делать упор на использование цифровых следов и работу с ними в каждом из изучаемых родов экспертиз.

Таким образом, все вышесказанное очередной раз подчеркивает теоретическое и практическое значение классификации цифровых следов, в частности, в делах, связанных с незаконным оборотом наркотических средств в компьютерных сетях.

§ 1.3. Собирание цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях

Собирание следов преступления представляет собой многоступенчатый и комплексный процесс, осуществляемый в соответствии с законодательством и существующими методиками.

Традиционно в криминалистике под собиранием следов понимают три последовательно сменяющих друг друга этапа: обнаружение, фиксацию и изъятие[69]. При анализе работ ученых можно отметить, что для каждого объекта имеются определенные особенности обнаружения, фиксации и изъятия.

Вопросы, связанные с обнаружением, фиксацией и изъятием следов, освещаются уже достаточно давно. Однако большинство работ посвящены собиранию «традиционных» следов, а, как уже было сказано, для цифровых следов требуется создание отдельных рекомендаций и методик.

При формулировании рекомендаций по собиранию цифровых следов важно учитывать несколько аспектов:

– общие особенности цифровых следов;
– особенности отдельных видов цифровых следов;
– особенности носителей цифровых следов;
– особенности конкретного проводимого следственного действия.

Обнаружение, изъятие и фиксация цифровых следов проходят всегда в рамках какого-то конкретного следственного действия. В рамках расследования дел о незаконном обороте наркотических средств, как демонстрируют судебная практика и результаты проведенного нами исследования, собирание цифровых следов происходит при производстве таких следственных действий, как осмотр, обыск и чуть реже выемка.

Тактика собирания цифровых следов определяется, конечно же, в первую очередь особенностями самих цифровых следов. Однако специфика конкретного следственного действия также оказывает влияние на порядок проводимых мероприятий в ходе процесса собирания.

В ходе невербальных следственных действий грамотно организованная работа по поиску, обнаружению и предварительному исследованию цифровых следов, имеющих криминалистическое значение, позволяет непосредственно на

---

[69] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика. Учебник для вузов. 4-е изд., переработанное и доп. М.: Норма- ИНФРА-М, 2014. 928 с.

месте получить сведения о способах преступления, обнаружить, зафиксировать и изъять методом консервирования на электронном носителе информации эти цифровые следы, выявить иные обстоятельства происшествия[70].

Как справедливо отмечают авторы монографии, одно из главных отличий осмотра места происшествия от обыска заключается в незамедлительности, так как обыск производится уже только по возбужденному уголовному делу. Соответственно, при проведении обыска у следователя есть время для более тщательной подготовки к следственному действию[71].

Сущностные различия выемки и обыска заключаются в том, что выемка производится только в отношении тех предметов, существование и местонахождение которых достоверно известно, при обыске подлежащие изъятию предметы могут быть известны ориентировочно, а иногда и вовсе неизвестны[72].

В продолжении развития данной позиции С. Б. Россинский пишет о том, что «выемка отличается от обыска изначальной определенностью подлежащих изъятию объектов, а также отсутствием поискового элемента в познавательных действиях органов предварительного расследования»[73].

Именно по указанным причинам для организации и производства выемки компьютерных средств (в широком смысле слова) отчасти снижается уровень оперативности действий и в целом требуется меньшее количество усилий.

Д. В. Овсянников придерживается мнения, что выемку, обыск или осмотр, если они включают в себя изъятие электронных носителей информации и

---

[70] Теория информационно-компьютерного обеспечения криминалистической деятельности... С. 89.

[71] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 100.

[72] Ратинов А. Р. Обыск и выемка. М.: Госюриздат, 1961. С. 8.

[73] Россинский С. Б. Размышления о сущности выемки как объекта уголовно-процессуального регулирования // Вестник Московского университета МВД России. 2018. №1. С. 42.

копирование с них информации, следует относить к комбинированным следственным действиям[74].

Не согласны с мнением Д. В. Овсянникова, так как каждое из этих следственных действий отличается по своей сущности, по целям друг от друга, иначе не было бы смысла выделять их в отдельные виды. А их различия, в свою очередь, влияют на тактические особенности.

Формальный подход к организации следственных действий, в особенности, связанных с собиранием цифровых следов, нередко приводит к утрате доказательственной информации.

Среди основных причин, по которым происходит утрата цифровых следов, следователи выделяют следующие:

– несвоевременного проведение следственного действия;

– ошибки, допущенные следователем, при проведении изъятия и фиксации цифровых следов;

– отсутствие осведомленности следователя о необходимых действиях для обеспечения сохранности цифровых следов;

– непривлечение к участию в следственном действии соответствующего специалиста;

– коррупционная составляющая;

– очистка данных устройства преступниками через удаленный доступ.

Соответственно, первые 4 причины можно отнести к субъективным ошибкам, так как они связаны с профессиональной некомпетентностью и халатностью самих следователей, а последнюю причину – к объективным ошибкам, так как на данный момент исключить на 100% возможность дистанционного удаления информации не представляется возможным.

Ссылаясь на результаты проведенного опроса, можно сказать, что сами сотрудники правоохранительных органов считают недостаточными современные

---

[74] Овсянников Д. В. Электронное копирование информации в система средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. 2014. № 2 (3). С. 130-135.

технико-криминалистические средства для обеспечения в полной мере эффективного собирания цифровых следов. Респонденты отмечают, что отсутствие методики, стандартов по собиранию цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, затрудняют собирания цифровых следов уже на этапе обнаружения.

Так как цифровые следы представляют собой именно компьютерную информацию, для их обнаружения зачастую требуется применение специальных средств и методов. Наглядную аналогию можно провести со следами пальцев. Сами по себе следы пальцев являются невидимыми для человеческого глаза, однако использование специальных технических средств позволяет без труда их обнаружить.

В зарубежных странах для ускорения процесса с получением максимального результата начали использовать ряд программ. Например, Cellebrite Pathfinder – это программа, основанная на алгоритмах машинного обучения. Cellebrite Pathfinder автоматически объединяет большие объемы разрозненных источников данных мобильных, облачных, компьютерных и телекоммуникационных сетей с целью выявления необходимой для правоохранительных органов информации[75].

Данная программа имеет возможности распознавания, обработки и анализа текста, обнаружения фото-, видеоизображений, относящихся к заданной категории (в частности, в категории «наркотические средства»). Не менее важным является способность Cellebrite Pathfinder обнаружения данных о местоположении подозреваемых лиц, обнаружение «горячих» точек. С помощью такой программы можно выстраивать в дальнейшем связи и закономерности передвижения, коммуникации лиц, участвующих в наркопреступлениях.

В отечественной практике также применяются специальные программы и программно-аналитические комплексы. К их числу относятся «Мобильный криминалист», UFED Touch (устройство исследования сотовых телефонов, которое

---

[75] Данные о программе Cellebrite Pathfinder // URL: https://www.dataexpert.eu/products/mobile-forensics-cellebrite/cellebrite-pathfinder/ (дата обращения: 23.01.2024).

позволяет безопасно извлекать информацию без потери данных), система считывания и анализа информации с мобильных телефонов и сим-карт XRY (швейцарского производства).

Данные программы используются как для обнаружения, так и для изъятия информации. Так, «Мобильный криминалист», позволяет анализировать данные, в том числе в хронологическом порядке, с составлением визуализированной схемы. Программа позволяет проводить исследования в облачных сервисах. UFED Touch в некоторых случаях предлагает обход блокировок исследуемого объекта, то есть декодирование, а система XRY предполагает более глубокий анализ данных на сим-картах мобильных телефонов и в их встроенной памяти, вплоть до восстановления ранее удаленных данных[76].

Однако ввиду санкционной политики компания Cellebrite (производитель системы UFED Touch) отказалась предоставлять обновление программного комплекса российской стороне.

В.Ф. Васюков отмечает, что правозащитники обнаружили уязвимость в программном обеспечении UFED Touch. Выявлена возможность внесения изменений не только в интересующий (проводимый) в настоящее время отчет, но и во все последующие (без оставления каких-либо электронных меток о данном противоправном действии)[77].

Безусловно, внедрение таких технологий требует проведения ряда масштабных процедур по проверке их функционирования, по их стандартизации, паспортизации. При собирании цифровых следов нельзя обойтись без использования передовых технологий. Ввиду того, что цифровые следы легко подвержены изменениям, а объем информации, с которым сталкиваются специалисты при работе с цифровыми следами зачастую велик, повышается

---

[76] Варакин Я. Г. Криминалистические технологии обнаружения, фиксации, изъятия цифровых следов преступления и иной доказательной информации // Вестник Сургутского государственного университета. 2021. № 4. С. 83.

[77] Васюков В. Ф. Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.

значимость оперативности обнаружения цифровых следов. Использование современных программ способно обеспечить в достаточной мере достижения эффективности обнаружения.

Исследование показывает, что есть и иные трудности, связанные с обнаружением цифровых следов.

В ходе анализа данных социальных сетей, мессенджеров, а также данных с сайтов, обнаружение криминалистически значимой компьютерной информации может быть осложнено тем, что такая информация бывает замаскированной. Причем маскировка может быть как лингвистической, так и компьютерно-технической.

Говоря о вариантах лингвистических маскировок, нужно отметить следующее: в речевых продуктах могут быть употреблены слова, фразы, которые на первый взгляд не принадлежат к семантическому полю «наркотические средства», однако при более детальном исследовании не только вырванных из контекста лексем, словосочетаний, но и всего речевого продукта в целом, лицо, обладающее специальными знаниями, может обнаружить использование маскировки слов наркотического дискурса.

Например, нередко для маскировки используются лексемы с семантическим полем «продукты питания». Согласно словарным данным наркотического сленга, масло – это концентрированная настойка опия; молоко – отвар дикорастущей конопли в молоке; пшено – папиросы с анашой или гашишем[78].

В своей работе А. Г. Данилин приводит примеры фраз, которые встречаются в разговорах при обсуждении наркотических средств: «Хочу нашего молока», «Мне нужно немного белого хлеба»[79].

---

[78] Наркоманский словарь Баяна Ширянова // URL: http://imperium.lenin.ru/EOWN/eown7/dictionary/dictionary.html (дата обращения: 15.01.2024).

[79] Данилин А. Г. - LSD. Галлюциногены, психоделия и феномен зависимости – М.: ЗАО Изд-во Центрполиграф. 2001. С. 209.

Несмотря на изменение способов совершений преступлений, связанных с незаконным оборотом наркотических средств, приведенная А. Г. Данилиным лексика все еще широко используется наркопреступниками.

Примечательно, что в одних речевых продуктах может не быть слов/словосочетаний, напрямую относящихся к наркотическому дискурсу, но при этом может идти речь о сбыте наркотических средств, а в других речевых продуктах используются, казалось бы, очевидные упоминания сбыта наркотических средств, но по результатам исследования смысл оказывается иным.

Так, на исследование поступил речевой продукт, представляющий собой переписку в групповом чате WhatsApp, где между Пользователем 1 и Пользователем 2 состоялся диалог, в рамках которого ими были употреблены следующие фразы:

Пользователь 1: «Уж не в снабжении ли наркотиками идет речь о помощи?»

Пользователь 2: «Тебе подогнать? Пиши в лс»

Без применения специальных лингвистических знаний можно сделать вывод, что Пользователь 2 сообщает, что при заинтересованности Пользователем 1 наркотическими средствами последний может ему написать. Имплицитно в представленном отрывке содержится информация о том, что Пользователь 2 может обеспечить сбыт наркотических средств.

Однако анализ целого речевого продукта с использованием лингвистических методов демонстрирует, что в предложении «Тебе подогнать? Пиши в лс» Пользователь 2 использует такое художественное средство, как иронию. Соответственно, фраза употреблена в ироническом значении со скрытым подтекстом обвинения собеседника в желании употребить наркотические средства.

Хоть сам по себе этап обнаружения не предполагает проведения полноценного исследования, у следователя есть несколько путей решения. Во-первых, следователь может привлечь специалиста-лингвиста для оказания помощи в обнаружении значимой для дела информации. На практике нередко сотрудники правоохранительных органов ограничиваются привлечением специалистов лишь в области компьютерно-технических знаний. Такой подход обусловлен следующим:

не все следователи осведомлены о возможностях разного рода специальных знаний, а также о современных способах маскировок и сокрытия информации. Поэтому привлеченный к участию специалист на этапе обнаружения может указать, что из всего массива информации стоит в дальнейшем извлечь. Во-вторых, еще до возбуждения уголовного дела следователь имеет право назначить судебную экспертизу.

Компьютерно-техническим вариантом маскировки является внедрение гиперссылок в текст, размещенный в социальных сетях, мессенджерах, сайтах и на иных источниках. Причем такие гиперссылки могут не отличаться визуально от других слов в речевом продукте. Гиперссылки переводят пользователей, например, на поставщиков наркотических средств, на каталог наркотических средств и т.д.

Это очередной раз демонстрирует важность участия специалиста на протяжении всего процесса собирания цифровых следов.

Ранее нами были выделены основные виды цифровых следов, встречающихся в делах, связанных с незаконным оборотом наркотических средств.

Для обнаружения сообщений, имеющих значение для дела, в социальных сетях и мессенджерах, необходимо проверить имеющиеся чаты как личные, так и групповые. Важно принимать во внимание наличие такого раздела, как архив, в котором могут быть скрыты отдельные диалоги. Проблема, с которой можно столкнуться на этапе обнаружения цифровых следов в мессенджерах, уже была озвучена, и касается она секретных чатов в Телеграме. Телеграм является важнейшим источником информации по делам о незаконном обороте наркотических средств, однако предусмотренная опция секретного чата на практике приводит к тому, что следователи видят, что между лицами велась переписка, но ее содержимое отсутствует и восстановлению не подлежит. На данный момент времени нет никаких ресурсов, способных повлиять на изменение изложенных обстоятельств.

Доступ к любым социальным сетям и мессенджерам может быть обеспечен с любого устройства. В связи с этим и с целью допущения дистанционного удаления чатов и иной информации, в первую очередь (еще до начала поиска цифровых

следов), необходимо завершить сеансы на других устройствах. И уже после данного шага можно приступать к той части работы, о которой было сказано выше.

На основании анализа протоколов следственных действий, анализа судебной практики нами был выявлен следующий пробел в практической деятельности следователей: при осмотре материального носителя, в большей степени, мобильного телефона, следователи обращают внимание только на те социальные сети и мессенджеры, которые присутствуют в телефоне в качестве установленных приложений. Однако пользователь может не устанавливать приложения, как раз исходя из соображений обеспечения конфиденциальности, и в случае проведения, например, осмотра телефона, у лица появляется возможность с другого устройства лично или посредством иного лица уничтожить всю информацию.

Поэтому при собирании цифровых следов и играют большую роль оперативность и учет всей специфики конкретного вида цифровых следов.

Рекомендуется через поисковик браузера заходить в мессенджеры и социальные сети и проверять на наличие активного аккаунта, если приложения отсутствуют на материальном носителе. В ряде случаев проверка истории браузера может помочь выявить, какими социальными сетями и мессенджерами пользовался владелец устройства.

Опрос действующих следователей продемонстрировал, что, выполняя даже указанную последовательность, они сталкиваются с отсутствием у них паролей от аккаунтов. В такой ситуации существует два пути решения: самый простой выход, если владелец устройства самостоятельно предоставляет необходимые пароли, однако не всегда стороны готовы по тем или иным причинам содействовать следствию, и тогда нужно учитывать, что, в большинстве устройств (компьютеры, планшеты, телефоны) логин/пароль от различных аккаунтов сохраняется в самой системе.

Весь описанный алгоритм действий применим также к комментариям и публикациям в социальных сетях, Телеграм-каналах, онлайн-форумах.

Фото-, видео-, аудиоматериалы могут содержаться в медиатеке соответствующего устройства, в записях диктофона, в папке «скрытое», для входа

в которую нужен пароль от устройства, а также в корзине или папке «удаленное». Для обеспечения полного обнаружения цифровых следов следует проверять все возможные источники на устройстве.

В практике США известен случай, когда по опубликованной фотографии удалось найти поставщика наркотических средств. В рамках операции «Темное золото» сотрудники правоохранительных органов просматривали данные онлайн-магазинов Даркнета. На одном из таких сайтов были опубликованы фотографии, представляющие собой изображение марихуаны на ладони человека. В виду того, что фотографии были сделаны в высоком разрешении, четко просматривались папиллярные узоры пальцев рук. Данный фотоматериал был направлен на дактилоскопическую экспертизу, в результате которой было обнаружено, что в базе данных уже присутствуют исследуемые отпечатки, принадлежащие Хосе Роберту Поррасу. Таким образом, была выявлена личность преступника[80].

При проведении действий, направленных на обнаружение информации в сети Интернет не всегда достаточно визуального осмотра, например, страницы сайта, так как эта информация не отражает всех цифровых следов, оставленных пользователей. На это указывают также Е. Р. Россинская и Т. А. Сааков[81]. В своей работе они приводят следующий показательный пример из судебной практики:

«В Следственное управление по Северо-Западному административному округу г. Москвы от гражданина N поступило сообщение о совершении преступления, предусмотренного ст. 280 УК РФ. В рамках осмотра предметов (документов), в соответствии со ст. 177 УПК РФ, следователем осуществлялась проверка содержания контент-сайта «XXXXXXX» на предмет наличия (отсутствия) в нем призывов к осуществлению экстремистской деятельности, предусмотренных ст. 280 УК РФ. В ходе следственной проверки было обнаружено, что на осматриваемом контенте, помимо экстремистских материалов, также

[80] Отчет по результатам проведенной сотрудниками правоохранительных органов США операции «Темное золото» // URL: https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35 (дата обращения: 23.01.2024).

[81] Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. №3. С. 113.

размещена информация, способствующая незаконному сбыту наркотических средств, которая выражена в виде всплывающих окон. По факту обнаружения признаков составов преступлений, предусмотренных ст. 280 УК РФ, ст. 228.1 УК РФ, было возбуждено уголовное дело. Специалисту, участвующему в производстве следственного действия, удалось посредством анализа исходного кода страницы сайта определить путь к контенту сайта, из которого данная информация поступала для последующего размещения на проверяемом в ходе осмотра сайте. В дальнейшем следствию удалось доказать причастность к совершённому преступлению, предусмотренному ст. 280 УК РФ, гражданина А и причастность к совершённому преступлению, предусмотренному ст. 228.1 УК РФ, гражданина В, обладающего правами администратора сайта, который удалось обнаружить специалисту в ходе осмотра исходного кода страницы сайта»[82].

Представляется, что пример из судебной практики наглядно демонстрирует доказательственное значение цифровых следов в целом, а в частности, полученных из сети Интернет. И несмотря на то, что информация в сети Интернет по большей части является доступной, только для ее получения зачастую необходимо применение специальных знаний, а как следствие привлечение специалистов соответствующей области.

При этом к участию в собирании цифровых следов не может быть привлечено любое лицо, чьим основным видом деятельности является IT-сфера. Специалист должен полностью понимать специфику цифровых следов и механизма их следообразования.

Обнаружение цифровых следов в теневом сегменте Даркнет осложнено особым уровнем конфиденциальности, который обеспечивается браузером TOR. Однако говорить о том, что в настоящее время сделать это невозможно не представляется нецелесообразным, так как различные исследования показывают обратное.

---

[82] Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых… С. 113.

А. А. Фролов и Д. С. Сильнов провели эксперимент, в результате которого они смогли не только обнаружить контент, связанный с детской порнографией, но и собрать данные о пользователях, распространяющих такую информацию, и выявить способы распространения. Для достижения указанных результатов ими использовался программных комплекс, состоящий из программ Паук (модуль сканирования, сбора информации сайта, предобработки данных и загрузки данных в БД), Искатель (модуль обработки данных из БД с целью поиска ссылок на контент и паролей к ним) и Бухгалтер (модуль формирования отчетов по информации из БД)[83].

Хотя объектом исследования являлся контент, касающийся детской порнографии, на наш взгляд, представляется возможным и необходимым применение использованных авторами средств и методов для обнаружения информации наркотического содержания.

Ю. А. Бондаренко по итогу анализа работ как отечественных, так и зарубежных ученых выделил следующие пассивные и активные действия, направленные на деанонимизацию пользователей TOR:

«К пассивным действиям по деанонимизации пользователей относятся: − анализ трафика пользователя, основанные на установлении временной взаимосвязи между запросом на создание соединения и установкой выходного соединения (являются очень ресурсозатратными);

– другие основанные на анализе трафика и нагрузки узла внутри сети:

– Low-Cost Traffic Analysisof Tor2 − низкозатратный анализтрафика в сетиTor с помощью специализированных программных средств);

– Low-Resource Routing Acts Against Tor3 − маршрутизация информационных потоков и их отслеживание;

[83] Фролов А. А., Сильнов Д. С. Исследование механизмов распространения запрещенного содержимого в Darknet // Современные информационные технологии и ИТ-образование. 2017. №4. С. 216-224.

– Stealthy Traffic Analysisof Low-Latency Anonymous Communication Using Throughput Fingerprinting4 − скрытый анализ трафика на основе собирания информации о пропускной способности оборудования;

– Timing – анализ закономерностей работы узлов сети Tor, посредством выявления временных шаблонов в сетевом потоке с последующей их корреляцией с другими, для реализации требуется свой сервер в сети;

– Circuit fingerprinting – после установления связи пользователя со скрытой службой (посредством наблюдения проходящего трафика) используется Website fingerprinting, который основан на классификации собранных о трафике данных.

Активные действия:

− Комбинированные Timing-действия (например, с использованием iframe, который содержит код, встраивающийся в https-трафик и отправляющий сигнал отслеживающему серверу);

Tagging действия − дублирование случайного сообщения на входном узле, его поиск в поступивших на выходной узел данных»[84].

Зарубежная компания Recorded Future в 2024 г. провела исследование, по результатам которого оказалась возможной деанонимизация пользователей Tor путем использования данных из логов инфостилеров. Стиллер – это вредоносная программа, способная украсть данные одного пользователя компьютера и передать их другому пользователю. А логи по своей сути являются результатом работы стиллера, иначе говоря, совокупностью собранных данных. Проведя достаточно большую работу, исследователи получили информацию о лицах, скачивающих и распространяющих материалы с сексуальным насилием детей. В исследовании они приводят три примера идентификации конкретных лиц. Им удалось выявить их имена, адреса электронной почты, номера телефонов, аккаунты в социальных

[84] Бондаренко Ю. А., Кизилов Г. М. Проблемы выявления и использования следов преступлений, оставляемых в сети "Darknet" // Гуманитарные, социально-экономические и общественные науки. 2019. №5. С. 99.

сетях, истории просмотров браузера, а также адреса криптовалютных кошельков и историю транзакций[85].

Использование такого опыта в деятельности правоохранительных органов определенным образом скажется на повышении эффективности обнаружения цифровых следов в теневом сегменте Даркнет.

При расследовании дел, связанных с незаконным оборотом наркотических средств, как показывает практика, наибольшее внимание уделяется именно данным социальных сетей, мессенджеров и данных сайтов сети Интернет, Даркнета. При этом не менее криминалистически значимая информация может содержаться в приложениях.

В Приговоре № 1-188/2023 от 26 июля 2023 г. по делу № 1-188/2023 Шатурского городского суда Московской области приводятся обстоятельства, согласно которым гражданин А оборудовал тайники с закладками, используя мобильное приложение «Мэпс.ми». Впоследствии при осмотре его мобильного телефона были найдены «скриншоты из приложения «Мэпс.ми» с географическими координатами местности в количестве 60 штук». При проверке следственно-оперативной группой данных координат были обнаружены 53 тайниками с закладками[86].

Обнаружение данных банковских приложений может позволить отследить историю совершенных операций, и что не менее значимо получателя денежных средств. Конечно, наркопреступники нередко используют либо наличную оплату, либо прибегают к использованию криптовалюты. И все же нельзя исключать возможность отслеживаемой бесконтактной оплаты и не проверять данную информацию.

Шпаковский районный суд Ставропольского края в вынесенном им Приговоре № 1-187/2023 от 19 июля 2023 г. по делу № 1-187/2023 излагает

---

[85] Caught in the Net: Using Infostealer Logs to Unmask CSAM Consumers URL: https://go.recordedfuture.com/hubfs/reports/cta-2024-0702.pdf (дата обращения: 10.03.2024).

[86] Приговор № 1-188/2023 от 26 июля 2023 г. по делу № 1-188/2023 Шатурского городского суда Московской области // URL: https://sudact.ru/regular/doc/7CPamAaBkmmJ/ (дата обращения: 20.01.2024).

следующие обстоятельства дела: гражданин А, используя личный мобильный телефон, через сайт интернет-магазина оформил заказ «с целью личного потребления ?-пирролидиновалерофенон, который является производным наркотического средства N-метилэфедрона, в крупном размере». Оплату заказа стоимостью 2 636 рублей гражданин А провел бесконтактным способом[87].

Соответственно, приведенные примеры свидетельствуют о том, что данные приложений также могут содержать в себе криминалистически значимую информацию, которая при соблюдении всех процессуальных норм может стать в дальнейшем доказательством.

При первичном исследовании устройства таких приложений на рабочем столе может и не быть, однако это еще не означает, что они действительно не содержатся в системе устройства. Любое приложение можно удалить с рабочего стола, но не с самого устройства. Соответственно, для обнаружения приложений необходимо перейти в настройки для получения информации об имеющихся в устройстве приложениях и осуществить уже там их поиск.

Следующим из видов цифровых следов, который следует рассмотреть отдельно от остальных является облачное хранилище данных. Несмотря на то, что в делах о незаконном обороте наркотических средств в компьютерных сетях данный вид цифровых следов встречается не так часто (по результатам опроса из более, чем 100 следователей, лишь 6 человек сталкивались с облачным хранилищем данных), важность облачного сервиса нельзя преуменьшать.

Облачные серверы используются повсеместно и являются удобным способом хранения информации без привязки к какому-либо материальному носителю. Однако эти и иные особенности облачных хранилищ обеспечивают определенный уровень конфиденциальности при осуществлении преступной деятельности.

Перед загрузкой в облачный сервер данные могут быть зашифрованы, соответственно, даже если правоохранительные органы получат доступ к данным,

---

[87] Приговор № 1-187/2023 от 19 июля 2023 г. по делу № 1-187/2023 Шпаковского районного суда Ставропольского края // URL: https://sudact.ru/regular/doc/DSn8SXFf2qg9/ (дата обращения: 20.01.2024).

они не смогут их прочитать без ключа шифрования. После загрузки данных пользователи могут удалять локальные копии и очищать журналы активности, чтобы затруднить отслеживание своих действий.

Информация к тому же может быть разбита на несколько частей и загружена в разные облачные хранилища, что впоследствии усложняет ее объединение и анализ. Есть также возможность использования временных или одноразовых облачных серверов, которые автоматически удаляют данные через определенное время.

В совокупности все перечисленные обстоятельства препятствуют извлечению цифровых следов из облачных хранилищ. Но, как справедливо, отмечает В. Ю. Шефер, «в данный период времени для извлечения криминалистической значимой информации в «облачных» сервисах существуют специализированные программные комплексы, которые позволяют извлечь информацию без повреждения и внесения изменений в объект исследования. Безопасное извлечение данных из облачных хранилищ требует специальных знаний. Оно выполняется как процесс выполнения извлечения информации из компьютеров или мобильных устройств, так как данные хранятся на удаленных серверах, что сильно затрудняет исследование значимой информации»[88]. С этой задачей вполне успешно справляется программа «Мобильный криминалист».

А с применением специальных знаний в области IT-технологий можно обойти применяемые преступниками способы сокрытия информации и извлечь необходимые данные.

На основании всего вышесказанного можно представить обобщенный порядок действий, направленных на обнаружение цифровых следов при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях:

---

[88] Шефер В. Ю. Основные принципы исследования криминалистически значимой информации в «облачных» сервисах // Экспертные чтения на Енисее: Материалы региональной (межвузовской) научно-практической конференции. Вып. 2. Красноярск: Красноярский государственный аграрный университет. 2021. С. 145.

– установление IP-адреса;

– проверка содержимого мессенджеров;

– поиск информации и анализ активности в социальных сетях;

– проверка содержимого истории браузера;

– анализ открытых ссылок в сети Интернет;

– анализ имеющихся на устройстве приложений (в особенности приложений VPN и Tor);

– анализ активности и совершенных действий в данных приложениях;

– проверка на наличие/отсутствие аккаунтов в облачных серверах;

– анализ данных карты памяти устройства;

– проверка медиатеки устройства (фотогалерея, аудиофайлы, электронные документы и т.д.).

Однако для того, чтобы обнаруженные цифровые следы не теряли своей значимости, необходимо обеспечить сохранность имеющихся данных путем грамотного изъятия их носителей.

Носителями компьютерной информации могут выступать жесткие диски, флеш-накопители, CD-, DVD-диски, карты памяти и т.д. Однако в делах о незаконном обороте наркотических средств в компьютерных сетях наиболее часто фигурируют компьютеры, смартфоны и планшеты.

Изъятие компьютера является наиболее сложным по своему процессу. В каждом случае необходимо учитывать существующие особенности, например, включен или выключен ли был компьютер при его обнаружении, подключен ли компьютер к локальной сети, а также в рамках какого невербального следственного действия происходит изъятие носителя.

Важно отметить, что при выключении компьютера значимая информация может быть утеряна. Но в ситуации, когда на включенном компьютере запущена программа, форматирующая, удаляющая информацию, необходимо немедленно отключить питание компьютера, чтобы сохранить оставшиеся на компьютере данные.

Авторы монографии сформулировали общие тактические рекомендации в виде определенного порядка действий при изъятии компьютера:

– внешний осмотр компьютерной техники;

– проверка наличия активных сетевых подключений;

– осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов);

– снятие копии (дампа) содержимого оперативной памяти;

– выключение компьютера и создание копии жесткого диска;

– отсоединение кабелей и внешних устройств (в случае изъятия взаимосвязанных объектов необходимо промаркировать имеющиеся кабельные соединения);

– составление протокола и упаковка изъятого[89].

И все же для рассматриваемой категории дел более распространены в качестве носителя смартфон и планшет. Их изъятие естественным образом отличается от изъятия компьютера. Необходимо иметь в виду, что, если устройство находится во включенном состоянии, команды дистанционного уничтожения информации могут быть применены без ведома следователя. Некоторые устройства имеют автоматический таймер для включения телефона с целью обновления, что также может поставить под угрозу данные, поэтому оптимальным вариантом является извлечение аккумулятора.

Если устройство невозможно выключить, его необходимо изолировать от вышки сотовой связи, поместив в сумку Фарадея или другой блокирующий материал, перевести в режим полета или отключить Wi-Fi, Bluetooth или другую систему связи. Цифровые устройства следует помещать в антистатическую упаковку, например, в бумажные пакеты или конверты и картонные коробки. Следует избегать пластика, поскольку он может передавать статическое электричество или способствовать накоплению конденсата или влажности.

---

[89] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 94.

Одна из серьезнейших проблем на практике связана с халатностью самих следователей. В результате опроса следователей выяснилось, что в отдельных случаях сотрудники правоохранительных органов могут проводить формальный осмотр обнаруженного мобильного устройства, фиксируя телефон в отключенном состоянии с пометкой в протоколе «мобильное средство не включается». Конечно, такие случаи больше исключение из правил. Однако даже небольшой процент действий данного рода при производстве следственных действий негативно отражается не только на раскрываемости дела, но и в целом на состоянии преступности.

Правовая регламентация изъятия электронных носителей закреплена в статье 164.1 УПК РФ. Положения данной статьи вызывают споры в научных кругах.

Ряд ученых придерживаются точки зрения, что закрепленное в ч.2 ст. 164.1 УПК РФ обязательное участие специалиста при изъятии электронных носителей является обоснованным ввиду необходимости гарантировать истинность, целостность и неизменность информации, содержащейся на изымаемом электронном носителе, со стороны лица, обладающего специальными познаниями[90], а также в силу отсутствия технической грамотности сотрудников правоохранительных органов[91].

Сторонники другой позиции, считают, что участие специалиста при изъятии электронных носителей не должно носить обязательный характер[92]. Привлечение специалиста к изъятию электронных носителей должно быть правом, а не обязанностью следователя. М. О. Медведева в качестве подтверждения мысли приводит довод, что с учетом уровня развития информационных технологий «любой пользователь современных гаджетов может производить манипуляции с

---

[90] Григорьев В. Н., Максимов О. А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. Серия: Право. 2019. N 2. С. 41.

[91] Логвиненко Е. А. Электронные документы как доказательства в расследовании преступлений // Пробелы в российском законодательстве. 2014. N 2. С. 235.

[92] Гузин А. Р., Валиева Ю. М. Проблемы регламентации собирания электронной информации в действующем законодательстве // Juvenisscientia. 2017. № 1. С. 33-35.

ними»[93]. А. Ю. Черданцев видит выходом из данной ситуации повышение уровня технической подготовленности следователей к грамотному выполнению изъятия компьютерной информации[94].

