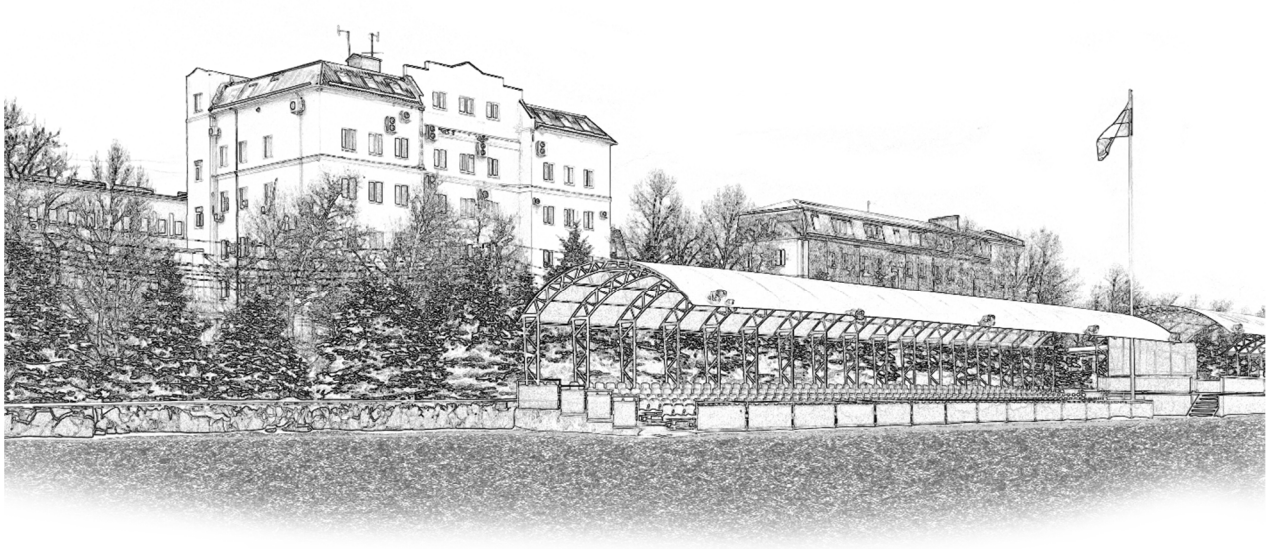
Краснодарский университет МВД России

О. Ю. Введенская

ОСОБЕННОСТИ ПРЕДВАРИТЕЛЬНОГО И ПЕРВОНАЧАЛЬНОГО ЭТАПОВ РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ



Краснодар
2025

Краснодарский университет МВД России

О. Ю. Введенская

ОСОБЕННОСТИ ПРЕДВАРИТЕЛЬНОГО И ПЕРВОНАЧАЛЬНОГО ЭТАПОВ РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Краснодар
2025

УДК 343.985
ББК 67.52
В241

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
О. Л. Подустова, кандидат юридических наук (Академия управления МВД России);
О. Л. Лазовская (Главное управление МВД России по Краснодарскому краю).

Введенская О. Ю.
В241 Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий / О. Ю. Введенская – Краснодар : Краснодарский университет МВД России, 2025. – 170 с.

ISBN 978-5-9266-2160-7

В монографии исследуются общественные отношения, складывающиеся в ходе предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий. Рассматриваются содержание и закономерности формирования криминалистической характеристики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, приводятся перспективные направления получения первоначальной информации о рассматриваемых преступлениях и алгоритмы ее проверки. Анализируется порядок использования специальных знаний, выделяются типичные следственные ситуации первоначального этапа расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, рассматривается порядок действий следователя, направленных на их разрешение.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.985
ББК 67.52

ISBN 978-5-9266-2160-7

Введение

Проблема наркомании на сегодняшний день является одной из наиболее серьезных угроз обществу. Практически ежедневно появляются новые виды наркотических средств, все большее количество людей оказываются вовлеченным в сферу деятельности, связанную с их сбытом и потреблением. Незаконный оборот наркотических средств представляет серьезную угрозу нормальному функционированию экономической сферы, здоровью населения и национальной безопасности.

Среди многообразия способов незаконного оборота наркотических средств наибольшую общественную опасность представляет их сбыт, поскольку, удовлетворяя потребительский интерес, он напрямую способствует наркотизации общества.

Преступники, осуществляющие незаконный сбыт наркотических средств, регулярно совершенствуют преступные навыки, используя в своей деятельности последние достижения науки и техники (малогабаритные воздушные и подводные беспилотные транспортные средства, современные телекоммуникационные технологии). Высокая эффективность применения информационных технологий в противоправной деятельности привела к тому, что преступность в информационно-телекоммуникационных сетях в целом признана первостепенной угрозой как на сегодняшний день, так и в перспективе[1].

Стратегия национальной безопасности Российской Федерации в качестве одной из основных задач государственной политики определяет предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в том числе незаконного распространения наркотических средств и психотропных веществ.

---

[1] См.: Бангкокская декларация «Партнерство во имя будущего» (Бангкок, 21 окт. 2003 г.) // Дипломатический вестник. 2003. № 11; Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 нояб. 2001 г.). Доступ из справ. правовой системы «КонсультантПлюс»; Окинавская хартия глобального информационного сообщества (о. Окинава, 22 июля 2000 г.) // Дипломатический вестник. 2000. № 8. С. 51–56; О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 2 июля 2021 г. № 400. Доступ из справ. правовой системы «КонсультантПлюс».

Общедоступность и достаточно широкие возможности сети Интернет делают ее удобной средой для развития общественных отношений любого вида (межличностной коммуникации, совершения финансовых операций, торговли и др.) в условиях трансграничности, удаленности, условной анонимности и децентрализации. Однако эти же свойства обусловливают повышенную общественную опасность преступлений, совершаемых в данной среде.

Исследование новых видов преступлений, специфических сред их совершения (например, сеть Интернет и ее криминогенная зона Даркнет, в которых в основном и осуществляется незаконный сбыт наркотических средств) – первоочередная задача криминалистики. Помимо расширения арсенала криминалистических знаний о способах совершения преступлений, механизмах следообразования, выявленные элементы преступной деятельности позволяют предложить действенные, практически значимые рекомендации по расследованию и предупреждению преступлений.

Анонимность, общедоступность, высокая скорость информационного взаимодействия, а также явное отставание правоохранительных органов в технических и правовых аспектах расследования преступлений, совершаемых с использованием информационных и телекоммуникационных технологий, отсутствие научно обоснованных методических рекомендаций по борьбе с рассматриваемым видом преступности значительно затрудняют противодействие ему.

Важность криминалистического исследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий определена непрерывно расширяющимися возможностями преступной деятельности, нехваткой специалистов в области информационной безопасности и недостаточной оснащенностью правоохранительных органов современными программно-аппаратными средствами в отличие от противостоящего им преступного мира.

Традиционной формой незаконного сбыта наркотических средств является их передача из рук продавца в руки покупателя. Однако с первых десятилетий XXI в. стали использоваться различные варианты скрытого размещения наркотических средств с информационным сопровождением (информирование о возможности покупки, цене, объеме, месте и времени размещения, условиях

получения и т. п.) посредством информационно-телекоммуникационных технологий. В настоящее время именно эта форма является доминирующей в структуре наркопреступности.

Активное использование преступниками новых информационных технологий привело к тому, что правоохранительные органы оказались не в полной мере готовы к эффективному расследованию таких преступлений. Около 90% опрошенных нами следователей указали на недостаточность профессиональных знаний, обеспечивающих расследование анализируемых преступлений, 98% отметили необходимость разработки частных методик их расследования.

Недостаточно разработанные методики подобного рода, пробелы в тактических рекомендациях производства отдельных следственных действий представляют собой значительную проблему теории криминалистики.

Таким образом, исследования криминалистических особенностей расследования преступлений, связанных с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий, являются актуальными как с теоретической, так и с практической точек зрения, поскольку могут значительно повысить эффективность борьбы с анализируемыми преступными проявлениями за счет улучшения качества работы с первоначальной криминалистически значимой информацией, ее проверки и последующего использования на первоначальном этапе расследования.

На сегодняшний день уголовно-правовые, криминологические и криминалистические вопросы борьбы с преступностью с использованием телекоммуникационных технологий достаточно подробно рассмотрены в работах Н.А. Архиповой, Р.С. Атаманова, Ю.В. Гаврилина, Н.Ю. Дусевой, Е.П. Ищенко, А.Н. Колычевой, В.С. Овчинского, А.Л. Осипенко, Е.Р. Россинской, А.А. Рудых, Д.А. Степаненко, Б.П. Смагоринского и других авторов.

Рекомендации по расследованию таких преступлений представлены в трудах Р.С. Атаманова, А.В. Варданяна, В.Б. Вехова, А.С. Егорышева, Д.А. Илюшина, С.А. Ковалева, И.Е. Мазурова, В.А. Мещерякова и др.

Также вопросы противодействия преступлениям, связанным с незаконным оборотом наркотических средств, в частности совершаемым путем их сбыта, достаточно подробно отражены в работах Е.С. Безруких, В.Ф. Васюкова, С.И. Земцовой, Е.А. Ошлыковой, А.С. Щуровой и других исследователей.

Российскими учеными подготовлен ряд научных статей, посвященных вопросам борьбы с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий (Е.Л. Глушков, А.В. Климачков, А.Л. Осипенко, П.В. Миненко, А.В. Шебалин и др.).

В монографии критически проанализированы положения теории и практики отдельных элементов расследования таких преступлений, уточнены существующие и сформулированы новые рекомендации по получению и использованию первоначальной криминалистически значимой информации и организации первоначального этапа расследования. Осуществлен криминалистический прогноз использования информационно-телекоммуникационных технологий для незаконного сбыта наркотических средств, выявлен механизм их использования при совершении рассматриваемых преступлений. Предложена типовая модель анализируемых противоправных деяний путем выделения и описания наиболее значимых элементов криминалистической характеристики рассматриваемой категории преступлений, определены корреляционные связи между ними. Определены наиболее перспективные методы и средства получения первоначальной криминалистически значимой информации об анализируемых преступлениях, разработаны рекомендации по проведению ее предварительной проверки. Выявлены особенности использования специальных знаний на первоначальном этапе расследования преступлений рассматриваемой категории, разработаны рекомендации, направленные на повышение его эффективности. Уточнены и дополнены рекомендации по производству отдельных следственных действий, направленных на определение пространственно-временных характеристик незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, а также по идентификации с их помощью личности пользователя.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Сущность незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

В настоящее время проблема употребления наркотиков приобретает все большую актуальность во всем мире. При этом на долю России на сегодня приходится 1/5 мирового наркотрафика[1].

Все способы незаконного оборота наркотических средств отражены в законе[2]. Это любые не санкционированные государством действия с ними. Вред, причиняемый незаконным оборотом наркотиков, рассматривается в двух аспектах – медицинском и социальном[3].

Очевидно, что наибольшую общественную опасность представляет их сбыт, так как он прямо обусловливает степень наркотизации общества.

Незаконный сбыт наркотических средств сегодня осуществляется в двух формах – традиционной и с использованием информационно-телекоммуникационных технологий.

Относительно реализации его традиционной формы все более или менее понятно: покупатель встречается со сбытчиком и приобретает его интересующие наркотические средства, наименование и условия продажи, как правило, распространяются в среде лиц, страдающих зависимостью от употребления наркотических средств. В свою очередь, незаконный сбыт наркотических средств

---

[1] См.: Стоп зависимость. Статистические сведения: сервис поиска реабилитационных центров и наркологических клиник. URL: https://stopz.ru/informaciya/narkomaniya/statistika-po-narkozavisimym-v-rossii/ (дата обращения: 09.02.2021).

[2] См.: О наркотических средствах и психотропных веществах: федер. закон от 8 янв. 1998 г. № 3-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[3] См.: Вьюнов А.В. Общественная опасность преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ // Уголовное право и криминология. 2006. № 11(62). С. 24.

с использованием информационно-телекоммуникационных технологий представляет особый интерес для исследования, поскольку большая его часть протекает в условиях неочевидности, скрытно от глаз правоохранительных и иных компетентных органов.

Ю.В. Гаврилин отмечает, что если до 2014 г. незаконный сбыт наркотиков осуществлялся в основном способом «из рук в руки», то с развитием информационно-телекоммуникационных технологий стали использоваться электронные торговые площадки, в частности в теневом сегменте сети Интернет[1].