Невозможно не согласиться с высказыванием С. Б. Россинского о том, что «участие специалиста в следственных действиях не является безусловным. Обладая необходимыми специальными знаниями и умея применять их на практике, следователь вполне может обойтись и без его помощи»[95].

В отдельных случаях следователь действительно может самостоятельно совершать действия по изъятию электронных носителей. Как показывает практика, необходимости изъятия самих электронных носителей у следователей чаще всего и не возникает. В особенности, когда расследуются дела незаконного оборота наркотических средств.

Совершенно справедливо в монографии авторы отмечают, что «при осмотре сайта в сети Интернет фиксация и последующее изъятие информации осуществляется не с электронно-вычислительных мощностей (серверов), при помощи которых поддерживается работоспособность определенного контент-сайта, а из информационно- телекоммуникационной сети Интернет, отображающей информацию, хранящуюся в памяти устройств хранения информации (жестких дисков серверов) электронно-вычислительных мощностей»[96].

---

[93] Медведева М. О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: Автореф. дис. ... канд. юрид. наук. М., 2018. С. 22.

[94] Черданцев А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. Т. 15. N 4. С. 55 - 60.

[95] Россинский С. Б. Следственные действия: монография. М.: Норма, 2018. С. 118.

[96] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 109.

По мнению Ю. В. Гаврилина и А. В. Победкина, приоритетным способом изъятия информации должно являться копирование (дублирование), а не изъятие носителя[97].

Как раз при изъятии компьютерной информации участие специалиста в обязательном порядке оправдано ввиду того, что работа с такой информацией невозможна без владения высоким уровнем специальных знаний в области IT-технологий. Уже было сказано, что исключительно повышение уровня компетенций следователей в области цифровых следов не обеспечит достижения эффективного и качественного результата.

Однако положения статьи 164.1 УПК РФ не предусматривают изъятия криминалистически значимой компьютерной или цифровой информации. Трактовать данную статью в широком смысле также не представляется возможным, так как никоим образом нельзя в понятие электронных носителей включить компьютерную или цифровую информацию. Представляется, что единственным решением образовавшегося пробела в законодательства будет изменение положений ст. 164.1 УПК РФ, дополнив ее таким образом: «При проведении следственный действий, в ходе которых осуществляется изъятие компьютерной и/или цифровой информации с удаленных серверов или электронных носителей информации участие специалиста обязательно»[98].

Копирование компьютерной информации направлено на обеспечение неизменности и сохранности цифровых следов. Сами цифровые следы по итогу могут быть представлены различными образами: переписка может быть представлена скриншотами или же распечаткой в бумажном варианте, данные о проведенных, данные о проведенных транзакциях – в виде электронного документа и др.

---

[97] Гаврилин Ю. В., Победкин А. В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 110.

[98] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 112.

Новацией в области представления цифровых следов является внедрение технологии блокчейн.

Блокчейн является распределенной и децентрализованной базой данных, сформированной участниками, в которой невозможно фальсифицировать данные из-за хронологической записи и публичного подтверждения всеми участниками сети транзакции. Основной и главной особенностью блокчейна является использование алгоритмов математического вычисления, и исключение «человека» и человеческого фактора при принятии решения системой[99].

Обычно о технологии блокчейн принято говорить в разрезе смарт-контрактов. Однако сущность и принципы работы данной технологии позволяют рассматривать ее возможности гораздо шире.

Мелани Свон выделяет три условные области применения данной технологии[100]:

1. blockchain 1.0 как валюта;
2. blockchain 2.0 как контракты;
3. blockchain 3.0 как приложения, сфера распространения которых не ограничивается финансовыми транзакциями, а затрагивает науку, образование, право и т.д.

В мировой судебной практике уже отмечены прецеденты использования блокчейн-технологий для обеспечения сохранности доказательств и последующего их представления в суде.

В Китае в 2018 г. рассматривалось дело Hangzhou Huatai Yimei Culture Media Co. Ltd. против Shenzhen Daotong Technology Development Co. Ltd. Ответчик нарушил авторские права истца при публикации статьи на одном из веб-сайтов сети Интернет. Истец сохранил соответствующие доказательства своей позиции на блокчейн-сервисе депонирования Baoquan.com. Суд рассмотрел действительность

---

[99] Колесов В. А. Использование технологии блокчейн в учебном процессе для защиты интеллектуальной собственности // В сборнике: дистанционные образовательные технологии Материалы II Всероссийской научно-практической интернетконференции. 2017. С. 343-347.

[100] Свон М. Блокчейн: Схема новой экономики. М.: Олимп-бизнес. 2017. С. 11.

доказательств, представленных истцом, проанализировав способ, которым Baoquan.com сохранил данные. Затем значение суммы хэш- файла пакета было рассчитано и сохранено в блокчейнах Factom и Bitcoin, в результате чего было установлено, что значения хэша, записанные в двух блокчейнах, и значение хэша, представленное истцом, были идентичны, а временные метки также были связаны со временем, когда было захвачено содержимое веб-страницы[101].

Как следствие, суд подтвердил, что блокчейн способен обеспечивать сохранность цифровой информации, а при рассмотрении вопроса о допустимости этих сведений в качестве доказательств следует учитывать источник данных, на надежность методов, используемых для их сбора и хранения, и на то, связаны ли такие доказательства с другими имеющимися доказательствами.

После данного дела Верховный народный суд Китая издал «Регламент по ряду вопросов при рассмотрении дел интернет-судами», в котором подтвердил юридическую силу депозитных сертификатов блокчейна и согласно которым, существуют три составляющих элемента доказательств хранилища блокчейна:

- во-первых, используемая технология ограничена блокчейном, который относится к технической системе. Данная система, которая совместно поддерживается несколькими сторонами, использует криптографию для обеспечения безопасности передачи данных и доступа сторон процесса, а также может обеспечить согласованное хранение данных, которые трудно подделать и трудно опровергнуть;
- во-вторых, хранилище и фиксированные объекты являются электронными доказательствами, то есть, это неприменимо к традиционным документальным доказательствам, вещественным доказательствам и т.д.;

[101] Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd. (2018) Zhe 0192 Civil Case, First Court No. 81, Hangzhou Internet Court of the People's Republic of China, 27 June 2018 China. URL: https://journals.sas.ac.uk/deeslr/article/view/5080/4973 (дата обращения: 21.07.2024).

– в-третьих, основной массив депозитарных доказательств представляет собой технологическую платформу блокчейн, которая может быть создана как самим судом, так и быть представлена сторонним предприятием[102].

Таким образом суд Китая заложил основы для внедрения блокчейн-технологий в сферу доказывания и доказательств.

В отечественной науке на настоящее время обсуждение такой инновации проходит недостаточно активно. Отдельные авторы говорят о возможностях использования технологии блокчейн в различных областях права[103]. Так, Б. А. Шахназаров отмечает высокий потенциал использования блокчейн-технологий в сфере интеллектуальной собственности[104].

Профессор Л. В. Бертовский видит следующим образом применение блокчейна в уголовном процессе: «к записям могут получить доступ только следователь, у которого есть один закрытый ключ, и руководитель, у которого есть другой. Затем к этой информации получат доступ только те, кому один из этих пользователей предоставит свой закрытый ключ. ...Но при этом у всех разный уровень доступа к данным файлам. Кто-то может лишь просматривать список документов в каждой папке. А кто-то (адресат конкретного документа) может знакомиться или скачивать данные себе. Причем никто другой не сможет получить доступ к файлу – только тот, кому он предназначался»[105].

На наш взгляд, блокчейн в действительности может обеспечить все основные потребности, возникшие в уголовном процессе и в судебной экспертизе. Проблема изменчивости цифровых следов может быть решена путем записи их в блокчейн-реестры, доступ к которым будет ограничен. Немаловажным представляется

---

[102] Русакова Е. П. К вопросу использования блокчейн-депозитария в формировании доказательственной базы в интернет-судах Китая / Е. П. Русакова, Т. А. Чернышева // Пробелы в российском законодательстве. 2022. Т. 15, № 6. С. 121.

[103] Михайлов С. В., Пономарева Н. В., Прудникова Л. Б. Блокчейн в современном правоприменении // Философия права. 2019. №1 (88). С. 60-64.

[104] Шахназаров Б. А. Комплексная взаимосвязь блокчейн-технологии и объектов интеллектуальной собственности в трансграничных частноправовых отношениях // Право. Журнал Высшей школы экономики. 2019. №S5. С. 121-147.

[105] Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. №6. С. 226-230.

упрощение их передачи экспертам при назначении судебной экспертизы. Исключается вероятность потери, порчи собранных доказательств.

Внедрение данной технологии требует помимо организационного, материального, методического регулирование, еще и правовой регламентации. При этом ввиду того технология блокчейн находится в стадии своего формирования и постоянно развивается, стандарты блокчейна должны быть достаточно гибкими, чтобы не ограничивать инновационную технологию[106].

Сохранность цифровых следов и их носителей, помимо сказанного, обеспечивается также благодаря фиксации совершенных действий, характеристик, свойств объектов в протоколе следственного действия.

Как отмечал Р. С. Белкин, «проблематика фиксации доказательственной информации — неотъемлемая часть комплекса проблем, связанного с изучением и использованием закономерностей собирания доказательств»[107].

Большая часть проанализированных нами протоколов характеризуется низким уровнем качества их заполнения, а также шаблонностью.

Среди основных ошибок, встречающихся в протоколах, связанных с фиксацией цифровых следов и их носителей, можно выделить следующие:

– отсутствие указания всех свойств (как внешних, так и внутренних) осматриваемого электронного носителя. так, отмечается, что не всегда в протоколах фиксируются все недостатки носителя, присутствовавшие при обнаружении;

– отсутствие описания порядка осуществленных действий при обнаружении и изъятии электронного носителя, а также способа упаковки носителя;

– отсутствие описания порядка осуществленных действий при обнаружении и изъятии цифровых следов;

---

[106] Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9.

[107] Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М.: Юрид. лит., 1987. С. 217.

– отсутствие информации об использованных технических средствах;

– отсутствие необходимой фотофиксации.

Природа данных ошибок сводится к непривлечению специалиста на одном из этапов собирания цифровых следов. При этом сама работа на этапах обнаружения и изъятия может быть проведена качественно и всесторонне, но без грамотной фиксации суду и иным участникам процесса невозможно оценить полученный результат, а в отдельных случаях признать доказательство достоверным и допустимым.

Например, в Приговоре № 1-120/2023 от 9 июня 2023 г. по делу № 1-120/2023 Ярославского районного суда отражено, что на определенном сайте интернет-магазина подсудимым были приобретены семена конопли, также изучены посредством использования сети Интернет способы, методы и основы выращивания конопли[108].

Данные факты, исходя из текста приговора, подтверждаются исключительно показаниями подсудимого. Однако из-за отсутствия привлечения специалиста, а также отсутствия всей информации в протоколе осмотра возникают вопросы: с какого носителя совершались указанные в приговоре действия подсудимым, точно ли именно подсудимый пользовался данными устройствами, заходил в сеть и совершал ряд операций?

Следователь в силу отсутствия специальных знаний зачастую не может определить, что и каким образом в протоколе нужно отобразить и как эти процессы следует описать. В связи с этим привлечение специалиста для четкого и полного отражения «в протоколе манипуляции, производимые как с осматриваемыми физическими объектами (средствами вычислительной техники, электронными носителями информации), так и непосредственно с объектами информационными»[109] представляется целесообразным.

---

[108] Приговор № 1-120/2023 от 9 июня 2023 г. по делу № 1-120/2023 Ярославского районного суда // URL: https://sudact.ru/regular/doc/fnQtVFPisVbb/ (дата обращения: 20.01.2024).

[109] Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex Russica. 2021. Т. 74. № 9. С. 107.

Посредством фиксации также дополнительно обеспечивается сохранность цифровых следов и их носителей, с помощью фиксации можно отследить, каким образом были обнаружены и изъяты цифровые следы.

При этом вариант составления четкого шаблона протокола следственных действий с закреплением той информации, которую необходимо внести по итогу собирания цифровых следов, не будет являться решением проблемы. Формальный подход к цифровым следам, как уже было продемонстрировано, не приводит к достижению поставленных целей.

Однако можно обобщить те сведения, которые должны быть отображены в протоколе следственных действий:

– сведения об использованных в ходе обнаружения, изъятии и фиксации технических средствах;

– сведения о внутренних свойствах изъятого устройства;

– сведения о внешнем состоянии изъятого устройства;

– сведения о сим-карте, если изъятым устройством является мобильный телефон/планшет;

– сведения о содержимом изъятого устройства;

– сведения о порядке совершенных действий, направленных на обнаружение цифровых следов;

– сведения о способе и порядке изъятия цифровых следов;

– приложение к самому протоколу в виде фотофиксации, скриншотов, выписок и др.

Повторимся, что в большинстве случаев привлечение специалиста для оказания помощи в составлении протокола в части фиксации результатов применения специальных знаний является абсолютно оправданным.

Собирание цифровых следов – сложный процесс, состоящий из сменяющих друг друга этапов, в каждом из которых присутствует своя специфика.

Ошибки, допущенные в ходе собирания цифровых следов, по цепочке оказывают влияние на последующие стадии расследования преступления.

Например, проведение недостаточного комплекса мер по обнаружению цифровых следов может послужить причиной формирования неполной доказательственной базы.

Ошибки, допущенные при изъятии и фиксации электронного носителя, компьютерной информации, становятся причиной утраты цифровых следов полностью или частично, а также создают условия, из-за которых впоследствии исследование в рамках назначенной судебной экспертизы не может быть проведено в полном объеме либо вообще проведение экспертизы не представляется возможным.

Во всех обозначенных и рассмотренных этапах собирания цифровых следов прослеживается необходимость участия специалиста, который бы смог обеспечить сохранность цифровых следов. Именно специалист владеет знаниями о том, какие методы, в каком порядке нужно применять в каждом конкретном случае, специалист знает, что необходимо фиксировать в протоколах следственных действий, какая информация является значимой.

В отдельных случаях такое участие должно быть обязательным (например, при изъятии компьютерной информации), в других — это должно оставаться правом решения следователя.

Если обращаться к опыту зарубежных стран, а именно США, то, как указывает Национальный институт юстиции, собиранием цифровых следов должны заниматься лица, обладающие специальными знаниями, иначе говоря, специалисты[110].

Специфика таких дел априори предполагает использование специальных знаний. После собирания цифровых следов (где существенную роль играет участие специалиста) специальные знания реализуются уже в ходе производства судебных

[110] National Institute of Justice. (2008, April). Electronic CSI, a Guide For First Responders, Electronic Crime Scene Investigation: A Guide for First Responders, Second edition // URL: https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders-second-edition (дата обращения: 20.01.2024).

экспертиз, назначение которых неизбежно при расследовании преступлений, совершенных с применением компьютерных технологий.

ГЛАВА 2. Производство судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях

§ 2.1 Особенности назначения судебных экспертиз при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях

Процесс расследования уголовных дел отличается тесной взаимосвязью проводимых следственных действий. Производству судебной экспертизы предшествует этап собирания объектов, в частности, цифровых следов. Эффективность и качество хода собирания цифровых следов оказывают непосредственное влияние на назначение судебной экспертизы. В свою же очередь, от корректности постановления (определения) о назначении судебной экспертизы во многом будет зависеть само судебно-экспертное исследование.

В науке вопросы выбора экспертного учреждения, постановки задач перед экспертами, определения объектов исследования, ошибки при назначении экспертизы и иные проблемы, возникающие на данном этапе, освещены подробно[111].

Однако имеющейся теоретической базы в настоящее время в аспекте исследуемой темы становится недостаточно. Неоднократно было сказано, что с появлением цифровых следов претерпели преобразование отдельные положения уголовно-правовых наук. Ранее было продемонстрировано, как цифровые следы повлияли на подход к криминалистической характеристике преступлений, на компетенцию следователей, а также на ход процесса собирания следов.

А по ряду причин наибольшему воздействию в рассматриваемом ключе подвержены именно судебные экспертизы. Во-первых, судебно-экспертная

---

[111] Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография / Е. Р. Россинская. — 4-е изд., перераб. и доп. - Москва: Норма: ИНФРА-М, 2024. 576 с.

деятельность является одной из самых динамичных и чувствительных к любым изменениям. Во-вторых, цифровые следы для судебной экспертизы – непосредственные объекты исследования, причем уже не только для судебной компьютерно-технической экспертизы, но и для других родов судебной экспертизы. Это также подчеркивает А. И. Семикаленова, говоря, что «цифровые следы являются объектами судебной компьютерно-технической экспертизы. Однако мы полагаем, что понятие цифровых следов невозможно замыкать только на данном виде экспертизы. К такому мнению нас подтолкнул анализ следственной, судебной и экспертной практики»[112].

Е. Р. Россинская также высказывается об этом следующим образом: «Вызванный цифровизацией процесс замены традиционных аналоговых способов отображения объектов судебных экспертиз (следов, фотоснимков, звукозаписей и пр.), представленными в цифровом виде — цифровыми следами, привел к тому, что цифровые следы стали в последние годы объектами исследования во многих родах (видах) судебных экспертиз, например: в фоноскопической, автороведческой, лингвистической, почерковедческой, фототехнической, видео-технической, портретной, судебно-бухгалтерской, финансово-экономической, судебно-технической экспертизе документов и других»[113].

Справедливо отмечает Н. С. Неретина: «Новые объекты со временем также могут попасть в область интереса правоприменителя, потребовав в интересах осуществления правосудия для разрешения вопросов, с ними связанных, специальных знаний. Появление новых объектов будет способствовать появлению новых родов и видов судебных экспертиз, поскольку подобные процессы могут нести с собой не только возможности улучшения и развития качества жизни, но и связанные с ними сложности, в том числе обеспечения прав человека и гражданина в цифровой среде, архивного хранения цифровых данных пользователей, защиты

---

[112] Семикаленова А. И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О. Е. Кутафина. 2019. №5 (57). С. 118.

[113] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 57.

передачи данных, юридической значимости электронных документов, а также угрозы личности, обществу и государству в связи с ростом компьютерной преступности, в том числе на международном уровне»[114].

Как следствие, появление цифровых следов приводит к возникновению ранее не существовавших экспертных задач, решение которых требует применения новых методов, приемов и средств исследования, а также создания новых экспертных методик. Е. Р. Россинская отмечает, что появление в качестве объектов исследования цифровых следов во многих родах (видах) судебных экспертиз оказывает существенное влияние на методики экспертного исследования и компетенцию судебных экспертов[115].

Важным компонентом обеспечения указанных трансформаций является расширение компетенций и навыков самого судебного эксперта, поскольку потеряется весь смысл, если мы сформируем все инструменты экспертного исследования, но не обучим пользованию ими.

Соответственно, судебные экспертизы во многом видоизменяются. Обобщая вышесказанное, можно выделить следующие аспекты, на которые оказало влияние появление цифровых следов в рамках судебной экспертизы:

- объекты экспертного исследования;
- задачи судебных экспертиз;
- методы, средства экспертного исследования;
- методики экспертного исследования;
- появление новых родов (видов) судебных экспертиз;
- компетенция судебных экспертов.

---

[114] Неретина Н. С. Генезис новых родов и видов судебных экспертиз в эпоху цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. №5 (57). URL: https://cyberleninka.ru/article/n/genezis-novyh-rodov-i-vidov-sudebnyh-ekspertiz-v-epohu-tsifrovizatsii (дата обращения: 20.03.2023).

[115] Россинская Е. Р. Цифровизация судебно-экспертной и криминалистической деятельности взаимосвязи и разграничения / Е. Р. Россинская // 2019. № S1. С. 571.

По принципу домино каждое из изменений влияет на все последующие составляющие части общего целого под названием «судебная экспертиза». Рассмотрим подробнее данную цепочку.

Перечень основных родов и видов судебных экспертиз закреплен в приказах МВД РФ[116], Следственного комитета РФ[117], ФСБ РФ[118] и Министерства юстиции РФ[119]. Ведомственные классификаторы в практической деятельности помогают с определением, какой род и вид назначаемой судебной экспертизы необходимо указывать в постановлении/определении о назначении судебной экспертизы. Однако наименования судебных экспертиз и сам их перечень различается в указанных приказах. Данная проблема не раз поднималась среди ученых. Так, Т.Ф. Моисеева подчеркивает, что «отсутствует единое наименование родов и видов экспертных исследований, что приводит к тому, что одни и те же исследования в системе экспертных учреждений МВД РФ и Минюста РФ обозначены по-разному (например, технико-криминалистическое исследование документов и судебно-техническое исследование документов). Очевидно, необходима унификация названий судебно-экспертных исследований на основе общепринятой научной классификации»[120].

---

[116] Приказ Министерства внутренних дел Российской Федерации от 29.06.2005 (в действующей редакции) № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

[117] Приказ Следственного комитета РФ от 24.07.2020 (в действующей редакции) № 77 «Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения Судебно-экспертный центр Следственного комитета РФ на право самостоятельного производства судебных экспертиз» // СПС «КонсультантПлюс».

[118] Приказ ФСБ России от 23.06.2011 (в действующей редакции) № 277 "Об организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности" (вместе с "Инструкцией по организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности") (Зарегистрировано в Минюсте России 06.09.2011 N 21744) // СПС «КонсультантПлюс».

[119] Приказ Министерства юстиции РФ от 20.04.2023 (в действующей редакции) № 72 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз // СПС «КонсультантПлюс».

[120] Моисеева Т. Ф. Классификации судебных экспертиз: необходимость унификации // Вестник экономической безопасности. 2016. №4. С. 69.

На это также указывают О. Г. Дьяконова и Е. В. Иванова, предлагая при этом принять на уровне постановления правительства Российской Федерации перечень, содержащий наименования наиболее часто выполняемых видов/родов судебных экспертиз, а ведомственные приказы привести в соответствие с данным списком[121].

Если обращаться к опыту зарубежных стран, в частности к практике Великобритании, следует отметить, что данный вопрос регулируется документом под названием «Кодекс практики», изданным Регулятором судебной экспертизы в 2023 г. В данном кодексе закреплен перечень судебных экспертиз. При этом действие Кодекса распространяется на территории Англии и Уэльса.

Таблица 1. Список судебных экспертиз по Кодексу практики Великобритании[122]

Number		Name	Code applies
		Incident examination	
INC	100	Incident scene examination	✓
INC	101	Collision investigation	×
INC	102	Examination of fire scenes	×
INC	103	Examination to establish the origin and cause of an explosion	×
INC	200	Forensic examination of detainees	×
INC	201	Forensic examination of deceased individuals	×
		Biology	
BIO	100	Forensic examination of sexual offence complainants	✓
BIO	200	Human biological material examination and analysis	✓
BIO	201	Non-human biological examination and analysis: vertebrates	✓
BIO	202	Non-human biological examination and analysis: plants, microbes and invertebrates	×
BIO	300	Human body fluid distribution analysis	✓
BIO	400	Human DNA analysis	✓
BIO	401	Human kinship analysis	✓
BIO	500	Taggant analysis	✓
		Drugs, toxicology and noxious materials	
DTN	100	Toxicology: analysis for drug(s), alcohol and/or noxious substances	✓
DTN	101	Toxicology: analysis for drugs and alcohol under the Road Traffic Act 1988, Transport and Works Act 1992, and Railways and Transport Safety Act 2003	✓
DTN	102	Toxicology: analysis for drugs in relation to s5A of the Road Traffic Act 1988	✓
DTN	103	Examination and analysis to identify and quantify controlled drugs and/or associated materials	✓
DTN	104	Toxicology: alcohol technical calculations	×
DTN	105	Examination and analysis relating to the preparation and production of drugs and/or psychoactive substances	×
DTN	200	Examination and analysis of corrosives and/or noxious substances	✓
DTN	300	Examination and analysis of residues of lubricants used in sexual offences, including oils, greases and lubricants	✓
DTN	400	Examination and analysis of ignitable liquids and their residues	✓
DTN	500	Examination and analysis of chemical and/or biological agents and associated materials	✓
DTN	501	Examination and analysis of explosives, explosives precursors and explosive residues	✓
DTN	502	Examination and analysis of radioactive material	×

[121] Дьяконова О.Г., Иванова Е.В. Классификация судебных экспертиз: экспертологический подход //Теория и практика судебной экспертизы. 2022. Том 17. №2. С.75-82.

[122] Forensic Science Regulator. Code practice. URL: https://assets.publishing.service.gov.uk/media/64da431cc8dee4000d7f1c1e/FINAL_2023.1.18_Code_of_Practice.pdf (дата обращения: 13.09.2024).

Таблица 1. Список судебных экспертиз по Кодексу практики Великобритании

DTN	503	Examination and analysis of suspected explosive devices and associated material	×
		Marks, traces and pattern	
MTP	100	Friction ridge detail: visualisation and enhancement	✓
MTP	101	Friction ridge detail: comparison	✓
MTP	200	Footwear: coding	✓
MTP	201	Footwear: screening	✓
MTP	202	Footwear mark comparisons	✓
MTP	300	Marks visualisation and enhancement	✓
MTP	301	Marks comparison	✓
MTP	400	Damage and physical fit	✓
MTP	500	Examination and analysis of particulate trace materials	✓
MTP	600	Examination and analysis of gunshot residue (GSR)	✓
MTP	601	Examination, analysis and classification of firearms, ammunition and associated materials	✓
MTP	602	Firearms: ballistics	✓
MTP	700	Document handwriting	✓
MTP	701	Document authenticity and origin	✓
		Digital	
DIG	100	Data capture, processing and analysis from digital storage devices	✓
DIG	101	Analysis of communications network data	×
DIG	102	Digital network capture and analysis	×
DIG	200	Cell site analysis for geolocation	✓
DIG	300	Recovery and processing of footage from closed-circuit television (CCTV) /video surveillance systems (VSS)	✓
DIG	301	Specialist video multimedia, recovery, processing and analysis	✓
DIG	400	Technical audio operations	✓
DIG	401	Speech and audio analysis	×
		Case and data management	
CDM	100	Case review	×
CDM	200	Control and management of a forensic database service	×

Как можно заметить, в их классификации есть отдельный род экспертиз «Цифровые». По факту эти экспертизы соответствуют нашим компьютерно-технической, видеотехнической и фоноскопической. Соответственно, в практике Великобритании несколько иное, более узкое понятие цифровых следов и экспертиз, чем в нашей отечественной теории и практике.

И все же отсутствие единообразия в наименованиях судебных экспертиз является лишь одной из проблемных сфер, связанной с ведомственными классификаторами. Другой аспект заключается в том, что данные приказы не могут быстро и гибко реагировать на происходящие изменения. Не все новые роды и виды экспертиз отражены в рассматриваемых классификаторах. В частности, в перечнях не предусмотрено экспертное исследование экономических показателей операций с цифровыми валютами и цифровыми финансовыми активами[123], которое

[123] Буйнов Д. О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности: диссертация ... кандидата юридических наук: 5.1.4. – Москва. 2023. С. 112.

имеет высокую значимость при расследовании дел, связанных с незаконным оборотом наркотических средств.

По этой причине нередко на практике следователи и судьи допускают ошибки при определении рода и вида назначаемой судебной экспертизы. Безусловно, следственные и судебные ошибки такого рода также связаны с недостаточной осведомленностью о возможностях судебных экспертиз.

Об этом свидетельствуют также результаты проведенного анкетирования среди сотрудников правоохранительных органов.

На вопрос «Какие судебные экспертизы, по Вашему мнению, можно назначать по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?» 44% опрошенных ответили «нет ответа», «затрудняюсь ответить» и «не знаю»; 45% назвали компьютерно-техническую экспертизу и лишь оставшиеся 11% перечислили иные роды экспертиз.

При этом интересен тот факт, что респондентами были допущены ошибки в наименовании компьютерно-технической экспертизы, например, *специально-техническая экспертиза, айти экспертиза, экспертиза достоверности коммуникаций и собственников устройств, экспертиза по телефонам, судебно-техническая экспертиза, экспертиза, изучающая цифровые следы.*

Если такие наименования будут фигурировать, собственно, в постановлении/определении о назначении судебной экспертизы, во-первых, встанет вопрос, как эксперту проводить исследования по несуществующей экспертизе. А во-вторых, неясно, какие задачи решают экспертизы с предложенными наименованиями. Например, экспертизой, изучающей цифровые следы, может быть любая, помимо компьютерно-технической экспертизы.

И такие ошибки допускаются несмотря на то, что в упомянутых выше приказах фигурирует только два варианта наименования данного рода экспертизы: компьютерная экспертиза и компьютерно-техническая экспертиза.

Такие показатели подчеркивают актуальность и значимость проблемы отсутствия единообразия классификации родов и видов экспертиз на уровне

ведомств, а также важность оперативного реагирования на появление новых родов и видов экспертиз.

А. А. Беляков и А. Д. Цветкова выделяют несколько причин следственных ошибок при назначении судебной экспертизы:

«1. При подготовке юристов даже уголовно-правовой специализации и следственного профиля для курсов судебной экспертизы выделяется незначительное количество учебных часов, нередко такие дисциплины и вовсе являются факультативными.

2. Перечни судебных экспертиз, которые могут проводиться в государственных учреждениях, установлены приказами различных ведомств и нередко противоречат друг другу как в части определения видов исследований в принципе, так и в части их наименований.

3. Помимо указанного, данные перечни носят назывной характер, что не позволяет неопытному следователю понять суть экспертизы, о которой упоминается в нормативном акте.

4. Постоянное появление новых объектов и направлений судебных исследований приводит к тому, что следователи, не успевая отслеживать все достижения науки, техники, ремесла, искусства, не знают о тех экспертизах, которые могут назначить, чтобы решать задачи раскрытия и расследования преступления.

5. В некоторых случаях может действовать когнитивное искажение – частное проявление некритичного подхода к оценке информации, согласно которому человек (в данном случае следователь) склонен без рациональных причин доверять тому, кто именуется экспертом»[124].

В продолжение предыдущих вопросов анкеты больше 79% опрошенных респондентов отметили, что назначали судебных экспертизы при расследовании дел, связанных с незаконным оборотом наркотических средств в информационно-

[124] Беляков А. А. Следственные ошибки при назначении судебных экспертиз / А. А. Беляков, А. Д. Цветкова // Академический юридический журнал. – 2024. – Т. 25, № 1(95). – С. 125-126.

телекоммуникационных сетях, где в качестве объектов экспертного исследования выступали цифровые следы.

Рисунок 4. Статистические данные по результатам ответа сотрудников правоохранительных органов на вопрос «Назначали ли Вы судебные экспертизы по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, где объектом выступали цифровые следы?»



Респонденты, положительно ответившие на данный вопрос, перечислили, какие же именно судебные экспертизы назначались ими. 92% опрошенных назначали компьютерно-техническую экспертизу.

Такой результат демонстрирует картину, при которой лица, назначающие экспертизу, не обладают достаточными знаниями о возможностях судебных экспертиз и решаемых ими задачах.

Если раньше, действительно, цифровые следы как объекты судебной экспертизы сводились к производству компьютерно-технической экспертизы, то сейчас данный перечень значительно расширен.

Если брать в качестве примера класс речеведческих экспертиз, то в рамках фоноскопической экспертизы цифровые следы и ранее становились объектами экспертного исследования, а в судебной автороведческой и лингвистической экспертизах цифровые следы, в частности, переписка в мессенджерах, именно в

настоящее время все чаще становится объектом исследования при расследовании незаконного оборота наркотических средств[125].

Ранее при раскрытии способов преступлений было упомянуто о появлении новых ролей среди участников преступления. Задачи, решаемые лингвистической экспертизой, позволяют выяснить интенцию авторов, тему речи, наличие в разговоре наркотического дискурса, а также позволяют определить принадлежность участникам определенной роли и внутреннюю иерархию.

Ввиду внедрения и активного использования криптовалют с целью совершения, сокрытия незаконного оборота наркотических средств трансформировался также класс экономических экспертиз. А. А. Савицкий, рассуждая о происходящих изменениям, говорит о необходимости выделения нового вида экспертизы в рамках судебной финансово-экономической экспертизы, а именно судебной экспертизы операций с цифровыми финансовыми активами (экономико-цифровая экспертиза)[126].

Перечень судебных экспертиз, где объектом исследования выступают цифровые следы, достаточно широкий. Однако по каждой категории расследуемых дел можно выделить те, которые чаще назначаются. Дела незаконного оборота наркотических средств характеризуются особой сложностью, чем и обуславливается необходимость комплексного подхода при расследовании данной категории преступлений. Не последнюю роль для решения данной задачи выполняют судебные экспертизы.

Оценить степень влияния цифровых следов на судебные экспертизы можно через почерковедческую экспертизу и экспертизу документов. Данные роды экспертиз являются уже традиционными и их можно было считать проработанными с точки зрения методологии до цифровых следов. Но появление

---

[125] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 231.

[126] Савицкий А. А. Актуальные вопросы становления и развития судебной экономико-цифровой экспертизы в условиях цифровизации социально-экономической сферы государства / А. А. Савицкий // Законы России: опыт, анализ, практика. 2021. № 3. С. 61.