Официальная статистика[2] лишь недавно обратила внимание на такие преступные проявления, показатели которых стали отражаться в отчетах, анализ которых свидетельствует о том, что число случаев незаконного сбыта наркотиков с использованием информационно-телекоммуникационных технологий стремительно растет в общей структуре преступлений рассматриваемого вида. А современные реалии дают основание полагать, что количество фактов совершения анализируемых преступных деяний значительно выше официально зарегистрированных. Это свидетельствует о высокой латентности исследуемых преступлений и о явном отставании органов правопорядка от лиц, осуществляющих незаконный сбыт наркотических средств рассматриваемым способом, в части технического и методического обеспечения, позволяющего эффективно выявлять, раскрывать и расследовать преступления, связанные с использованием информационно-телекоммуникационных технологий.

В частности, О.А. Решняк и С.А. Ковалев отмечают, что чем больше людей овладевают навыками работы с информационно-телекоммуникационными технологиями, тем больше таких преступлений совершается[3].

---

[1] Гаврилин Ю.В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4(56). С. 124.

[2] См.: Состояние преступности. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 25.01.2022).

[3] Решняк О.А., Ковалев С.А. Проблемы расследования преступлений, совершенных с использованием современных компьютерных технологий // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сб. ст. Межведомственного круглого стола и Всерос. круглого стола, 19 окт. 2016 г. Орел: Орлов. юрид. ин-т МВД России, 2017. С. 206–208.

Базовой структурой телекоммуникационных технологий являются сети электросвязи[1], локальные или глобальные, и, соответственно, используемые ими стандарты передачи данных (например, 2G – GSM/CDMA, 3G, 4G – LTE, 5G и др.). В связи с этим понятие телекоммуникационных технологий достаточно объемное и включает в себя средства коммуникации, т. е. оборудование, при помощи которого такие каналы могут функционировать (средства компьютерной техники, маршрутизаторы и т. п.), и различные методы, средства и алгоритмы передачи информации (например, телефонная связь, спутниковая связь, радиосвязь, Интернет).

Информационные технологии – это процессы обработки информации: текстовой, графической, мультимедийной, сетевой, баз данных и др.

Таким образом, на основе представленной характеристики можно определить информационно-телекоммуникационные технологии как совокупность программных и технических средств, методов и процессов обработки, хранения, представления и передачи информации[2].

Главенствующее же место в совершении незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий занимает «сеть сетей» – глобальная сеть Интернет, в связи с чем именно она и будет чаще всего упоминаться в исследовании.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть определена как технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[3].

---

[1] См.: Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. С. 133.

[2] См.: Гараев С.Т. Сущность информационно-телекоммуникационных технологий // Инновационная наука. 2016. № 6-2. С. 52–56.

[3] Об информации, информационных технологиях и о защите информации: федер. закон от 20 июля 2006 г. № 149-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

Глобальная сеть Интернет – это совокупность сетей, протоколов и сервисов различных организации и назначения. С их помощью осуществляется большой перечень мероприятий, в том числе направленных на совершение преступлений.

В основе организации любых информационно-телекоммуникационных технологий лежат строгие алгоритмы, устанавливающие порядок и условия их функционирования. Именно они определяют форму и содержание любых мероприятий, осуществляемых с их использованием, в частности направленных на совершение преступлений.

Незаконный сбыт наркотических средств, совершаемый рассматриваемым способом, представляет собой не единичный факт преступного сбыта наркотических средств, а совокупность взаимосвязанных, но осуществляемых асинхронно по отношению друг к другу транзакций, направленных на совершение множественных фактов незаконного сбыта наркотиков, осуществляемых как в материальном, так и в информационно-телекоммуникационном пространстве.

А.Л. Осипенко определяет сетевую преступность как предусмотренные уголовным законом общественно опасные деяния, совершенные на основе удаленного доступа к объекту посягательства с использованием глобальных компьютерных сетей как средства достижения цели[1].

Р.И. Дремлюга в своем исследовании рассматривает информационно-телекоммуникационную сеть Интернет как обособленное пространство, обладающее набором присущих только ему свойств, таких как удаленность, анонимность, неперсонофицируемость, отсутствие централизации (единого управления), высокая латентность, транснациональный характер[2].

Именно эти свойства делают компьютерные сети удобной площадкой для распространения большого количества разнородной общедоступной информации. Они же и затрудняют предупреждение, выявление и расследование преступлений, совершаемых с их использованием.

---

[1] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск: Омск. акад. МВД России, 2009. С. 103.

[2] Дремлюга Р.И. Интернет-преступность. Владивосток: Дальневост. ун-т, 2008. С. 46–50.

В.В. Агафонов и Л.Ю. Чистова отмечают, что практически бесконтрольное распространение тематических информационных материалов в сети Интернет подстрекает или побуждает к незаконному обороту наркотиков[1].

Например, общедоступные поисковые ресурсы[2] представляют порядка 8 млн результатов по запросу «купить наркотики»: ссылки на сайты по продаже наркотических средств, в том числе и оптом, рекомендации и подробные инструкции по их приобретению.

Аналогичная картина наблюдается и на других поисковых ресурсах.

Однако нельзя утверждать, что распространение информации в сети Интернет происходит совсем бесконтрольно. Государство предпринимает меры как законодательного, так и организационного характера, связанные с попытками ограничения и контроля информационной и технологической составляющей сети.

В частности, запрещенной к распространению в сети Интернет (причиняющей вред здоровью или развитию детей)[3] является информация, способная вызвать у детей желание употребить наркотические средства.

Также запрещена к распространению любая информация о способах незаконного оборота наркотических средств, распространяемая посредством сети Интернет[4]. Интернет-ресурсы, на которых она размещена, подлежат внесению в «Единый реестр доменных имен[5], указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интер-

---

[1] Агафонов В.В., Чистова Л.Ю. Способы совершения преступлений в сфере незаконного оборота наркотиков с использованием Интернета и электронных средств связи // Вестник Московского университета МВД России. 2011. № 3. С. 116.

[2] См.: www.yandex.ru; www.google.com

[3] См.: О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон от 29 дек. 2010 г. № 436-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[4] См.: Кодекс Российской Федерации об административных правонарушениях: федер. закон от 30 дек. 2001 г. № 195-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[5] Имя-символ, помогающее находить адреса интернет-серверов. URL: https://ru.wikipedia.org/?curid=29843&oldid=119919862 (дата обращения: 12.01.2021).

нет, содержащие информацию, распространение которой в Российской Федерации запрещено»[1] (далее – Реестр). Порядок формирования и функционирования Реестра определен подзаконными нормативными актами[2].

Обеспечить тотальный контроль государства за содержанием информационного сетевого контента невозможно, в связи с чем предпринимаются меры, направленные на воздействие на технологическую составляющую и связанные с ограничением возможности распространения такой информации и доступа к ней.

Все это отнесено к компетенции Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Оператор связи обязан аккумулировать и хранить информацию о трафике абонентов, ежедневно направляя его в Роскомнадзор, где он анализируется. При выявлении запрещенной информации в трафике абонентов, Роскомнадзор вносит ее в Реестр и доводит эти сведения до оператора связи, оказывающего услуги по предоставлению доступа к сети Интернет (Реестр обновляется каждые сутки в 9:00 и 21:00 час), который обязан незамедлительно проводить блокировку ресурсов с этой информацией[3].

---

[1] См.: Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] См.: О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено: постановление Правительства РФ от 26 окт. 2012 г. № 1101. Доступ из справ. правовой системы «КонсультантПлюс».

[3] См.: О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс»; О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей: федер. закон от 5 мая 2014 г. № 97-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс»; О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации: федер. закон от 28 июля 2012 г. № 139-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

Однако как организаторы соответствующих информационных ресурсов, так и их пользователи активно прибегают к различным способам обхода блокировки сайтов (используют программы-анонимайзеры[1], различные браузерные расширения[2], VPN[3] и др.).

В ответ на это Роскомнадзор активно внедряет новые технологии: например, если ранее анализировались заголовки сайтов и содержание стартовой страницы, то технология DPI[4] позволяет анализировать весь объем передаваемых с сайта данных. А также требует от операторов связи устанавливать специальное оборудование противодействия угрозам[5]. Однако реальные возможности контролирующих органов на сегодняшний день ограничены лишь соединениями, осуществляемыми через оператора связи.

За первое полугодие 2019 г. в Реестр был внесен лишь один интернет-ресурс с информацией о незаконных действиях с наркотическими средствами[6]. Учитывая объемы трафика информационных ресурсов соответствующей тематики, необходимо отметить, что это прямо указывает на использование иных телекоммуникационных технологий, обеспечивающих доступ к ресурсам сети Интернет и не попадающих под юрисдикцию контролирующих органов.

Существование таких технологий и дает почву для развития и процветания анализируемых преступлений.

Из вышесказанного следует, что государственному контролю подлежит именно информационная составляющая (содержание)

---

[1] Программный продукт для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера. URL: https://ru.wikipedia.org/?curid=1134937&oldid=117937134 (дата обращения: 14.01.2021).

[2] Встроенные в браузер программы, обеспечивающие функционирование дополнительных опций.

[3] Обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети. URL: https://ru.wikipedia.org/?curid=115247&oldid=119669730 (дата обращения: 14.01.2021).

[4] Технология проверки сетевых пакетов по их содержимому с целью регулирования и фильтрации трафика, а также накопления статистических данных. URL: https://ru.wikipedia.org/ ?curid=4175971&oldid=118835547 (дата обращения: 14.01.2021).

[5] См.: О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[6] См.: Результаты анализа сведений о выполнении мероприятий плана деятельности Роскомнадзора за 1 полугодие (2 квартал) 2019 года. URL: https://rkn.gov.ru/docs/docP_2550.pdf (дата обращения: 19.09.2019).

информационно-телекоммуникационных технологий, посредством которых и осуществляется незаконный сбыт наркотиков, причем значительная роль здесь отводится интернет-соединениям.

Результаты проведенного анализа уголовных дел свидетельствуют, что в 100% случаях сбытчиками наркотических средств использовались мессенджеры[1].

Осуществлять контроль их функционирования весьма сложно. Это обусловлено использованием ими как множества IP-адресов (их блокировка может затронуть иные интернет-ресурсы), так и технологий сквозного шифрования сообщений, что затрудняет целевую блокировку их источников. На протяжении последних лет государство периодически разрабатывает законопроекты о контроле за мессенджерами, как правило, связанные с идентификацией пользователей, что явно нарушает принципы организации сети Интернет. Однако на сегодняшний день каких-либо конкретных мер так и не принято.

Одной из возможных мер, позволяющих обойти контроль компетентных органов, представляется распространение информации посредством PUSH-уведомлений[2]. Контроль за их содержанием отнесен к компетенции разработчика. Сегодня по такому пути развивается мессенджер (социальная сеть) Telegram, являясь большой торговой площадкой, в частности и для продажи запрещенных к гражданскому обороту на территории Российской Федерации товаров.

Более сложный путь – разработка специальных приложений. Их функционирование также находится в ведении разработчика, что затрудняет контроль за ними. В то же время этот путь технически сложен и актуален до момента попадания в поле зрения компетентных органов.

Лица, использующие соответствующие информационные ресурсы, заинтересованы в обходе блокировки, в минимизации кон-

[1] Программа для мгновенного обмена сообщениями через Интернет. URL: https://ru.wikipedia.org/?curid=133371&oldid=119482795 (дата обращения: 19.09.2019).

[2] Один из способов распространения информации (контента) в Интернете, когда данные поступают от поставщика к пользователю на основе установленных параметров. Пользователь же, в свою очередь, либо отвергает, либо принимает данные. URL: https://ru.wikipedia.org/ ?curid=3713894&oldid=118505820 (дата обращения: 09.12.2021).

троля их функционирования, в сохранении трафика и, учитывая незаконное содержание распространяемой информации, в анонимности и в целевом охвате аудитории. Вследствие этого возможно прогнозировать переход к использованию еще не известных практике незаконного сбыта наркотических средств телекоммуникационных технологий, обеспечивающих доступ к тематическим сетевым информационным ресурсам, с применением которых он может быть совершен. В связи с этим особый интерес могут представлять сети и телекоммуникационные технологии малого радиуса действия, которые недоступны ни операторам, оказывающим услуги по предоставлению доступа к сети Интернет, ни Роскомнадзору:

технологии, работающие по протоколам ZigBee или IEEE 802.15.4[1], обеспечивающим функционирование сетей малого радиуса действия;

технологии Bluetooth, NFC (Near field communication) для рассылки рекламных материалов на малом расстоянии пользователям, использующим эту же технологию;

микроконтроллерные аппаратно-программные средства (типа Arduino[2] с использованием дополнительных плат и возможности программирования) для работы в режиме «клиент – сервер»[3], что открывает наркоторговцам особые возможности, например, WI-FI-роботы способны как осуществлять передачу данных на малом расстоянии (кафе, парки и иные места массового пребывания людей), выступая в роли ретранслятора или базовой станции, так и переносить на себе материальные объекты небольших размеров.

Также, анализируя стандартные интернет-технологии, стоит обратить внимание на такие прикладные программы, как социальные сети близкоконтактного взаимодействия (например, «Друг вокруг»[4]).

---

[1] Протоколы, обеспечивающие работу беспроводных персональных сетей передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей) малого радиуса действия.

[2] Торговая марка аппаратно-программных средств (программная оболочка и смонтированные печатные платы для построения простых систем автоматики и робототехники).

[3] Вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами. URL: https://ru.wikipedia.org/?curid=89964&oldid=115688996 (дата обращения: 14.01.2021).

[4] Социальная сеть, где выборка пользователей осуществляется согласно их геопозиции.

Анализ современной правоприменительной практики не выявил фактов использования таких телекоммуникационных технологий для незаконного сбыта наркотических средств, но их существование, активная разработка и внедрение позволяют сделать вывод об их соответствии потребностям наркоторговцев, а также прогнозировать их использование в преступных целях на ближайшую перспективу.

В связи с изложенным представляется целесообразным обратиться к такому направлению, как практическое криминалистическое прогнозирование, представляющее собой основанное на результатах практики предвидение особенностей криминалистической деятельности по борьбе с преступлениями конкретного вида[1]. Это позволит прогнозировать в ближайшей перспективе возможные направления и формы использования современных информационно-телекоммуникационных технологий для незаконного сбыта наркотических средств, дополнительных опций мессенджеров, специально разработанного прикладного программного обеспечения, сетей близкоконтактного взаимодействия и технологий малого радиуса действия.

Перечень информационно-телекоммуникационных технологий, которые будут использоваться, не является исчерпывающим, их стремительное развитие определяет возможность разработки с целью незаконного сбыта наркотических средств новых, еще не известных практике технологий.

Тем не менее представленный практический криминалистический прогноз использования современных информационно-телекоммуникационных технологий для незаконного сбыта наркотических средств даст возможность правоохранительным органам скорректировать существующие и разработать новые рекомендации по получению первоначальной информации об анализируемых преступлениях и ее проверке, по совершенствованию организационных, тактических и методических основ предварительного расследования.

---

[1] См.: Аверьянова Т.В. и др. Криминалистика: учеб. / под ред. А.И. Бастрыкина. М.: Экзамен, 2014. С. 212.

1.2. Понятие и структура криминалистической характеристики незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Расследование любого преступления начинается с постижения его криминалистической сущности. Ключевую роль в этом процессе играет формирование криминалистической характеристики преступления.

Первые упоминания о криминалистической характеристике преступления в современном ее понимании появились в 60–70-х гг. XX столетия.

Л.А. Сергеев и А.Н. Колесниченко выделяли наиболее типичные признаки преступлений, которые могут указать на перспективные направления расследования[1].

Р.С. Белкин также отмечал необходимость формирования криминалистической характеристики на основании признаков множества, характерных для конкретного вида преступлений, в целях определения наиболее рациональных направлений расследования[2].

М.В. Субботина видит назначение криминалистической характеристики преступлений в формировании следственных версий, особенно на первоначальном этапе расследования, когда известны не все обстоятельства совершенного преступления[3].

П.В. Абрамова, отмечая системный характер криминалистической характеристики, определяет ее целью обобщение данных о признаках определенного вида преступлений, установление и учет

---

[1] См.: Колесниченко А.Н. Общие положения методики расследования отдельных видов преступления. Харьков, 1965. 47 с.; Сергеев Л.А. Сущность и значение криминалистических характеристик преступлений: руководство для следователей. М.: Юрид. лит., 1971. С. 437.

[2] Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике. М.: Юрид. лит., 1988. С. 187.

[3] Субботина М.В. Расследование преступления на базе криминалистической методики // Роль и значение деятельности Р.С. Белкина в становлении современной криминалистики: материалы Междунар. науч. конф. (к 80-летию со дня рождения Р.С. Белкина). М., 2002. С. 176–179.

закономерных связей между ними, а также наличия качеств мысленной (информационной) модели расследования преступлений[1].

Ю.П. Гармаев называет целью существования криминалистической характеристики преступлений формирование методики расследования и определяет ее ценность в ходе проверки «теории практикой»[2].

Теоретическая значимость криминалистической характеристики преступлений состоит в том, что на ее основании сформированы методики расследования, включенные в учебные курсы[3]. Ее практическое значение заключено в том, что, имея информацию об одних элементах (например, о следах и орудиях совершения преступления), следователь, анализируя связи между ними, может предположить наличие и содержание других (например, определенных профессиональных навыков у преступника) и на основании полученных выводов, составив определенный план действий, запланировать к проведению необходимые следственные действия и иные мероприятия.

Таким образом, формирование криминалистической характеристики преступлений служит целям расследования и лежит в основе криминалистических методик. И если этот факт не является дискуссионным, то однозначное понимание сущности криминалистической характеристики в научной среде отсутствует.

Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская определяют криминалистическую характеристику как вероятностную модель события, которая может являться основанием для вероятностных умозаключений – следственных версий[4].

---

[1] Абрамова П.В. К вопросу о структуре криминалистической характеристики преступлений, совершенных против правосудия // Научный журнал КубГАУ. 2014. № 104(10). С. 1609.

[2] Гармаев Ю.П. Теоретические основы формирования криминалистических методик расследования преступлений: автореф. дис. … д-ра юрид. наук. М., 2003. С. 19.

[3] См.: Криминалистика: учеб. для вузов / под ред. А.Ф. Волынского. М.: Закон и право: ЮНИТИ-ДАНА, 1999. 615 с.

[4] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. 3-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2012. С. 657.

А.А. Закатов и Б.П. Смагоринский считают, что криминалистическая характеристика – это связанные в определенную систему криминалистически значимых сведений знания о типичных элементах преступления и условиях их совершения[1].

Е.П. Ищенко и А.А. Топорков рассматривают данное понятие в качестве абстрагированной от частностей модели преступления, содержание которой имеет практическое значение[2].

По мнению С.А. Ковалева и В.Б. Вехова, криминалистическая характеристика – это результат исследования, проводимого на типовой модели преступлений определенного вида, конечный результат и продукт этого модельного исследования, который в процессе конкретного практического расследования используется следователем для построения индивидуальной информационной модели криминального события[3].

Н.П. Яблоков считает, что криминалистическая характеристика преступлений является научно самостоятельной понятийной категорией криминалистики, имеющей значение как для ее общей теории, так и для практической следственной деятельности и особенно для методики расследования преступлений[4].

А.В. Шмонин предлагает заменить понятие «криминалистическая характеристика преступлений» на термин «технология преступлений», имея в виду не простой набор информации, а совокупность задач и приемов решения вопросов расследования, что, по его мнению, приблизит содержание данного понятия к нуждам практики[5].

В рамках существующего плюрализма мнений представляется наиболее объективной позиция О.Я. Баева, который говорит о криминалистической характеристике как о системе значимых

---

[1] Закатов А.А., Смагоринский Б.П. Криминалистика: учеб. Волгоград: Волгоград. акад. МВД России, 2000. С. 279.

[2] Ищенко Е.П., Топорков А.А. Криминалистика: учеб. для вузов. 2-е изд., испр., доп. и перераб. М.: Контракт, ИНФРА-М, 2010. С. 472.

[3] Ковалев С.А., Вехов В.Б. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: монография. М.: Буки-Веди, 2015. С. 48.

[4] Яблоков Н.П. Криминалистика: учеб. М.: Юриспруденция, 2005. С. 269.

[5] Шмонин А.В. Методология криминалистической методики: монография. М.: Юрлитинформ, 2010. С. 67.

для конкретного вида преступлений элементов и связях между ними, отмечая их главенствующее значение[1].

Таким образом, сущность криминалистической характеристики, помимо определенных, специфичных для отдельного вида преступлений элементов, заключается в криминалистически значимых связях между ними. Выявление этих взаимосвязей и представляет, с одной стороны, большую научную проблему, а с другой – ценность для процесса расследования, формируя за счет детерминирующих связей между элементами и их способности отражать признаки друг друга основу доказательственной базы.

Без установления таких корреляционных связей, носящих закономерный характер, криминалистическая характеристика представляет собой набор сведений, не имеющих никакого практического значения. Р.С. Белкин называл такие «научные» разработки «фантомами криминалистики»[2].

При рассмотрении места криминалистической характеристики преступления в методике расследования возникает вопрос ее соотношения с предметом доказывания. Эти понятия однозначно не тождественны, так как круг обстоятельств, подлежащих доказыванию, является исчерпывающим, строго определенным уголовно-процессуальным законом и единым для преступлений любого вида. В основе же криминалистической характеристики лежат наиболее типичные, обобщенные для конкретного вида преступлений признаки. Криминалистическая характеристика в сравнении с предметом доказывания вторична и является инструментом для установления содержания элементов последнего[3].

Сталкиваясь с определенным преступлением, следователь руководствуется личным опытом или опытом коллег, т. е. сложившейся правоприменительной практикой, предполагая, что совершенное преступление аналогично тем, по которым уже имеется ка-

---

[1] Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2001. С. 230.

[2] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: НОРМА, 2001. С. 221–222.

[3] См.: Кошелева И.С., Михальчук А.Е. Еще раз к вопросу о значении криминалистической характеристики преступлений // Проблемы противодействия преступности в современных условиях: материалы междунар. науч.-практ. конф. Уфа: РИО БашГУ, 2004. Ч. III. С. 130–131.

кой-либо опыт, выстраивает свои предположения на основе анализа и синтеза элементов, уже известных ему на определенном этапе расследования преступления.

Чем более типичным окажется совершенное преступление, тем больший успех принесет такой подход[1].

Однако в ходе правоприменительной практики необходимо помнить о том, что каждое преступление по своей природе индивидуально, лишь отдельные его элементы могут быть типичными, а могут и не быть таковыми[2].

Следует согласиться с мнением В.Ф. Ермоловича о том, что единой структуры криминалистической характеристики для различных видов преступлений быть не может[3].

Исследователи незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий представляют состав его криминалистический характеристики следующим образом.

А.А. Голубчикова ведет речь о совокупности сведений о лицах, совершающих незаконный сбыт наркотиков; о предмете преступления (понимая под ним предмет материального мира, на который воздействует преступник для достижения преступного результата); о месте совершения преступления, отмечая в качестве особенности криминалистической характеристики отсутствие потерпевшего[4].

Такая характеристика представляет собой набор не связанных и не отражающих признаки друг друга элементов, в связи с чем можно поставить под сомнение криминалистическую ценность.

---

[1] См.: Стороженко О.Ю. Понятие и структура криминалистической характеристики преступлений, совершаемых в российском сегменте сети Интернет // Казанская наука. 2014. № 11. С. 197.

[2] См.: Там же. С. 197.

[3] Ермолович В.Ф. Криминалистическая характеристика преступлений. Минск: Амалфея, 2001. С. 273–274.

[4] Голубчикова А.А. Криминалистическая характеристика незаконного сбыта наркотических средств – курительных смесей, совершенного бесконтактным способом // Молодежь и XXI век – 2018: материалы VIII Междунар. молодежной науч. конф.; Юго-Запад. гос. ун-т. Курск, 2018. Т. 3. С. 348–351.