новых объектов (например, подписи, выполняемые на экране мобильного устройства), как отмечают в своей работе Е. Р. Россинская и Н. Ф. Бодров, оказали «существенное влияние на методологию и методики экспертного исследования»[127]. Как следствие, расширился и перечень задач, которые могут решаться в рамках данных экспертиз.

Однако, как демонстрирует анализ следственной и судебной практики, необходимость в назначении почерковедческой экспертизы и экспертизы документов возникает крайне редко.

Без производства компьютерно-технической экспертизы чаще всего невозможно обойтись при расследовании незаконного оборота наркотических средств в информационно-телекоммуникационных сетях.

Опираясь на ранее раскрытые способы совершения и сокрытия незаконного оборота наркотических средств в информационно-телекоммуникационных сетях, можно проследить тенденцию повышения значимости лингвистической, автороведческой экспертиз, а также судебной экспертизы операций с цифровыми финансовыми активами.

Поэтому дальнейшее исследование трансформаций, происходящих в судебных экспертизах, а также особенностей назначения судебных экспертиз и оценки результатов заключений экспертов, будет проводиться на примере компьютерно-технической экспертизы, лингвистической и автороведческой экспертиз.

Естественным и логичным последствием происходящих преобразований в судебных экспертизах является и изменение компетенций судебного эксперта.

Ранее в исследовании затрагивался вопрос компетенции в сфере цифровых следов сотрудников правоохранительных органов, в частности, следователей. Данная тема еще больше актуальна именно для судебных экспертов.

---

[127] Россинская Е. Р. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе / Е. Р. Россинская, Н. Ф. Бодров // Криминалистика: вчера, сегодня, завтра. 2022. № 1(21). с. 125.

В. В. Зайцев фиксирует рост дефицита «специалистов и экспертов, обладающих достаточными компетенциями в области компьютерных технологий и цифровизации судебно-экспертной деятельности»[128].

Компетенцию эксперта принято рассматривать в двух аспектах: как круг полномочий, прав и обязанностей эксперта и как комплекс знаний в области теории, методики и практики судебной экспертизы определенного рода, вида[129].

При этом компетенция делится на объективную (объем знаний, которыми должен владеть эксперт) и субъективную компетенцию или компетентность эксперта (степень, в которой конкретный эксперт владеет этими знаниями)[130].

С. Б. Россинский подчеркивает, что «правоприменителю зачастую приходится в каждом конкретном случае устанавливать компетенцию экспертов по представленным им различным дипломам, аттестатам, свидетельствам и т.п. документам, притом, что многие субъекты правоприменения слабо разбираются в их содержании и значимости»[131].

Знание о цифровых следах и умение работы с ними необходимы теперь не только для экспертов в области компьютерно-технической экспертизы, но и для всех остальных. В связи с этим возникает вопрос разграничения компетенции таким образом, чтобы новые навыки экспертов не затрагивали деятельность экспертов компьютерно-технической экспертизы.

В научной литературе представлены следующие мнения на этот счет.

---

[128] Зайцев В. В. Цифровые технологии в криминалистике и судебной экспертизе / В. В. Зайцев // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2023. № 1(21). С. 12.

[129] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2024. С. 86.

[130] Россинская Е. Р., Галяшина Е. И., Зинин А. М. Теория судебной экспертизы: учебник / под ред. Е. Р. Россинской. М.: Норма; ИНФРА-М, 2016. С. 131.

[131] Россинский С. Б. О практике производства экспертиз в негосударственном судебно-экспертном учреждении / С. Б. Россинский // Эксперт-криминалист. 2010. № 4. С. 31.

А. А. Саркисян справедливо высказывается, что «в эпоху цифровизации эксперт должен обладать цифровой грамотностью, владеть навыками взаимодействия с электронными системами, базами данных»[132].

Т. А. Сааков отмечает, что «эксперт для производства того или иного рода (вида) экспертиз, где предоставленный для исследования объект зафиксирован на электронно-цифровом носителе информации, должен обладать соответствующими знаниями, которые позволили бы ему учесть специфику работы с цифровыми следами»[133].

Высказывания обоих авторов по своей сути намечают вектор развития компетенций судебного эксперта. При обсуждении компетенции экспертов в области цифровых следов необходимо учитывать аспект цифровой грамотности. Это подразумевает, что, помимо изучения судебной экспертологии и теории цифровизации судебно-экспертной деятельности, эксперт должен:

– владеть знаниями о характере и специфике тех цифровых следов, с которыми он взаимодействует в процессе производства определенного рода/вида экспертизы — в каком виде эти объекты должны быть ему представлены на исследование, какие методы допустимо применять при исследовании данных объектов;

– владеть знаниями о механизме следообразования цифровых следов;

– владеть навыками применения современных компьютерных технологий, IT-технологий для проведения исследования, а также уметь их интегрировать в экспертные методики;

– владеть навыками использования современных баз данных.

Т. А. Сааков уже в упомянутой работе выделяет специфику образовательной деятельности, реализуемой в Институте судебных экспертиз Университета имени О.Е. Кутафина (МГЮА) по двум специализациям: речеведческие и экономические

---

[132] Саркисян А. А. Профессия судебного эксперта в условиях цифровизации / А. А. Саркисян // Союз криминалистов и криминологов. 2020. № 1. С. 89.

[133] Сааков Т. А. Влияние процесса цифровизации на трансформацию компетенции судебного эксперта. Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. С. 123.

экспертизы. Особенность проявляется в том, что обе программы обучения включают в себя изучение цифровых следов в рамках дисциплины «Компьютерно-техническая экспертиза»[134].

Безусловно, такой подход обеспечивает достижение по окончанию обучения формирование необходимого уровня компетенций эксперта. Однако в рамках дисциплины «Компьютерно-техническая экспертиза» обучающиеся получают знания и навыки о работе с цифровыми следами в целом без учета особенностей относительно профильного рода/вида экспертизы.

Например, эксперт-речевед должен знать, каким образом должен быть зафиксирован и представлен в дальнейшем на исследование речевой продукт, содержащийся на сайте сети Интернет. Специфика данного объекта исследования будет иной для эксперта-экономиста. Такие характерные черты объектов можно изучить только в рамках профильных дисциплин.

По данной причине представляется, что программа дисциплин, направленных на изучение профильных родов/видов экспертиз, также должна включать в себя разделы, посвященные цифровым следам как объектам конкретного рода/вида экспертизы.

Придерживается такой точке зрения также ученый Ф. Г. Аминев. По его мнению, для экспертов «необходимо организовать полноценные курсы повышения квалификации по применению цифровых технологий в конкретном виде судебной экспертизы»[135].

Е. Р. Россинская посвятила одну из работ анализу изменениям компетенции эксперта в русле цифровизации судебно-экспертной деятельности. Профессор утверждает, что «теперь для эффективной работы с цифровыми следами эксперты также должны обладать глубокими знаниями в области IT-технологий», а «внедрение искусственного интеллекта и нейросетей в судебно-экспертную деятельность обусловливает необходимость появления новых компетенций в

---

[134] Сааков Т. А. Влияние процесса цифровизации... С. 126.

[135] Аминев Ф. Г. О проблемах формирования компетентности судебного эксперта в условиях цифровизации // Криминологический журнал. 2024. №1. С. 11.

судебной экспертологии», среди которых следует выделить: общие компетенции экспертов при исследовании цифровых следов и их носителей; аналитика экспертных данных, инженера экспертных данных, а также инженера машинного обучения[136].

Вопрос интеграции навыков в области цифровых следов в образовательные программы для экспертов поднимает ряд важных аспектов, касающихся их квалификации и компетенции. Следует подчеркнуть, что включение в образовательный процесс элементов, связанных с цифровыми следами, не подразумевает автоматического формирования у эксперта двойной компетенции. Это, скорее, расширение спектра необходимых навыков и умений, которыми должен обладать эксперт. Эксперт даже при таком образовании не может выполнять компьютерно-технические экспертизы, так как производство данного рода экспертизы основано на глубоких теоретических и практических знаниях в области информационных технологий, программирования, сетевой безопасности и других смежных дисциплин. Данный род экспертизы требует высокой степени специализации и опыта, что не может быть компенсировано лишь добавлением навыков работы с цифровыми следами.

О необходимости использования судебным экспертом возможностей как самостоятельного обучения, так и прохождения переподготовки в системе повышения квалификации в организациях, оказывающих качественные образовательные услуги пишет Н. С. Колесникова[137].

Таким образом, необходимо признать, что расширение образовательных программ за счет новых компетенций не приводит к замене одной формы экспертизы другой, а служит лишь дополнением к существующему набору профессиональных навыков.

---

[136] Россинская Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. 2024. Т. 19, № 3. С. 20-32.

[137] Колесникова Н. С. Заключение судебного эксперта в системе криминалистически значимой информации: автореф. дис. …. канд. юрид. наук. — Москва, 2021. С. 5.

О. А. Соколова указывает, что «в настоящее время при производстве определенного вида (рода) экспертизы наблюдается процесс экстраполяции методов других наук, например, технических, естественных, что позволяет утверждать об их интегративном характере. В условиях бурно развивающихся цифровых технологий объекты исследования конкретной экспертизы претерпевают значительные изменения, что, в свою очередь, приводит к усложнению экспертных технологий. На основании проведенного исследования можно сделать вывод о комплексном характере объектов исследования и об интегративности методов, применяемых при их исследовании, что актуализирует проблему компетентности (квалификации) судебного эксперта»[138].

Стоит отметить, что производство любого рода/вида экспертизы невозможно без использования методов самых различных научных областей. Так, Е. Р. Россинская в контексте этого вопроса указывает следующее: «Судебно-экспертное исследование по своей гносеологической сущности является разновидностью процесса познания объективной действительности, осуществляемого путем применения методов различных наук»[139].

В связи с этим необходимо оговориться, что интегративный характер был присущ судебным экспертизам изначально, это признак, отражающий специфику данной деятельности. В настоящее же время за счет появления новых технологий и развития науки в целом расширяется список научных методов, используемых в судебно-экспертной деятельности.

При этом невозможно не согласиться с точкой зрения относительности комплексности объектов исследования. Один и тот же объект в рамках расследования одного дела, безусловно, может быть исследован экспертами из разных областей. При таких обстоятельствах заходит речь о понятиях *комплекс экспертиз, комплексная экспертиза* и *комиссионная экспертиза*.

---

[138] Соколова О. А. Перспективы формирования компетенций судебного эксперта в условиях повсеместной цифровизации // Криминологический журнал. 2024. №1. С.140.

[139] Россинская Е. Р., Галяшина Е. И., Зинин А. М. Теория судебной экспертизы: учебник / под ред. Е. Р. Россинской. М.: Норма; ИНФРА-М, 2016. С. 98.

Вопрос комплексности экспертиз был достаточно подробно рассмотрен рядом ученых, среди которых Р. С. Белкин, Т. В. Аверьянова, Ю. Г. Корухов, Н. П. Майлис, Е. Р. Россинская, Ю. К. Орлов, Е. А. Сахаровой и многие другие.

Уже было сказано, что для расследования незаконного оборота наркотических средств в информационно-телекоммуникационных сетях чаще всего требуется производства не одной экспертизы, а целого комплекса.

В теории выработалось четкое разграничение между рассматриваемыми терминами, однако на практике все еще наблюдается отсутствие понимания их различий, что приводит к следственным ошибкам, которые будут далее в исследовании проанализированы.

В ст. 200 и ст. 201 УПК РФ закреплены положения о комиссионной и комплексной экспертизах. Согласно ст. 201 УПК РФ комплексной является та судебная экспертиза, в производстве которой участвуют эксперты разных специальностей. Исходя из толкования нормы, экспертиза может быть признана комплексной, если в ее производстве участвует не менее двух экспертов разных специальностей.

Но в указанной норме не подчеркивается основная сущность комплексной экспертизы, которая состоит в том, что для производства одной экспертизы необходимо одновременное применение специальных знаний из различных областей с целью решения общей задачи.

Е. Р. Россинская подчеркивает, что «отличительной особенностью комплексной экспертизы является невозможность решения вопроса без одновременного совместного участия экспертов различных родов судебных экспертиз в написании заключения и формулировании общего вывода»[140].

Из-за такой неточности в формулировке статьи кодекса у лиц, назначающих судебную экспертизу, происходит смешение *комплекса экспертиз* и *комплексной экспертизы.*

---

[140] Россинская Е. Р. Методологические и правовые проблемы комплексных судебных экспертиз в условиях реформирования законодательства о судебно-экспертной деятельности // Вестник Московского университета МВД России. 2014. № 6. С. 15.

Например, при обнаружении переписки в мессенджере у подозреваемого следователю для формирования доказательственной базы необходимо знать следующее:

1. Присутствуют ли в представленном речевом продукте высказывания наркотического дискурса?
2. Является ли гражданин А. автором высказываний в представленной на исследование переписке от имени Пользователь 1?

Разрешение первой задачи требует назначения лингвистической экспертизы, вторая же задача является предметом исследования автороведческой экспертизы. Вопросы, интересующие лицо, назначающее экспертизу, не объединены одной задачей и не требуют одновременного применения различных специальных знаний. Соответственно, в данном случае верным будет назначить данные экспертизы по отдельности, что в конечном счете образует комплекс экспертиз.

Однако анализ практики демонстрирует случаи назначения при таких вопросах комплексной судебной лингвистическо-автороведческой экспертизы. Потому что формально для решения этих вопросов требуется участие экспертов разных специальностей.

Естественно, на практике все усложняется еще тем обстоятельством, что одни и те же экспертизы в зависимости от каждого уголовного дела могут быть назначены как в качестве комплекса экспертиз, так и в качестве комплексной экспертизы. Поэтому упростить практическую деятельность лиц, назначающих экспертизу, оговорив заранее, какие экспертизы надо назначать в комплексе, а какие комплексными, не представляется возможным.

Неочевидным, например, является назначение комплексной компьютерно-технической и автороведческой экспертизы.

При исследовании обнаружено, что один из самых распространенных вопросов касается определения владельца IP-адреса сайта. Не все преступные действия совершаются в теневой сети Даркнет, фиксируются случаи, когда на сайтах Интернета маскируют информацию о наркотических средствах или гиперссылки, переводящие уже на Даркнет.

Определение владельца IP-адреса способно доказать причастность подозреваемого. Однако нельзя исключать тот факт, что владелец IP-адреса и лицо, осуществляющее деятельность на том же сайте, могут быть разными пользователями.

Для установления данных обстоятельств назначения только компьютерно-технической экспертизы может оказаться недостаточным, потому что важно также проанализировать речевую составляющую того же сайта для установления авторства.

Только при назначении такой комплексной экспертизы в ряде случаев исследование будет полным и объективным.

Тем не менее, для более удобного применения в практической деятельности теоретических знаний основные признаки и вместе с тем различия понятий *комплекс экспертиз, комплексная экспертиза* и *комиссионная экспертиза* можно представить в следующем виде:

Таблица 2. Разграничение понятий "комиссионная экспертиза", "комплексная экспертиза", "комплекс экспертиз"

	Комиссионная экспертиза	Комплексная экспертиза	Комплекс экспертиз
Участие двух и более экспертов одной специальности	+	-	
Участие двух и более экспертов разных специальностей	-	+	
Одновременное применение специальных знаний различных областей	-	+	
Совокупность судебных экспертиз, проведенных в рамках расследования и рассмотрения одного уголовного дела			+
Решение общих задач	+	+-	-
Производство экспертизы в отношение одного объекта или группы объектов	+	+	+-

Д. А. Кудряшов выделяет ряд ошибок, допускаемых следователями при назначении судебной экспертизы: во-первых, это ошибки при назначении комплексной экспертизы, связанные с отсутствием представления о возможностях судебно-экспертного учреждения, а во-вторых, ошибки, связанные с некорректной постановкой вопросов[141].

Стоит подчеркнуть, что названные ошибки зачастую связаны между собой и вытекают одна из другой.

Так, в одном из проанализированных нами постановлений о назначении судебной компьютерно-технической экспертизы следователь поставил перед экспертом следующие вопросы:

1. Имеется ли на представленном объекте – мобильном телефоне марки «Самсунг», изъятом в ходе личного досмотра Исомидиновой С. В. какие-либо сведения или информация (пользовательская, графическая, видео-информация, фото-информация, переписка в программах мессенджерах и программах-клиентах социальных сетей, файлы, в том числе удаленные, содержащие ключевые слова, касающиеся незаконного оборота наркотических средств и психотропных веществ)? Если имеется, то каково ее содержание, вид ее представления (явный, скрытый, удаленный, архивный)?

2. К какому формату относится указанная информация (текстовые документы, графические файлы, базы данных и т.д.)? Каковы дата и время ее создания и изменения? Если указанная информация имеется, прошу предоставить ее в удобном для просмотра виде.

В поставленных вопросах произошло смешение задач, относящихся к компетенции экспертов различных специальностей.

Эксперт в рамках проведения компьютерно-технической экспертизы в действительности может ответить на такие вопросы, как:

---

[141] Кудряшов Д. А. Актуальные проблемы назначения комплексных судебных экспертиз / Д. А. Кудряшов // Вопросы экспертной практики. 2019. № S1. с. 348.

– Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?

– Какого вида (явный, скрытый, удаленный, архив) информация имеется на носителе?

– К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и др.) и какими программными средствами они обеспечиваются?

Если представлять задачу в упрощенном виде, то она сводится к нахождению информации на носителе и определению ее вида, характеристик и параметров.

Но в рамках компьютерно-технической экспертизы эксперт не может точечно выявлять и вычленять информацию, относящуюся к наркотическому дискурсу, даже по ключевым словам. Это уже выходит за рамки его компетенций, и эти вопросы должны быть поставлены при назначении судебной лингвистической экспертизы.

Важно отметить, что лингвистическая экспертиза проводится в отношении конкретного речевого продукта, а так как в рассматриваемом варианте объекта как такового еще нет (для его выявления в том числе и проводится компьютерно-техническая экспертиза), то и нельзя говорить о назначении комплексной экспертизы.

Корректным было бы назначить в первую очередь судебную компьютерно-техническую экспертизу, а затем уже судебную лингвистическую экспертизу.

Особый интерес представляет также второй вопрос из анализируемого постановления, а именно часть «Если указанная информация имеется, прошу предоставить ее в удобном для просмотра виде».

Вопрос, выносимый на разрешение эксперта, не может быть выражен в форме просьбы, приказа, рекомендации и т.д. Это всегда вопросительное высказывание.

То, как эксперт представит в конечном счете результаты проведенного исследования, не может диктовать следователь и любые иные лица. Эксперт выполняет исследование и оформляет в дальнейшем его результаты, руководствуясь методическими данными, научными рекомендациями, личным профессиональным опытом.

К сожалению, такие ошибки не являются единичными, как показало исследование.

Вот еще один из примеров некорректных вопросов из постановления о назначении судебной компьютерно-технической экспертизы: «Извлечь из представленного объекта – мобильного телефона марки «Самсунг», изъятого в ходе личного досмотра всю имеющуюся информацию».

Только сам эксперт на основании поставленных перед ним вопросов может определить те задачи, которые ему надо решить в каждом конкретном исследовании.

Существуют отдельные монографии, учебники, справочники (например, Справочник по подготовке, организации, назначению и производству судебных экспертиз в судебно-экспертных учреждениях Минюста России 2024 г.), в которых отражены типовые вопросы различных родов судебных экспертиз. Среди таковых следует отметить монографию, имеющую на данный момент 4 издания, Е. Р. Россинской «Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе». При назначении судебной экспертизы и постановке вопросов правоприменитель может руководствоваться изложенными в монографии данными, что значительно снижает возможность допущения ошибки.

Однако вопросы, выносимые на разрешение эксперта, разнятся в зависимости от категории уголовного дела. В связи с этим предлагается представить типовые вопросы, необходимость разрешения которых наиболее высока при расследовании незаконного оборота наркотических средств:

Судебная компьютерно-техническая экспертиза[142]*:*

– Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?

– Какого вида (явный, скрытый, удаленный, архив) информация имеется на носителе?

– К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа и др.) и какими программными средствами они обеспечиваются?

– Имеются ли признаки работы данного компьютерного средства в сети Интернет?

– Каково содержание установок программы удаленного доступа к сети и протоколов соединений?

– Какие имеются адреса Интернета, по которым осуществлялся доступ с данного компьютерного средства?

Судебная лингвистическая экспертиза:

– Имеется ли в представленном на исследование речевом продукте информация о предложении приобретения наркотических средств?

– Имеются ли в представленном речевом продукте высказывания, относящиеся к наркотическому дискурсу?

– Имеется ли в речевом продукте информация о приобретении, хранении, перевозке и сбыте наркотических средств?

– Имеется ли в речевом продукте информация о роли каждого из участников (ФИО1, ФИО2 и т.д.)? Если да, то каковы их коммуникативные роли?

– Имеется ли в речевом продукте информация о том, что участники (ФИО1, ФИО2 и т.д.) совместно осуществляют преступную деятельность?

Судебная автороведческая экспертиза (при наличии необходимых образцов для исследования):

---

[142] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном… С. 222-224.

– Является ли автором речевого продукта, содержащегося на сайте (данные сайта), ФИО?

– Является ли ФИО автором сообщений, направленных в переписке с ФИО от имени «Пользователь 1» в мессенджере/социальной сети/Интернет-форуме?

В результате проведенного анализа постановлений о назначении судебной экспертизы были также выделены ключевые аспекты, связанные с допущением ошибок в части описания цифровых следов и их материальных носителей.

Во-первых, при описании материального носителя правоприменитель порой ограничивается лишь наименованием (персональный компьютер Asus, мобильный телефон Xiaomi и т.д.). Такое описание не позволяет идентифицировать объект и отличить его от других. Этот аспект имеет особую важность для цифровых следов, потому что они не отделимы от материальных носителей.

Следовательно, при описании материального носителя необходимо указывать идентификационные признаки объекта, причем как внешние, так и внутренние (которые следователь или привлеченный к участию специалист могут установить на этапе изъятия).

Во-вторых, при изложении обстоятельств дела, указываются те факты, которые не имеют значения для производства экспертизы (например, при описании найденных наркотических средств приводят положения Постановления Правительства РФ от 30 июня 1998 № 681). И при этом не описывают то, каким образом были изъяты цифровые следы.

Эксперту для производства экспертизы не направляют полностью все материалы уголовного дела. Он получает объекты исследования, постановление (определение) о назначении судебной экспертизы, а также в отдельных случаях дополнительную документацию, относящуюся к предмету экспертного исследования.

Целесообразно утверждать, что часть необходимой информации для эксперта относительно объекта исследования содержится именно в постановлении (определении) о назначении экспертизы.

По факту лица, назначающие экспертизу, должны обеспечивать и гарантировать достоверность и допустимость направляемого на экспертизу объекта. Эксперт, в свою очередь, на подготовительной стадии экспертного исследования должен оценивать объект на пригодность. Но, на практике, к сожалению, не всегда этот процесс выглядит таким образом.

Абсолютно точно было подмечено А. Ю. Шапошниковым, что «если из системы убрать элементы, обеспечивающие подлинность объектов судебной экспертного исследования, то это создает безграничные возможности для фальсификации доказательств и ставит под сомнение достоверность результатов экспертного исследования»[143].

Когда мы говорим о таком сложном объекте, как цифровые следы, пригодность определяется в том числе через анализ соблюдения всех условий их получения и изъятия. Уже было сказано, что цифровые следы значительно подвержены изменениям.

Если эксперт не обладает знаниями о том, каким образом изымался объект, то в ряде случаев он не может быть уверенным в том, что от момента изъятия до получения им объекта информация осталась прежней.

Урегулировать данный пробел описанием именно самого цифрового следа, а не материального носителя тоже не всегда удается. Если при назначении судебной лингвистической экспертизы или судебной автороведческой экспертизы следователь/суд могут четко обозначить границы объекта исследования, то для судебной компьютерно-технической экспертизы или судебной экономической экспертизы это не представляется возможным. Лицо, назначающее судебную экспертизу, не может зафиксировать, например, данные из системы 1С.

---

[143] Шапошников А. Ю. Проблема обеспечения подлинности объектов, направляемых для экспертного исследования: системный подход // Юридический вестник Самарского университета. 2015. №4. С. 96.

Вследствие этого представляется целесообразным предоставлять эксперту информацию об условиях изъятия цифровых следов либо путем внесения ее в постановление (определение) о назначении судебной экспертизы, либо путем направления эксперту также протокола осмотра доказательств.

Протокол будет напрямую относиться к предмету исследования, а значит, это не нарушает положения процессуального законодательства ст. 17 ФЗ ГСЭД о праве эксперта знакомиться с материалами дела в рамках предмета проводимой экспертизы[144].

Существуют и другие процессуальные ошибки, допускаемые при назначении судебной экспертизы. Однако выделенные в работе ошибки являются самыми частыми и при этом значимыми при расследовании незаконного оборота наркотических средств.

Выделение ошибок из практики — это лишь один аспект, направленный на повышение качества осуществляемой следственной и экспертной деятельности. Не менее значимым является обозначение способов предотвращения ошибок.

Прежде всего, правоприменитель и эксперт должны постоянно повышать свою квалификацию, чтобы успевать за изменениями, происходящими как в науке, так и в практике. Причем в данном контексте важно подчеркнуть значимость междисциплинарности уголовно-правовых наук и комплексности их изучения в той степени, которая необходима каждому для своей профессиональной деятельности и улучшения навыков.

На основе проведенного исследования стоит выделить следующие особенности назначения судебной экспертизы при расследовании преступлений, связанных с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях:

---

[144] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 13.

1. Необходимо подробно описывать вид материального носителя и информацию, которая содержится на нем. Это необходимо для обеспечения достоверности объекта и последующего анализа данных.

2. Необходимо предоставлять эксперту информацию об изъятии цифровых следов. Это позволяет эксперту оценить целостность и сохранность цифровых следов, а также выявить возможные факторы, которые могли повлиять на их состояние. Таким образом, предоставление полной информации об изъятии способствует более точному и обоснованному заключению эксперта.

3. Необходимо при предоставлении объектов эксперту учитывать род назначаемой экспертизы. Разные роды экспертиз требуют различного подхода к подготовке объектов, что связано с особенностями методик анализа и необходимыми условиями работы экспертов. Так, для производства судебной лингвистической экспертизы речевой продукт из сайта оптимальнее всего предоставлять в виде скриншота, но для производства судебной компьютерно-технической экспертизы такой формат представления цифровых следов уже не подойдет (необходимо предоставлять непосредственный доступ к сайту).

4. Следует определять необходимость назначения комплексной экспертизы, комиссионной экспертизы или комплекса экспертиз.

5. При назначении комплекса экспертиз важно определять очередность производства назначаемых судебных экспертиз.

Учет правоприменителем особенностей назначения судебной экспертизы в конкретной категории дел позволяет устранять ошибки.

И наконец, действенным и простым решением в вопросе исключения ошибок при назначении экспертизы выступает привлечение специалиста. Ч.1 ст. 58 УПК РФ предусматривает привлечение специалиста в том числе для постановки вопросов эксперту. Однако правоприменитель не всегда пользуется такой возможностью, закрепленной в законе, так как убежден в том, что самостоятельно может выполнить данные задачи.

В этой связи интересно высказывание Ю. К. Орлова о том, что «все действия, которые может выполнить специалист, в принципе может выполнить следователь

(дознаватель), если он обладает соответствующими знаниями и навыками (за исключением, разумеется, случаев, когда участие специалиста обязательно по закону)» [145].

Производство судебной экспертизы, начиная буквально от ее назначения, является настолько специфическим процессом, что порой сложно объективно оценить достаточность своих знаний в этой сфере.

Участие специалиста не должно быть обязательным при назначении экспертизы, не всегда оно оправданно. У следователя существуют и другие инструменты, с помощью которых он может без ошибок назначить судебную экспертизу. Но когда возникают те или иные сомнения, присутствует потребность в специальных знаниях, не следует пренебрегать привлечением специалиста для консультации.

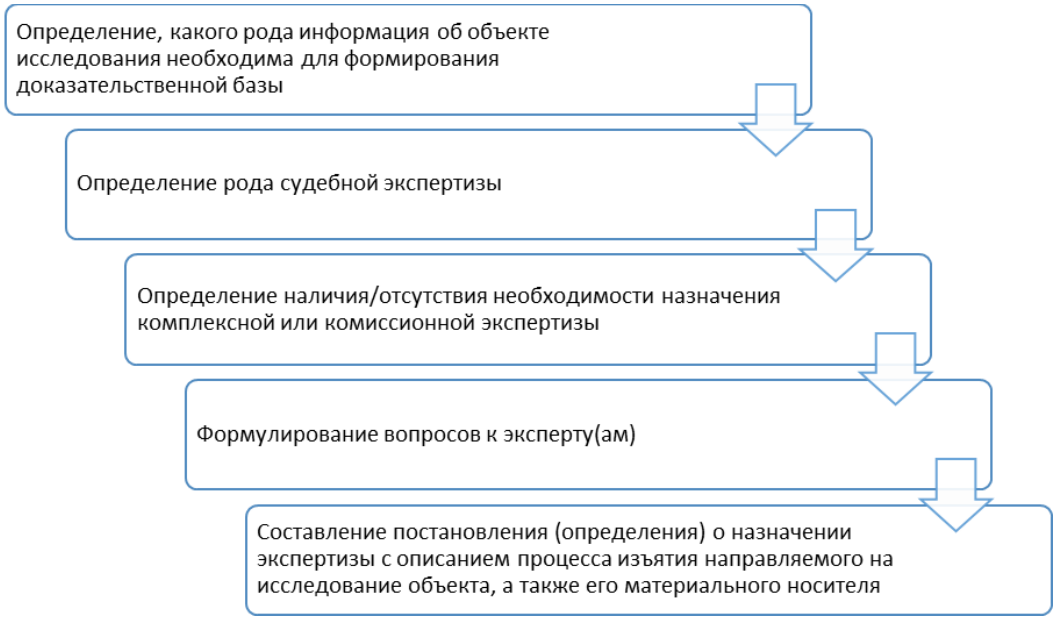
Конечно, так как каждое уголовное дело является уникальным, то не представляется возможным и целесообразным составить определенный шаблон постановления (определения) о назначении экспертизы, который бы мог применяться лицом, назначающим экспертизу.

При этом можно выделить ряд последовательных действий, которые бы охватывали и учитывали все нюансы и особенности данной стадии судебной экспертизы в рамках расследования незаконного оборота наркотических средств в компьютерных сетях:

---

[145] Орлов Ю. К. Современные проблемы доказывания и использования специальных знаний в уголовном судопроизводстве: научно-учебное пособие. – М.: Проспект, 2017. С. 110.

Схема 1. Последовательность действий при назначении судебной экспертизы



Одна допущенная ошибка не только приводит к последующим, но и в целом усложняет весь процесс расследования и рассмотрения дела.

Назначение судебной экспертизы, во-первых, напрямую относится к необходимым умениям и навыкам следователя-криминалиста[146], а во-вторых, влияет на экспертное исследование и в дальнейшем на качество заключения эксперта.

§ 2.2 Судебно-экспертные технологии производства экспертиз по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях

Производство судебно-экспертного исследования представляет собой сложный, многогранный процесс, требующий определенного уровня регламентации как теоретической, так и организационной.

Обеспечению в реализации указанных аспектов способствуют именно судебно-экспертные технологии. Данное понятие не является новым для судебной

[146] Приказ Министерства труда и социальной защиты Российской Федерации от 23 марта 2015 г. № 183н «Об утверждении профессионального стандарта «следователь-криминалист». // СПС «КонсультантПлюс».

экспертологии. Еще в 1983 г. М. Я. Сегай рассмотрел вопрос необходимости включения в экспертную деятельность судебно-экспертных технологий, под которыми предлагал понимать «целостную систему рациональной организации экспертного производства»[147]. При этом ученый-криминалист выделял общую экспертную технологию (технология экспертного производства в целом) и частную экспертную технологию (технология производства определенного вида судебной экспертизы и конкретного экспертного производства)[148].

Определение, сформулированное ученым в 1983 г., было несколько широким и не отражало глубинную суть. И уже через год в совместной работе с В. К. Стринжа авторы представляют следующее понятие судебно-экспертных технологий: «Совокупность правил, приемов и рекомендаций по обеспечению эффективного производства судебных экспертиз в судебно-экспертных учреждениях любого профиля и ранга»[149].

Понятия, представленные в последующем другими учеными, никак не противоречат и не противопоставляются определению М. Я. Сегая и В. К. Стринжа, а лишь дополняют и более подробно раскрывают его.

Р. С. Белкин также включил понятие судебно-экспертной технологии в изданную им «Криминалистическую энциклопедию»: «... совокупность правил, приемов и способов наиболее рациональной и эффективной организации производства экспертиз в судебно-экспертных учреждениях»[150].

Н. А. Замараева понимает под экспертной технологией «систему правил, приемов и способов наиболее рациональной и эффективной организации и осуществления деятельности эксперта по исследованию объектов судебной экспертизы на основе соответствующей им материально-технической базы при

---

[147] Сегай М. Я. Судебная экспертиза в условиях НТР: особенности и пути оптимизации // Современные проблемы судебной экспертизы и пути повышения эффективности деятельности СЭУ в борьбе с преступностью. Киев, 1983. С. 41-43.