Е.В. Кушпель и П.Е. Кулешов разрабатывают криминалистическую характеристику анализируемых преступлений вокруг способа их совершения, называя его бесконтактным, поскольку в этом случае непосредственный контакт приобретателя с наркосбытчиками отсутствует, а передача наркотических средств осуществляется путем производства «закладок». Исследователи выделяют элементы криминалистической характеристики такого способа: это лица, сбывающие и приобретающие наркотические средства; интернет-сайты, посредством которых размещается соответствующая информация; способы оплаты; способы подготовки и совершения[1].

По мнению О.А. Решняк, «бесконтактный» сбыт психоактивных веществ с использованием компьютерных технологий – это деятельность лица, направленная на возмездную либо безвозмездную передачу таких веществ другому лицу, при которой заинтересованные стороны не вступают в непосредственный (визуальный) контакт, условия их приобретения и оплаты обсуждаются посредством электронных средств связи, а получение – в заранее обговоренном и скрытом от посторонних лиц месте (тайнике)[2].

Таким образом, бесконтактный сбыт заключается в отсутствии непосредственного контакта между сбытчиком и покупателем в ходе совершения преступления (продажа, оплата, передачи и т. п.).

Все изученные эпизоды незаконного сбыта наркотических средств могут быть отнесены к совершенным «бесконтактным» способом. Абсолютное большинство респондентов (97%) отметили такой способ как наиболее популярный на сегодняшний день у наркосбытчиков. Однако в практической деятельности нередко встречаются и иные вариации, когда продажа наркотиков осуществляется с использованием информационно-телекоммуникационных технологий, но в последующем предполагает контакт покупателя со сбытчиком, т. е. вышеописанные схемы нарушаются.

---

[1] Кушпель Е.В., Кулешов Е.П. Криминалистическая характеристика и особенности организации первоначального тапа расследования незаконного сбыта наркотиков бесконтактным способом // Защитник закона. 2018. № 2. С. 105–114.

[2] Решняк О.А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота психоактивных веществ: дис. ... канд. юрид. наук. Волгоград, 2019. С. 12.

Например, *Г., желая избежать уголовного наказания за незаконный сбыт наркотических средств, предложил Ф., не поставив его в известность о своих истинных намерениях, за денежное вознаграждение оформить на свое имя грузоперевозку мебели из другого региона. В грузоотправлении содержался полимерный сверток с наркотическим веществом, который Г. намеревался лично передать лицу, приобретшему данное наркотическое вещество через специализированный сайт сети Интернет и заранее оплатившему «заказ» посредством платежных онлайн-сервисов переводом на имя Г.*

Таким образом, называть все факты сбыта наркотических средств, совершаемые с использованием информационно-телекоммуникационных технологий, «бесконтактными» неправильно. Кроме того, принимая во внимание и анализируя иные способы передачи наркотических средств в рамках изучаемых преступлений, возможно значительно обогатить их криминалистическую характеристику.

В.В. Клевцов представляет состав криминалистической характеристики незаконного сбыта наркотиков с использованием информационно-телекоммуникационных технологий весьма обширным: это обстоятельства совершенного преступления, способ совершения преступления, непосредственный предмет преступного посягательства, личность преступника и потерпевшего, механизм следообразования, данные о способах сокрытия преступлений, обстоятельства, способствующие совершению преступления[1].

В данной модели не конкретизированы элементы рассматриваемого преступления, ввиду чего они вряд ли смогут отражать свойства друг друга и иметь какие-либо связи между собой. То есть ее криминалистическая ценность крайне мала. Кроме того, представляется спорным существование такого элемента, как характеристика личности потерпевшего. По анализируемой категории уголовных дел в качестве потерпевшей стороны может выступать только Российская Федерация.

[1] Клевцов В.В. Особенности криминалистической характеристики преступлений, связанных с распространением «дизайнерских» наркотиков с использованием сети Интернет // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. тр. Всерос. науч.-практ. конф., 29 мая 2015 г. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 195–199.

А.М. Моисеев и С.В. Кондратюк выстраивают методику расследования рассматриваемых преступных посягательств на основе их криминалистически значимых признаков, выделяя в первую очередь их трансграничный характер[1].

Однако в основе работы информационно-телекоммуникационных систем и технологий лежат не признаки, а строгие алгоритмы функционирования, обеспечивающие достижение целей создания этих систем. Существование таких алгоритмов обеспечивает типичность элементов криминалистической характеристики рассматриваемого вида преступлений и наличие взаимосвязей между ними.

Например, для передачи данных в сети Интернет используется стек протоколов TCP/IP[2] – это набор строгих правил (алгоритмов), образующий стандарт передачи данных.

Свойства анализируемых преступлений отражены в обстановке их совершения и определяются двойственностью природы информационно-телекоммуникационных технологий.

С одной стороны, информационно-телекоммуникационная сеть Интернет представляет собой информационную площадку, где на серверах аккумулируется и хранится большой объем разнородной и общедоступной информации – от технологий производства до незаконного сбыта наркотических средств: «где взять?», «из чего приготовить?», «как использовать?», «где хранить?», «как перевезти/продать?», «кто это может сделать?». Ответы на эти вопросы можно найти на информационных ресурсах сети Интернет, являющейся средой незаконного оборота наркотических средств. Это отражается в таких свойствах рассматриваемых преступлений, как массовость (охват большой аудитории) и использование больших объемов разнородной информации, и составляет информационную составляющую технологий рассматриваемого вида.

С другой стороны, Интернет – особая среда, в рамках которой протекают различные коммуникационные процессы: обеспечение доступа к хранящейся информации, ее обработка и передача. Все

---

[1] Моисеев А.М., Кондратюк С.В. Криминалистические признаки наркосбыта посредством сети Интернет // Балканский юридический вестник. 2017. № 1. С. 43–46.

[2] Набор сетевых протоколов, на которых базируется работа Интернета. URL: https://ru.wikipedia.org/?curid=601749&oldid=114435509 (дата обращения: 25.05.2021).

это осуществляется посредством использования сетевых протоколов, программных средств и аппаратного обеспечения, что и образует информационно-телекоммуникационную систему. Совокупность правил осуществления этих процессов и составляет вышеобозначенные строгие алгоритмы, что обусловливает технологическую (материальную) составляющую информационно-телекоммуникационных технологий и отражается в таких свойствах анализируемых преступлений, как коммуникативный характер (совершение преступления за счет постоянной связи между его участниками), технологичность (функционирование алгоритмов, лежащих в основе преступного деяния, по определенным правилам и стандартам) и дистанционность (удаленность).

Таким образом, за счет двойственной природы информационно-телекоммуникационных технологий (информационно-технологической) криминалистическая характеристика анализируемых преступлений включает в себя как элементы, типичные для незаконного сбыта наркотических средств, совершенного традиционным (без использования информационно-телекоммуникационных технологий) способом: предмет[1], время совершенного преступления[2], личность приобретателя наркотиков[3] и иные, описанные в ранних исследованиях, так и элементы с взаимными связями, являющимися ключевыми в формировании информационной модели преступления, содержание которых типично для анализируемых преступлений:

криминалистически значимые сведения о *способах* совершения таких преступлений, которые определяются алгоритмами функционирования используемых информационно-телекоммуникационных технологий;

---

[1] См.: Крайнова П.Ю. Особенности отдельных элементов криминалистической характеристики сбыта наркотических средств и психотропных веществ на территории учреждений ФСИН России // Юридическая наука и практика: альманах науч. тр. Самар. юрид. ин-та ФСИН России. Самара, 2016. С. 135–137.

[2] См.: Дондуков Б.Г. Криминалистическая характеристика времени незаконного сбыта наркотических средств, психотропных веществ или их аналогов // Вестник Сибирского юридического института МВД России. Право. 2010. № 1(5). С. 176–179.

[3] См.: Кусмарцев Н.А. Основные элементы криминалистической характеристики незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов // Государство и право в условиях гражданского общества: сб. ст. Междунар. науч.-практ. конф. Уфа, 2015. С. 48–50.

способы совершения преступлений, в свою очередь, формирующие обстановку их совершения и обусловливающие механизм *следообразования*;

сведения *о личности* типичных преступников (в частности, об их умениях и навыках) определяют содержание конкретного способа преступления, что отобразится в его следах; криминалистически значимые сведения о лицах, прямо не связанных общим умыслом с наркосбытчиками, но обеспечивающих возможность совершения незаконного сбыта наркотических средств рассматриваемым способом (о создателях используемых в преступных целях информационно-телекоммуникационных технологий и систем) также лягут в основу *способа* совершения преступления, его *следов* и *типичной обстановки*;

об *обстановке* совершения преступления: круг таких сведений в отличие от иных преступлений не ограничивается совокупностью условий окружающей среды, существующих в определенный отрезок времени[1]. Большая часть незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий протекает в информационно-телекоммуникационном пространстве, следовательно удаленно, разрозненно во времени и пространстве и т. п.[2], и представляет собой совокупность условий, необходимых для работы таких технологий и систем, для реализации заданных условий их функционирования.

Использование конкретного аппаратного средства или программного продукта оставит определенные следы, обнаружение которых возможно только в местах, связанных с его функционированием. Для использования этого продукта или средства необходимы определенные знания и умения, а характеристики процесса его функционирования обусловят обстановку совершенного преступления.

Например, следователь располагает информацией, что для рассылки рекламы интернет-магазина по продаже наркотических

[1] См.: Голубчикова А.А. Указ. соч. и др.

[2] См.: Дремлюга Р.И. Указ. соч. С. 46–50.

средств в социальной сети «Одноклассники» преступники использовали программу-бот[1]. Зная алгоритм функционирования этой программы, можно установить место нахождения следов этого действия (в нем будут отражены все задействованные этапы и узлы), детализировать механизм их образования (порядок совершаемых действий), найти источник следообразующего воздействия, составить представление о некоторых навыках и умениях преступника, конкретизировать возможные элементы обстановки преступления. Объединив их со сведениями, полученными в рамках аналогичного анализа других используемых программных и аппаратных средств, можно составить информационную модель совершенного преступления. По аналогичной схеме могут быть восполнены и иные информационные пробелы.

Таким образом, криминалистическая характеристика незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий – это абстрактная модель, полученная в результате изучения процессов функционирования информационно-телекоммуникационных технологий и систем, в которой обобщены типичные сведения об основных элементах незаконного сбыта наркотических средств, а также особенностях сбыта наркотических средств, совершаемого с их использованием.

Ее состав определяется двойственной природой преступления (материальной и информационной) и, помимо элементов, характеризующих его материальную плоскость (место, время, предмет преступного посягательства и др.), включает элементы, обусловленные технологической сущностью совершаемых преступлений (способ совершения преступления, формируемые следы, личность преступника, двойственная обстановка, обеспечивающая возможность их совершения) и существующие в рамках строгих алгоритмов функционирования используемых в преступном процессе информационно-телекоммуникационных систем и технологий, предопределяющих возможность выделения жестких связей между ними.

Наличие таких связей обусловливает типичность элементов криминалистической характеристики анализируемых преступлений и

[1] Программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия и имеющая в этом некое сходство с человеком. URL: https://ru.wikipedia.org/ ?curid=9860&oldid=119695929 (дата обращения: 30.01.2021).

позволяет предположить через содержание известных содержание еще не установленных, а также прогнозировать их качественную составляющую на первоначальном этапе расследования.

1.3. Типичные способы незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Как указывал Р.С. Белкин, знания о способе совершения преступления – путь познания истины по делу[1].

Определение способа совершения преступления позволяет раскрыть содержание преступных действий и на основании этого выбрать наиболее эффективные направления расследования. В связи с изложенным способ совершения преступления можно смело назвать ключевым звеном криминалистической методики расследования отдельных видов преступлений.

В условиях активно развивающейся, причем как качественно, так и количественно, преступности в сфере незаконного оборота наркотиков, а также постоянного интенсивного развития технической сферы изучение и использование данных о способах незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий приобретает особое значение.

В первую очередь, способ совершения преступления представляет собой систему обусловленных целью и мотивами, психическими и физическими особенностями преступника приемов, действий, в которых находят отражение особенности человека, его знания, умения, навыки, привычки и иные характеристики[2]. Именно это и лежит в основе его связи с другими элементами криминалистической характеристики преступления.

Криминалистика (в широком смысле) в понятие «способ совершения преступления» включает такие элементы, как мероприятия по

---

[1] См.: Белкин Р.С. Курс криминалистики: учеб. пособие. М.: ЮНИТИ-ДАНА: Закон и право, 2001. С. 805.

[2] См.: Еникеев М.И. Юридическая психология: учеб. для вузов. М.: НОРМА, 2001. С. 105.

подготовке преступления, способы его непосредственного совершения и действия по сокрытию[1].

В.В. Новик, рассматривая криминалистическое содержание способа совершения преступления, определяет его как комплекс действий по подготовке, совершению (исполнению) и сокрытию преступления[2].

Еще Р.С. Белкин указывал на факт существования полноструктурного способа совершения преступления, обосновывая неоспоримую теоретическую и практическую значимость его рассмотрения как системы действий по подготовке, совершению и сокрытию преступления, предопределенных условиями внешней среды и психофизическими свойствами личности[3].

А.С. Князьков предлагает следующие варианты полноструктурного способа совершения преступления:

а) преступление совершено без подготовки и сокрытия, в результате внезапно возникшего умысла на посягательство;

б) преступление было подготовлено, однако его сокрытие не производилось;

в) преступление не было подготовлено, однако осуществлялось его сокрытие;

г) совершено неосторожное преступление[4].

Ряд ученых также представляют структуру способа совершения преступления в виде различных совокупностей мероприятий по его подготовке, совершению и сокрытию[5].

---

[1] См.: Харлов А.С. Способ совершения преступления как элемент криминалистической характеристики хищений сотовых телефонов // Бизнес в законе. 2010. № 1. URL: http://cyberleninka.ru/article/n/sposob-sovershheniya-prestupleniya-kak-element-kriminalisticheskoy-harakteristiki-hischeniy-sotovyh-telefonov (дата обращения: 17.10.2018).

[2] См.: Новик В.В. Способ совершения преступления. Уголовно-правовой и криминалистический аспекты. СПб., 2002. С. 32.

[3] См.: Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования / под ред. Р.С. Белкина, Т.В. Аверьяновой. М.: Новый юрист, 1997. С. 131–133.

[4] Князьков А.С. Криминалистическая характеристика преступления в контексте его способа и механизма // Вестник Томского государственного университета. Право. 2011. № 1. С. 54.

[5] См.: Колмаков В.П. Следственный осмотр. М.: Юрид. лит., 1969. 196 с.; Куранова Э.Д. Об основных положениях методики расследования отдельных видов преступлений // Вопросы криминалистики. М.: Госюриздат, 1962. Вып. 6–7. С. 152–167; Ермолович В.Ф. Криминалистическая характеристика преступлений. Минск: Амалфея, 2001. С. 54–55 и др.

А.Л. Дудников, напротив, считает невозможным выделение единой структуры способа совершения различных преступлений[1].

А.Л. Осипенко делает вывод, что для рассматриваемых способов характерна следующая схема: подготовка к преступлению; основной этап реализации противоправных действий; устранение следов; использование результатов[2].

Особая криминалистическая значимость способа совершения преступления, как отмечают отдельные авторы, состоит в том, что для каждого вида преступления существует свой системный набор действий[3].

В.В. Агафонов и Л.Ю. Чистова включают в способ незаконного сбыта наркотических средств с использованием сети Интернет и электронных средств связи следующие действия:

подготовительные: подготовку тайников, разработку маршрута движения к ним;

непосредственный сбыт: размещение информации о продаже наркотических средств на ресурсах сети Интернет, их фасовка в соответствии с заказом, продажа через курьера, оставляющего «закладки»;

действия, направленные на сокрытие анализируемого преступления, проводятся на стадии подготовки[4].

Е.Л. Глушков отмечает организованный характер рассматриваемой преступности и считает ее отправной точкой создание организатором соответствующего ресурса в сети Интернет, далее осуществляются приобретение наркотиков в целях последующей

---

[1] Дудников А.Л. Криминалистическое понятие «способ преступления» // Проблемы законности. 2012. № 120. С. 232–242.

[2] Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск: Омск. Акад. МВД России, 2009. С. 243.

[3] См.: Гавло В.К., Клочко В.Е., Ким Д.В. Криминалистическая характеристика преступлений как направление познания и систематизации криминалистически значимой информации о преступной деятельности, необходимой для решения криминалистических задач в складывающихся судебно-следственных ситуациях // Судебно-следственные ситуации: психолого-криминалистические аспекты / под ред. В.К. Гавло. Барнаул: Алтай. ун-т, 2006. С. 116.

[4] Агафонов В.В., Чистова Л.Ю. Способы совершения преступлений в сфере незаконного оборота наркотиков с использованием Интернета и электронных средств связи // Вестник Московского университета МВД России. 2011. № 3. С. 119–121.

продажи, фасовка, обработка заказов и организация их получения конечным потребителем[1].

О.А. Решняк называет способ незаконного сбыта психоактивных, в частности наркотических, веществ с использованием компьютерных технологий бесконтактным, когда их передача от продавца покупателю исключает личный контакт заинтересованных сторон[2].

Большинство представленных выше схем соответствуют структуре «традиционного» преступления и не могут быть названы полными, так как не конкретизируют перечень основных мероприятий, связанных с использованием информационно-телекоммуникационных технологий. Кроме того, ни одна из них, за исключением представленной А.Л. Осипенко, не содержит упоминания об использовании преступных результатов, что является неотъемлемой частью способа совершения преступления.

Таким образом, анализируя способы незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, можно сделать следующие выводы.

Способы совершения рассматриваемого преступления в общем виде являются полноструктурными, т. е. они включают в себя все возможные элементы (этапы). При этом они не соответствуют какой-либо из вышеприведенных форм, так как границы этапов размыты (например, мероприятия по подготовке и сокрытию реализуются на протяжении всего преступления), что обусловлено множественностью преступных фактов (транзакций[3]) в рамках единого преступления.

Способы совершения анализируемых преступлений включают в себя три основных этапа: организационный, рабочий и использование преступных результатов. Но такое разделение обусловлено не столько следованием этапов друг за другом, сколько их содержанием и назначением. Специфика незаконного сбыта

---

[1] Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 2. С. 45–53.

[2] См.: Решняк О.А. Указ. соч. С. 12–13.

[3] Группа логически объединенных последовательных операций по работе с данными, обрабатываемая или отменяемая целиком. URL: https://ru.wikipedia.org/?curid=1063938&oldid=111941905 (дата обращения: 24.01.2021).

наркотических средств с использованием информационно-телекоммуникационных технологий состоит в том, что пока реализуется организационный этап для одной партии наркотических средств (например, создание условий для передачи наркотического средства), ведется подготовка незаконного сбыта другой и использование преступных результатов, полученных в результате ранее осуществленного незаконного сбыта наркотиков. И таких одновременно осуществляемых транзакций, образующих единое преступление, может быть неограниченное количество.

Мероприятия *организационного этапа* заключаются в создании благоприятных условий для совершения преступления и в обеспечении бесперебойной работы преступников. Они осуществляются до, во время и после совершения преступления.

Необходимо отдельно рассмотреть вопрос организации торговых площадок (используемых как для продажи наркотических средств, так и для их приобретения в целях последующей продажи), поскольку именно они определяют алгоритмы функционирования используемых в преступных целях информационных систем и ресурсов, детерминирующие связь элементов криминалистической характеристики. В 100% изученных уголовных дел наркосбытчики для размещения интернет-магазинов использовали уже действующие площадки (информационные ресурсы) в сети Интернет. Сегодня представляются актуальными следующие варианты их организации.

1. С использованием Даркнета[1] – анонимной сети[2], существующей в рамках Tor-соединений[3], защищенных и скрытых.

---

[1] Скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. URL: https://ru.wikipedia.org/?curid=5269174&oldid=119722570 (дата обращения: 01.02.2022).

[2] Компьютерная сеть, созданная для достижения анонимности в Интернете и работающая поверх глобальной сети. URL: https://ru.wikipedia.org/?curid=1900707&oldid=118861412 (дата обращения: 25.01.2022).

[3] Система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. URL: https://ru.wikipedia.org/?curid=2680264&oldid=119884969 (дата обращения: 07.02.2022).

Это различным образом организованные одноранговые сети[1], в которых информация поступает от одного компьютерного устройства к другому.

Такие технологии объединения отдельных компьютеров в единую сеть ни в коей мере не являются преступными и появились еще до возникновения самой сети Интернет. Однако именно к ним было приковано внимание криминального мира, поскольку они могут использоваться для дистанционного взаимодействия (реализовывать различные формы передачи информации и интерактивного общения), не предполагают управления из единого центра и, как следствие, не поддаются эффективному контролю и внешнему мониторингу[2].

Если ранее этот способ организации торговых площадок представлял практически безграничный простор для противоправной деятельности, то после ареста создателя сайта SilkRoad[3] его популярность значительно снизилась в связи с преданием гласности основных параметров его функционирования. Вместе с тем возможности использования данного способа в противоправных целях остаются весьма значительными и по сей день.

На российском же даркнет-рынке лидирующее место занимает схожая торговая площадка Hydra (Гидра).

2. С использованием стандартных интернет-соединений. Речь ведется как о создании специализированных криминальных интернет-ресурсов (содержащих запрещенную к распространению информацию[4]), так и об использовании уже правомерно существующих (например, социальные сети, мессенджеры, баннеры на вебсайтах и т. п.) в преступных целях.

---

[1] Созданная поверх другой сети компьютерная сеть, основанная на равноправии участников (каждая рабочая станция одновременно является и клиентом, и сервером, как отвечая на запросы других, так и направляя свои).

[2] См.: Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. С. 119.

[3] С англ. «Шелковый путь» – анонимная торговая интернет-площадка, находившаяся в зоне .onion анонимной сети Tor и работавшая с 2011 по 2013 г. URL: https://ru.wikipedia.org/? curid=3984697&oldid=118882341 (дата обращения: 25.12.2021).

[4] См.: О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон от 29 дек. 2010 г. № 436-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс» и др.

3. В рамках ранее обозначенных, еще не используемых для незаконного сбыта наркотических средств, но весьма перспективных для достижения анализируемых преступных целей телекоммуникационных технологий (специально разработанные приложения, сети и технологии близкоконтактного взаимодействия, малого радиуса действия и др.). Это еще неизвестный практике способ организации торговых площадок, однако в скором времени он, вероятно, станет весьма распространенным.

Специфика содержательной части *рабочего этапа* анализируемых преступлений связана как с особенностями приобретения наркотиков, которые будут отражены в алгоритмах функционирования торговых площадок, так и со способом передачи наркотических средств их приобретателю. В 100% изученных уголовных дел она осуществлялась в форме закладок, т. е. бесконтактно, что в общем представляется типичным для рассматриваемой категории преступлений. Однако как отмечалось выше, в практике анализируемых преступлений встречаются и исключения.

Согласно постановлению Верховного Суда РФ[1] незаконный сбыт наркотических средств считается оконченным преступлением с момента выполнения лицом всех необходимых действий по их передаче приобретателю независимо от их фактического получения им.

Таким образом, реализация рабочего этапа включает в себя две части: непосредственную продажу и доставку. Данный этап может быть усечен в случае пресечения преступной деятельности после продажи наркотических средств, что не влияет на общую квалификацию преступления.

Классификация способов, составляющих рассматриваемый этап, может быть проведена как в зависимости от наименования торговых площадок для продажи наркотиков (что обусловит использование определенных информационно-телекоммуникационных технологий, задействованных в их работе), так и в зависимости от порядка передачи наркотиков потребителю (производство закладок, личная передача, передача через посредников и т. п.).

[1] См.: О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ от 15 июня 2006 г. № 14. Доступ из справ. правовой системы «КонсультантПлюс».

В связи с тем, что незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий относится к категории сетевых преступлений, значительную роль играют *мероприятия, направленные на использование полученных за незаконный сбыт наркотиков денежных средств*. Все финансовые операции проводятся с использованием заранее подготовленных средств: электронных кошельков, онлайн-сервисов, криптовалюты и т. п. Часть вырученных денежных средств распределяется между преступниками, другая же часть направляется на обеспечение дальнейшей незаконной деятельности: на приобретение наркотических средств, реагентов, оплату торговой площадки, услуг третьих лиц и др. То есть эти мероприятия носят также и организационный характер, они замыкают «преступный круг», одновременно являясь началом и концом анализируемой преступной деятельности.

Мероприятия, связанные с использованием информационно-телекоммуникационных технологий, определяют содержание информационной составляющей преступления, а не связанные с ними – материальной, что характеризует процессы, протекающие в ходе их реализации.