[148] Сегай М. Я. Судебная экспертиза в условиях… С.41-43.

[149] Сегай М. Я., Стринжа В. К. Актуальные проблемы экспертной технологии в условиях НТР // Криминалистика и судебная экспертиза. Киев, 1984. Вып. 29. С. 7.

[150] Белкин Р. С. Криминалистическая энциклопедия. - М., 1997. С. 266.

соблюдении процессуальных и иных норм, регулирующих проведение экспертизы в судебно-экспертных учреждениях и в негосударственных организациях»[151].

А. М. Зинин и Н. П. Майлис представляют следующее определение судебно-экспертных технологий: «...совокупность осуществляемых в определенной последовательности операций, действий, выполняемых на основе специальных познаний, в связи с проведением исследования каких-либо объектов, являющихся вещественными доказательствами, в целях поиска ответов на поставленные перед экспертом вопросы»[152].

Если разбирать указанные выше определения на составляющие части, то становится очевидно, что судебно-экспертные технологии включают в себя самостоятельные разделы, тесно связанные между собой.

Е. Р. Россинская выделяет четыре элемента структуры судебно-экспертных технологий:

– методология судебно-экспертной деятельности;

– процесс экспертного исследования и его стадии;

– судебно-экспертные методики, их типизация, стандартизация и паспортизация, валидация экспертных методик;

– профилактическая деятельность эксперта, экспертные ошибки и их профилактика[153].

Без представления, анализа и четкой регламентации каждой структурной составляющей невозможно осуществление судебно-экспертной деятельности.

Для того, чтобы качественно провести экспертное исследование, прежде всего, нужно ответить на два вопроса: «С помощью чего?» и «Как?».

---

[151] Замараева Н. А. Правовые и организационно-методические проблемы использования компьютерных технологий при производстве судебных экспертиз: дис. ... канд. юрид. наук. М., 2001. С. 22.

[152] Зинин А. М., Майлис Н. П. Судебная экспертиза. М., Право и закон; Юрайт-Издат, 2002. С. 126.

[153] Россинская Е. Р., Галяшина Е. И., Зинин А. М. Теория судебной экспертизы: учебник / под ред. Е. Р. Россинской. М.: Норма; ИНФРА-М, 2016. С. 49.

На первый вопрос дает ответ методология судебно-экспертной деятельности, определяя те методы, которые должны и могут использоваться в том или ином роде/виде экспертизы. Методология также не стоит на месте и продолжает развиваться. Приемы, средства и методы, применяемые в экспертной деятельности, видоизменяются: одни теряют свою актуальность, а другие внедряются.

А как раз для ответа на вопрос *Как?* стоит обратиться к понятию процесса экспертного исследования и его стадий, так как при проведении такого рода исследований крайне важно соблюдать определенную логическую последовательность действий, где одно вытекает из другого.

Но для полного понимания, как проводить экспертизы, также необходимы принятие судебно-экспертных методик и следование им.

Как указывает А. А. Корчагин: «Повышение эффективности судебно-экспертной деятельности напрямую зависит от научно-методического обеспечения, так как любая экспертиза представляет собой исследование научного характера. С учетом реалий, необходимо развивать судебно-экспертные технологии»[154].

При этом существует проблема, связанная с тем, что мир достаточно быстро меняется, оказывая влияние в том числе и на судебно-экспертную деятельность, а методическое обеспечение не всегда поспевает за возникающими тенденциями.

С одной стороны, это абсолютно объяснимо: например, у нас появляется такой новый объект, как цифровые следы. В научном сообществе замечают данное явление, вследствие чего возникают различные дискуссии. Но несмотря на быстрое реагирование науки, нужно немало времени для того, чтобы прийти к какому-либо мнению и сформировать устойчивую теоретическую базу, которая будет в дальнейшем использоваться на практике.

---

[154] Корчагин А. А., Сат А. Х. Судебно-экспертные технологии: история и современность // Проблемы науки. 2016. №11 (12). С. 39.

Отсутствие единообразной позиции в обозначенных вопросах может привести к применению разных подходов при производстве судебных экспертиз, что является причиной экспертных ошибок.

Хорошим регулятором в этом смысле являются судебно-экспертные методики, стандартизирующие исследования судебных экспертиз. Однако их принятие или даже внесение в них каких-либо нововведений порой обременяется достаточно сложным процессом согласования. В результате этого многие экспертные методики уже устарели и не полностью отвечают требованиям экспертной деятельности.

О важности создания судебно-экспертных методик на основе современных технологий с учетом требований и накопленных знаний всех судебно-экспертных наук, прикладных научно-технических и гуманитарных отраслей говорят многие ученые, в том числе В. Я. Колдин, О. А. Крестовников[155].

Другая сложность обусловлена отсутствием доступности существующих судебно-экспертных методик для общего пользования всем экспертным сообществом.

Стандартизация методик, о которой нередко говорят, предполагает по итогу следование общему для всех алгоритму исследования в рамках того или иного рода/вида экспертизы.

На уровне государственных экспертных учреждений принимаются методики, которым следуют все сотрудники соответствующего ведомства, но которые не предоставляются для рассмотрения другими экспертами.

Из этого вытекает вопрос: «На основании какого методического обеспечения должны проводить исследования эксперты негосударственных экспертных учреждений»?

---

[155] Колдин В. Я., Крестовников О. А. Судебно-экспертные науки и технологии. Теория и практика судебной экспертизы. №1 2006. С. 71.

Согласно ч. 2 ст. 195 УПК РФ, судебную экспертизу могут проводить государственные судебные эксперты и иные эксперты из числа лиц, обладающих специальными знаниями.

Постановление Пленума Верховного Суда Российской Федерации от 21.12.2010 г. № 28 разъясняет, что под иными экспертами следует понимать экспертов негосударственных судебно-экспертных учреждений, а также лиц, не работающие в судебно-экспертных учреждениях[156].

Следовательно, негосударственные судебные эксперты, обладают ровно таким же перечнем прав и обязанностей, как и государственные. Они все в совокупности равно составляют экспертное сообщество. Однако в ситуации невозможности использования утвержденных на уровне ведомств экспертных методик страдает качество заключений негосударственных экспертов.

Представляется, что единственно верное решение кроется в налаживании взаимодействия и выстраивании системы обмена опытом между государственными и негосударственными экспертами. Обобщение и анализ реализации на практике указанных теоретических положений в конечном счете приводит к выявлению пробелов в экспертной деятельности и что не менее значимо – экспертных ошибок.

Профилактическая деятельность эксперта способствует не только снижению количества экспертных ошибок, но и определению вектора развития экспертной деятельности.

Так, в монографии коллектива авторов под редакцией Е. Р. Россинской «Судебная экспертиза: типичные ошибки» ведущие эксперты различных специальностей в ходе анализа основных ошибок по каждому роду экспертиз параллельно выделяют некоторые недостатки в методологии экспертной деятельности, в необходимости обновления методик и т.д.[157]

---

[156] Постановление Пленума Верховного Суда РФ от 21.12.2010 N 28 (ред. от 29.06.2021) "О судебной экспертизе по уголовным делам" // СПС «КонсультантПлюс».

[157] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. 736 с.

Чтобы вывести экспертную деятельность на новый уровень важно развивать судебно-экспертные технологии в целом. Но, как отмечает В. Я. Колдин, экспертные технологии будут совершенствоваться только при условии системно-структурного, информационного и функционального анализа структуры и инфраструктуры экспертной деятельности[158]. Поэтому здесь можно говорить о взаимном влиянии экспертных технологий и экспертной деятельности друг на друга.

Проследить высокую потребность совершенствования судебно-экспертных технологий можно как раз на примере отдельных судебных экспертиз, назначаемых в рамках расследования дел незаконного оборота наркотических средств.

Бесспорно, одной из самых востребованных экспертиз в рамках данной категории дел является компьютерно-техническая экспертиза. Ученые обосновывают это высокой ролью в преступлениях сети Интернет, исследование которой требует «специальных знаний в области информационно-вычислительных технологий и информационно-вычислительной техники»[159].

Коллективом авторов под ред. Е. Р. Россинской было представлено новое определение судебной компьютерно-технической экспертизы, звучащее следующим образом: это «самостоятельный класс судебных экспертиз, проводимый в целях:

- определения статуса объекта как компьютерного средства;
- определения его состояния и назначения;
- выявления и изучения его роли в рассматриваемом уголовном, гражданском или административном деле;

---

[158] Смирнова С. А., Колдин В. Я. Судебно-экспертные технологии: современный облик и перспективы. Теория и практика судебной экспертизы. 2019;14(4). С. 140.

[159] Муравьев К. В., Ермаков М. Г. Современные возможности судебно-компьютерной экспертизы и меры по совершенствованию практики её назначения при расследовании преступлений, связанных с незаконным оборотом наркотических средств «Дистанционным» способом // Вестник Восточно-Сибирского института МВД России. 2019. №3 (90). С. 191.

– получения доступа к информации на электронных носителях с последующим ее всесторонним исследованием»[160].

Если ранее судебная компьютерно-техническая экспертиза относилась к классу инженерно-технических[161], то теперь она уже выделилась в отдельных класс экспертиз.

Еще в 2000 г. Е. Р. Россинской и А. И. Усовым были выделены несколько видов компьютерно-технической экспертизы: аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, а затем и компьютерно-сетевая[162].

Итоги анализа следственной и экспертной практики свидетельствуют о том, что в рамках расследования дел, связанных с незаконным оборотом наркотических средств, перед экспертами чаще всего ставятся вопросы, относящиеся к информационно-компьютерной и компьютерно-сетевой экспертизам.

Обусловлено это тем, что именно данные виды отвечают особенным задачам данных преступлениях, так как предметом компьютерно-сетевой экспертизы является «исследование обстоятельств и фактов, связанных с применением телекоммуникационных и сетевых технологий», а информационно-компьютерной – «задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе»[163].

Уже из определений рассматриваемых видов компьютерно-технической экспертизы можно сделать вывод, что цифровые следы не являются абсолютно новыми объектами исследования данного рода экспертиз.

---

[160] Теория информационно-компьютерного обеспечения криминалистической деятельности… С. 175.

[161] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. — М.: Право и Закон, 2001. 414 с.

[162] Усов А. И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А. И. Усов // Под ред. Е. Р. Россинской – М.: Издательство «Экзамен», издательство «Право и закон», 2003. 368 с.

[163] Смолина А. Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы: диссертация ... кандидата технических наук: 05.13.19 - Томск, 2017. С. 18.

Специфика заключается несколько в ином: цифровые следы из года в год видоизменяются, причем весьма оперативно. Именно этим и определяется потребность в постоянном обновлении знаний компьютерно-технической экспертизы.

Методическое обеспечение составляют труды ряда ученых, среди которых А. И. Усов[164], Е. Р. Россинская[165], В. С. Зубаха[166], Л. Г. Эджубов[167], В. А. Мещеряков[168], Г. В. Саенко, О. В. Тушканова[169] и многие другие.

Указанные, а также иные методические пособия используются экспертами в ходе проводимых исследований. Однако, как можно заметить, все труды являются далеко не новыми. Это, конечно, не означает, что они стали непригодными для производства компьютерно-технической экспертизы, но в какой-то части они не актуальны.

А. И. Семикаленова и Н. А. Хатунцев также указывают на недостаточное методическое обеспечение судебной компьютерно-технической экспертизы, а также на нахождение ее еще на стадии накопления и систематизации экспертного опыта[170].

---

[164] Усов А. И. Концептуальные основы судебной компьютерно-технической экспертизы: дис. … д-ра юрид. наук. — М. 2002. 402 с.

[165] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. — М.: Право и Закон. 2001. 414 с.

[166] Общие положения по назначению и производству компьютерно-технической экспертизы: Метод. рекомендации / В. С. Зубаха, А. И. Усов, Г. В. Саенко [и др.]; М-во внутр. дел Рос. Федерации. Гос. учреждение "Эксперт.-криминалист. центр М-ва внутр. дел Рос. Федерации". - Москва: ГУ ЭКЦ МВД России, 2001. 71 с.

[167] Производство судебной компьютерно-технической экспертизы [Текст] / М-во юстиции Российской Федерации, Гос. учреждение Российский федеральный центр судебной экспертизы. Актуальные комплексные экспертные задачи / [Эджубов Л. Г. и др. ; под ред. Усова А. И.]. — Москва : РФЦСЭ, 2009-, 2011. — 295 с

[168] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: специальность 12.00.09 "Уголовный процесс" : диссертация на соискание ученой степени доктора юридических наук / Мещеряков В. А. – Воронеж, 2001. 387 с.

[169] Саенко Г. В., Тушканова О. В. Компьютерная экспертиза. Типовые экспертные методики исследования вещественных доказательств. Ч. I / под ред. Ю. М. Дильдина; общ. ред. В. В. Мартынова. М.: ЭКЦ МВД России, 2010.

[170] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 485.

Без должного методического обеспечения затрудняется сам процесс экспертного исследования, а также возрастает и количество экспертных ошибок. Большинство ошибок, выделенных в монографии под ред. Е. Р. Россинской, как раз связаны либо с отсутствием соответствующих методик исследования, либо с недостаточным уровнем знаний экспертов методик, рекомендаций и принципов исследования цифровых следов.

В большинстве экспертных методик приводится порядок работы с уже устаревшими операционными системами, отсутствуют рекомендации по исследованию облачных серверов, делается акцент именно на персональных компьютерах, хотя сейчас более актуальны как устройства смартфоны, планшеты (особенно в преступлениях, связанных с незаконным оборотом наркотических средств). Например, в методике, представленной Г. В. Саенко и О. В. Тушкановой, имеется описание действий эксперта с DVD- и/или CD-дисками, которые в наше время при совершении преступных деяний используются крайне редко.

В методиках отсутствуют рекомендации относительно работы с цифровыми следами. Для судебной компьютерно-технической экспертизы в отличие, например, от судебной лингвистической или автороведческой экспертиз, крайне важно соблюдать определенный порядок действий. В противном случае это может привести не просто к изменению объекта, но и к полной его потере.

В уже упомянутой работе А. И. Семикаленова совместно с Н. А. Хатунцевым приводят пример нарушения экспертом порядка действий в рамках производства судебной компьютерно-технической экспертизы аппаратных средств. Во всех методических рекомендациях экспертам запрещается осуществлять загрузку с исследуемого носителя информации, так как это может повлечь за собой изменение данных. Но эксперт проигнорировал данные принципы, в результате чего данные жесткого диска уже не соответствовали исходным[171].

[171] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 481–482.

Заполняет этот пробел в методическом обеспечении во многом труд Е. Р. Россинской и И. А. Рядовского, в котором авторы обозначают тактические особенности работы с цифровыми следами[172]. Несмотря на то, что они были сформулированы для невербальных следственных действий, эти приемы можно перенести, собственно, уже и на экспертное исследование.

Если же говорить о судебной компьютерно-технической экспертизе в разрезе рассматриваемой в данном исследовании категории преступлений, то стоит остановиться на следующем.

Уже отмечалось, что незаконный оборот наркотических средств в современном мире тесно связан с теневым сегментом Даркнет. Особенности Даркнета и принципы его работы были изложены в 1 главе. Остановимся на возможностях исследования Даркнета как объекта компьютерно-технической экспертизы.

Оговоримся, что, если о сети Интернет в существующих экспертных методиках еще идет речь, то о Даркнете ничего не написано. При этом ввиду их различий переносить способы исследования Интернета на Даркнет не представляется возможным.

В отечественной науке в основном уделяется внимание Даркнету через рассмотрение криминалистических аспектов, в частности выделение способов своевременного выявления преступной деятельности. В зарубежной литературе можем отметить аналогичную ситуацию. Например, в исследовательском институте RAND Europe была разработана стратегия для обнаружения и пресечения торговли наркотическими средствами[173].

---

[172] Россинская Е. Р. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика / Е. Р. Россинская, И. А. Рядовский // Lex Russica (Русский закон). – 2021. – Т. 74, № 9(178). – С. 102-118.

[173] Taking Stock of the Online Drugs Trade. URL: https://www.rand.org/randeurope/research/projects/2016/online-drugs-trade-trafficking.html (дата обращения: 18.10.2024).

Основная задача при исследовании Даркнета сводится к деанонимизации пользователей TOR. Теоретики и практики нередко высказываются об отсутствии возможности деанонимизации[174].

Однако, как демонстрируют результаты отдельных авторов, все же существуют способы деанонимизации пользователей TOR. В этой связи большой интерес представляют работы Ю. А. Бондаренко и Г. М. Кизилова, С. М. Авдошина, А. В. Лазаренко.

Способы, выделенные первыми двумя учеными, были описаны ранее в 1 главе, поэтому подробнее остановимся на остальных.

А. В. Лазаренко предлагает брать за основу классификации атак, направленных на деанонимизацию TOR, не по виду действий (активные/пассивные), а по ресурсам, необходимым атакующему для осуществления атаки[175].

Таблица 3. Классификация атак[176]

	Ресурсы	**Атаки**
1.	Коррумпированный входной узел	• Website fingerprinting атака
2.	Коррумпированные входной и выходной узлы	• Анализ трафика • Тайминг атаки •Circuit fingerprinting атака • Атака с пометкой ячеек (тэггинг атака)
3.	Коррумпированный выходной узел	•Сниффинг перехваченного трафика (если пользователь не использует протокол https)
4.	Коррумпированный входной, выходной узел и внешний сервер	• Тайминг атака с использованием браузера и внедрения JavaScript кода • Атака анализа траффика с использованием браузера и внедрения JavaScript кода
5.	Автономная система	• Атаки BGP похищения • Атаки BGP прослушивания •RAPTOR атака
6.	Большое количество любых коррумпированных узлов	• Packet spinning атака • Атака перегрузки с использованием длинных путей •CellFlood DoS атака

[174] Смушкин А. Б. Криминалистические аспекты исследования Даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. №3 С. 105.

[175] Лазаренко А. В. Технологии деанонимизации пользователей Tor // Новые информационные технологии в автоматизированных системах. 2016. №19. С. 259.

[176] Лазаренко А. В. Технологии деанонимизации пользователей... С. 259.

Из всех видов атак отдельно выделяются те, которые, на взгляд А. В. Лазаренко, являются наиболее успешно применимыми в практической деятельности[177]:

– Website fingerprinting атака – «частный случай атак анализа траффика, во время которых локальный наблюдатель пытается выяснить информацию о контенте (посещенный веб-сайт), обозревая потоки траффика внутри анонимного соединения. Атакующий собирает метаинформацию: размер пакета, направление траффика. Сбор происходит без нарушения шифрования».

– Атаки уровня автономной системы – «под автономной системой понимается система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими одинаковую политику маршрутизации с интернетом».

– Модификация ПО Tor – во-первых, можно создать собственную версию браузера, что в итоге приведет к доступу к IP адресу клиента и к конечному ресурсу, во-вторых, «свою версию ПО можно установить на коррумпированные узлы», что позволит получить исходный код Tor.

Уже в совместной работе с С.М. Авдошиным авторы приходят к выводу, что «атакующему, имеющему большой запас ресурсов, например государственным службам, частным корпорациям и т.д., не составит большого труда деанонимизировать большое число пользователей сети Tor»[178].

Имеет место быть рассмотрение применения таких технологий в рамках судебной компьютерно-технической экспертизы. Однако их нужно не просто заимствовать, а адаптировать именно под принципы, цели и задачи экспертного исследования. Для практики расследования преступлений, совершаемых с использованием Даркнета, в частности незаконного оборота наркотических средств, такое расширение возможностей судебной компьютерно-технической

---

[177] Лазаренко А. В. Технологии деанонимизации пользователей... С. 259-261.

[178] Авдошин С. М. Методы деанонимизации пользователей Tor / С. М. Авдошин, А. В. Лазаренко // Информационные технологии. 2016. Т. 22, № 5. С. 369.

экспертизы положительно бы отразилось на качестве формируемой доказательственной базы.

Другим источником криминалистически значимой информации по делу выступают результаты, полученные в ходе производства судебной лингвистической экспертизы, а также судебной автороведческой экспертизы.

Судебная лингвистическая и судебная автороведческая экспертизы относятся к классу речеведческих экспертиз, которые, как утверждает Е. И. Галяшина объединены рядом критериев: «общностью исследуемых объектов – продуктов речевой деятельности человека, сходным комплексом специальных речеведческих знаний, необходимых для производства экспертизы, единством методологии в решении идентификационных и диагностических задач»[179].

При этом лингвистическая и автороведческая экспертизы представляют собой два абсолютно самостоятельных по всем параметрам рода экспертизы. Однако, как показало исследование, правоприменитель не всегда различает данные роды экспертиз и считает, что это один и тот же род экспертизы. Соответственно, в постановлении (определении) о назначении экспертизы указывается неверное наименование рода экспертизы. Так, в одном из постановлений о назначении экспертизы следователь написал «назначить смысловую экспертизу». Возникают вопрос: «Что такое смысловая экспертиза, является ли это автороведческой или все же лингвистической экспертизой?». Естественно, по вопросам к эксперту можно сделать вывод, что следователь имел в виду лингвистическую экспертизу. Но как проводить экспертизу, которой, согласно всем принятым ведомственным и научным классификациям, не существует, а главное, в какое экспертное учреждение и кому ее назначать. Такие ошибки приводят к усложнению всего процесса.

Появление цифровых следов несколько иначе повлияло на судебную лингвистическую и судебную автороведческую экспертизы. Если раньше,

---

[179] Галяшина Е. И. Речеведческие экспертизы в судопроизводстве // Законы России: опыт, анализ, практика. 2011. № 12. С. 12.

например, одним из объектов судебной почерковедческой экспертизы была подпись, отраженная на бумажном носителе, то сейчас в перечень объектов входит также действия, выполненные человеком от руки на планшетах, смартфонах и иных электронных носителях. Для рассматриваемых же нами родов речеведческих экспертиз, несмотря на всю цифровую трансформацию, все еще необходимо, чтобы в качестве объекта выступал четко зафиксированный речевой продукт. Эксперты исследуют речевой след, а не цифровой след.

Речевой след – следовой контакт, возникший в результате соответствующего взаимодействия между носителем информации и речепорождающим субъектом и отражающий признаки следообразующего объекта – вербализованного продукта речемыслительной деятельности человека[180].

Что же тогда изменилось? Для судебной лингвистической экспертизы, как и для судебной автороведческой экспертизы, важно учитывать то, где и в каком контексте создавался речевой продукт. Особенности речевых продуктов, образованных в информационно-телекоммуникационных сетях, определяют необходимость к применению нового подхода при описании объектов.

Цифровизация судебно-экспертной деятельности привела не только к расширению возможностей экспертиз, но к и появлению новых вызовов перед экспертами. Рассмотрим данные трансформации детально.

Судебная лингвистическая экспертиза представляет собой процессуально регламентированное экспертное лингвистическое исследование формально-языковой и содержательно смысловой сторон речевого произведения с целью выявления словесных конструкций и смысловых единиц текста, подпадающих под признаки конкретного противоправного деяния, ответственность за которое

---

[180] Галяшина Е. И. Речевые следы как объекты судебных экспертиз (в свете идей Р. С. Белкина) / Е. И. Галяшина // Современное развитие криминалистики и судебной экспертизы как реализация идей Р. С. Белкина: Материалы Международной научно-практической конференции «К 95-летию со дня рождения ученого, педагога, публициста», Москва, 22–23 ноября 2017 года. – Москва: Общество с ограниченной ответственностью "Проспект", 2018. С. 189.

предусмотрено соответствующей законодательной нормой[181]. Это один из самых подвижных и изменчивых родов экспертиз ввиду того, что развитие отдельных сфер общества непременно влечет за собой появление не только новых объектов, но и новых видов лингвистической экспертизы.

М. Л. Подкатилина, используя в качестве основания классификации объект и задачи исследования, предлагает следующее видовое деление лингвистической экспертизы:

– «нейминговая экспертиза;

– лингвистическая экспертиза нормативных правовых актов и документов;

– лингвистическая экспертиза текстов массовой информации и агитационных материалов, писем и обращений;

– лингвистическая экспертиза произведений науки, литературы и искусства;

– лингвистическая экспертиза звучащей речи;

– лингвистическая экспертиза рекламных текстов;

– лингвистическая экспертиза словесных и комбинированных товарных знаков и знаков обслуживания;

– лингвистическая экспертиза экстремистских материалов»[182].

Представленная классификация не определяет четко место лингвистической экспертизы по делам, связанным с незаконным оборотом наркотических средств. Исследование текстов в рамках данной категории дел может быть как в лингвистической экспертизе текстов массовой информации и агитационных материалов, писем и обращений, так и в лингвистической экспертизе звучащей речи.

---

[181] Галяшина Е. И. Речеведческие экспертизы в судопроизводстве: насущные потребности, проблемы и пути их решения // Теория и практика судебной экспертизы. 2019. Том 14. № 4. С.10.

[182] Подкатилина М. Л. Судебная лингвистическая экспертиза экстремистских материалов: монография / под ред. Е. И. Галяшиной. – М.: Юрлитинформ, 2013. С.13.

Другой вариант классификации предлагает В. Д. Никишин, представляя видовое деление лингвистических экспертиз через термин «дискурс»:

– экспертиза текстов экстремистско-террористического дискурса;

– экспертиза текстов религиозного экстремистско-террористического дискурса (судебная экспертиза материалов религиозного характера экстремистско-террористической направленности);

– экспертиза текстов диффамационного дискурса;

– экспертиза текстов коррупционного дискурса;

– экспертиза текстов порнографического дискурса;

– экспертиза текстов наркотического дискурса;

– экспертиза нормативно-правового и договорного дискурса.

– экспертиза текстов неймингового дискурса (неймингновая экспертиза);

– экспертиза текстов рекламного дискурса[183].

Представляется, что такой вариант деления лингвистических экспертиз является наиболее актуальным, так как в отдельный вид выделена экспертиза текстов наркотического дискурса, о которой и пойдет дальше речь.

Основу методического обеспечения лингвистической экспертизы текстов наркотического дискурса составляют методические рекомендации, принятые в 2006 г. ФСКН России[184].

Во многом экспертная методика актуальна до сих пор и совершенно оправданно применяется экспертами при проведении исследований. Однако неудивительно, что за 18 лет возникли такие феномены, которые не охватываются данными методическими рекомендациями.

---

[183] Никишин В. Д. Теоретические и организационно-правовые аспекты судебной экспертизы материалов религиозного характера экстремистской и террористической направленности: дис … канд. юрид. наук. 12.00.12 / Никишин Владимир Дмитриевич. — М., 2018. С.70.

[184] Голощапова Т. И., Смирнов А. А., Полосина А. М., Курьянова И. В. Лингвистическая экспертиза текстов, в которых имеется информация, относящаяся к семантическому полю «наркотики»: методические рекомендации для экспертов, следователей, оперативных сотрудников / под ред. А. М. Черенкова. М.: ЭКУ 9-го Департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, 2006. 43 с.

В рассматриваемой работе авторы разделяют лингвистическую экспертизу кратких записей и лингвистическую экспертизу текстов среднего и большого объема, к которым относят статьи, буклеты, произведения публицистической или научной литературы.

Такие объекты можно встретить в делах об административных правонарушениях о пропаганде наркотических средств по ст. 6.13. КоАП РФ, на чем, собственно, и сделан упор в методике. Но уже в уголовных делах основным источником сведений являются переписки в мессенджерах и социальных сетях, которые нельзя отнести ни к кратким записям, ни к текстам среднего/большого объема. Для исследования данного объекта нужно применять несколько иной подход.

Во-первых, редко можно встретить в переписках единый текст даже среднего объема. Чаще всего пользователи дробят предложения на составные части, причем каждый делает с учетом своего индивидуального стиля. Во-вторых, речевая составляющая представлена не только вербальными, но также и невербальными компонентами, которые невозможно игнорировать при проведении лингвистического исследования. Довольно большое количество сообщений сопровождаются также смайлами, эмодзи, стикерами, значение которых зависит в каждом конкретном случае от контекста и от авторской задумки.

Креолизованный текст – это текст, смысл которого образуется вербальной и невербальной знаковыми системами[185]. Креолизованные тексты наиболее сложны в своем исследовании, так как в данном случае необходимо также изучать и невербальную составляющую. При этом исследование невербальной составляющей должно быть вспомогательной частью экспертизы, способствовать более глубокому и полному изучению вербальной составляющей, которая является главной для эксперта-лингвиста.

---

[185] Сорокин Ю. А. Креолизованные тексты и их коммуникативная функция // Оптимизация речевого воздействия / Ю. А. Сорокин. – М.: НиолаПресс, 1990. 186 с.

Значимость исследования креолизованных текстов повышается за счет того, что вербальный и невербальный компоненты совместно используются для маскировки предмета речи.

Маскировки для эксперта-лингвиста составляют основную сложность при исследовании текстов наркотического дискурса.

Практически во всех научных трудах, касающихся лингвистического исследования текстов наркодискурса, большая роль отводится анализу жаргона наркоманов.

Слова, которые являются общеупотребительными (например, наркотики, героин, марихуана и т.д.), не составляет труда отнести к семантическому полю «наркотические средства». Но на практике лица, связанные с наркотическими средствами, чаще употребляют лексику, свойственную именно для них, во-первых, ввиду деформации, в том числе языковой, а во-вторых, с целью сокрытия информации от третьих лиц.

В этой связи важно обозначить, что использование в речи жаргона не всегда является признаком маскировки. Жаргон не так часто, как показывает исследование, употребляется именно с целью маскировки.

Следует разграничивать понятия «жаргон» и «маскировка». Жаргон является отражением индивидуально-авторского стиля, приобретаемого в результате принадлежности к определенной группе людей.

О. П. Ермакова говорит о том, что жаргон наркоманов составляет отдельную касту, почему он и «ограничен узким кругом носителей, и лишь отдельные слова выходят за пределы этой сферы»[186].

В как таковой жаргон изначально не заложена никакая цель, это просто один из видов лексики. А лингвистическая маскировка представляет собой прием сокрытия информации от третьих лиц. Таким образом, сущность маскировки

[186] Ермакова О. П., Земская Е. А., Розина Р. И. // Источники пополнения и тематические группы жаргона. Слова, с которыми мы все встречались: Толковый словарь русского общего жаргона: Ок. 450 слов. М.: Азбуковник, 1999. С. 10.

состоит в достижении конкретной цели: зашифровать информацию так, чтобы она была понятна лишь ограниченному кругу лиц.

Исследование жаргона способствует решению лингвистической задачи определения наличия/отсутствия высказываний, относящихся к наркотическому дискурсу.

Эксперту-лингвисту «для точного определения лексического значения жаргонных слов необходимо обращаться к специализированным словарям жаргона наркоманов»[187].

Лексика — это очень подвижный, активный и изменчивый пласт речи, требующий постоянного обновления и переосмысления. В словарях жаргона наркоманов не отражены слова, употребляемые в обиходе наркоманов в последние годы. В результате чего экспертам-лингвистам не всегда удается отнести те или иные слова к семантическому полю «наркотики» путем поиска словарного значения слова.

На этот пробел указывают также ученые, выделяя в качестве последствия недостаточности изучения жаргона наркоманов разную оценку такой лексики лингвистами[188].

На практике эксперты-лингвисты прибегают к ряду методов, в частности, к контекстологическому анализу речевого продукта с целью толкования отдельных лексем. Нередко использование такого метода дает возможность отнесения слов, словосочетаний к семантическому полю «наркотики».

Несмотря на большой инструментарий экспертов-лингвистов, потребность в расширении словарного перечня жаргонов присутствует. Обновление словарей

---

[187] Голощапова Т. И., Смирнов А. А., Полосина А. М., Курьянова И. В. Лингвистическая экспертиза текстов, в которых имеется информация, относящаяся к семантическому полю «наркотики»: методические рекомендации для экспертов, следователей, оперативных сотрудников / под ред. А. М. Черенкова. М.: ЭКУ 9-го Департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, 2006.

[188] Артемова Т. В., Катышев П. А., Оленев С. В., Паули Ю. С., Соколова С. К. Функции жаргона наркоманов и словообразовательные средства их осуществления (на материале социолингвистических опросов и словарей жаргона) Вестник Кемеровского государственного университета 2014 № 3 (59) Т. 3. С. 165-169.

занимает значительное время даже не столько по причине сбора и обработки информации, сколько ввиду требуемого времени для выпуска в печать книги. В условиях высокой скорости перемен, происходящих в обществе, такой способ не сможет постоянно восполнять пробелы в нехватке знаний в области наркотического сленга/жаргона.

Представляется, что эффективным решением в данной ситуации будет являться обобщение экспертами-лингвистами экспертной практики. Если мы говорим о государственных экспертных учреждениях, то в рамках каждого ведомства эксперты-лингвисты могут проводить с определенной периодичностью анализ выполненных экспертных исследований текстов наркотического дискурса с выделением впоследствии лексики, не зафиксированной ранее в словарях, но используемой наркотическим сообществом. Для этого могут быть созданы, например, анкеты для экспертов, содержащие вопросы относительно объектов исследования (их вид, коммуникативная ситуация речевого продукта, а также выделенная лексика, относящаяся к семантическому полю «наркотики»). Либо следует создать специальный реестр учета сленговой и жаргонной лексики, куда эксперты бы могли вносить полученные ими данные.