Материальная составляющая способа совершения преступления представляет собой действия в реальном физическом пространстве (непосредственное получение наркотических средств и реагентов для их изготовления, производство, фасовка, хранение, перемещение, распределение преступных ролей и т. п.), в рамках которых будут задействованы соответствующие субъекты и объекты материального мира.

Информационная же составляющая рассматриваемых способов представляет собой результат функционирования используемых информационно-телекоммуникационных технологий и объектов. Это способ подключения к сети Интернет, организация торговых площадок, различные информационные ресурсы, содержащие сведения об источниках получения наркотических средств и реагентов, о методиках их изготовления, рекомендации по хранению и перемещению наркотиков, данные о возможности приобретения специальных средств для этого, примеры схем незаконного сбыта, финансовые инструменты для осуществления расчетов, отдельные элементы схем обналичивания преступных доходов и мер

конспирации, рекламные и кадровые (подбор персонала преступных организаций) возможности, средства коммуникации участников незаконного сбыта и т. п.

Ю.Н. Жданов и В.С. Овчинский называют отличительной чертой нашего времени окончательное стирание границ между реальностью и виртуальностью[1].

В связи с этим нет необходимости рассматривать вопрос о том, какая составляющая способа первична, а какая вторична. Представляется, что материальная и информационная составляющие способов совершения преступлений равнозначны и существуют параллельно, обеспечивая реализацию друг друга.

Такое разделение всех рассматриваемых в рамках конкретного способа совершения преступления мероприятий на две взаимосвязанные части (плоскости) позволяет определить направление и содержание поисковых действий.

Специфика рассматриваемого способа совершения незаконного сбыта наркотических средств заключается в том, что он представляет собой не линейную последовательность простых действий, а одновременно протекающие взаимосвязанные последовательности действий в реальном (физическом) и информационном пространстве – транзакции, представляющие собой цепочки элементарных, осмысленных, логически законченных операций по передаче, получению и использованию объектов, по получению, передаче, хранению и преобразованию информации. Содержание этих операций практически полностью определяется алгоритмами работы используемых информационно-телекоммуникационных систем и ресурсов. Каждая транзакция – конкретный факт незаконного сбыта наркотических средств. Они существуют параллельно и асинхронно друг с другом в рамках способа совершения преступления. Между мероприятиями внутри транзакций существует строгая логическая связь.

Начало транзакции – это получение и обработка (уяснение требований и согласование условий выполнения) заказа, далее следует оплата, без которой, естественно, наркотические средства заказчику переданы не будут. Требуемые масса и наименование товара обозначаютя в заказе и т. д. Общие (узловые) мероприятия

[1] Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. С. 16.

способа будут едины для всех транзакций, они носят обеспечительный характер, их проведение осуществляется на протяжении всего преступного процесса параллельно транзакциям (они повторяются, изменяются, совершенствуются и т. п.). А индивидуальные мероприятия присущи конкретному акту незаконного сбыта наркотических средств, осуществляемого анализируемым способом, они обусловлены особенностями его проведения и индивидуализируют каждый преступный факт.

Каждая транзакция, в свою очередь, состоит из ряда действий, направленных на ее осуществление. Последовательность их реализации как частей единого целого обусловлена формой организации торговой площадки, а также алгоритмами функционирования используемых информационно-телекоммуникационных систем и ресурсов.

Например, организация незаконного сбыта наркотических средств в рамках Даркнета подразумевает использование Tor-соединений (обеспечивающих анонимность), доменов .onion, с которыми не могут работать стандартные соединения, VPN-сетей (обеспечивающих повышенную конфиденциальность), нестандартных коммуникационных портов и протоколов[1].

При этом для работы в Даркнете наркосбытчику следует:

провести организационные мероприятия в материальной составляющей способа совершения преступлений, обеспечивающие возможность использования этой формы организации торговой площадки для сбыта наркотических средств;

скачать и установить Tor-браузер;

установить VPN-соединение;

создать анонимную личность, от лица которой будет осуществляться коммуникация (создание адреса электронной почты, регистрация на соответствующих ресурсах, размещение информационного контента магазина и т. п.);

параллельно вести работу в реальном (физическом) пространстве, т. е. реализовать мероприятия всех обозначенных выше этапов.

[1] См.: Гаврилин Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: науч.-практ. пособие. М.: Акад. управления МВД России, 2021. С. 45–46.

Информационная составляющая способа совершения преступлений определяет содержание материальной.

Мероприятия, проводимые в физическом пространстве, представляют собой достаточно простые традиционные действия, зачастую не являющиеся сами по себе преступными. Применительно к мероприятиям информационной сферы речь ведется о разделении конкретного действия на множество других, обусловленных алгоритмами и принципами функционирования информационных систем, технологий и ресурсов.

Причем в рамках криминалистической характеристики говорят о нормальном функционировании используемых систем и ресурсов в соответствии с алгоритмами и параметрами, заложенными в них. Именно это и обеспечивает типичность ее элементов. Однако с точки зрения криминалистической технологии и с учетом материальной составляющей способа совершения преступления нарушения каких-либо заданных параметров функционирования используемых систем и ресурсов тоже будут иметь определенные вариации. Что, соответственно, вновь обеспечит типичность элементов преступления, существующих в этом режиме работы.

Таким образом, рассмотрев содержание типичных способов незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, можно прийти к выводу, что они представляют собой совокупность действий как в физическом, так и в информационном пространстве. Структура способов характеризуется не временной (подготовка, совершение, сокрытие), а логической последовательностью действий. Мероприятия, направленные на достижение преступного результата, выполняются по мере необходимости. Достижение положительного результата одного из них не влечет за собой реализацию следующего, а определяет необходимость проведения целого ряда других мероприятий, зачастую разнородных, но связанных с выполненным тем же преступным умыслом и обусловленных заданными алгоритмами функционирования информационно-телекоммуникационных систем, технологий и ресурсов. Содержание способов совершения анализируемых преступлений позволяет выделить взаимообеспечивающие друг друга материальную и информационную составляющие. Мероприятия материальной составляющей представляют собой действия в физическом пространстве и

носят обеспечительный характер, а информационной – состоят из ряда взаимосвязанных транзакций (осуществляемых преимущественно в информационной плоскости преступления), последовательность действий внутри которых определяется алгоритмами функционирования используемых информационно-телекоммуникационных систем, технологий и ресурсов. Все это обеспечивает типичность способа совершения анализируемого преступления как элемента криминалистической характеристики, позволяет определять направления и тактику поиска преступника, эффективно организовать следственные действия и оперативные мероприятия на первоначальном этапе расследования.

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

Независимо от выбранного преступником способа совершенное преступление, как и всякий материальный процесс, оставляет следы в окружающей обстановке и в сознании людей.

Переносятся отображения в воспринимающие их объекты при помощи различных форм движения – физического, химического, биологического, социального (психического) и др., что зависит от природы оригинала и отражающего объекта. Изучением закономерностей возникновения этих следов и построением оптимальных и эффективных технологий их выявления, сбора, хранения, переработки, передачи и использования для познания события преступления и связанных с ним обстоятельств занимается криминалистика[1].

Термин «след» может быть употреблен как в процессуальном, так и в криминалистическом значении[2].

---

[1] См.: Безруких Е.С. Особенности взаимодействия следователя и оперативного работника на первоначальном этапе расследования преступлений в сфере незаконного оборота наркотиков: дис. … канд. юрид. наук. Калининград, 2003. С. 84–86.

[2] См.: Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 210.

Процессуальное значение следа заключается в возможности формирования на основе отображаемой им информации доказательственной базы.

Криминалистика же рассматривает «след» в более широком смысле и включает в него всю совокупность получаемой информации, которая может быть использована для розыскных мероприятий, выдвижения поисковых версий, определения направления действий следователя и т. п.

В криминалистике следы преступления принято разделять на идеальные и материальные. Такие следы называют традиционными[1].

По мнению Н.П. Яблокова, основными в способе совершения преступления как объективно и субъективно обусловленной системе поведения субъекта на протяжении совершения преступления выступают именно материальные и идеальные следы[2].

Идеальным следом принято называть отображение события в сознании человека, мысленный образ его восприятия, существующий в виде показаний свидетелей, потерпевших, подозреваемых и обвиняемых, экспертов и т. п.

Ю.Г. Корухов отмечает, что именно следовой контакт, «обусловленный системой сил, определяющих направление взаимных перемещений», определяет объем и качество информации[3].

Очевидно, что постоянное изменение средств и способов совершения преступлений, их развитие влечет за собой возникновение качественно новых видов следов преступной деятельности, что требует внимания ученых-криминалистов.

Так, В.А. Мещеряков[4] дополняет ранее предложенную классификацию, выделяя виртуальные следы, оставленные в ходе совершения компьютерных преступлений.

Современные исследователи называют виртуальными следы совершение любых действий (включение, создание, открывание, активация, внесение изменений, удаление) в информационном

---

[1] См.: Филиппов А.Г. Криминалистика: учеб. 2-е изд., перераб. и доп. М.: Спарк, 2000. С. 73.

[2] Яблоков Н.П. Криминалистика: учеб. М., 2012. С. 34–35.

[3] Корухов Ю.Г. Трасология и трасологическая экспертиза: учеб. / отв. ред. И.В. Кантор. М.: ИМЦ ГУК МВД России, 2002. С. 20.

[4] Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронеж. гос. ун-т, 2001. С. 74–76.

пространстве компьютерных и иных цифровых устройств, их систем и сетей[1].

В.В. Поляков также признает существование виртуальных следов преступления. Дополняя мнения предыдущих исследователей, он отмечает, что в отношении виртуальных следов не может быть применено деление в зависимости от механизма следообразования, характерного для других видов преступлений: на поверхностные и объемные, локальные и периферические и т. д., поскольку эти следы не обладают физическими и химическими характеристиками (массой, цветом, геометрической формой и т. д.[2]

А.Г. Волеводз полагает, что «виртуальные следы» представляют собой данные о происхождении информации, относя к таковым: таблицы размещения файлов (FAT, NTFS или др.), системные реестры операционных систем, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и т. д.[3]

В.Е. Козлов считает, что виртуальный след – это система команд ЭВМ, где виртуальный объект будет являться следообразующим[4].

По мнению А.Б. Смушкина, виртуальные следы занимают условно промежуточную позицию между материальными и нематериальными и могут оставаться не только в компьютерных, но и в любых цифровых устройствах[5].

В то же время В.А. Милашев указывает на несоответствие термина «виртуальный» форме существования таких следов[6] и

---

[1] См.: Аскольская Н.Д. Виртуальные следы как элемент криминалистической характеристики компьютерных преступлений // Закон и право. 2020. № 5. С. 173.

[2] Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук. Омск, 2008. С. 17.

[3] Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Рос. следователь. 2002. № 1. С. 4.

[4] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телеком, 2002. С. 144.

[5] Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 44–45.

[6] Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: дис. ... канд. юрид. наук. М., 2004. С. 63–65.

определяет их как «бинарные» – изменения компьютерной информации, произошедшие в связи с удаленным воздействием[1].

По мнению В.Б. Вехова, Б.П. Смагоринского и С.А. Ковалева, такие следы нельзя называть «виртуальными», авторы определяют их как «электронные следы» – имеющую криминалистическое значение компьютерную информацию, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[2].

В.Я. Колдин предлагает называть такие следы «компьютерно-техническими»[3].

Е.Р. Россинская считает рассматриваемые следы материальными, так как они зафиксированы на материальных носителях вследствие изменения свойств или состояний отдельных их элементов[4].

Кроме того, в различных источниках рассматриваются разновидности этих следов:

электронно-цифровые – совокупность информации о посещениях пользователя, криминалистически значимая информация, выраженная посредством электромагнитных воздействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники, в результате создания определенного набора двоичного, его преобразования, выразившегося в модификации, копировании, удалении или блокировании, зафиксированная на материальном носителе, без которого не может существовать[5];

информационные следы, появление которых прогнозировал еще Д.А. Турчин[6] – это изменения информационной среды в виде

---

[1] Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф. дис. … канд. юрид. наук. М., 2004. С. 18.

[2] Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики // Судебная экспертиза. Волгоград: ВА МВД России, 2016. Вып. 2. С. 17.

[3] Криминалистика: информационные технологии доказывания [Электронный ресурс]: учеб. для вузов / под ред. В.Я. Колдина. М.: Зерцало-М, 2007. 752 с

[4] Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 112.

[5] См.: Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. дис. … канд. юрид. наук. М., 2019. С. 10.

[6] Турчин Д.А. Теоретические основы трасологической идентификации в криминалистике. Владивосток: Дальневост. ун-т, 1983. С. 91.

сигналов и кодов на электронных носителях, отражающие особую среду – информационную, поскольку ни в какой другой среде они находиться не могут[1].

В общем, с существованием, спецификой и определением криминалистического значения этой категории следов согласны практически все исследователи, однако их наименование является предметом дискуссии. Сегодня, в век цифровой эпохи, появилась возможность описать практически любое реальное явление в виде модели. С одной стороны, модель может абсолютно точно воспроизвести событие, а с другой – дать оценку адекватности описания реальности этой моделью весьма проблематично, что обусловлено свойствами виртуальных следов, описанными В.А. Мещеряковым. За основу в исследовании будет принято именно его мнение по данному вопросу, при этом существование иных точек зрения не оспаривается.

Две плоскости существования способов незаконного сбыта наркотических средств (материальная и информационная) обусловливают вид и содержание следов незаконного сбыта наркотических средств, совершенного анализируемым способом. Предлагаем рассмотреть типичную следовую картину рассматриваемых преступлений на примере основных (узловых) мероприятий в рамках способов незаконного сбыта наркотических средств, реализуемых в двух плоскостях, как для общих мероприятий, так и для мероприятий организационного этапа, индивидуализирующих каждый конкретный факт незаконного сбыта наркотиков с использованием информационно-телекоммуникационных технологий.

Применительно к данным, отраженным в табл. 1., нужно указать, что идеальные следы представляют собой показания, полученные от лиц, наделенных процессуальным статусом свидетеля, эксперта или подозреваемого по расследуемому уголовному делу, либо же сведения, содержащиеся в объяснениях лиц, непосредственно наблюдавших преступный процесс, но в последующем не наделенных процессуальным статусом.

«Иными» следами названы относящиеся к указанной группе, но образованные вследствие особенностей способа реализации конкретного преступного процесса.

---

[1] См.: Шаповалова Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики): автореф. дис. … канд. юрид. наук. Владивосток, 2006. 21 с.

Таблица 1

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

Информационная составляющая способа совершения преступления	Материальная составляющая способа совершения преступления
Общие мероприятия	
Подбор кадров	
Виртуальные следы: в зависимости от наличия и формы контактов между работодателем и персоналом (переписка, информация о соединениях между абонентами, следы размещения рекламы на информационных ресурсах и серверах и др.).	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: документы по учету кадров, фото, видеозаписи, иные.
Приискание наркотических средств и реагентов	
Виртуальные следы: трафик абонента сети, журнал посещений тематических сетевых ресурсов, переписка, информация о соединениях между абонентами операторов мобильной связи, регистрационные данные и следы использования платежных систем и финансовых операций, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: информационные тематические материалы (книги, пособия, справочники), транспортные накладные, аптечные рецепты, чеки, билеты, иные.
Производство и хранение наркотических средств	
–	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: наркотические средства, приспособления для их изготовления, хранения, упаковка, следы в местах хранения наркотических средств (трасологические и др.), иные.
Подбор торговой площадки, создание сетевого ресурса	
Виртуальные следы: трафик пользователя, журнал посещений тематических сетевых ресурсов, следы использования соответствующего программного обеспечения и эксплуатации аппаратных средств (Tor, VPN, приложения и т. п.), переписка, информация о соединениях между абонентами мобильной связи, следы регистрации домена/аккаунта, следы использования платежных систем и проведения онлайн-операций, иные в зависимости от организации торговой площадки.	Идеальные следы: показания лиц, осведомленных о преступном процессе.

Продолжение таблицы

Информационная составляющая способа совершения преступления	Материальная составляющая способа совершения преступления
Размещение рекламы	
Виртуальные следы: переписка, следы взаимодействия с владельцами интернет-ресурсов, следы использования платежных систем и проведения онлайн-операций по оплате хостинга, следы использования программ-ботов, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: рекламная информация, зафиксированная на материальных носителях, иные.
Разработка и внедрение мер конспирации	
Виртуальные следы: переписка, следы использования соответствующего программного обеспечения и аппаратных средств, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: зафиксированная на материальных носителях специальная терминология, правила поведения, иные.
Организация связи между участниками	
Виртуальные следы: информация о соединениях между абонентами, сведения биллинговых служб и сервисов геолокации, следы использования программного обеспечения и аппаратных средств, в том числе средств связи, переписка, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: средства связи, иные.
Подбор финансовых инструментов	
Виртуальные следы: аккаунты и история платежных систем и онлайн-сервисов, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: финансовые договоры, чеки, иные.
Распределение преступных результатов	
Виртуальны следы: аккаунты и история платежных систем и онлайн-сервисов, переписка, информация оператора мобильной связи, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: денежные средства и материальные блага.
Индивидуальные мероприятия	
Получение и обработка заказов	
Виртуальные следы: трафик пользователя, журнал посещений, следы использования соответствующего программного обеспечения, переписка между сбытчиком и покупателем, информация о соединениях операторов мобильной связи, сведения биллинговых служб и сервисов геолокации, переписка, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе.

Окончание таблицы

Информационная составляющая способа совершения преступления	Материальная составляющая способа совершения преступления
Оплата	
Виртуальные следы: аккаунты и история платежных систем и онлайн-сервисов, банковские транзакции, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: денежные средства, материальные блага, в зависимости от формы расчета.
Фасовка	
–	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: наркотические средства, весы, другие приспособления, упаковочный материал, тара, иные.
Перемещение покупателю	
Виртуальные следы: переписка, информация о соединениях между абонентами, сведения биллинговых систем и сервисов геопозиционирования, иные.	Идеальные следы: показания лиц, осведомленных о преступном процессе. Материальные следы: наркотические средства, их следы, упаковка, иные.

Таким образом, незаконный сбыт наркотических средств, совершенный рассматриваемым способом, формирует следовую картину, включающую все известные современной криминалистике виды следов. Рассмотрение следовой картины с точки зрения двойственности (информационной и материальной) способов анализируемых преступлений укажет на разнообразие следовоспринимающих объектов и следов.

А.Л. Осипенко отмечает особую сложность обнаружения следов преступлений, совершаемых с использованием сети Интернет, объясняя ее тем, что такие следы будут распределены по множеству объектов[1].

[1] Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. 2012. № 3. С. 11.

Криминалистика традиционно[1] рассматривает отображение свойств следообразующего объекта как результат его воздействия на определенный следовоспринимающий объект, что позволяет индивидуализировать и идентифицировать их. Вместе с тем механизм образования виртуальных следов гораздо сложнее и связан, в частности, с распределением свойств следообразующего объекта на несколько следовоспринимающих, что требует особого подхода к работе с ними.

Данное положение подтверждает и ряд современных ученых[2], отмечая специфику рассматриваемой следовой картины: большая часть следов совершения указанных преступлений редко остается в виде изменений внешней среды, соответственно, и не рассматривается трасологией.

При этом, если места нахождения и механизм следообразования «традиционных» (материальных и идеальных) следов преступления будут определены содержанием способа изготовления и перемещения наркотических средств, то места нахождения и механизм следообразования «виртуальных» определится порядком функционирования торговых площадок по продаже наркотических средств.

Например, если говорить об использовании информационных ресурсов, доступ к которым осуществляется посредством стандартных интернет-соединений, местами нахождения следов и следовоспринимающих объектов являются: рабочие места и компьютерные системы всех задействованных в незаконном сбыте наркотических средств лиц, а также архивы данных провайдера, транзитных провайдеров (в случае их использования), организаторов распространения информации в сети Интернет, серверы и т. п.

Следы незаконного сбыта наркотических средств посредством Даркнета следует искать в установленном программном обеспечении компьютерных устройств лиц, задействованных в преступном процессе, в открытых форумах и электронных документах, созданных ими же, системах обращения криптовалюты и т. п.

---

[1] См.: Коржев М.А. Криминалистическое значение следов человека // Инновационная наука. 2015. № 7. С. 75.

[2] См.: Аносов А.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, телекоммуникационных и высоких технологий: учеб. пособие: в 2 ч. М.: Акад. управления МВД России, 2019. Ч. 1. С. 106.

Механизм образования следов использования телекоммуникационных технологий и места их нахождения будут определяться используемыми аппаратными средствами, операционной системой и программным обеспечением, используемыми протоколами связи, службами доступа к файлам в сети, параметрами настройки оборудования на связь с определенными абонентами и т. п.

Порядок обнаружения следов во многом определяется алгоритмами функционирования используемых информационно-телекоммуникационных технологий.

Например, в случае использования сервиса Torrent[1] в преступных целях порядок обнаружения следов будет соответствовать порядку его работы:

1) подключение к BitTorrent-трекеру[2];
2) обмен информацией о скачивании/раздаче файла (анонс);
3) взаимодействие пиров[3].

Первоначально проводятся общие мероприятия: анализ истории просмотренных сайтов, кэш-памяти браузера, cookies-файлов, «мусора» в различных директориях, отведенных под временные файлы, корзины, доступных интернет-каналов и их параметров, установленных плагинов браузеров, активных рабочих процессов и т. п.

Все вышеописанное представляет собой результат воздействия мероприятий, образующих способы анализируемых преступлений, на объекты, связанные с их совершением. Типичность алгоритмов функционирования информационно-телекоммуникационных технологий, используемых в преступном процессе, обеспечивает типичность механизма следообразования и оставленных совершенным преступлением следов. А специфика типичных следов незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, заключающаяся в их форме, содержании, условиях возникновения и содер-

[1] Пиринговый (P2P) сетевой протокол для кооперативного обмена файлами через Интернет. URL: https://ru.wikipedia.org/?curid=11466&oldid=119878518 (дата обращения: 07.02.2022).

[2] Сервер, хранящий информацию о клиентах сети BitTorrent. URL: https://ru.wikipedia.org/?curid=61183&oldid=119742643 (дата обращения: 01.02.2022).

[3] Участник одноранговой сети. URL: https://ru.wikipedia.org/?curid=405967 &oldid=117668898 (дата обращения: 04.02.2022).

жания, требует, помимо совершенствования существующих категорий, развития новых, отражающих информационную сущность современной преступности.

1.5. Криминалистически значимые сведения о личности типичных преступников

Попытки выделить преступников из общей массы людей осуществлялись всегда, ведь одним из непременных условий организации борьбы с преступностью является осведомленность о лицах, совершающих преступления.

Личность преступника является предметом исследования множества наук: криминалистики, криминологии, философии, социологии, психологии и др. Результаты изучения личности преступника отражены в трудах ряда отдельных исследователей[1].

Так, Л.М. Прозументов считает проблему личности преступника одной из центральных проблем наук криминального цикла. Без ее всестороннего изучения невозможно полно установить иные элементы преступления[2].

В.К. Гавло отмечает, что криминалистика рассматривает личность преступника в аспекте криминалистически значимых связей между ним и совершенным преступлением, что делает личность типичного преступника следообразующим объектом – основным источником информации о совершенном преступлении[3].

Так, личность преступника – это совокупность свойств, обусловливающих выбор конкретного способа совершения преступления, оставляющего определенный набор следов в существующей обстановке.

Говоря о наркосбытчиках, А.С. Щурова рассматривает их характеристику с точки зрения криминологии, отмечая организованный характер накропреступности, и представляет ее через систему признаков, свойств, качеств, иных показателей, характеризующих

---

[1] См.: Антонян Ю.М., Кудрявцев В.Н., Эминов В.Е. Личность преступника. СПб: Юридический Центр пресс, 2004. 366 с. и др.

[2] Прозументов Л.М., Шеслер А.В. Личность преступника: криминологический аспект: учеб. пособие. Томск: Томск. филиал РИПК МВД России, 1995. С. 3.

[3] Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Изд-во Томск. ун-та, 1985. С. 197.

личность, таких как социальный статус, социальные функции, нравственно-психологические установки, правовой статус[1].

Групповой характер анализируемых преступлений не позволяет объединить все признаки личностных характеристик преступников и дать их обобщенную характеристику, поскольку мотивы, социальный и правовой статус разных «звеньев» преступной цепи будут отличаться.