Какой бы способ обобщения ни был выбран, важно, чтобы полученные и оформленные результаты были доступны не только для экспертов отдельно взятого государственного экспертного учреждения.

Обобщение экспертной практики в целом является важной составляющей деятельности эксперта, хотя и несколько недооцененной. Систематическое обобщение в конечном счете влияет на повышение качества заключений экспертов, способствует уменьшению количества экспертных ошибок, а также устранению возникающих противоречий.

А. П. Липатовой были выделены признаки, указывающие на факт наличия в речевом продукте лингвистической маскировки:

– «смысловое несоответствие отражённого в речи содержания понятия (совокупности признаков) его объёму;

– соседство неясной (или аномальной) и нулевой номинации;

– несочетаемость двух номинаций, относящихся к одному и тому же объекту и встречающихся не рядом, но в рамках одного разговора;

– непривычный способ обращения с предметом, нехарактерный для номинации контекст;

– оценка объекта без детализации, конкретизации;

– паузы перед введением номинации»[189].

На основании данных признаков четко прослеживается, что использование жаргонной лексики является далеко не единственным способом сокрытия информации.

Самый сложный способ для выявления экспертами имплицитности высказывания обусловлен использованием участниками разговора слов так называемого «разового кода». М. В. Хитина определяет «разовый код», как «специфическое образование, когда обычным словам придаются особые «тайные значения», причем так, чтобы для постороннего слушателя речь не казалась странной и имела бы свой обычный смысл, складывающийся из нормативных лексических значений»[190].

В таком случае, к сожалению, достаточно сложно декодировать информацию, иногда даже с учетом анализа контекста эксперту-лингвисту не удается выявить маскировку. Все усугубляется тем, что обозначенная проблема не связана никак с недостаточной развитой методологией, отсутствием методического обеспечения, поэтому и нет решения выхода из данной ситуации.

Слова «разового кода» характерны как для письменной, так и для устной речи. Но существуют способы маскировки, которые присущи исключительно текстам устной речи. Речь идет о невербальных компонентах. Ранее уже было отмечено, что особенностью современной коммуникации является активное

---

[189] Липатова А. П. Продуктивные модели "разового кода" арго наркоманов / А. П. Липатова // Антинаркотическая безопасность. 2015. № 1(4). С. 116.

[190] Хитина М. В. Делимитативные признаки устно-речевого дискурса. М.: ООО Типография Сарма, 2004. С. 106.

внедрение в речь смайлов, стикеров и эмодзи. В связи с чем они также представляют объект лингвистического исследования (важно, что исследуются они не в отрыве от вербальной составляющей, а вместе с ней).

В результате анализа следственной и экспертной практики удалось определить ряд смайлов, относящихся по своей сути к наркотическому дискурсу:

 – внутривенный катетер;

 – доза;

 – героин;

 – таблетки.

Как можно заметить, представленные смайлы соответствуют вербальной версии жаргона наркоманов (бабочка, конфета, лед, колеса), что подтверждает требование учета невербальных компонентов. В экспертных методиках смайлы, стикеры, эмодзи не рассматриваются как часть речевого продукта. Как следствие не обозначены и способы исследования речевых продуктов с невербальными компонентами, в частности. Поэтому в этой части также прослеживается необходимость обновления методических рекомендаций.

В методике, представленной ФСКН России, помимо прочего, отсутствуют вопросы, касающиеся определения коммуникативных ролей наркопреступников. Это можно объяснить тем, что на время, когда данные методические рекомендации были выпущены, социальные сети, мессенджеры не были настолько развиты и не использовались повсеместно.

При описании новых способов преступления в 1 главе акцент был сделан также на появлении новых участников наркогрупп, а также на возрастание роли коммуникации при совершении наркопреступлений.

На возможность лингвистической экспертизы определения выполняемых функций наркопреступников, а также иерархии в рамках группы указывают многие

ученые и эксперты, среди которых Е. И. Галяшина, Т. А. Распопова, М. А. Балаш, А. В. Коряковцев, П. А. Манянин.

Так, А. В. Коряковцев и П. А. Манянин в работе приводят пример конкретной судебной лингвистической экспертизы, результаты которой позволили определить факт совместной преступной деятельности, а также роли и степень вовлеченности в совершение преступления каждого из участников беседы[191].

Несмотря на наличие научной литературы, посвященной данной части экспертного исследования, все еще отсутствует единой представление о том, как же решать эти задачи.

М. А. Балаш и А. В. Коряковцев обоснованно отмечают, что эксперты не располагают «научно-обоснованными и апробированными методиками лингвистического исследования продуктов речевой деятельности, связанными с расследованием преступлений, совершенных организованной группой или преступным сообществом (преступной организацией)»[192].

Так, в части проанализированных заключений экспертов для определения иерархии и роли лиц были использованы количественные методы. Эксперты учитывали, кто из собеседников чаще и больше пишет сообщений, и в том числе на основании этого делали вывод о лидерстве участника.

Однако такой формальный подход является недопустимым. Большее количество сообщений очень часто обосновывается такой особенностью коммуникации в Интернете, как членение предложений и даже словосочетаний на отдельные сообщения. Лицо может буквально отправлять по одному слову,

---

[191] Манянин П. А. О возможностях судебной лингвистической экспертизы при установлении ролей и функций наркопреступников / П. А. Манянин, А. В. Коряковцев // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXIII международной научно-практической конференции: В 2 частях, Красноярск, 02–03 апреля 2020 года. Том 1. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2020. С. 202-204.

[192] Балаш М. А., Коряковцев А. В. Практика использования лингвистической экспертизы при доказывании совершения наркопреступлений группой лиц // Юрислингвистика. 2012. №1. С. 113.

которые в совокупности будут составлять одно предложение. Соответственно, такая особенность никак не может быть признаком ведущей позиции в группе.

Таким образом, существует необходимость обновления экспертных методик в области лингвистического исследования текстов наркотического дискурса.

Поддерживают эту идею и практикующие эксперты-лингвисты. На вопрос: «Считаете ли Вы необходимым обновление методического обеспечения в области лингвистического исследования текстов наркотического дискурса?», – 64,9% опрошенных ответили положительно, 9% – отрицательно и 26,1% не задумывались об этом.

Состояние методического обеспечения судебной автороведческой экспертизы также требует совершенствования.

Судебная автороведческая экспертиза — экспертиза письменного текста, позволяющая установить автора спорного речевого произведения или охарактеризовать его по определенным признакам. Ее сущность состоит в исследовании продуктов речевой деятельности с целью определения фактического авторства[193]. Автороведческая экспертиза характеризуется сложностью, объемностью проведения исследования, и при этом ее результаты способы предоставить для следователя и суда криминалистически значимую информацию по делу.

Однако, как выясняется, автороведческую экспертизу назначают значительно реже по сравнению, например, с лингвистической экспертизой.

Из числа опрошенных следователей ни один не назначал автороведческую экспертизу, и более того никто не отметил ее как потенциально назначаемую экспертизу в рамках дел незаконного оборота наркотических средств.

Однако значимость данного рода экспертизы в рамках расследования незаконного оборота наркотических средств недооценивается.

---

[193] Галяшина Е. И. Судебное речеведение… С.138.

Для начала стоит отметить, что выделяют два вида судебной автороведческой экспертизы[194]:

1. Судебная автороведческая идентификационная экспертиза.

2. Судебная автороведческая диагностическая экспертиза.

Экспертные методики автороведческой экспертизы не направлены в общем-то на исследование текстов Интернет-коммуникации. Такая проблема отмечается, например Т. П. Соколовой[195].

Методика под ред. И. И. Рубцовой, Е. И. Ермоловой, А. И. Безруковой[196], методика С. М. Вула[197] рассчитаны больше на тексты художественного, публицистического, научного и официально-делового стилей. Тексты перечисленных стилей существенным образом отличается от речевых продуктов, создаваемых в рамках Интернета.

Этой же позиции придерживается А. В. Громова: «В связи с тем, что переписка в мессенджере представляет собой новый тип объекта автороведческой исследования, в целях криминалистической идентификации участников переписки по создаваемым ими текстам необходима корректировка и дополнение перечня идентификационно значимых признаков письменной речи, приводимых в существующих методиках производства автороведческих экспертиз»[198].

Пробелы в методическом обеспечении заполняют научные работы и исследования Т. П. Соколовой, Е. А. Чубиной, А. В. Громовой, Т. А. Литвиновой, П. А. Волынкина и других ученых.

---

[194] Сааков Т. А. Судебно-диагностическое исследование демографических характеристик автора по признакам письменной речи: дис … канд. юрид. наук. 12.00.12 / Сааков Т. А.— М., 2020. С. 121.

[195] Соколова Т. П. Проблемы экспертной идентификации в судебном автороведении // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 2 (90). С. 67—76.

[196] Комплексная методика производства автороведческих экспертиз: Методические рекомендации / И. И. Рубцова, Е. И. Ермолова, А. И. Безрукова [и др.]. М., 2007. 192 с.

[197] Вул С. М. Судебно-автороведческая идентификационная экспертиза: методические основы: методическое пособие. — Харьков : ХНИИСЭ, 2007. 64 с.

[198] Громова А. В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник ВолГУ. Серия 2: Языкознание. 2021. №2. С. 92.

Авторы определяют требования к текстам веб-коммуникации, которые должны проверяться экспертами на подготовительной стадии. Сам объект исследования, как и сравнительные образцы, должны больше оцениваться не количественно (минимальный объем текста), а качественно (наличие в тексте признаков идиостиля автора)[199].

Рассылки сообщений с информацией о наркотических средствах зачастую соответствуют минимальному объему 150 слов, установленному методиками автороведческой экспертизы. Однако созданы они по определенному шаблону, в которой не отражаются индивидуальные признаки автора. Если подходить формально, то объект пригоден для исследования, но в реальности его исследование ни к чему не приведет.

В связи с этим следует полностью поддержать данную точку зрения, высказываемую в научной среде, на уровне внесения корректировок в экспертные методики.

В новом подходе нуждаются также и методы, применяемые в автороведческом исследовании. В особенности количественные методы[200]. Количественные методы во многом сводятся к простому подсчету, например, лексем, и соотношением их с установленными нормами. Мало того, что в этом опять же прослеживается некий формализм, вместе с тем, многие критерии являются уже неактуальными. Хотя значимость количественных методов для автороведческой экспертизы высока. Если в лингвистической экспертизе количественные методы являются факультативными, и потребность в их применении возникает нечасто, то при производстве автороведческой экспертизы без них нельзя обойтись.

---

[199] Соколова Т. П. Проблемы экспертной идентификации в судебном автороведении. С. 70.

[200] Соколова Т. П. Проблемы применения количественных методов в судебной автороведческой экспертизе // Вестник Университета имени О. Е. Кутафина. 2024. №3 (116). С. 77-84.

Выработка стандарта количественных методов судебной автороведческой экспертизы, а также модификация их использования составляют важнейшую часть развития методологического обеспечения данного рода судебной экспертизы.

Новаторской является идея, предложенная А. В. Громовой, Т. А. Литвиновой. Авторы видят будущее в применении «компьютерного» подхода при идентификации автора речевого продукта, который «заключается в построении классификатора, на входе которого — численные значения различных квантифицируемых параметров текста, извлеченных, как правило, автоматически (униграммы и n-граммы, т.е. последовательности из n элементов — символов (букв, знаков препинания, цифр и т.п.), слов, частей речи и т.д.); реже — синтаксические и семантические параметры; на выходе — класс объекта (текста), т.е. принадлежность тому или иному автору»[201]. Однако так как речевые продукты, образованные в рамках незаконного оборота наркотических средств в компьютерных сетях, обладают небольшим объемом, то к ним такой подход не может быть применен.

При этом не стоит уходить в абсолютную автоматизацию исследовательского объекта. Для получения объективных результатов важно соблюдение баланса и сочетаемости работы самого эксперта и использования компьютерных технологий.

Как отмечают И. В. Огорелков, Т. П. Соколова и Е. А. Чубина, «недостаточное понимание требуемой совокупности признаков, а также принципов и правил, по которым строится общение в виртуальной коммуникации, нередко приводит экспертов к ошибочным выводам»[202].

Потенциал автороведческой экспертизы как способа получения криминалистически значимой информации при должном ее методическом и

---

[201] Литвинова Т. А., Громова А. В. Компьютерные технологии в судебной автороведческой экспертизе: проблемы и перспективы использования // Вестник Волгоградского государственного университета. Серия 2 : Языкознание. 2020. Т. 19. № 1. С. 81.

[202] Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. — 2-е изд., перераб. и доп. — Москва: Проспект, 2024. С. 231.

методологическом обеспечении велик. Однако на практике сильно недооценивается данный род судебной экспертизы.

При изучении материалов уголовных дел удалось установить следующую сложность, с которой сталкиваются следователи в процессе доказывания: в ходе следственных действий обнаруживаются переписки с обсуждением наркотических средств, фиксируются данные с сайтов Даркнета, посвященные также наркотическим средствам. Однако подозреваемый полностью отрицает свою причастность, говоря, что он не вел представленный веб-сайт, а переписка от его имени осуществлялась абсолютно другим человеком.

В таком случае следователи прибегают к назначению судебной компьютерно-технической экспертизы, чтобы определить, с какого устройства были осуществлены те или иные действия, кому принадлежит IP-адрес и т.д. Но ввиду различных факторов, например, использования Tor или иной системы шифрования, установить данные факты не всегда представляется возможным.

И далее следователи не рассматривают варианты назначения других судебных экспертиз, по сути лишаясь значимой для дела информации.

Эксперт-авторовед может ответить на вопрос (при наличии требуемых образцов), проведя исследование: «Является ли автором текста (переписки, сайта и т.д.) гражданин ФИО»?

Если по отдельному ряду преступлений расследование и формирование доказательственной базы возможно без назначения судебной экспертизы, то для наркопреступлений заключения экспертов являются одним из источников получения криминалистически важной информации по делу.

Судебно-экспертные технологии производства экспертиз по делам, связанным с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях, требуют совершенствования, а в некоторых случаях изменений. Достичь этого можно путем:

– обобщения экспертной практики в результате совместной деятельности экспертов как государственных, так и негосударственных экспертных учреждений (создание общих баз данных по каждому роду/виду судебных экспертиз,

проводящих исследования в рамках расследования незаконного оборота наркотических средств в компьютерных сетях);

– внедрения современных технологий и методов в экспертные исследования (адаптация технологий по деанонимизации пользователей Tor в исследования судебной компьютерно-технической экспертизы);

– обновления экспертных методик; создание общих стандартов для всего экспертного сообщества в части внесения положений об особенностях механизма следообразования цифровых следов и особенностях исследования конкретных видов цифровых следов, образованных в ходе незаконного оборота наркотических средств;

– мониторинга изменений в способах преступлений, связанных с незаконным оборотом наркотических средств, и анализ их влияния на технологии экспертного исследования.

Состояние развития экспертных технологий той или иной экспертизы определяет качество заключения эксперта, которое в дальнейшем становится частью системы доказательств.

§ 2.3 Оценка и использование результатов судебных экспертиз при расследовании незаконного оборота наркотических средств в компьютерных сетях

По своей сути весь уголовный процесс в части доказывания состоит из отдельных, но при этом взаимосвязанных и даже взаимозависимых действий. В разрезе судебной экспертизы эта цепочка выглядит следующим образом: собирание объектов (обнаружение, изъятие и фиксация) → вынесение постановления (определения) о назначении судебной экспертизы → передача объектов исследования и необходимой части материалов дела эксперту → производство экспертного исследование и оформление его результатов → передача лицу, назначившему экспертизу, заключения эксперта.

Заключение эксперта в отдельных делах играет ведущую роль. В диссертационном исследовании уже обозначались возможности судебных экспертиз при расследовании дел, связанных с незаконным оборотом наркотических средств. Данные теоретические положения подтверждаются на практике. В отдельных проанализированных уголовных делах именно на основании результатов заключения эксперта по судебной компьютерно-технической экспертизе удалось доказать прямую причастность лица к совершению преступления.

И все же говорить о преимущественном положении заключения эксперта относительно других доказательств, перечисленных в ст. 74 УПК РФ, было бы некорректно.

Вектор рассмотрения заключения эксперта в качестве особого доказательства во многом связан с тем, что для его получения необходимо привлечь лицо, обладающее специальными знаниями, которыми не владеет ни один другой участник уголовного процесса.

Однако каждое доказательство обладает особенностями, не характерными для других. Это и определяет разнообразие доказательств, используемых при расследовании и рассмотрении уголовного дела.

Один из аргументов, подтверждающих также равноценность заключения эксперта наряду со всеми иными доказательствами, является необходимость его оценки. Несмотря на то, что судебно-экспертное исследование проводится сведущим лицом, это не исключает как субъективных, так и объективных факторов совершения ошибок, а в худшем случае – дачи заведомо ложного заключения.

Еще в 1970-х годах ученые указывали, «то, что выводы эксперта основаны на исследовании, проведенном с применением специальных методик, приборов и оборудования, совсем не исключает возможности и необходимости их оценки следователем и судом в полном объеме, чтобы установить допустимо ли

заключение эксперта, обосновано ли оно, достоверны ли установленные экспертом факты»[203].

Соответственно, получение правоприменителем заключения эксперта является не последним звеном в обозначенной цепочке. Для того, чтобы можно было использовать результаты проведенной судебной экспертизы, заключение эксперта должно пройти стадию оценки.

На этом этапе важно ответить на два главных вопроса:

– Кто должен заниматься оценкой заключения эксперта?

– По каким критериям должна осуществляться оценка заключения эксперта?

Рассуждая о том, кто должен, а главное может оценивать заключение эксперта, Р. С. Белкин говорит о несостоятельности следователя и суда ввиду отсутствия необходимых знаний оценить научную обоснованность проведенного исследования, правильность выбора и применения методов исследования, соответствие этих методов современным достижениям соответствующей области научного знания[204].

Соглашаясь с позицией Р. С. Белкина, Т. В. Аверьянова писала о том, что заключение сложной, в том числе комплексной экспертизы… может оценить только специалист того же профиля, что и эксперт, т.е. лицо, обладающее специальными знаниями[205].

Невозможно оспорить факт того, что никто, кроме как эксперта или специалиста соответствующей области не может рассмотреть заключение с точки зрения научности проведенного исследования (соблюдены ли все условия, правильно ли применялись методы, пригодна ли методика исследования и т.д.). Но оценивать заключение эксперта является исключительным правом судьи или следователя. Специалист в свою очередь не оценивает заключение эксперта, а

---

[203] Белкин Р. С., Винберг А. И., Дорохов В. Я., Карнеева Л. М. и др. Теория доказательств в советском уголовном процессе. М.: Юридическая литература, 1973. С. 725.

[204] Белкин Р. С. Курс криминалистики. М., ЮНИТИ-ДАНА, Закон и право. 2001. С. 623.

[205] Аверьянова Т. В. Проблемы оценки достоверности заключения комплексного экспертного исследования // Вестник экономической безопасности. 2018. №1. С. 14.

оказывает консультационную помощь судье или следователю при осуществлении ими оценки. В связи с этим не согласимся с Т. В. Аверьяновой в части утверждения о допустимости оценки специалистом заключения эксперта.

И. Н. Сорокотягин представляет несколько иное мнение, утверждая, что следователь и судья как правило не имеют достаточно полного представления о специфике производства экспертиз. Однако их опыт, знания, подготовка по специальным вопросам позволяют им разобраться в научной обоснованности экспертного заключения[206].

Как раз для того, чтобы следователь, судья могли оценивать заключения эксперта, не обладая специальными знаниями, имея при этом свой уникальный опыт и достаточный уровень подготовки, нужно определить четкие критерии оценивания и инструментарий, к которому они могли бы прибегать при возникновении трудностей на данном этапе.

Рассмотрим уже выработанные в науке критерии оценки заключения эксперта.

А. В. Кудрявцева считает, что оценка заключения эксперта должна исходить из общих и специальных оснований. К последним относятся психологические, гносеологические и юридические основания[207].

Интересным представляется выделенное автором психологическое основание. Сама А. В. Кудрявцева раскрывает его через уверенность субъекта оценки заключения эксперта в его объективности и возможности критически относиться к заключению эксперта[208].

При этом, на наш взгляд, общие и специальные юридические основания пересекаются и сущностно отражают одно и то же.

Критерии оценки заключения эксперта можно определить также через анализ стадий оценки.

---

[206] Сорокотягин И. Н., Сорокотягина Д. А. Судебная экспертиза: учебник и практикум для бакалавриата и специалитета. Москва: Юрайт, 2019. С. 141.

[207] Кудрявцева А. В. Судебная экспертиза в уголовном процессе России. – Челябинск, 2001. С. 348-349.

[208] Кудрявцева А. В. Судебная экспертиза в уголовном процессе… С. 348-349.

Например, Е. Р. Россинская выделяет 7 стадий оценки заключения эксперта:

1. Проверка соблюдения требований закона при назначении экспертизы.

2. Проверка подлинности и достаточности исследовавшихся вещественных доказательств и образцов.

3. Оценка научной обоснованности экспертной методики и правомерности ее применения в данном конкретном случае.

4. Проверка и оценка полноты и всесторонности заключения.

5. Оценка логической обоснованности хода и результатов экспертного исследования.

6. Проверка относимости результатов экспертного исследования к данному уголовному или гражданскому делу, делу об административном правонарушении.

7. Проверка соответствия выводов эксперта имеющимся по делу доказательствам[209].

Апеллируя представленному выше мнению, Ю. С. Кудрявцев говорит о невозможности отнесения к оценке заключения эксперта стадии соответствия выводов эксперта имеющимся по делу доказательствам. Автор аргументирует это следующим образом: «Выводы эксперта могут согласовываться с остальными доказательствами, а могут и противоречить им. Однако если эксперт выполнил исследование в полном объеме, а выводы обоснованы, убедительны и достоверны, то суд не может не учитывать результаты проведенного исследования»[210].

По его мнению, оценку заключения эксперта необходимо рассматривать в более узком смысле, как «оценку действий эксперта по производству экспертизы и полученных при этом результатов, начиная с момента получения определения суда о назначении экспертизы и заканчивая направлением материалов вместе с заключением инициатору. К данным действиям относятся: прием экспертной организацией (либо экспертом) материалов для производства экспертизы, их

---

[209] Россинская Е. Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе: монография. М.: Право и закон. 1996. С. 53-59.

[210] Кудрявцев Ю. С. Об оценке экспертного заключения // Судебная власть и уголовный процесс, 2018. № 3. С. 104.

регистрация; соблюдение процедуры передачи материалов эксперту, если материалы экспертизы направлены в экспертное учреждение; применение при проведении исследования методик и методов, направленных на решение поставленных перед экспертом вопросов; использование технических средств, необходимых при производстве исследования; оценка полученных результатов и формирование выводов; оформление проведенного исследования».[211]

Подытоживая сказанное, Ю. С. Кудрявцев выделяет три стадии оценки заключения эксперта:

1. «Оценка заключения эксперта с точки зрения соблюдения процессуального законодательства, ведомственных нормативных актов, регулирующих производство экспертизы в экспертном учреждении.

2. Оценка заключения эксперта с точки зрения объективности, полноты, всесторонности и убедительности.

3. Оценка заключения эксперта с точки зрения оформления, дающего возможность проверить обоснованность и достоверность сделанных выводов на базе общепринятых научных и практических данных»[212].

Прежде всего, стоит не согласиться с позицией, что выводы эксперта не должны соотноситься с иными доказательствами. Во-первых, для следователя/суда, как для не носителя специальных знаний, это является одним из способов проверки правильности выводов, изложенных в заключении эксперта. Во-вторых, эксперт может выполнить исследование в полном объеме, ход исследования будет им четко изложен, а выводы аргументированы, но это не исключает возможных допущенных экспертных ошибок.

Справедливо в этой связи высказывание А. Н. Петрухиной о том, что, если выводы эксперта вполне обоснованы проведённым им исследованием, это ещё не

---

[211] Кудрявцев Ю. С. Об оценке экспертного… С. 104.
[212] Кудрявцев Ю. С. Об оценке экспертного... С. 105.

означает достоверности заключения эксперта, так как выводы эксперта могут противоречить другим доказательствам[213].

В случае, если результаты экспертизы противоречат иным доказательствам, правоприменитель должен более тщательно подойти к оценке заключения эксперта, например, путем получения заключения специалиста. В-третьих, оценка с этой точки зрения может навести следователя/суд на мысль о вероятности недостоверности других доказательств. Так, лицо в своих показаниях может отрицать связь с подозреваемым, но результаты судебной компьютерно-технической экспертизы покажут, что IP-адрес, с которого происходила покупка наркотических средств, принадлежит именно этому лицу.

Оценка оформления заключения эксперта необходима для проверки соответствия заключения требованиям, установленным законодательством. И при этом оценка оформления заключения эксперта в меньшей степени способствует определению достоверности и научной обоснованности выводов эксперта, как на то указывает Ю. С. Кудрявцев.

Учитывая тот факт, что к заключению эксперта применяются все те же общие нормы и требования, как и ко всем доказательствам, считаем, что при оценке заключения эксперта необходимо руководствоваться такими понятиями, как допустимость, достоверность, относимость и полнота.

Каждому из этих свойств присущи конкретные критерии, которые должны оцениваться следователем и судом.

Допустимость заключения эксперта предполагает проверку соблюдения требований закона не только при назначении экспертизы, как писала Е. Р. Россинская, но и при производстве судебной экспертизы.

Правоприменитель должен обращать свое внимание на то, не собирал ли эксперт самостоятельно объекты и сравнительные образцы для исследования. В случае, когда объектом исследования выступают цифровые следы, данный вопрос

---

[213] Петрухина А. Н. Заключение эксперта и его оценка в уголовном процессе: Автореф. дис. … канд. юрид. наук. М., 2012, с. 10.

становится еще более актуальным. Нередко, например, эксперты-лингвисты, исследуя речевой продукт веб-сайт, переходят на имеющиеся там гиперссылки и проводят анализ их содержания, что является грубой экспертной ошибкой.

Если заключение эксперта было проведено по объектам, полученным с нарушением законодательства, оно априори не может быть использовано в качестве доказательства.

Наглядно демонстрирует важность оценки на первоначальном этапе критерия допустимости следующий кейс из судебной практики:

Адвокатом в защиту осужденной была подана кассационная жалоба на приговор Ломоносовского районного суда г. Архангельска и на апелляционное определение судебной коллегии по уголовным делам Архангельского областного суда. Гражданка Л. была признана виновной в совершении преступления, предусмотренного ч. 3 ст. 30 и п. п. "а", "г" ч. 4 ст. 228.1 УК РФ. Еще в рамках рассмотрения дела в суде первой инстанции сторона защиты указывала о недопустимости отдельных доказательств, но суд, по мнению защиты, проигнорировал данный факт. В частности, «в постановлении о назначении компьютерной судебной экспертизы, заключении эксперта, протоколе осмотра предметов, протоколе допроса эксперта, постановлении о признании и приобщении к уголовному делу вещественных доказательств, а также в тексте приговора приводится различное наименование изъятого телефона»[214].

Кассационная жалоба, как и апелляционная жалоба ранее, осталась без удовлетворения. Но все же нельзя обойти стороной то обстоятельство, что данные изъятого объекта различаются в разных процессуальных документах. Суду в таком случае необходимо установить, в чем заключаются данные различия и насколько они существенны: если различие состоит лишь в разном написании наименования (на русском в одном документе, на английском – в другом), то это не может стать причиной признания доказательства недопустимым. Если же отличаются марки,

[214] Кассационное определение Третьего кассационного суда общей юрисдикции от 17.10.2024 N 77-2226/2024 (УИД 29RS0014-01-2023-003613-30) // СПС «Консультант Плюс».

например, телефона, его свойства и иные данные, то такое доказательство не может быть принято судом.

Именно поэтому критерий допустимости должен оцениваться уполномоченным на то лицом в первую очередь.

После этого следует перейти к оценке достоверности заключения эксперта, которая включает в себя: проверку соответствия направленных на экспертизу объектов и исследованных по итогу объектов; оценку использованной при исследовании экспертной методики (ее научной обоснованности и актуальности), оценку примененных методов, а также оценку аргументации и логической обоснованности результатов эксперта.

Данный критерий является наиболее сложным для оценки заключения эксперта правоприменителем, так как предполагает оценку с научной точки зрения.

Следователь или судья, как уже было сказано, на основании своего опыта и навыков могут самостоятельно оценить обоснованность исследования, определить, насколько логично эксперт излагает доводы и результаты.

Именно для этого язык эксперта должен быть понятным. Это означает, что эксперт, прибегая к специальной терминологии, все равно должен обосновывать свои выводы таким образом, чтобы люди, не обладающие специальными знаниями, могли бы разобраться в изложенном и четко понять всю суть заключения эксперта. Для достижения этой цели эксперт также должен прибегать к иллюстрированию хода исследования.

Например, для судебной лингвистической и судебной автороведческой экспертиз эксперты могут использовать маркировку текста, его частей, слов для обозначения тех или иных явлений. Для судебной компьютерно-технической экспертизы эксперты могут фиксировать свои действия с помощью скриншотов и т.п.

Точная оценка заключения эксперта зависит не только от лица, проводящего эту оценку, но и от организации и оформления исследования самим экспертом.

И все же, судебные экспертизы, проводимые в рамках расследования дел, связанных с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях, отличаются чаще всего своей сложностью.

Анализ практики показывает, что в действительности, у следователя или судьи периодически возникают трудности при оценке экспертиз. Однако в этом случае предусмотрена возможность либо допросить эксперта по возникшим вопросам, либо привлечь к участию специалиста.

Согласно Постановлению Пленума ВАС РФ от 04.04.2014 № 23 «О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе», «для оказания содействия суду в уяснении вопросов, требующих специальных знаний, в том числе возникающих при исследовании заключения эксперта, суд может привлечь специалиста»[215].

Специалист оказывает помощь суду или следователю при осуществлении ими оценки заключения эксперта. Специалист не может оценивать заключение эксперта с точки зрения сущности проведенного исследования и полученных экспертом результатов, поскольку сделать это не представляется возможным без проведения исследование. Если же наделить специалиста такими полномочиями, то понятие повторной экспертизы потеряет свой смысл. Эксперта от специалиста отличает уголовная ответственность за заведомо ложное заключение. Исследовательская деятельность специалиста по всем параметрам сводится к деятельности эксперта.

Поэтому правоприменитель в зависимости от возникших потребностей должен различать привлечение специалиста и назначение повторной экспертизы.

Как отмечается в Постановлении Пленума Верховного суда РФ от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)», «специалист высказывает свое суждение по заданным ему вопросам как в устном виде, что

---

[215] Постановление Пленума ВАС РФ от 04.04.2014 N 23 "О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе" // СПС «Консультант Плюс».

отражается в протоколе судебного заседания, так и в виде заключения, которое приобщается к материалам дела»[216].

Согласно ч.2 ст.74 УПК РФ заключение специалиста является отдельным доказательством, не подменяющим заключение эксперта.

Как на то указывает А. М. Зинин, «заключению специалиста свойственны некоторые элементы экспертного процесса, ряд его этапов, в том числе таких, как осмотр и предварительное изучение объектов, выявление их признаков, анализ этих признаков путем применения необходимых в данной ситуации методик и формирование выводов. Однако он не может проводить углубленное исследование объектов, осуществлять эксперименты, что характерно для экспертизы»[217].

Тем не менее С. Б. Россинский верно указывает на то, что «не следует отождествлять заключение специалиста с короткой справкой. Оно может быть достаточно аргументированным и зачастую предполагает изложение специалистом подробной аргументации своего суждения»[218].

Вопрос оценки следователями, судьями научной, логической обоснованности заключения, использованных методов и методик подтверждает очередной раз необходимость унификации и стандартизации экспертных методик. С одной стороны, следователи, судьи смогут опираться при оценке на установленные стандарты, и с другой стороны, это будет способствовать повышению качества заключений экспертов.

Если критерий допустимости оценивается на отдельной стадии, то оценку достоверности и полноты заключения эксперта трудно отделить друг от друга, эти критерии рассматриваются параллельно.

---

[216] Постановлении Пленума Верховного суда РФ от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» // СПС «Консультант Плюс».

[217] Зинин А. М. Заключение специалиста: сущность, содержание и форма / А. М. Зинин // Вестник Университета имени О.Е. Кутафина (МГЮА). 2016. № 8(24). С. 34.

[218] Россинский С. Б. Уголовный процесс: учебник / С. Б. Россинский. — М. : Эксмо, 2009. С. 235.

Оценка полноты заключения эксперта подразумевает проверку факта исследования всех представленных перед экспертом объектов, а также факта исследования по всем поставленным перед экспертом вопросам.

Соответственно сперва необходимо удостовериться в том, что вопросы, указанные в постановлении (определении) о назначении судебной экспертизы, совпадают с теми, на которые эксперт давал ответы.

При оценке полноты исследования правоприменитель должен обращать внимание не только на то, все ли вопросы отражены в заключении и все ли объекты исследованы, но и на то, не было ли исследовано ничего лишнего.

Одна из экспертных ошибок связана с переформулированием самим экспертом вопросов, поставленных перед ним. Даже если вопросы составлены с ошибками, но при этом поставленные задачи входят в компетенцию эксперта, то в заключении они должны быть отражены без искажения смысла.

Однако, «если при производстве экспертизы эксперт по своей инициативе установит обстоятельства, имеющие значение для дела, по поводу которых ему не были поставлены вопросы, он должен указать их в своем заключении»[219]. Экспертная инициатива – важная составляющая деятельности судебного эксперта.

У лиц, назначающих экспертизу, не всегда есть объективные и субъективные возможности определить полный объем вопросов, подлежащих исследованию. И в таком случае эксперт в рамках экспертной инициативы может дать ответы на дополнительные вопросы.

Важно оговориться, что, как указывает на то С. Л. Мельник, «экспертная инициатива может иметь место лишь в отношении объектов, указанных в постановлении о назначении экспертизы»[220].

Что касается исследования дополнительных объектов, то экспертная инициатива работает в несколько ином ключе. Если эксперт усматривает

---

[219] Зайцева Е. А. Концепция развития института судебной экспертизы в условиях состязательного уголовного судопроизводства. Монография. М.: Юрлитинформ, 2010. С. 197.

[220] Мельник С. Л. О границах экспертной инициативы // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2017. № 2 (48). С. 20–22.

необходимость в дополнительных материалах, он должен заявить об этом лицу, назначившему экспертизу. Самостоятельно собирать объекты, ссылаясь на экспертную инициативу, эксперт не имеет права.

Разграничение экспертной инициативы и факта выхода эксперта за пределы компетенции – необходимый навык при оценке заключения эксперта.

Рассмотрим пример из практики. Следователем было вынесено постановление о назначении судебной-компьютерно-технической экспертизы с постановкой перед экспертом вопроса: *К какому типу относятся выявленные данные (текстовые, графические, база данных, электронная таблица, мультимедиа и др.) в мобильном телефоне марки Xiaomi?*

Эксперт, естественно, перед началом производства экспертизы ознакомился с постановлением о назначении ему экспертизы, откуда установил, что экспертиза назначена в рамках расследования уголовного дела по ст. 228.1 УК РФ.

При проведении исследования эксперт обнаружил, что в текстовой информации присутствуют ключевые слова, относящиеся к обсуждению наркотических средств, «наркота», «доза», и решил, что эти обстоятельства являются значимыми для дела и касаются непосредственно объекта исследования, соответственно, это также необходимо указать в своем заключении.

Очевидно, что в рассматриваемом случае эксперт допустил ошибку, обосновав свои действия экспертной инициативой, и зашел в компетенцию эксперта-лингвиста.

Экспертная инициатива, конечно же, не сводится исключительно к вопросу объема исследования и объектов, однако в разрезе рассматриваемой проблемы, именно эти формы реализации представляют наибольший интерес.

Так, экспертная ошибка, связанная с выходом эксперта за рамки своих компетенций, в конкретном уголовном деле стала одной из причин для апелляционной, а затем и кассационной жалобы.

В рамках расследования дела была назначена судебная компьютерно-техническая экспертиза, результаты которой в дальнейшем суд использовал для обоснования своих выводов.

Однако в данном заключении эксперт после обнаружения переписки-диалогов пришел к выводу, что владелец аккаунта (аккаунт принадлежал осужденному) занимался размещение "кладов" (тайников с наркотическими веществами) на территории города.

Мало того, что исследования относительно смысла текста не относится к компетенции эксперта в области компьютерно-технической экспертизы, так еще эксперт в своих формулировках дал юридическую оценку действий осужденного.

Сам суд первой инстанции в мотивировочной части ссылался именно на эти выводы эксперта.

Совершенно справедливо кассационная жалоба была в этой части была удовлетворена, и судебной коллегией принято решение «исключить из описательно-мотивировочной части приговора указание на заключение компьютерной судебной экспертизы N 177-2021 от 24 августа 2021 г. в той части, в которой содержатся выводы эксперта об обнаружении переписки-диалогов, из которых следует, что владелец аккаунта (Р.Д.А.) занимался размещением «кладов» (тайников с наркотическими веществами) на территории города, и ссылки на указанное заключение эксперта, как на доказательства виновности осужденного»[221].

Неспособность суда на определенном этапе оценить достоверность заключения эксперта в конечном итоге приводит к затягиваю и усложнению всего процесса.

Разграничение экспертной инициативы и выхода эксперта за рамки компетенции в общем виде можно представить следующим образом:

[221] Кассационное определение Седьмого кассационного суда общей юрисдикции от 06.12.2022 N 77-5773/2022 // СПС «Консультант Плюс».

Таблица 4. Разграничение экспертной инициативы и выхода эксперта за рамки компетенции

Выход эксперта за пределы компетенции	**Экспертная инициатива**
Исследование по вопросам, не поставленным перед экспертом	Установление фактов и их отражение в заключении, по которым не ставился вопрос, но которые имеют значение для дела и напрямую относятся к объекту исследования
Редактирование вопросов с изменением их смысловое содержание и объема исследования	Редактирование вопросов без изменения их сущности
Исследование по вопросам, выходящим за рамки компетенции конкретного эксперта	Заявление ходатайства о предоставлении дополнительного материала для исследования
Самостоятельный отбор объектов исследования	

И наконец, последнее, что необходимо оценивать относительно заключения эксперта – относимость. В понятие относимости включается проверка соответствия выводов эксперта имеющимся по делу доказательствам и проверка относимости результатов экспертного исследования к конкретному уголовному делу.

Но для того, чтобы следователь или суд могли оценивать заключения экспертов, у них должны быть определенные инструменты для этого.

С. В. Хомутов в этой связи выделяет процессуальные и непроцессуальные формы оценки заключения эксперта.

К процессуальным С. В. Хомутов относит следующие:

– «оценка заключения эксперта следователем (судом), в том числе используя право присутствия следователя при производстве судебной экспертизы и получения разъяснений эксперта по поводку проводимых им действий (ст. 197 УПК РФ);

– оценка заключения эксперта путем сопоставления с другими доказательствами по делу;

– допрос эксперта, проводившего судебную экспертизу»[222].

Среди непроцессуальных форм автор выделяет следующие:

[222] Хомутов С. В. По вопросу различных подходов к оценке заключения эксперта / С. В. Хомутов // Вестник Восточно-Сибирского института МВД России. 2019. № 1(88). С. 268.

– «оценка заключения эксперта членами комиссии при проведении комиссионных, комплексных экспертиз;

– оценка заключения эксперта в ходе беседы следователя и эксперта, проводившего экспертизу;

– оценка заключения эксперта руководителем судебно-экспертной организации;

– оценка заключения эксперта коллегами того же экспертного коллектива;

– рецензирование заключения эксперта (внутри коллектива и вне коллектива);

– оценка заключения эксперта самим экспертом, проводившим экспертизу»[223].

Прежде всего отметим, что выделенные выше пункты все же представляют собой инструменты для оценки заключения эксперта, а не формы его оценки. Поэтому нами предлагается в дальнейшем использовать понятие «способы оценки заключения эксперта».

Далее остановимся подробнее на отдельных способах оценки, выделенных С. В. Хомутовым. Первый способ процессуальной оценки вызывает некоторые вопросы. По сути, когда следователь присутствует при производстве судебной экспертизы, он никак не может оценить заключение эксперта, потому что его еще нет. Следователь может наблюдать за ходом исследования, получать соответствующие разъяснения, но эти действия не связаны с оценкой заключения эксперта, в связи с чем, представляется некорректным выделения данного права следователя как формы оценки.

Оценка заключения эксперта путем сопоставления с другими доказательствами по делу, скорее, является не отдельной формой, а стадией оценки заключения эксперта.

---

[223] Хомутов С. В. По вопросу различных подходов… С. 268.

Оценка заключения эксперта в ходе беседы следователя и эксперта, проводившего экспертизу, дублирует такой способ оценки, как допрос эксперта. Коммуникация эксперта и следователя вне рамок, установленных законом, по сути, нарушает обязанность эксперта не вступать в личные контакты с участниками процесса. Следователь может обратиться к специалисту за получением консультации при оценке заключения, но никак не к эксперту.

Не очень ясно также, что автор подразумевает под рецензированием заключения как внутри, так и вне коллектива, а также оценка заключения другими сотрудниками экспертного учреждения. Очевидно, что сюда не включаются случаи рецензирования собственно экспертами, проводившими комиссионную или комплексную экспертизу (этот способ выделен отдельно). Тогда возникает вопрос, как эксперт, который не привлекался для производства экспертизы, может вносить корректировки и рецензировать заключение.

В целом выделенные непроцессуальные способы оценки в своем большинстве направлены на оценку заключения либо самим экспертом, либо иными сотрудниками экспертного учреждения. А как уже ранее нами отмечалось, единственным субъектом, наделенным правом оценки заключения эксперта, является суд и следователь. Соответственно, такая классификация способов оценки заключения эксперта противоречит действующему законодательству РФ. В связи с этим мы считаем нецелесообразным разделение способов оценки заключения эксперта на процессуальные и непроцессуальные.

Обобщая все вышесказанного, предлагаем рассматривать следующие способы оценки заключения эксперта.

– оценка заключения эксперта следователем (судом) через проверку соответствия его критериям допустимости, достоверности, полноты и относимости;

– допрос эксперта, проводившего судебную экспертизу;

– привлечение специалиста для оказания консультационной помощи при оценке заключения эксперта.

Важность использования результатов судебных экспертиз при рассмотрении дел, связанных с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях, уже не раз обозначалась в нашем диссертационном исследовании.

Обоснованные результаты экспертного исследования при их грамотной оценке и использовании нередко ложатся в основу выводов суда, излагаемых непосредственно в приговоре.

Значение заключения эксперта можно доказать также от обратного. Несвоевременное назначение судебной экспертизы и неиспользование результатов заключения эксперта могут стать причиной дальнейшего спора между сторонами.

Так, в 2023 г. гражданин П.А.В. был признан Ленинским районным судом г. Екатеринбурга виновным в покушении на незаконный сбыт аналога наркотического средства в крупном размере, совершенном с использованием информационно-телекоммуникационных сетей (включая сеть Интернет), группой лиц по предварительному сговору.

Однако после вынесения приговора адвокатом осужденного была подана апелляционная жалоба, а затем уже кассационная жалоба. Наряду со всеми доводами, защитник указал, что суд первой инстанции вынес приговор, основываясь на предположениях домыслах, так как ввиду неназначения лингвистической экспертизы не были установлены сведения, действительно ли в смс-сообщениях есть информация о том, как добывались наркотические средства и какова была их масса, о сбыте наркотических средств.

Помимо этого, не было доказано посредством получения результатов судебной компьютерно-технической экспертизы, действительно ли интернет-магазин, через который осуществлялся незаконный оборот наркотиков, был создан и использовался П.А.В., а также не установлены лица, которые передавали друг другу смс-сообщения[224].

---

[224] Кассационное определение Седьмого кассационного суда общей юрисдикции от 11.04.2024 N 77-1014/2024 (УИД 66RS0004-01-2021-014213-07) // СПС «Консультант Плюс».

Сложные дела, в особенности дела, связанные с использованием информационно-телекоммуникационных средств, где задействована группа лиц требуют более всестороннего подхода в получении доказательственной базы.

Результаты судебных экспертиз наряду с другими доказательствами способствуют установлению истины по каждому уголовному делу. Правоприменитель при расследовании конкретного уголовного дела может считать, что назначение судебной экспертизы лишь затянет процесс, и необходимость в ней не так высока. Однако, как это усматривается из анализа практики, такой подход в дальнейшем и приводит к затягиванию процесса ввиду недоказанности (недостаточной доказанности) всех обстоятельств дела.

Заключение

В рамках диссертационного исследования были рассмотрены основные проблемы, возникающие при расследовании незаконного оборота наркотических средств в компьютерных сетях.

С переходом преступной деятельности в онлайн-пространство изменилась сама криминалистическая характеристика преступлений. Для компьютерных преступлений стало более актуальным их рассмотрение с точки зрения типовой информационной модели преступления, поскольку данные преступления отличаются от «традиционных» преступлений.

Преступления незаконного оборота наркотических средств с использованием информационно-телекоммуникационных сетей претерпели значительные изменения в области способов преступления. Установлены новые способы незаконного оборота наркотических средств в компьютерных сетях, включающие в себя: распространение информации о наркотических средствах в социальных сетях и мессенджерах; использование мессенджера Телеграм для приискания соучастников преступления, для поиска самих наркотических средств, привлечения покупателей, планирования преступления; создание торговых площадок в теневом сегменте Даркнет, а также; использование Даркнета с целью реализации приватной коммуникации; использование маркетплейсов с целью сбыта наркотических средств; использование криптовалют, виртуальных валют для оплаты заказов наркотических средств; использование технологий шифрования, обеспечивающих высокий уровень конфиденциальности.

Помимо этого, изменилась характеристика личности преступников: использование информационно-телекоммуникационных сетей требует определенного (зачастую высокого) уровня владения технологиями. Данный уровень зависит от ряда факторов, которые необходимо учитывать при расследовании преступлений. Анализ компьютерных навыков личности преступника способствует выявлению участников преступлений, выполняющих

новые функции в рамках незаконного оборота наркотических средств в компьютерных в сетях: кадровики, кураторы, диспетчеры, дропы (дропперы), коллекторы.

В конечном итоге трансформации, связанные с использованием компьютерных технологий в преступной деятельности, привели к появлению цифровых следов и изменению механизма их следообразования. В рамках настоящего исследования цифровые следы рассматриваются в качестве объектов судебных экспертиз. Однако направлению цифровых следов на экспертное исследование предшествует стадия их собирания.

От качества проведенной работы на стадии собирания цифровых следов зависит течение дальнейшего процесса, в том числе производства судебных экспертиз. Поэтому на данном этапе важно учитывать ряд аспектов, направленных на обеспечение сохранности цифровых следов, а именно:

– общие особенности цифровых следов;

– особенности носителей цифровых следов (в зависимости от вида материального носителя будут отличаться способы изъятия, упаковки и передачи для исследования самих носителей. Халатное, формальное отношение может привести к утрате значимой для дела информации);

– особенности конкретного проводимого следственного действия каждому следственному действию присущи собственные характерные черты, на основании которых должна выстраиваться тактика собирания цифровых следов (например, осмотр места происшествия требует большей оперативности, чем обыск или выемка);

– особенности отдельных видов цифровых следов (различные виды цифровых следов требуют использования определенных технологий и подходов при их собирании, изъятии и фиксации).

Преступления, совершаемые с использованием компьютерных технологий, отличаются друг от друга по фигурирующим в них видам цифровых следов. В связи

с этим следователям необходимо при собирании цифровых следов в рамках расследования наркопреступлений следует учитывать их классификацию.

Представляется, что для преступлений, связанных с незаконным оборотом наркотических средств, классификация в зависимости от направленности действий лица в компьютерных сетях выглядит следующим образом:

1. Активные цифровые следы: сообщения в социальных сетях и мессенджерах; публикации в социальных сетях и Телеграм-каналах; комментарии в социальных сетях, Телеграм-каналах, онлайн-форумах; поисковые запросы в сети Интернет и теневом сегменте Даркнет; данные о совершенных транзакциях; фото-, видео-, аудиоматериалы; электронные документы; активность в приложениях и программах; облачное хранилище данных.

2. Пассивные цифровые следы: GPS-данные; история браузера; куки-файлы; кэш браузера; метаданные файлов; данные IP-адреса.

Все вышесказанное определяет особенности назначения судебной экспертизы в ходе расследования преступлений, связанных с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях:

– *Обусловленные объектами исследования, их материальными носителями и экспертными задачами:* следует подробно описывать вид материального носителю и информацию, которая содержится на нем; предоставлять эксперту информацию о способах и технологиях изъятия цифровых следов; учитывать род назначаемой экспертизы при определении способа и формата предоставления объектов исследования эксперту.

– *Обусловленные необходимостью назначения комплекса экспертиз, комплексной экспертизы, комиссионной экспертизы:* следует определять необходимость назначения комплексной/комиссионной экспертизы или комплекса экспертиз; определять очередность производства судебных экспертиз при назначении комплекса экспертиз.

Однако для того, чтобы в практической деятельности можно было учесть все особенности, необходимо расширять сферу компетенций сотрудников

правоохранительных органов путем внедрения в их обучение разделов, посвященных цифровым следам в целом, цифровым следам как объектам судебной экспертизы и цифровым следам как цифровым доказательствам.

Под влиянием цифровых следов претерпели трансформацию судебная экспертология (в частности, сформировалось учение о цифровизации судебно-экспертной деятельности) и сами судебные экспертизы. Анализ экспертной практики демонстрирует появление новых родов, видов судебных экспертиз, а также изменения в области объектов, задач, методов, средств исследования в уже устоявшихся судебных экспертизах. По этой причине компетенция судебного эксперта должна быть расширена, а подходы к обучению судебных экспертов должны быть скорректированы с учетом особенностей расследования незаконного оборота наркотических средств в компьютерных сетях.

Компетенция судебного эксперта при производстве различных родов/видов судебных экспертиз в рамках дел незаконного оборота наркотических средств должна включать в себя: знание судебной экспертологии, теории цифровизации судебно-экспертной деятельности, знание о специфике конкретных видов цифровых следов, знание о механизме следообразования цифровых следов, умение применять в исследовании и интегрировать в экспертные методики компьютерные технологии, IT-технологии, владение современными базами данных, а также знание методик, решающих задачи, возникающие в рамках расследования незаконного оборота наркотических средств в компьютерных сетях.

Во всех рассмотренных в исследовании судебных экспертизах методики являются устаревшими (в частности, не учитывают трансформации механизма следообразования цифровых следов).

Методики судебной компьютерно-технической экспертизы направлены на исследование тех цифровых следов, которые по большей мере уже неактуальны. Методики судебной лингвистической и судебной автороведческой экспертиз не охватывают особенности текстов Интернет-коммуникации, вследствие чего на практике возникают трудности при исследовании таких объектов.

Для расследования незаконного оборота наркотических средств и формирования доказательственной базы перечисленные судебные экспертизы имеют существенное значение. Возможности судебной компьютерно-технической экспертизы потенциально позволяют решать задачи по деанонимизации пользователей Tor, судебной лингвистической экспертизы – определять факт наличия/отсутствия высказываний наркотического дискурса, устанавливать роли и иерархию участников группы, а в результате производства судебной автороведческой экспертизы можно получить информацию о причастности того или иного лица к публикуемому наркоконтенту.

– Такого рода исследования проводятся на данный момент, но отсутствие стандартизированного и единого методического обеспечения зачастую приводит к экспертным ошибкам, выявляемым уже в последующих этапах расследования и рассмотрения уголовного дела, а именно при оценке заключения эксперта. В целом судебно-экспертные технологии производства экспертиз по делам, связанным с незаконным оборотом наркотических средств в информационно-телекоммуникационных сетях, необходимо совершенствовать путем: обобщения экспертной практики в результате совместной деятельности экспертов как государственных, так и негосударственных экспертных учреждений (создание общих баз данных по каждому роду/виду судебных экспертиз, проводящих исследования в рамках расследования незаконного оборота наркотических средств в компьютерных сетях); внедрения современных технологий и методов в экспертные исследования (адаптация технологий по деанонимизации пользователей Tor в исследования судебной компьютерно-технической экспертизы); обновления экспертных методик; создание общих стандартов для всего экспертного сообщества в части внесения положений об особенностях механизма следообразования цифровых следов и особенностях исследования конкретных видов цифровых следов, образованных в ходе незаконного оборота наркотических средств; мониторинга изменений в способах преступлений, связанных с незаконным оборотом наркотических средств, и анализ их влияния на технологии экспертного исследования.

Вместе с тем для обеспечения эффективного применения результатов судебно-экспертного исследования заключение эксперта должно пройти стадию оценки.

– Оценка заключения эксперта – сложный процесс ввиду того, что охватывает целый комплекс аспектов, которые должны быть рассмотрены и оценены уполномоченным лицом. Так как заключение эксперта занимает равное положение наряду с остальными доказательствами, то оно должно оцениваться следователем, судом с точки зрения допустимости, достоверности, полноты и относимости. Именно данные критерии позволяют объективно и всесторонне оценить результаты экспертного исследования лицам, не обладающим специальными знаниями. Следует иметь в виду то, что следователь, суд может обратиться к специалисту за консультацией в части проверки научной обоснованности примененных методов, методик и т.д., но не за самой оценкой заключения. При этом сам правоприменитель должен обладать определенными знаниями о цифровых следах для осуществления этапа оценки заключения эксперта. Этим подчеркивается необходимость изменения и расширения компетенции следователя, суда в сфере цифровых следов путем изучения вопросов: механизма следообразования цифровых следов; особенностей исследования цифровых следов, образованных в ходе незаконного оборота наркотических средств; возможностей использования IT-технологий и их интеграция в экспертные методики в рамках расследования незаконного оборота наркотических средств; особенностей представления результатов судебной экспертизы, назначенной в рамках расследования незаконного оборота наркотических средств.

Таким образом производство различных родов и видов судебных экспертиз в рамках расследования незаконного оборота наркотических средств, совершенного с использованием компьютерных технологий, позволяют получить значимые для дела сведения. Как показал анализ следственной и судебной практики, часто возникают ситуации, когда в рамках одного уголовного дела нельзя обойтись без назначения целого комплекса экспертиз либо комплексной экспертизы.

Список использованных источников и литературы

Законодательство, нормативные правовые акты

1. Конституция Российской Федерации 12 дек. 1993 г. [Электронный ресурс] (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020.) – Доступ из справ.-правовой системы «КонсультантПлюс». – Текст: электронный.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ [Электронный ресурс]: принят Гос. Думой Федер. Собр. РФ 22 нояб. 2001 г.: одобр. Советом Федерации Федер. Собр. РФ 05 дек. 2001 г.: офиц. текст: по состоянию на 28 дек. 2024 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

3. Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ (с изм. и доп., вступ. в силу с 01 янв. 2025 г.) [Электронный ресурс]: принят Гос. Думой Федер. Собр. РФ 20 дек. 2001 г.: одобр. Советом Федерации Федер. Собр. РФ 26 дек. 2001 г.: офиц. текст: по состоянию на 01 янв. 2025 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп., вступ. в силу с 08 янв. 2025 г.) [Электронный ресурс]: принят Гос. Думой Федер. Собр. РФ 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. РФ 05 июня 1996 г.: офиц. текст: по состоянию на 08 янв. 2025 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

5. О государственной судебно-экспертной деятельности в Российской Федерации от 31 мая 2001 г. № 73-ФЗ [Электронный ресурс]: принят Гос. Думой Федер. Собр. РФ 05 апр. 2001 г.: одобр. Советом Федерации Федер. Собр. РФ 16 мая 2001 г.: офиц. текст: по состоянию на 08 янв. 2025 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

6. Приказ Министерства внутренних дел Российской Федерации от 29.06.2005 (в действующей редакции) № 511 «Вопросы организации производства

судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» – Доступ из справ.-правовой системы «КонсультантПлюс».

7. Приказ Министерства труда и социальной защиты Российской Федерации от 23 марта 2015 г. № 183н «Об утверждении профессионального стандарта «следователь-криминалист». – Доступ из справ.-правовой системы «КонсультантПлюс».

8. Приказ Министерства юстиции РФ от 20.04.2023 (в действующей редакции) № 72 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз – Доступ из справ.-правовой системы «КонсультантПлюс».

9. Приказ Следственного комитета РФ от 24.07.2020 (в действующей редакции) № 77 «Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения Судебно-экспертный центр Следственного комитета РФ на право самостоятельного производства судебных экспертиз» – Доступ из справ.-правовой системы «КонсультантПлюс».

10. Приказ ФСБ России от 23.06.2011 (в действующей редакции) № 277 "Об организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности" (вместе с "Инструкцией по организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности") (Зарегистрировано в Минюсте России 06.09.2011 N 21744) – Доступ из справ.-правовой системы «КонсультантПлюс».

11. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) "Об информации, информационных технологиях и о защите информации". URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 07.02.2024).

Акты высших судебных инстанций

12. Постановление Пленума ВАС РФ от 04.04.2014 N 23 "О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе" // СПС «Консультант Плюс».

13. Постановление Пленума Верховного Суда РФ от 15.06.2006 N 14 (ред. от 16.05.2017) "О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами"// СПС «Консультант Плюс»

14. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" // СПС «Консультант Плюс»

15. Постановление Пленума Верховного Суда РФ от 21.12.2010 N 28 (ред. от 29.06.2021) "О судебной экспертизе по уголовным делам" // СПС «КонсультантПлюс».

16. Постановлении Пленума Верховного суда РФ от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» // СПС «Консультант Плюс».

Словари и энциклопедии

17. Белкин Р. С. Криминалистическая энциклопедия. – М.: БЕК, 1997. – 342 с.

18. Большой толковый словарь русского языка / гл. ред. С. А. Кузнецов. – Москва: Рипол классик, 2008. – URL: https://gufo.me/dict/kuznetsov/электронный (дата обращения: 07.03.2024).

19. Наркоманский словарь Баяна Ширянова – URL: http://imperium.lenin.ru/EOWN/eown7/dictionary/dictionary.html (дата обращения: 15.01.2024).

20. Ожегов С. И. Толковый словарь русского языка: 80000 слов и фразеол. выражений / С. И. Ожегов, Н. Ю. Шведова. Ин-т рус. яз. им. В. В. Виноградова. – 4-е изд., доп. – Москва: Азбуковник, 2003 г. – URL: https://gufo.me/dict/ozhegov/совершить (дата обращения: 07.02.2024).

Монографии, книги, учебники и учебные и научно-практические пособия

21. Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р. Криминалистика. Учебник для вузов. 4-е изд., переработанное и доп. – М.: Норма-ИНФРА-М, 2014. – 928 с.

22. Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. – М.: Юрид. лит., 1987. – 270 с.

23. Белкин Р. С. Курс криминалистики. – М., ЮНИТИ-ДАНА, Закон и право. 2001. – 837 с.

24. Белкин Р. С., Винберг А. И., Дорохов В. Я., Карнеева Л. М. и др. Теория доказательств в советском уголовном процессе. – М.: Юридическая литература, 1973. – 736 с.

25. Возгрин И. А. Научные основы криминалистической методики расследования преступлений. Часть IV. – СПб: Санкт-Петербургский юридический институт МВД России, 1993. – 79 с.

26. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2009. – 485 с.

27. Вул С. М. Судебно-автороведческая идентификационная экспертиза: методические основы: методическое пособие. – Харьков: ХНИИСЭ, 2007. – 64 с.

28. Галяшина Е. И. Судебная лингвистическая экспертиза: учебник / Е. И. Галяшина. – Москва: Общество с ограниченной ответственностью "Проспект", 2025. – 424 с.

29. Галяшина Е. И. Судебное речеведение / Е. И. Галяшина. – Москва: Юридическое издательство "Норма", 2020. – 320 с.

30. Голощапова Т. И., Смирнов А. А., Полосина А. М., Курьянова И. В. Лингвистическая экспертиза текстов, в которых имеется информация, относящаяся к семантическому полю «наркотики»: методические рекомендации для экспертов, следователей, оперативных сотрудников / под ред. А. М. Черенкова. – М.: ЭКУ 9-го Департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, 2006. – 43 с.

31. Данилин А. Г. LSD. Галлюциногены, психоделия и феномен зависимости – М.: ЗАО Изд-во Центрполиграф. 2001. – 521 с.

32. Ермакова О. П., Земская Е. А., Розина Р. И. // Источники пополнения и тематические группы жаргона. Слова, с которыми мы все встречались: Толковый словарь русского общего жаргона: Ок. 450 слов. – М.: Азбуковник, 1999. – 320 с.

33. Ермолович В. Ф. Криминалистическая характеристика преступления. – Минск: «АМАЛФЕЯ», 2001. – 303с.

34. Зайцева Е. А. Концепция развития института судебной экспертизы в условиях состязательного уголовного судопроизводства. Монография. – М.: Юрлитинформ, 2010. – 416 с.

35. Зинин А. М., Майлис Н. П. Судебная экспертиза. – М., Право и закон; Юрайт-Издат, 2002. – 318 с.

36. Комплексная методика производства автороведческих экспертиз: Методические рекомендации / И. И. Рубцова, Е. И. Ермолова, А. И. Безрукова [и др.]. – М., 2007. – 192 с.

37. Криминалистика в 3 т. / под ред. Р. С. Белкина, В. Г. Коломацкого, И. М. Лузгина. – М.: Академия МВД России, Т. 1: История, общие и частные теории, 1995. – 278 с.

38. Кудрявцева А. В. Судебная экспертиза в уголовном процессе России. Монография / А. В. Кудрявцева; М-во образования Рос. Федерации. Южно-Урал. гос. ун-т. – Челябинск : Изд-во ЮУрГУ, 2001. – 411 с.

39. Лейбниц Г. Новые опыты о человеческом разумении автора системы предустановленной гармонии // Лейбниц Г. Сочинения. В 4 т., Т.2 – М., 1983. – 689 с.

40. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков – Издательство Воронежского государственного университета. 2002. – 408 с.

41. Настольная книга судьи: судебная экспертиза: теория и практика, типичные вопросы и нестандартные ситуации: монография / под ред. Е. Р. Россинской. – 2-е изд., перераб. и доп. – Москва: Проспект, 2024. – 448 с.

42. Общие положения по назначению и производству компьютерно-технической экспертизы: Метод. рекомендации / В. С. Зубаха, А. И. Усов, Г. В. Саенко [и др.]; М-во внутр. дел Рос. Федерации. Гос. учреждение "Эксперт.-криминалист. центр М-ва внутр. дел Рос. Федерации". – Москва: ГУ ЭКЦ МВД России, 2001. – 71 с.

43. Овсюков Д. А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: монография / под науч. ред. С. М. Кочои. – М.: Проспект, 2023. – 280 с.

44. Орлов Ю. К. Современные проблемы доказывания и использования специальных знаний в уголовном судопроизводстве: научно-учебное пособие. – М.: Проспект, 2017. – 217 с.

45. Подкатилина М. Л. Судебная лингвистическая экспертиза экстремистских материалов: монография / под ред. Е. И. Галяшиной. – М.: Юрлитинформ, 2013. – 180 с.

46. Ратинов А. Р. Обыск и выемка. – М.: Госюриздат, 1961. – 218 с.

47. Россинская Е. Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе: монография. – М.: Право и закон. 1996.

48. Россинская Е. Р., Галяшина Е. И., Зинин А. М. Теория судебной экспертизы: учебник / под ред. Е. Р. Россинской. – М.: Норма; ИНФРА-М, 2016. – 368 с.

49. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. – М.: Право и Закон, 2001. – 414 с.

50. Россинский С. Б. Следственные действия: монография. – М.: Норма, 2018. – 238 с.

51. Россинский С. Б. Уголовный процесс: учебник / С. Б. Россинский. – М.: Эксмо, 2009. – 735 с.

52. Саенко Г. В., Тушканова О.В. Компьютерная экспертиза. Типовые экспертные методики исследования вещественных доказательств. Ч. I / под ред. Ю.М. Дильдина; общ. ред. В.В. Мартынова. – М.: ЭКЦ МВД России, 2010.

53. Свон М. Блокчейн: Схема новой экономики. – М.: Олимп-бизнес. 2017. – 234 с.

54. Сорокин Ю.А. Креолизованные тексты и их коммуникативная функция // Оптимизация речевого воздействия / Ю.А. Сорокин. – М.: НиолаПресс, 1990. – 186 с.

55. Сорокотягин И.Н., Сорокотягина Д.А. Судебная экспертиза: учебник и практикум для бакалавриата и специалитета. – Москва: Юрайт, 2019. – 288 с.

56. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография / Е. Р. Россинская. — 4-е изд., перераб. и доп. – Москва: Норма: ИНФРА-М, 2024. – 576 с.

57. Судебная экспертиза: типичные ошибки: монография / Е. Р. Россинская, Н. Ф. Бодров, Е. И. Галяшина и др.; под ред. Е. Р. Россинской. – 2-е изд., перераб. и доп. – Москва: Проспект, 2024. – 736 с.

58. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под ред. Е.Р. Россинской – Москва: Проспект, 2023. – 256 с.

59. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А.И. Усов // Под ред. Е.Р. Россинской – М.: Издательство «Экзамен», издательство «Право и закон», 2003. – 368 с.

60. Хитина М. В. Делимитативные признаки устно-речевого дискурса. – М.: ООО Типография Сарма, 2004. – 157 с.

61. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под редакцией В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 490 с.

62. Maras Marie-Helen. Cybercriminology: Oxford University Press, 2016. – 448 p.

Статьи и тезисы докладов

63. Авдошин С. М. Методы деанонимизации пользователей Tor / С. М. Авдошин, А. В. Лазаренко // Информационные технологии. 2016. Т. 22, № 5. С. 362-372.

64. Аверьянова Т.В. Проблемы оценки достоверности заключения комплексного экспертного исследования // Вестник экономической безопасности. 2018. №1. С. 12-16.

65. Аминев Ф.Г. О проблемах формирования компетентности судебного эксперта в условиях цифровизации // Криминологический журнал. 2024. №1. С. 9-12.

66. Артемова Т. В., Катышев П. А., Оленев С. В., Паули Ю. С., Соколова С. К. Функции жаргона наркоманов и словообразовательные средства их осуществления (на материале социолингвистических опросов и словарей жаргона) Вестник Кемеровского государственного университета 2014 № 3 (59) Т. 3. С. 165-169.

67. Балаш М.А., Коряковцев А.В. Практика использования лингвистической экспертизы при доказывании совершения наркопреступлений группой лиц // Юрислингвистика. 2012. №1. С. 111-116.

68. Бахтеев Д. В. Криминалистические особенности производства процессуальных действий с цифровыми следами / Д. В. Бахтеев, Е. В. Смахтин // Российский юридический журнал. 2019. № 6(129). С. 61-68.

69. Беляков А. А. Следственные ошибки при назначении судебных экспертиз / А. А. Беляков, А. Д. Цветкова // Академический юридический журнал. – 2024. – Т. 25, № 1(95). – С. 124-132.

70. Бертовский Л.В. Технология Блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. №6. С. 226-230.

71. Бондаренко Ю.А., Кизилов Г.М. Проблемы выявления и использования следов преступлений, оставляемых в сети "Darknet" // Гуманитарные, социально-экономические и общественные науки. 2019. №5. С. 97-101.

72. Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143-155.

73. Варакин Я. Г. Криминалистические технологии обнаружения, фиксации, изъятия цифровых следов преступления и иной доказательной информации // Вестник Сургутского государственного университета. 2021. № 4. С. 81-87.

74. Васюков В. Ф. Некоторые вопросы проведения следственных действий, направленных на обнаружение, фиксацию и изъятие электронных сообщений, переданных посредством мобильных абонентских устройств сотовой связи // Российский следователь. 2016. № 23. С. 15–18.

75. Васюков, В. Ф. Некоторые особенности повышения квалификации следователей правоохранительных органов / В. Ф. Васюков, А. К. Шеметов // Правовая парадигма. – 2021. – Т. 20, № 2. – С. 100-106.

76. Винокуров В.Н., Агафонов А.В. Особенности квалификации сбыта наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право. 2023. № 1.

77. Воронин М. И. О правовой природе электронных (цифровых) доказательств // Вестник Университета имени О. Е. Кутафина. 2020. №10 (74). URL: https://cyberleninka.ru/article/n/o-pravovoy-prirode-elektronnyh-tsifrovyh-dokazatelstv (дата обращения: 20.03.2023).

78. Гаврилин Ю.В., Победкин А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России:

необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. 2018. № 3 (47). С. 106-114.

79. Галяшина Е. И. Речевые следы как объекты судебных экспертиз (в свете идей Р. С. Белкина) / Е. И. Галяшина // Современное развитие криминалистики и судебной экспертизы как реализация идей Р.С. Белкина: Материалы Международной научно-практической конференции «К 95-летию со дня рождения ученого, педагога, публициста», Москва, 22–23 ноября 2017 года. – Москва: Общество с ограниченной ответственностью "Проспект", 2018. С. 189-193.

80. Галяшина Е.И. Речеведческие экспертизы в судопроизводстве // Законы России: опыт, анализ, практика. 2011. № 12. С. 12-29.

81. Галяшина Е.И. Речеведческие экспертизы в судопроизводстве: насущные потребности, проблемы и пути их решения // Теория и практика судебной экспертизы. 2019. Том 14. № 4. С.6-18.

82. Григорьев В.Н., Максимов О.А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. Серия: Право. 2019. N 2. С. 33-44.

83. Громова А.В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник ВолГУ. Серия 2: Языкознание. 2021. №2. С. 87-98.

84. Гузин А.Р., Валиева Ю.М. Проблемы регламентации собирания электронной информации в действующем законодательстве // Juvenisscientia. 2017. № 1. С. 33-35.

85. Дерюгин Р.А., Жижелева А.А. Технологии XXI века в юриспруденции Материалы Всероссийской научно-практической конференции // под редакцией Д.В. Бахтеева. 2019. С. 40-46.

86. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. N 10. С. 109-115.

87. Дык Буй Минь, Хуи Нгуен Нгок, Линь Лай Тхи, Хю Нгуен Ба, Чыонг Нгуен Динь Принцип работы Tor-браузера // Проблемы Науки. 2017. №1 (83). С. 52-55.

88. Дьяконова О.Г., Иванова Е.В. Классификация судебных экспертиз: экспертологический подход //Теория и практика судебной экспертизы. 2022. Том 17. №2. С.75-82.

89. Евсеева С.А. Некоторые проблемы расследования преступлений в отношении несовершеннолетних киберпреступников // Вестник Уфимского юридического института МВД России. 2019. N 3 (85). С. 70-73.

90. Зайцев В. В. Цифровые технологии в криминалистике и судебной экспертизе / В. В. Зайцев // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2023. № 1(21). С. 8-13.

91. Замараева Н.А. Правовые и организационно-методические проблемы использования компьютерных технологий при производстве судебных экспертиз: дис. ... канд. юрид. наук. М., 2001. 202 с.

92. Зинин А. М. Заключение специалиста: сущность, содержание и форма / А. М. Зинин // Вестник Университета имени О.Е. Кутафина (МГЮА). 2016. № 8(24). С. 32-37.

93. Зиннуров Ф.К., Хайруллова Э.Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С 274-278.

94. Зиновьева Н.С. К вопросу о месте криптографии и стеганографии в криминалистической науке // Гуманитарные, социально-экономические и общественные науки. 2019. №2. С. 87-89.

95. Зуев С.В. IT-следователь в цифровой среде уголовного судопроизводства / С.В. Зуев, А.И. Зазулин // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 48-54.

96. Ищенко Е. П. Как наполнить фантом криминалистической характеристики преступлений реальным содержанием // Информационный бюллетень № 17 по материалам Криминалистических чтений «Научная состоятельность криминалистической характеристики преступлений». М., 2002.

97. Канатьев К.Н., Большаков В.Н., Анисимов А.Р., Скоморохина Е.Р., Чикенев С.Д. Анализ возможностей технологии Блокчейн в управлении данными, Инновации и инвестиции, № 5, 2023, С. 174-178.

98. Клоченко Л.Н. К вопросу об унификации терминологии, обозначающей психическое насилие, в уголовном праве // Российский следователь. 2013. № 9. С. 24 - 27.

99. Колдин В. Я., Ищенко Е. П. Типовая информационная модель преступления как основа методики расследования // Известия высших учебных заведений. Правоведение. № 6 (269). 2006. С. 128–144.

100. Колдин В.Я., Крестовников О.А. Судебно-экспертные науки и технологии. Теория и практика судебной экспертизы. №1 2006. С. 71-88.

101. Колесов В.А. Использование технологии Блокчейн в учебном процессе для защиты интеллектуальной собственности // В сборнике: дистанционные образовательные технологии Материалы II Всероссийской научно-практической Интернет-конференции. 2017. С. 343-347.

102. Конон А.В. Криминалистическое учение о следах в отечественной и зарубежной литературе // Евразийский Союз Ученых. 2016. № 5-1 (26). С. 120-122.

103. Корчагин А.А., Сат А.Х. Судебно-экспертные технологии: история и современность // Проблемы науки. 2016. №11 (12). С. 37-39.

104. Кудрявцев Ю. С. Об оценке экспертного заключения // Судебная власть и уголовный процесс, 2018. № 3. С. 102-106.

105. Кудряшов Д.А. Актуальные проблемы назначения комплексных судебных экспертиз / Д. А. Кудряшов // Вопросы экспертной практики. 2019. № S1. С. 347-350.

106. Лазаренко А. В. Технологии деанонимизации пользователей Tor // Новые информационные технологии в автоматизированных системах. 2016. №19. С. 257-262.

107. Липатова А. П. Продуктивные модели "разового кода" арго наркоманов / А. П. Липатова // Антинаркотическая безопасность. 2015. № 1(4). С. 114-120.

108. Литвинова Т. А., Громова А. В. Компьютерные технологии в судебной автороведческой экспертизе: проблемы и перспективы использования // Вестник Волгоградского государственного университета. Серия 2 : Языкознание. 2020. Т. 19. № 1. С. 77-88.

109. Литвяк Л.Г., Пирогова Е.Н. К вопросу о понятии электронных или информационно- телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. №11-2. URL: https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-elektronnyh-ili-informatsionno-telekommunikatsionnyh-setey-dlya-tseley-ugolovnogo-zakona (дата обращения: 26.03.2024).

110. Логвиненко Е.А. Электронные документы как доказательства в расследовании преступлений // Пробелы в российском законодательстве. 2014. N 2. С. 232-237.

111. Лубин А. Ф. Некоторые тактические проблемы выявления и оценки цифровых следов компьютерных преступлений / А. Ф. Лубин, С. А. Лубин // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 4(64). С. 121-125.

112. Манянин П.А. О возможностях судебной лингвистической экспертизы при установлении ролей и функций наркопреступников / П. А. Манянин, А. В. Коряковцев // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXIII международной научно-практической конференции: В 2 частях, Красноярск, 02–03 апреля 2020 года. Том 1. – Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2020. С. 202-204.

113. Мельник С.Л. О границах экспертной инициативы // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2017. № 2 (48). С. 20–22.

114. Михайлов С.В., Пономарева Н.В., Прудникова Л.Б. Блокчейн в современном правоприменении // Философия права. 2019. №1 (88). С. 60-64.

115. Моисеева Т.Ф. Классификации судебных экспертиз: необходимость унификации // Вестник экономической безопасности. 2016. №4. С. 68-72.

116. Муравьев К.В., Ермаков М.Г. Современные возможности судебно-компьютерной экспертизы и меры по совершенствованию практики её назначения при расследовании преступлений, связанных с незаконным оборотом наркотических средств «Дистанционным» способом // Вестник Восточно-Сибирского института МВД России. 2019. №3 (90). С. 182-192.

117. Неретина Н.С. Генезис новых родов и видов судебных экспертиз в эпоху цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. №5 (57). URL: https://cyberleninka.ru/article/n/genezis-novyh-rodov-i-vidov-sudebnyh-ekspertiz-v-epohu-tsifrovizatsii (дата обращения: 20.03.2023).

118. Николаев К.Д. Объект и предмет преступлений, связанных с незаконным оборотом наркотиков // Вестник Воронежского института МВД, 2009, №4. С. 42-46.

119. Овсянников Д.В. Электронное копирование информации в система средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. 2014. № 2 (3). С. 130-135.

120. Перов В. А. Компьютерная криминалистика: электронный след понятие и виды / В. А. Перов // Уголовное судопроизводство: проблемы теории и практики. 2021. № 1. С. 94-96.

121. Перов В.А. Криптовалюта как объект гражданского права // Гражданское право. 2017. № 5. С. 7-9.

122. Попова Ю.В. Организация деятельности криптоказино: проблемы привлечения к уголовной ответственности (статья 171.2 Уголовного кодекса РФ) // Молодой ученый. — 2019. № 47 (285). С. 358-359.

123. Россинская Е. Р. Система теории цифровизации судебно-экспертной деятельности / Е. Р. Россинская // Теория и практика судебной экспертизы. 2024. Т. 19, № 3. С. 20-32.

124. Россинская Е. Р. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и

практика / Е. Р. Россинская, И. А. Рядовский // Lex Russica (Русский закон). – 2021. – Т. 74, № 9(178). – С. 102-118.

125. Россинская Е.Р. Методологические и правовые проблемы комплексных судебных экспертиз в условиях реформирования законодательства о судебно-экспертной деятельности // Вестник Московского университета МВД России. 2014. № 6. С. 12-18.

126. Россинская Е.Р. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе / Е. Р. Россинская, Н. Ф. Бодров // Криминалистика: вчера, сегодня, завтра. 2022. № 1(21). с. 121-135.

127. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. №2 (89). С. 193-202.

128. Россинская Е.Р. Цифровизация судебно-экспертной и криминалистической деятельности взаимосвязи и разграничения / Е. Р. Россинская // 2019. № S1. С. 569-574.

129. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. №3 (15). С. 106-123.

130. Россинский С.Б. О практике производства экспертиз в негосударственном судебно-экспертном учреждении / С. Б. Россинский // Эксперт-криминалист. 2010. № 4. С. 30-33.

131. Россинский С.Б. Размышления о сущности выемки как объекта уголовно-процессуального регулирования // Вестник Московского университета МВД России. 2018. №1. С. 42-45.

132. Русакова, Е. П. К вопросу использования Блокчейн-депозитария в формировании доказательственной базы в интернет-судах Китая / Е. П. Русакова, Т. А. Чернышева // Пробелы в российском законодательстве. 2022. Т. 15, № 6. С. 120-125.

133. Сааков Т.А. Влияние процесса цифровизации на трансформацию компетенции судебного эксперта. Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. С. 121-128.

134. Савенков А.Н., Россинская Е.Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. № 10. С. 156-168.

135. Савицкий А.А. Актуальные вопросы становления и развития судебной экономико-цифровой экспертизы в условиях цифровизации социально-экономической сферы государства / А. А. Савицкий // Законы России: опыт, анализ, практика. 2021. № 3. С. 60-64.

136. Саркисян А. А. Профессия судебного эксперта в условиях цифровизации / А. А. Саркисян // Союз криминалистов и криминологов. 2020. № 1. С. 87-93.

137. Саркисян К. Т. Способы совершения преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях / К. Т. Саркисян // Криминалистика: вчера, сегодня, завтра. 2024. № 4(32). – С. 176-185.

138. Саркисян К.Т. Проблемы собирания цифровых следов при производстве следственных действий по делам, связанных с незаконным оборотом наркотических средств в компьютерных сетях // Актуальные проблемы российского права. 2025 №1. С. 188-196.

139. Сегай М.Я. Судебная экспертиза в условиях НТР: особенности и пути оптимизации // Современные проблемы судебной экспертизы и пути повышения эффективности деятельности СЭУ в борьбе с преступностью. Киев, 1983. С. 41-43.

140. Сегай М.Я., Стринжа В.К. Актуальные проблемы экспертной технологии в условиях НТР // Криминалистика и судебная экспертиза. Киев, 1984. Вып. 29. С. 3-7.

141. Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О. Е. Кутафина. 2019. №5 (57). С. 115-120.

142. Смирнова С.А., Колдин В.Я. Судебно-экспертные технологии: современный облик и перспективы. Теория и практика судебной экспертизы. 2019;14(4). С. 137-144.

143. Смушкин А.Б. Криминалистические аспекты исследования Даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. №3 С. 102-111.

144. Соколова О.А. Перспективы формирования компетенций судебного эксперта в условиях повсеместной цифровизации // Криминологический журнал. 2024. №1. С.140-145.

145. Соколова Т. П. Проблемы экспертной идентификации в судебном автороведении // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 2 (90). С. 67-76.

146. Соколова Т.П. Проблемы применения количественных методов в судебной автороведческой экспертизе // Вестник Университета имени О. Е. Кутафина. 2024. №3 (116). С. 77-84.

147. Усов А.И., Лапина И.А., Омельянюк Г.Г. Новые тенденции в сфере судебно-экспертной деятельности как ответ на вызовы современности / И. А. Лапина, Г. Г. Омельянюк, А. И. Усов // Судебная экспертиза Беларуси. 2021. № 1 (12). С. 5–13.

148. Фролов А.А., Сильнов Д.С. Исследование механизмов распространения запрещенного содержимого в Darknet // Современные информационные технологии и ИТ-образование. 2017. №4. С. 216-224.

149. Хомутов, С. В. По вопросу различных подходов к оценке заключения эксперта / С. В. Хомутов // Вестник Восточно-Сибирского института МВД России. 2019. № 1(88). С. 264-274.

150. Худяков В. В., Ананьев А. А. Цифровые следы // Криминологический журнал. 2023. №4. С. 243-246.

151. Черданцев А.Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. Т. 15. N 4. С. 55-60.

152. Чудинов А.М. Проблемы уголовно-правовой характеристики состава преступления, предусмотренного статьей 228.1 Уголовного кодекса Российской Федерации (сбыт наркотических средств, психотропных веществ или их аналогов) // Вестник Прикамского социального института. 2023. №3 (96). С. 59-68.

153. Шапошников А. Ю. Проблема обеспечения подлинности объектов, направляемых для экспертного исследования: системный подход // Юридический вестник Самарского университета. 2015. №4. С. 92-97.

154. Шахназаров Б.А. Комплексная взаимосвязь Блокчейн-технологии и объектов интеллектуальной собственности в трансграничных частноправовых отношениях // Право. Журнал Высшей школы экономики. 2019. №S5. С. 121-148.

155. Шефер В.Ю. Основные принципы исследования криминалистически значимой информации в «облачных» сервисах // Экспертные чтения на Енисее: Материалы региональной (межвузовской) научно-практической конференции. Вып. 2. Красноярск: Красноярский государственный аграрный университет. 2021. С. 144-146.

156. Яблоков Н.П. Криминалистическая характеристика преступлений как составная часть общей теории криминалистической теории// Вестник МГУ. Серия «Право».2000, № 2. С.3-14.

157. Casemajor, N., Couture, S., Delfin, M., Goerzen, M. and Delfanti, A. (2015), «Non-participation in digital media: toward a framework of mediated political action», Media, Culture & So- ciety, Vol. 37 №. 6. pp. 850-866.

158. Caught in the Net: Using Infostealer Logs to Unmask CSAM Consumers URL: https://go.recordedfuture.com/hubfs/reports/cta-2024-0702.pdf (дата обращения: 10.03.2024).

159. Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd. (2018) Zhe 0192 Civil Case, First Court No. 81, Hangzhou Internet Court of the People’s Republic of China, 27 June 2018 China. URL: https://journals.sas.ac.uk/deeslr/article/view/5080/4973 (дата обращения: 21.07.2024).

160. Micheli, Marina; Lutz, Christoph; Büchi, Moritz (2018). Digital footprints: an emerging dimension of digital inequality. Journal of Information, Communication and Ethics in Society, 16(3): P. 242-251.

161. National Institute of Justice. (2008, April). Electronic CSI, a Guide For First Responders, Electronic Crime Scene Investigation: A Guide for First Responders, Second edition // URL: https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders-second-edition (дата обращения: 20.01.2024).

162. Sadiku M., Tembely M., Musa S. Digital Forensics // International Journal of Advanced Research in Computer Science and Software Engineering. 2017. №. 7. P. 274–276.

163. Taking Stock of the Online Drugs Trade. URL: https://www.rand.org/randeurope/research/projects/2016/online-drugs-trade-trafficking.html (дата обращения: 18.10.2024).

Авторефераты и диссертации

164. Бессонов А. А. Частная теория криминалистической характеристики преступлений. Автореф. дисс. доктора юрид. наук. М., 2017. 45 с.

165. Буйнов Д.О. Теория и практика собирания и экспертного исследования цифровых следов по уголовным делам в сфере экономической деятельности: диссертация ... кандидата юридических наук: 5.1.4. – Москва. 2023. 229 с.

166. Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: автореф.дис. … д-ра юрид.наук. М., 1970. 30 с.

167. Иванова Е.В. Концептуальные основы использования специальных знаний при выявлении и расследовании преступлений, связанных с опасными для здоровья веществами: Теория и практика: дис. … д-ра юрид. наук. М., 2014. 468 с.

168. Коврижных Б. Н. Деятельность органов прокуратуры по делам о нераскрытых убийствах: автореф. дис. на соиск. учен. степ. канд. юрид. наук / Б. Н. Коврижных; Харьк. юрид. ин-т.– Х., 1969. 22 с.

169. Колесникова Н. С. Заключение судебного эксперта в системе криминалистически значимой информации: автореф. дис. …. канд. юрид. наук. — Москва, 2021. 26 с.

170. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: Автореф. дисс.... док. юрид. наук. Харьков, 1967. 28 с.

171. Лазарева Л.В. Особенности первоначального этапа расследования незаконного оборота синтетических наркотических средств: дис. ... канд. юрид. наук. М., 2001. 202 с.

172. Медведева М.О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: Автореф. дис. ... канд. юрид. наук. М., 2018. 28 с.

173. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: специальность 12.00.09 "Уголовный процесс" : диссертация на соискание ученой степени доктора юридических наук / Мещеряков Владимир Алексеевич. – Воронеж, 2001. 387 с.

174. Никишин В.Д. Теоретические и организационно-правовые аспекты судебной экспертизы материалов религиозного характера экстремистской и террористической направленности: дис … канд. юрид. наук. 12.00.12 / Никишин Владимир Дмитриевич. — М., 2018. 276 с.

175. Петрухина А.Н. Заключение эксперта и его оценка в уголовном процессе: Автореф. дис. … канд. юрид. наук. М., 2012. 32 с.

176. Сааков Т.А. Судебно-диагностическое исследование демографических характеристик автора по признакам письменной речи: дис … канд. юрид. наук. 12.00.12 / Сааков Тигран Артемович. М., 2020. 277 с.

177. Саркисян А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты: автореферат дис. ... кандидата юридических наук: 5.1.4. / Москва, 2024. 168 с.

178. Сергеев Л.А. Расследование и предупреждение хищений, совершаемых при производстве строительных работ: автореф. дис. ... канд. юрид. наук. Москва. 1966. 16 с.

179. Смолина А.Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы: диссертация ... кандидата технических наук: 05.13.19 / Томск, 2017. 132 с.

180. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: дис. … д-ра юрид. наук. — М. 2002. 402 с.

Судебная и экспертная практика

181. Кассационное определение Седьмого кассационного суда общей юрисдикции от 11.04.2024 N 77-1014/2024 (УИД 66RS0004-01-2021-014213-07) – Доступ из справ.-правовой системы «Консультант Плюс».

182. Кассационное определение Третьего кассационного суда общей юрисдикции от 17.10.2024 N 77-2226/2024 (УИД 29RS0014-01-2023-003613-30) – Доступ из справ.-правовой системы «Консультант Плюс»

183. Приговор № 1-120/2023 от 9 июня 2023 г. по делу № 1-120/2023 Ярославского районного суда // URL: https://sudact.ru/regular/doc/fnQtVFPisVbb/ (дата обращения: 20.01.2024).

184. Приговор № 1-187/2023 от 19 июля 2023 г. по делу № 1-187/2023 Шпаковского районного суда Ставропольского края // URL: https://sudact.ru/regular/doc/DSn8SXFf2qg9/ (дата обращения: 20.01.2024).

185. Приговор № 1-188/2023 от 26 июля 2023 г. по делу № 1-188/2023 Шатурского городского суда Московской области // URL: https://sudact.ru/regular/doc/7CPamAaBkmmJ/ (дата обращения: 20.01.2024).

186. Приговор Московского областного суда по делу № 2-102/2022. URL: https://oblsud--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=34472938&delo_id=1540006&new=0&text_number=1 (дата обращения: 20.03.2024).

Интернет-ресурсы

187. Данные о программе Cellebrite Pathfinder // URL: https://www.dataexpert.eu/products/mobile-forensics-cellebrite/cellebrite-pathfinder/ (дата обращения: 23.01.2024).

188. Информация об истории и работе Tor. URL: http://torproject.org/ (дата обращения: 16.01.2024).

189. Отчет по результатам проведенной сотрудниками правоохранительных органов США операции «Темное золото» // URL: https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35 (дата обращения: 23.01.2024).

190. Характеристика состояния преступности в Российской Федерации за январь-август 2022 года // URL: https://xn--b1aew.xn--p1ai/reports/item/32515852/ (дата обращения: 23.08.2023).

191. Характеристика состояния преступности в Российской Федерации за январь-август 2023 года // URL: https://xn--b1aew.xn--p1ai/reCports/item/44036297/?ysclid=ls8zlzbdh0573477495 (дата обращения: 01.02.2024).

192. Forensic Science Regulator. Code practice. URL: https://assets.publishing.service.gov.uk/media/64da431cc8dee4000d7f1c1e/FINAL_2023.1.18_Code_of_Practice.pdf (дата обращения: 13.09.2024).

Приложение № 1. Форма анкеты для проведения опроса сотрудников правоохранительных органов по актуальным вопросам, связанным с назначением судебных экспертиз в рамках расследования незаконного оборота наркотических средств в компьютерных сетях

Уважаемые коллеги!

Просим Вас, пройти анонимную анкету в целях получения Вашего, компетентного мнения с теоретической и практической стороны об особенностях назначения судебных экспертиз в рамках расследования незаконного оборота наркотических средств в компьютерных сетях.

Благодарим Вас, за принятое участие!

1. Ваш возраст _____

2. Ваш стаж практической работы по специальности: _____

3. Актуальна ли сейчас в России проблема борьбы с незаконным оборотом наркотических средств в компьютерных сетях?

- Актуальна
- Не актуальна
- Не задумывался

4. Отмечаете ли Вы увеличение за последние годы совершения преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

- Да
- Нет
- Не задумывался

5. Что Вы понимаете под цифровыми следами?

_____

_____

6. Как часто при расследовании преступлений, связанных с незаконным

оборотом наркотических средств в компьютерных сетях, Вы сталкиваетесь с цифровыми следами?

- Постоянно
- Периодически
- Не сталкивался

7. С какими видами цифровых следов Вы сталкиваетесь при расследовании дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

- Данные социальных сетей и мессенджеров
- Данные сайтов сети «Интернет», сети «Даркнет», а также история посещения сайтов
- Данные приложений, содержащие информацию, например, о местоположении и о проведенных транзакциях
- Облачное хранилище данных
- Другое: _____

8. Считаете ли обязательным участие специалиста при собирании цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

- Обязательно
- Не обязательно
- Зависит от обстоятельств

9. Считаете ли Вы обязательным участие специалиста при составлении протоколов следственных действий по итогу собирания цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

- Обязательно
- Не обязательно
- Зависит от обстоятельств

10. Считаете ли необходимым расширение Ваших компетенций в области собирания цифровых следов?

- Да

- Нет
- Не задумывался

11. Как Вы считаете, современные технико-криминалистические средства позволяют в полной мере обеспечить эффективное собирание цифровых следов?

- Да
- Нет
- Не всегда
- Затрудняюсь ответить

12. Считаете ли Вы необходимым создание методики, стандартов по собиранию цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

- Да
- Нет
- Не задумывался

13. В случае положительного ответа на предыдущий вопрос, как Вы считаете, должна ли эта методика быть общей для всех видов преступлений или необходима отдельная методика для преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

_____

_____

14. Известны ли Вам случаи утраты цифровых следов при производстве следственных действий по преступлениям, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

- Да
- Нет

15. В случае положительного ответа на предыдущий вопрос, расскажите, как и по какой причине цифровые следы были утрачены?

_____

_____

16. Как Вы оцениваете значимость цифровых следов при расследовании и раскрытии преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

- Одно из ведущих значений
- Значимость на уровне с другими объектами
- Отсутствие значимости
- Не задумывался

17. С какими основными трудностями Вы сталкиваетесь при работе с цифровыми следами по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

_____

_____

_____

18. Считаете ли Вы достаточным урегулирование вопросов цифровых следов в законодательстве Российской Федерации?

- Да
- Нет
- Не задумывался

19. Как Вы думаете, усложняет ли процесс расследования и раскрытия преступлений, связанных с незаконным оборотом наркотических средств, перемещение деятельности в онлайн-пространство?

- Да
- Нет
- Не задумывался

20. В будущем будет ли возрастать количество преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

- Да
- Нет
- Не задумывался

21. Какие судебные экспертизы, по Вашему мнению, необходимо назначать по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

_____

_____

22. Назначали ли Вы судебные экспертизы по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, где объектом выступали цифровые следы?

- Да
- Нет

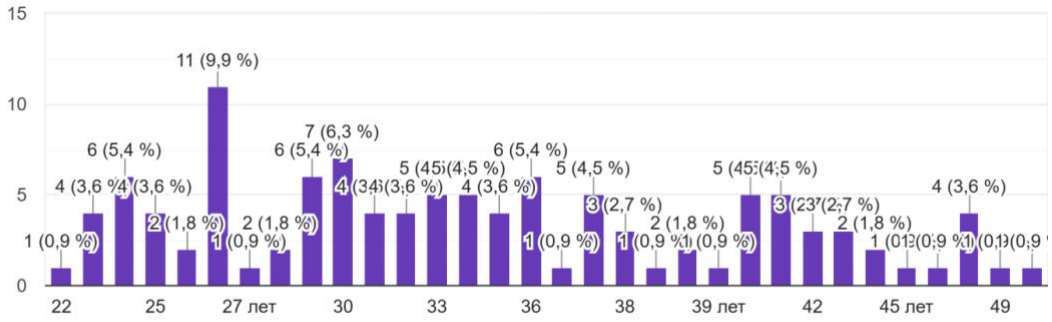
23. В случае положительного ответа на предыдущий вопрос, расскажите, какие именно судебные экспертизы Вы назначали?

_____

_____

Приложение № 2. Результаты анкетирования сотрудников правоохранительных органов по актуальным вопросам, связанным с назначением судебных экспертиз в рамках расследования незаконного оборота наркотических средств в компьютерных сетях

1. Ваш возраст



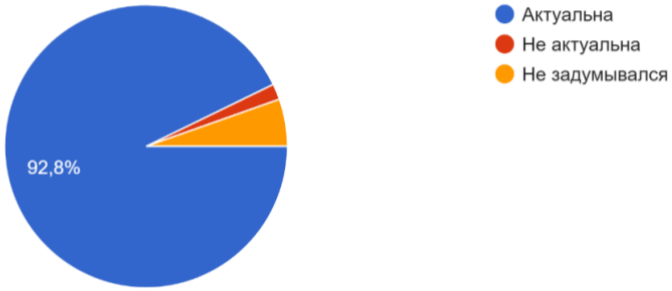
2. Ваш стаж практической работы по специальности:

1. **20 лет**	2. **18 лет**
3. **15 лет**	4. **11 лет**
5. **5 лет**	6. **18 лет**
7. **5 лет**	8. **12 лет**
9. **2 года**	10. **9 лет**
11. **8 лет**	12. **18 лет**
13. **1 год**	14. **3 месяца**
15. **1 год**	16. **5 лет**
17. **5 лет**	18. **6 лет**
19. **1 год**	20. **19 лет**
21. **2 года**	22. **10 лет**
23. **17 лет**	24. **10 лет**
25. **1,5 года**	26. **10 лет**
27. **6 лет**	28. **12 лет**
29. **15 лет**	30. **7 лет**
31. **2 года**	32. **17 лет**
33. **15 лет**	34. **9 лет**
35. **18 лет**	36. **21 лет**
37. **29 лет**	38. **6 лет**

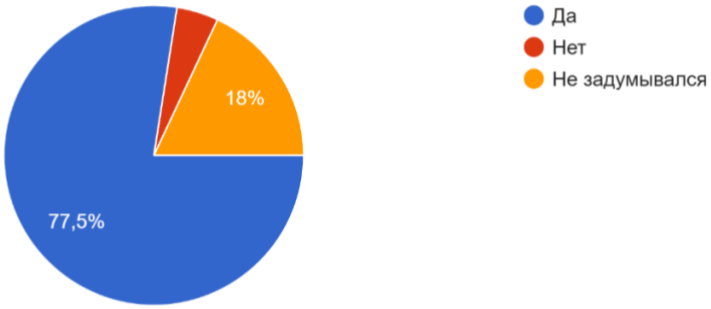
39. **7 лет**	40. **3 лет**
41. **5 лет**	42. **7 лет**
43. **13 лет**	44. **10 лет**
45. **16 лет**	46. **2 года**
47. **7 лет**	48. **15 лет**
49. **6 лет**	50. **4 года**
51. **6 лет**	52. **18 лет**
53. **6 лет**	54. **4 года**
55. **2 года**	56. **12 лет**
57. **6 лет**	58. **21 год**
59. **6 лет**	60. **20 лет**
61. **15лет**	62. **10 лет**
63. **6 лет**	64. **20 лет**
65. **16 лет**	66. **12 лет**
67. **6 лет**	68. **Вот-вот только закончу учебу по специализация**
69. **7 лет**	70. **25 лет**
71. **12 лет**	72. **19 лет**
73. **19 лет**	74. **2 месяца стажер, 4 месяца на должности**
75. **9 лет**	76. **16 лет**
77. **Работаю по другому направлению деятельности**	78. **10 лет**
79. **18 лет**	80. **12,5 лет**
81. **4 года**	82. **3 года**
83. **15 лет**	84. **17 лет**
85. **3 года 4 месяца**	86. **7 лет**
87. **7 лет**	88. **8 лет**
89. **16 лет**	90. **7 лет**
91. **1 год**	92. **12 лет**
93. **6 лет**	94. **15 лет**
95. **7 лет**	96. **15 лет**
97. **7 лет**	98. **4 года 5 месяцев**
99. **15 лет**	100. **8 лет**
101. **Нет**	102. **6 лет**
103. **1 год**	104. **9 лет**
105. **5 лет**	106. **7 лет**
107. **16 лет**	108. **15 лет**

109. **1 год**	110. **27 лет**
111. **10 лет**	

3. Актуальна ли сейчас в России проблема борьбы с незаконным оборотом наркотических средств в компьютерных сетях?



4. Отмечаете ли Вы увеличение за последние годы совершения преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?



5. Что Вы понимаете под цифровыми следами?

1. Мессенджер, история посещений в браузере, геоточки
2. Данные при использовании интернета
3. IP-адреса
4. -
5. -
6. Ничего
7. Переписки с мобильных приложений
8. Следы, связанные с компьютерной информацией
9. Данные, которые оставляются при использовании интернета
10. İp-адрес, домен, токен
11. Информация в интернете
12. Нет ответа

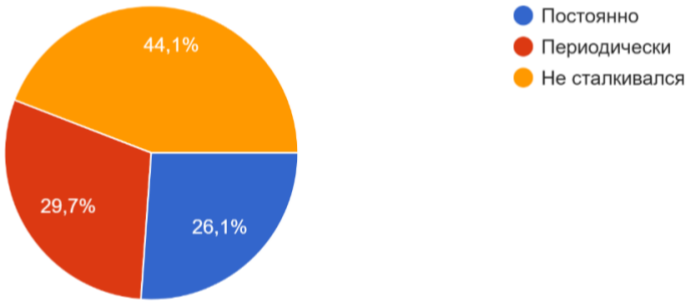
13. Логины, пароли, id
14. Информация, содержащаяся в мобильных устройствах и иных цифровых носителях
15. Значимая компьютерная информация
16. Следы которые остаются в интернете
17. Переписки в различных мессенджерах, рассылки , движения средств по счетам , детализации
18. Географические координаты места нахождения тайника
19. Следы преступной деятельности, сохранившиеся в виде информации на электронных носителях, в т.ч. персональных коммуникационных устройствах, на серверах с возможностью доступа через сеть (либо невозможностью)
20. Информация содержащаяся на электронных устройствах, а также доступы к этой информации пользователей
21. Информация, которую оставляет преступник при покупке наркотических средств через сеть Интернет
22. Данные, которые остаются при использовании интернета, письма, заполненные анкеты, транзакции и т.д.
23. Оставление информации в цифровом поле
24. IP адреса
25. Это данные, которые оставляет «жулик» при использовании интернета
26. Затрудняюсь ответить
27. Сообщения в смс или соц. сетях
28. Оставленные следы преступления
29. ...
30. Айпи адреса, куки, кеш файлы иные сведения и данные
31. Не понимаю
32. IP адрес
33. Все действия, которые производятся в сети Интернет
34. Ip адреса
35. Данные, которые остаются при использовании интернета
36. Следы операций совершенных с использованием интернета, переписка, история запросов в поисковике и др.
37. Ip ,адрес
38. Информация о посещении интернет сайтов
39. Сведения о переводах и покупках по средствам сети
40. Это доказательство оставление при использовании удаленных сетей
41. Информация о деятельности лица в виртуальном пространстве, на электронных устройствах.
42. Возможность отследить человека совершившего преступление
43. Свои данные
44. Переписка в мессенджерах и переводы денежных средств
45. Отслеживание перевода денежных средств

46. Переписки, звонки, изображения
47. Следы оставленные в сети интернет
48. Следы в сети Интернет, на мобильных устройствах
49. Информация, которую оставляет человек, при использовании сети Интернет.
50. Диалоги, геолокации в мессенджерах или теги, ссылки в интернете
51. Телефонные звонки, смс сообщения, сообщения в мессенджерах, истории переводов денежных средств
52. Набор действий в Интернете
53. Любые данные, оставляемые в цифровом пространстве
54. Цифровой след это след оставленный действиями программ, функций
Информация, которую вы оставляете о себе и своих действиях при пользовании интернетом.
55. Следы, оставленные преступниками в сфере компьютерных технологий
56. Следы в сети Интернет, подтверждающие причастность лица к тому или иному преступлению
57. Следы (доказательства) оставленные на цифровых носителях (телефон, ПК, флешка)
58. Использование интернета
59. Информацию
60. Информация о лицах, либо их деятельности оставшаяся в сети интернет
61. Информация о человеке в интернете
62. Данные, которые мы оставляете при использовании интернета.
63. Информация оставленная при пользовании интернетом
64. Следы оставленные при входе на компьютер или посещение какого либо сайта
65. Отдельная категория следов, компьютерная информация, то есть сведения, представленные в форме электрических сигналов
66. Криминалистически значимая информация, выраженная посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники.
67. Денежные переводы, переписки
68. Информация в интернете оставленная пользователем
69. Информация оставленная в сети интернет злоумышленниками(IP адреса, прокси-сервер, фото-видео, номера телефонов и т.д.)
70. Остатки информации в базах данных
71. Источник
72. Информация, которая остаётся в виртуальной среде от любого действия в интернете, зачастую её может обнаружить только специалист
73. Данные, оставленные пользователем интернета
74. Информация, которую мы оставляем о своих действиях при пользовании сети интернет
75. Данные, оставленные пользователем в сети интернет, позволяющие по ним установить его местонахождение или иную информацию о его личности
76. Приложения, истории просмотров

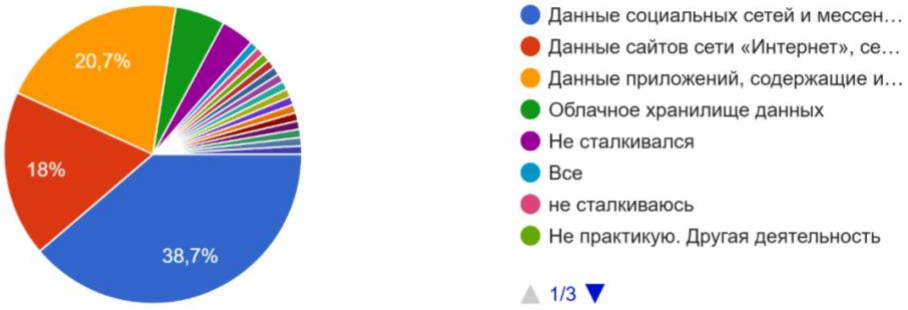
77. Данные, которые остаются в интернете
78. Информация в сетях интернет
79. Информация о человеке в интернете
80. Информация, которую оставляет человек при пользовании интернетом
81. Следы, оставленные в сети «Интернет». Такие данные включают: веб-сайты, которые посещают, отправляемые электронные письма и информацию, которая указывается в онлайн-формах.
82. Криминалистически значимая компьютерная информация о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи
83. Переписка в мессенджерах
84. Определенный набор действий в сети Интернет, либо на устройствах, несущие информацию о пользователе, а также о страницах, Интернет-ресурсах им посещаемых
85. Доказательства на электронных носителях
86. Ничего
87. Мессенджеры, фотографии
88. То, что оставляет след на информационных носителях
89. Информация, содержащая на электронных носителях
90. Следы, оставленные преступником в сети Интернет
91. Следы оставленные в сети интернет и в компьютерной технике (сотовых телефонах)
92. Следы оставленные преступником в сети интернет
93. Всевозможные данные заполненные пользователем, которые он оставил на различных сайтах
94. Следы в виртуальном мире, позволяющие установить определённые обстоятельства
95. Это данные которые остаются при использовании интернета
96. Информация которая остается после посещения интернет ресурсов
97. Сведения в сети, подтверждающее совершение преступление
98. Следы оставленные в цифровых носителях
99. Данные с сайтов, социальных сетей, мессенджеров, логины пароли и т.д.
100. Уникальный набор действий в интернете
101. Различные данные
102. Следы оставленные на носителях информации
103. Это след который оставляет юзер при посещении сайта, форума и т.д., такие данные сохраняются в виде куки-файла
104. Не имею представления
105. Сведения о переводах, переписках
106. Сведения о себе оставленные в интернете
107. -
108. Следы в средствах связи, в информационно-телекоммуникационной сети
109. Ссылки, переводы

110.	Переписка в соц. сетях. IP адрес
111.	Данные, которые люди оставляют в сети интернет.

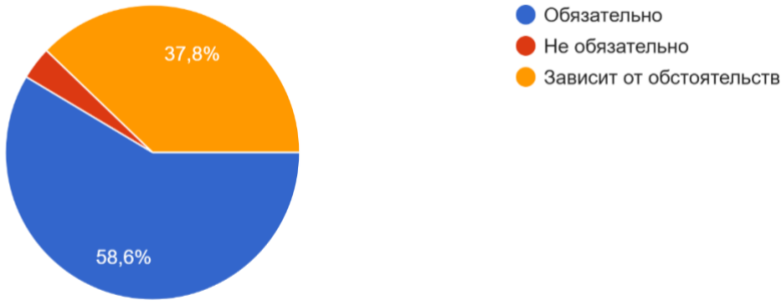
6. Как часто при расследовании преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях, Вы сталкиваетесь с цифровыми следами?



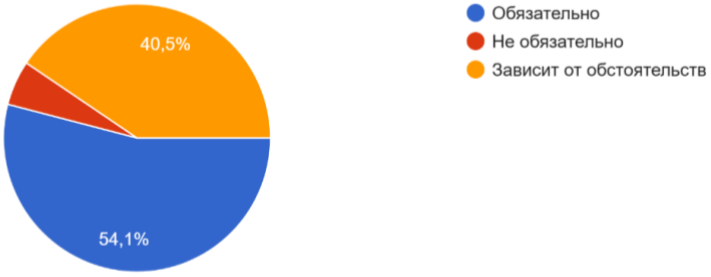
7. С какими видами цифровых следов Вы сталкиваетесь при расследовании дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях?



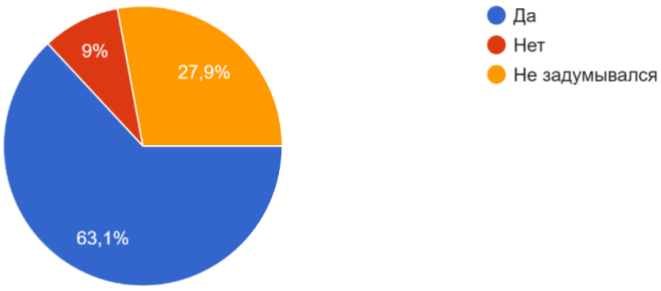
8. Считаете ли обязательным участие специалиста при собирании цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?



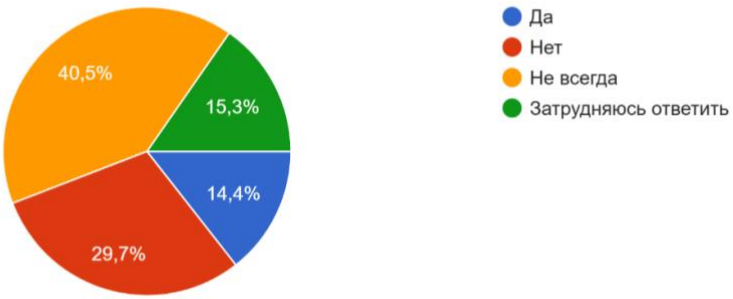
9. Считаете ли Вы обязательным участие специалиста при составлении протоколов следственных действий по итогу собирания цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?



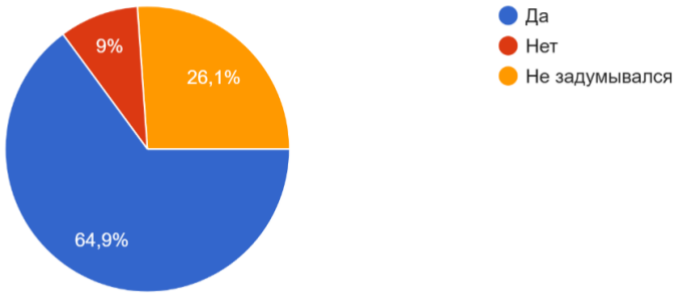
10. Считаете ли необходимым расширение Ваших компетенций в области собирания цифровых следов?



11. Как Вы считаете, современные технико-криминалистические средства позволяют в полной мере обеспечить эффективное собирание цифровых следов?



12. Считаете ли Вы необходимым создание методики, стандартов по собиранию цифровых следов по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?



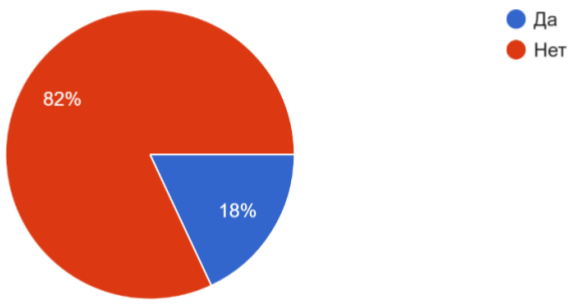
13. В случае положительного ответа на предыдущий вопрос, как Вы считаете, должна ли эта методика быть общей для всех видов преступлений или необходима отдельная методика для преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?

1.	Отдельная для преступлений в сверке незаконного оборота наркотических и психотропных веществ в компьютерных сетях
2.	Отдельно
3.	Общая
4.	Отдельная
5.	Отдельная
6.	Да
7.	Отдельная методика по каждому виду
8.	Должна
9.	Общей для всех видов преступлений, совершаемых с использованием информационно-коммуникационных технологий
10.	Отдельная методика для отдельного вида преступления
11.	Общая
12.	Отдельная
13.	Общая
14.	Отдельная
15.	Отдельно
16.	Для всех
17.	Только для преступлений, связанных с нон в сети интернет
18.	Да
19.	Отдельная методика

20. Нужна общая методика, для отслеживания цифрового следа во всех направлениях
21. Отдельная методика
22. Отдельная методика
23. Своя
24. На каждый случай, свои методы
25. Отдельная
26. Считаю, что методика для преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях должна быть отдельной. Конечно, могут быть сходства в методиках. Преступления по линии НОН могут быть и весьма сложные, и чтоб распутать некую паутину. Необходимо достаточно знаний и правильных действий, чтоб установить лицо и раскрыть преступление! А стандартная методика для всех преступлений, в данном случае может и не до конца включать все действия в раскрытии преступлений по линии НОН.
27. Отдельная
28. Отдельная, конкретная
29. Затрудняюсь ответить
30. Общей для всех видов
31. Индивидуальная методика, по каждому виду преступлений
32. Обшей
33. Отдельная
34. Должна быть общая, узко специализированная методика
35. Отдельная, по категориям преступлений
36. Не знаю
37. Общая для цифровых следов по всем преступлениям
38. Отдельная
39. Отдельная
40. Необходима отдельная методика
41. Незаконный оборот наркотиков является специфическим видом преступности, по этому я считаю что необходимо выработать методику именно по преступлениям в сфере НОН
42. Да
43. Есть общие моменту, а есть индивидуальные, касающиеся конкретного вида преступления
44. Должна быть общей
45. Считаю что нужно создать отдельную методику для раскрытия данных преступлений в сфере оборота наркотиков в сети интернет и регулярно ее обновлять.
46. общая
47. Общая методика
48. Отлично
49. Отдельная, методика
50. Отдельная методика
51. Отдельная

52. Общая с учетом специфики
53. Необходима отдельная методика
54. Отдельная
55. Для всех одна
56. Необходима отдельная
57. Для всех
58. Нужна отдельная методика
59. Возможна общая методика
60. Должна быть отдельная
61. Отдельные методики для большинства преступлений
62. Отдельной
63. Отдельная
64. Необходима отдельная методика
65. Данная методика должна быть адаптивна к разного рода преступлениям в сфере НОН, в настоящее время есть на вооружении некоторые
66. Отдельная
67. Отдельной категории
68. Отдельная методика
69. «Дистанционное мошенничество» также совещается с использованием телефона и сети интернет

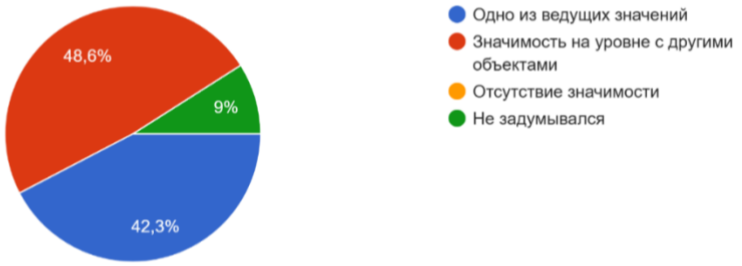
14. Известны ли Вам случаи утраты цифровых следов при производстве следственных действий по преступлениям, связанным с незаконным оборотом наркотических средств в компьютерных сетях?



15. В случае положительного ответа на предыдущий вопрос, расскажите, как и по какой причине цифровые следы были утрачены?

1. Включен смартфон с доступом к сети
2. Утрат не было
3. Непроведение неотложного осмотра и фиксации информации, к которой имелся доступ с изъятого устройства на момент его обнаружения; программное удаление информации по истечении определенного времени; намеренное противодействие преступников (очистка устройства через удаленный доступ, применение специальных программ); блокировка устройства и невозможность взлома (подбора пароля); прекращение функционирования конкретного интернет-ресурса
4. Неправильное изъятие при проведении следственных действий
5. Удалённым способом была уничтожена информация
6. Не своевременно проведенный осмотр или экспертиза
7. Не компетентность следователя
8. Телефон не был введен в режим полета и дистанционного были удалены геоданные и переписка
9. Нет
10. Нету
11. Нет
12. Удаляемые сообщения, файлы полученные путем мессенджера
13. Коррупционная составляющая
14. Не сталкивался
15. Не знаю
16. -
17. Не своевременность изъятие, фигурант успевает облачно всё почистить
18. Гаджеты на которых была информация, приводят в негодность при задержании
19. Следователь при проведении процедуры осмотра смартфона передала его в руки подозреваемому, после чего последний удалили информацию с телефона и разбил телефон.
20. Нет
21. При осмотре с включенным Интернетом
22. При выключении авиарежима телефона исчезала переписка
23. Удаление мессенджера с другого аппарата
24. Восстановили изъятую сим- карту и удалили переписку в мессенджерах
25. Переписка в социальных сетях
26. Мне известны только случаи утраты информации в следствии не полной осведомленности сотрудников как необходимо действовать для их сохранности
27. В мессенджере «телеграм» не сохраняется информация , если был выключен таймер на автоудаление, либо пользователь удалил переписку
28. Через удаленный доступ удалена информация с с/т

16. Как Вы оцениваете значимость цифровых следов при расследовании и раскрытии преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?



17. С какими основными трудностями Вы сталкиваетесь при работе с цифровыми следами по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

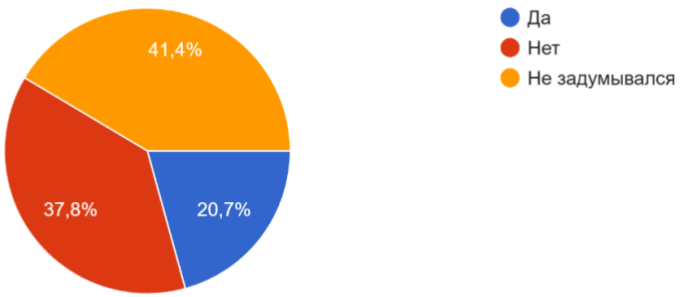
1.	Ответы на запросы
2.	Совершенствование
3.	Не имею
4.	Не сталкивался
5.	Не сталкивался
6.	Не сталкивалась
7.	Нет
8.	Не сталкивался
9.	не расследую
10.	Не сталкивалась
11.	-
12.	Отсутствие необходимых знаний и навыков
13.	Не предоставлялось возможности
14.	Не сталкивалась
15.	Не сталкивалась
16.	Не сталкивался
17.	Трудности в истребовании данных
18.	Пока не сталкивался
19.	Низкая квалификация специалистов; отсутствие программ аналитической обработки Big Data; проблематичность идентификации личности в сети, в т.ч. при использовании мессенджеров; отказ во взаимодействии иностранных государств, биткоин-бирж; отсутствие возможности взлома современных коммуникационных устройств
20.	Отсутствие паролей от устройств, краткий срок хранения информации, информация на серверах в иностранных компаниях, шифрование информации

21.	Квалификация в описании цифровых следов
22.	Использование динамических ip-адресов, vpn, сервисов, обеспечивающих повышенную анонимность
23.	Удаление следов
24.	Долгие сроки предоставления информации
25.	Длительность проведения экспертиз
26.	Не сталкиваюсь
27.	Нет специалистов
28.	Нет ответа
29.	.....
30.	Нет
31.	Не сталкивался
32.	Не сталкивался
33.	Не расследовал такие дела
34.	Бюрократия
35.	Анонимность
36.	Не входит в сферу деятельности.
37.	Доступность в расшифровке
38.	Не сталкивался
39.	Не знаю
40.	Отсталость возможностей МВД
41.	Я
42.	Не сталкивался
43.	Не занимаюсь расследованием таких дел
44.	Не сталкиваюсь
45.	Не сталкивался
46.	Отсутствие доступа к информации, длительное время запросов и результатов
47.	Мало знаний в данной области
48.	Доступ к мобильным устройствам
49.	Нехватка знаний
50.	Не сталкивался
51.	Не сталкивался
52.	Не расследую уголовные дела
53.	Не сталкивалась
54.	Доступ к информации
55.	Длительность ответов на запросы
56.	Не сталкивался

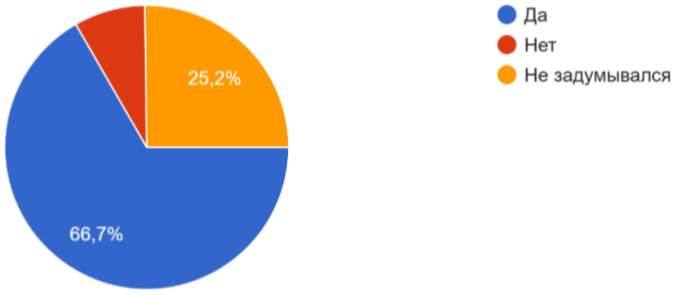
57. Извлечение необходимой информации из телефона, восстановление удаленных данных
58. Доступ
59. Отсутствие информации
60. Нет трудностей
61. Не всегда полученная информация может быть достоверна в полной мере(псевдоним, ложные данные о месте нахождения и т.д.)
62. Не сталкивалась
63. С недостаточно кфалифицированными работниками
64. Не достаточное обеспечение
65. Не сталкивался
66. Моей основной деятельностью не являются преступления в сфере незаконного оборота наркотиков
67. Не сталкивался с такими делами
68. Не сталкивался
69. Не работал
70. Не занимаюсь данной процедурой
71. Невозможность разблокировать смартфоны айфон
72. Анонимность
73. Отсутствие понимания где, какие именно и каким образом можно обнаружить и изъять. Отсутствие единой судебной практики к какому виду доказательств относить цифровые следы: иные документы, вещественные доказательства или нечто иное....
74. -
75. Не сталкиваюсь
76. Сложность их нахождения
77. Не сталкиваюсь
78. Не сталкивалась
79. Нет достойного оборудования
80. Не сталкивалась
81. Долго ждать ответы на запросы
82. Не сталкивалась
83. Трудность в установлении и фиксации цифровых следов
84. Невозможности исследования переписки без выключенного интернета, в том числе сведений по электронным кошелькам
85. Сложность при восстановлении удаленных следов
86. Эксперты не могут получить информацию из телефонов, когда нет паролей
87. Не сталкиваюсь
88. Копирование
89. Пароли на носителях
90. Отсутствие опыта

91. Сложность в обнаружении
92. Использование криптовалюты при совершении преступления, техническое обеспечение на низком уровне
93. Нет трудностей
94. Подбор пароля к современным телефонам
95. Пароли
96. Отсутствие специальных познаний у сотрудников в данной области
97. Нет
98. Затрудняюсь ответить
99. Весь процесс преступной деятельности происходит в даркнете с использованием специальных приложений сокрытия преступной деятельности типа тор браузер итп
100. Не сталкивался
101. Затрудняюсь ответить
102. Не сталкивался
103. Отсутствии технических возможностей по востановлению удаленных/утраченных данных
104. Не сталкиваюсь
105. Нет сведений
106. Не возможность открытия приложений, и иного ПО, используемого фигурантами при совершении преступления
107. -
108. Платформа «mega", трудно отследить, обменники и тд
109. Нет специализированных знаний в этой области
110. Очень часто не могут снять пароль с устройства
111. Затрудняюсь ответить

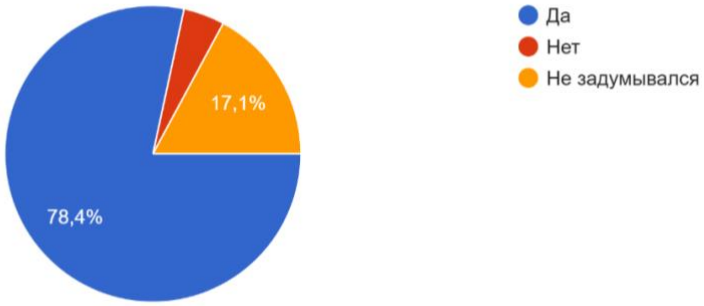
18. Считаете ли Вы достаточным урегулирование вопросов цифровых следов в законодательстве Российской Федерации?



19. Как Вы думаете, усложняет ли процесс расследования и раскрытия преступлений, связанных с незаконным оборотом наркотических средств, перемещение деятельности в онлайн-пространство?



20. В будущем будет ли возрастать количество преступлений, связанных с незаконным оборотом наркотических средств в компьютерных сетях?



21. Какие судебные экспертизы, по Вашему мнению, необходимо назначать по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях?

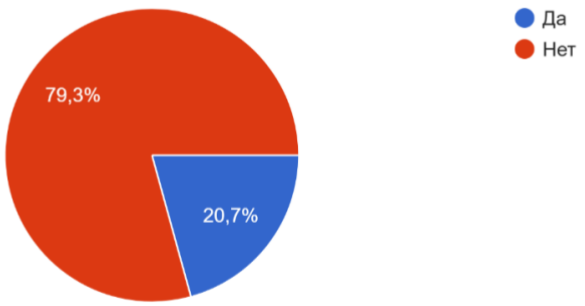
1.	Определение принадлежности голоса в некоторых случаях
2.	Соответствующие
3.	Компьютерную
4.	Не знаю
5.	-
6.	Не сталкивалась
7.	Компьютерная
8.	Компьютерная
9.	компьютерные
10.	Компьютерные
11.	-

12.	Компьютерные
13.	Компьютерная криминалистическая экспертиза
14.	Компьютерная
15.	Компьютерная
16.	Не задумывался
17.	Компьютерные судебные
18.	Затрудняюсь ответить
19.	Компьютерные
20.	Компьютерные, химические
21.	Компьютерная судебная экспертиза
22.	Компьютерные
23.	Компьютерные
24.	Компьютерные
25.	Компьютерно-технические
26.	Затрудняюсь ответить
27.	Не задумывался
28.	Нет ответа
29.	.....
30.	Не знаю
31.	Все
32.	Затрудняюсь ответить
33.	Не знаю
34.	Следователь разберётся, прокурор подскажет
35.	Компьютерная
36.	По поиску цифровых следов подтверждающих наличие переписки, договорённости, передачи денежных средств, наркотических средств
37.	Проведение специально-технической экспертизы
38.	Не задумывался
39.	Айти
40.	Компьютерные
41.	Компьютерная экспертиза, КЭМВИ
42.	Не задумывался
43.	Затрудняюсь ответить
44.	Не знаю
45.	Не могу ответить
46.	Достоверность коммуникаций и собственников устройств
47.	Судебно-компьютерная экспертиза

48.	Не знаю
49.	Затрудняюсь ответить
50.	Не знаю
51.	Судебная компьютерно-техническая экспертиза
52.	Не расследую уголовные дела
53.	Не знаю
54.	Затрудняюсь ответить
55.	Все необходимые
56.	Затрудняюсь ответить
57.	Химическая, компьютерная
58.	Все возможные, для детального установления истины
59.	Затрудняюсь
60.	Экспертизы по телефонам
61.	Судебно-химическая экспертиза, судебно-техническая экспертиза
62.	Техническую (компьютерную)
63.	🤷 (смайл человека, пожимающего плечами)
64.	Компьютерно-техническую
65.	Не знаю
66.	Перечень большой
67.	Технико-криминалистическая
68.	Техническую
69.	Не задумывался
70.	Не знаю
71.	Исследование электронных носителей информации с целью добывания информации для доказывания фактов сбыта
72.	Не задумывался
73.	Вид экспертизы зависит от предмета исследования
74.	-
75.	Не задумывался
76.	Не сталкивался
77.	Не знаю
78.	Компьютерная
79.	Токсилогическую
80.	Компьютерные
81.	Компьютерно-технические
82.	Компьютерно-техническая
83.	Компьютерные и т.д.

84. Компьютерные, лингвистические, при наличии аудиосообщений фоносокопические
85. Компьютерные
86. Физико-химические, биологические, дактилоскопические, компьютерные, психиатрические
87. Компьютерная
88. Компьютерные
89. Компьютерные
90. Компьютерные
91. Химическая, компьютерная
92. Компьютерно- техническая экспертиза
93. Не знаю
94. Компьютерная
95. компьютерная
96. Компьютерную
97. Компьютерные
98. Не знаю
99. Компьютерные
100. Судебно-техническая
101. Изучающая цифровые следы
102. Не знаю
103. Мне известна лишь одна судебная экспертиза которую уместно здесь применить, это компьютерно-техническая
104. Не имею представления
105. Компьютерные
106. Технико-криминклистические, компьютерные, бухгалтерские, финансово аналитические
107. -
108. Компьютерная
109. Компьютерно-техническую экспертизу
110. -
111. Компьютерная экспертиза.

22. Назначали ли Вы судебные экспертизы по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях, где объектом выступали цифровые следы?



23. В случае положительного ответа на предыдущий вопрос, расскажите, какие именно судебные экспертизы Вы назначали?

1.	Нет
2.	Нет
3.	Компьютерную
4.	-
5.	Не назначал
6.	Не назначала
7.	Нет
8.	-
9.	не назначала
10.	Не назначала
11.	-
12.	Компьютерные
13.	-
14.	Компьютерная
15.	Не назначала
16.	Не назначала
17.	Компьютерная
18.	Компьютерная, генетическая,
19.	Компьютерные (компьютерно-технические), экспертам органов внутренних дел, СК России, ФСБ России
20.	Нет
21.	Нет
22.	Компьютерные, ЭКЦ МВД

23.	Компьютерные
24.	Восстановить информацию
25.	Компьютерно-технические
26.	Не назначал
27.	Не назначал
28.	Нет ответа
29.	.....
30.	Нет
31.	Все
32.	Не назначал
33.	Не назначал
34.	Нет
35.	Компьютерная
36.	Ответ на предыдущий вопрос отрицательный.
37.	Не назначал
38.	Не назначал
39.	Не назначала
40.	У меня отрицательный ответ
41.	Экспертизы не назначались
42.	Компьютерно-технические
43.	Нет
44.	Не
45.	Не назначал
46.	СМЭ по телесным
47.	Нет
48.	Не назначал
49.	Не назначила
50.	Не назначали
51.	Не назначал
52.	Не расследую уголовные дела
53.	Нет не назначала
54.	Нет
55.	Не назначал
56.	Не назначал
57.	Компьютерная
58.	Нет
59.	Нет

60.	Нет
61.	Не в моей компетенции
62.	Не назначала
63.	Никакие
64.	Не назначал
65.	Нет
66.	Отрицательный ответ
67.	Никакие
68.	Не назначал
69.	Не назначал
70.	Нет
71.	Не назначал
72.	Нет
73.	Компьютерно-техническая
74.	-
75.	Нет
76.	Нет
77.	Не назначал
78.	Не отправляла
79.	Нет
80.	Не назначала
81.	Нет
82.	Компьютерно-техническую обвиняемому
83.	Компьютерные в специализированные подразделения ЭКЦ
84.	Компьютерные экспертизы по изъятым мобильным телефонам
85.	Компьютерные в ЭКЦ ГУ МВД по Нижегородской области
86.	-
87.	Компьютерные ЭКЦ ГУ МВД РФ
88.	Не назначались
89.	Не назначали
90.	Не назначали
91.	Компьютерная
92.	Компьютерно-техническую судебную экспертизу в ЭКЦ МВД
93.	Не назначал
94.	Следователи назначают компьютерные экспертизы в ЭКЦ УВД
95.	Компьютерная ЭКЦ МВД по РК
96.	Не назначали

97. Нет
98. Нет
99. Не назначал
100. Не назначал
101. Затрудняюсь ответить
102. Ответ не положительный
103. Как было сказано ранее, компьютерно-техническая экспертиза в процессе которой при возможности определенные субъекты ОРД в системе ОВД восстанавливают утраченные-удаленные данные и цифровые следы
104. Не назначал
105. Компьютерные
106. Компьютерные ЭКЦ
107. -
108. Компьютерная
109. Не назначала
110. -
111. Не назначал.