А.В. Климачков представляет оперативно-розыскную характеристику личности рассматриваемых преступников как ключевое звено в оперативно-розыскной деятельности, выделяя среди них организатора, оператора и закладчика в рамках организованного характера незаконного сбыта наркотических средств[2].

Проведенное нами исследование подтверждает групповой характер преступлений рассматриваемого вида: 7% преступлений совершены в составе организованных преступных групп (ОПГ), 63% – в составе группы лиц по предварительному сговору. Однако приведенные показатели не свидетельствуют о том, что деятельность участников преступлений, совершенных группой лиц по предварительному сговору, менее организована в сравнении с ОПГ. Такая квалификация возможна лишь потому, что низшее звено – «закладчик», которого, как правило, и привлекают к уголовной ответственности за незаконный сбыт наркотических средств, не осведомлен о личностях остальных членов группы и ее деятельности в целом. Однако ему известен противоправный характер его действий, чем и объясняется такая уголовно-правовая квалификация формы организации незаконного сбыта наркотических средств. В связи с этим преступники, представляющие наибольшую общественную опасность, остаются вне поля зрения правоохранительных органов, и их незаконная деятельность продолжается.

---

[1] Щурова А.С. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети Интернет): уголовно-правовое и криминологическое исследование: дис. … канд. юрид. наук. СПб., 2017. С. 63.

[2] Климачков А.В. Оперативно-розыскная характеристика личности участников незаконного сбыта наркотических средств, совершаемого с использованием сети Интернет // Алтайский юридический вестник. 2017. № 3(19). С. 111–116.

Также, рассматривая деятельность ОПГ, занимающихся незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий, необходимо обратить внимание на уровень их организованности.

Высокоорганизованный уровень деятельности характеризуется усиленными мерами конспирации (все участники действуют во исполнение единой преступной цели, однако не всегда осведомлены о личностях друг друга) и трансграничным характером (информационно-телекоммуникационные технологии позволяют ее участникам осуществлять свою преступную деятельность из разных уголков страны и даже мира, а также обеспечивают обширный территориальный охват рынков сбыта наркотических средств). Это обеспечивает скрытный и длительно протекающий характер преступных действий, в связи с чем деятельность таких ОПГ полностью пресечь удается редко. Например, в проведенном исследовании фактов деятельности высокоорганизованных ОПГ не встречалось. Однако криминалистическую характеристику личности таких преступников описывает О.А. Решняк[1], выделяя: организаторов, оптовых сбытчиков, перекупщиков, розничных сбытчиков, изготовителей, расхитителей, перевозчиков, организаторов притонов, «склад», пособников, закладчиков и др.

Среди участников высокоорганизованных ОПГ наиболее уязвимы «закладчики» (наркокурьеры, анонимные курьеры и т. п.), так как их деятельность протекает «на улице», а не в информационном пространстве и изолированно от других членов. В связи с этим, как было отмечено выше, хотя они и не располагают сведениями о своих сообщниках, но знают об их наличии, такая деятельность по признакам определяется как преступление, совершенное группой лиц по предварительному сговору.

Эти лица относятся к низшему звену анализируемой преступной деятельности. Их вовлечение в наркобизнес осуществляется по типовой схеме: на ресурсах сети Интернет (веб-сайты, социальные сети, баннеры, Push-уведомления в различных приложениях и т. п.) или же на стенах домов, заборах размещаются объявления с предложениями работы и координатами для дальнейшей связи. Это могут быть номера мобильных для обмена смс-сообщениями

[1] Решняк О.А. Указ. соч. С. 79–82.

или для переписки в мессенджерах (Telegram, Jubber, ICQ и др.), адреса электронной почты, ссылки на аккаунты в социальных сетях («ВКонтакте», «Одноклассники» и др.). Откликнувшимся на объявление лицам разъясняют характер и схему работы.

В случае согласия с обозначенными условиями работы потенциальный «закладчик» вносит предоплату (как страховку на случай форс-мажора с заказом). Далее ему направляются сообщения (различными способами) с геометками нахождения либо уже расфасованного наркотического средства, либо общей массы, которую «закладчик» должен сам расфасовать в соответствии с деталями полученного заказа. Последний осуществляет их «закладку», о месте которой тем же способом сообщает своим «работодателям». Срок работы «закладчиков», как показывает практика, составляет в среднем 1–2 месяца, после чего они попадают в поле зрения правоохранительных органов.

Например, осужденный Ф. в ходе судебного заседания пояснил, что откликнулся на объявление о наборе анонимных курьеров, размещенное в сети Интернет, после чего через мессенджер Telegram связался по указанным в объявлении реквизитам, где ему разъяснили характер работы, на которую он согласился. Наркотические средства забирал согласно геометкам, направленным ему через тот же мессенджер, раскладывал их в укромные места, делал фото и отправлял его вместе с геолокацией места обратно. Заработок выплачивали биткоинами, процент рассчитывали поддерживающие с ним связь через мессенджер лица. Сведениями об их личности, а также о первоначальном источнике наркотических средств Ф. не располагал[1].

Проведенный нами анализ уголовных дел [2] также позволяет выявить более низкий уровень организации ОПГ, как правило, функционирующих в рамках одного территориального образования Российской Федерации. Именно с их деятельностью чаще всего и сталкиваются правоохранительные органы. В таких ОПГ возможно четко выделить лишь роль организатора. Криминальные же обязанности иных членов организованной преступной группы весьма разнообразны: приискание первоисточника получения

[1] См.: Архив Красноармейского районного суда Краснодарского края. Уголовное дело № 1-238/2018 по п. «г» ч. 4 ст. 228.1 УК РФ, ч. 1 ст. 228 УК РФ.

[2] См. Там же.

наркотических средств, их изготовление, фасовка, контроль функционирования интернет-ресурса, обеспечение рекламы информационного ресурса, кадровая работа, разработка и реализация мер противодействия и т. п. Их четкое распределение осуществляется в рамках функционирования конкретного объединения преступников. Участники такой ОПГ, как правило, лично знакомы друг с другом, состоят в товарищеских отношениях либо представлены кем-либо из членов группы.

Организаторы, находясь во главе преступных организаций и обладая лидерскими качествами, заняты по большей части выполнением административных функций (обеспечительных, распределительных, кадровой работой и т. п.), хотя могут выполнять и любую другую в зависимости от распределения обязанностей внутри конкретной преступной организации. Примечательно, что среди организаторов встречаются бывшие и действующие сотрудники правоохранительных органов, почерпнувшие знания об особенностях, тенденциях и мерах противодействия незаконному сбыту наркотических средств во время службы. Чем выше образовательный уровень и возраст организатора, тем меньше работы, несвойственной его роли, он выполняет.

Иные участники – это «рабочее» («промежуточное») звено наркобизнеса, которое характеризуется весьма разнородным составом, что обусловливает выполняемые данными лицами функции. Причем роли между ними распределяются в зависимости от наличия определенных знаний и умений, а также от степени доверия «организатора» и включают в себя любые функции, направленные на осуществление преступной деятельности, за исключением организаторской.

Проведенный анализ уголовных дел позволяет сделать вывод, что роль «закладчика» типична для группы лиц по предварительному сговору. В составе же анализируемых ОПГ функция производства закладок зачастую распределена между иными участниками.

Обобщенные социальные характеристики таких лиц показывают, что абсолютное большинство из них – мужчины. Однако зачастую в роли организаторов и иных участников выступают и женщины.

Средний возраст организаторов и иных участников составляет 30–40 лет, что совпадает с возрастом социальной активности и говорит о наличии определенного жизненного опыта. Типичные «закладчики» в среднем на 10 лет моложе. Этот факт определяет содержание реализуемых ими функций, не требующих специальной квалификации.

Большая часть характеризуемых преступников не связаны семейными узами, что свидетельствует об их слабой привязанности к традиционным ценностям. Тем не менее у большинства из них находятся на иждивении несовершеннолетние дети.

80% официально не трудоустроены и, соответственно, не имеют постоянного источника дохода, а живут лишь за счет средств, полученных от преступной деятельности. Это свидетельствует о высокой доходности наркобизнеса. Данный показатель применительно к «закладчикам» указывает на сложности приобретения законного источника дохода в силу особенностей личности (общая инфантильность, низкий образовательный уровень, желание незамедлительного обогащения и т. п.). Официально же трудоустроенные являются представителями различных специальностей и занимаются незаконным сбытом наркотических средств в качестве дополнительного источника дохода.

Лишь незначительная часть всех изученных преступников имеют высшее образование, для большинства характерен средний или невысокий образовательный уровень.

Также в их среде не выявлено профессионалов в области информационно-телекоммуникационных технологий. Абсолютное большинство анализируемых преступников обладают знаниями об информационных и телекоммуникационных технологиях на бытовом уровне, и используют их уже существующие широкие возможности для совершения преступлений, не прилагая усилий к разработке новых способов незаконного сбыта наркотических средств.

Приблизительно в равных частях в структуре характеризуемых преступников наблюдаются как ранее судимые за аналогичные преступления, так и осужденные за совершение иных преступных деяний лица, что говорит о совершенствовании ранее полученных преступных навыков за счет использования информационно-телекоммуникационных технологий. Значительная же часть

ранее не привлекавшихся к уголовной ответственности также свидетельствует об активном вовлечении в наркобизнес новых лиц.

Относительно небольшой общий процент изученных преступников систематически употребляют наркотические средства. Этот факт также свидетельствует об активном вовлечении в наркобизнес новичков и о том, что наркопреступники осознают вред, причиняемый употреблением наркотических средств.

Наркосбытчики ведут не привлекающий к себе внимания образ жизни, по месту проживания, как правило, характеризуются положительно.

Представленные сведения описывают современное структуру качественное состояние преступности, связанной с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий.

Кроме того, в рамках настоящей работы в результате анализа правоприменительной практики нами выявлены следующие закономерности.

Совершение рассматриваемых преступлений согласно строгим алгоритмам функционирования информационно-телекоммуникационных систем и технологий становится возможным за счет знаний, умений и навыков, требуемых для их использования.

В данном случае под знаниями понимается глубокое теоретическое осмысление процессов функционирования информационно-телекоммуникационных технологий, под умениями – возможность осуществления операций с ними, а под навыками – возможность осуществления операций с информационно-телекоммуникационными технологиями, направленных на достижение желаемого результата.

Все это детерминирует связь анализируемого элемента криминалистической характеристики со следами и способом рассматриваемого вида преступления. Чем обширнее навыки, знания и умения преступника, тем более высокотехнологичный способ совершения преступления им будет выбран, тем затруднительнее окажется процесс обнаружения и фиксации следов преступления.

С учетом двойственной природы способов совершения анализируемых преступлений все совершаемые в преступных целях транзакции имеют материальную и информационную составляющие. Большая часть мероприятий материальной составляющей

представляет собой действия, для совершения которых достаточно определенного жизненного опыта и некоторых практических навыков, как правило, полученных на предыдущих местах работы, в то время как мероприятия информационной составляющей способа совершения преступления являются более сложными и представляют собой алгоритмизированную последовательность множества действий.

Е.А. Ошлыкова отмечает высокий профессионализм рассматриваемой категории преступников как в области изготовления наркотических средств, так и в сфере применения способов незаконного сбыта[1].

Результаты изучения уголовных дел свидетельствуют, что необходимые для реализации преступного умысла знания (методики, схемы, алгоритмы и т. п.) в большей части получены преступниками посредством информационных ресурсов сети Интернет, которую можно смело назвать «большой энциклопедией преступности». Тем не менее независимо от источника приобретения этих знаний и навыков факт их наличия позволит составить криминалистическое представление о роли лица в иерархии преступной организации, укажет на особенности способа и иных элементов криминалистической характеристики совершенного преступления.

Для примера предлагаем рассмотреть необходимые для реализации ключевых мероприятий способа анализируемого преступления знания и умения.

Общие

Подбор кадров:

знать основы и принципы работы используемого программного обеспечения;

уметь работать с информационными ресурсами;

владеть обстановкой рынка сбыта наркотических средств для формирования предложений, основами организаторской работы.

Приискание наркотических средств и реагентов для их изготовления:

[1] Ошлыкова Е.А. Методика расследования незаконного сбыта наркотических средств и поддержания государственного обвинения по уголовным делам данной категории: дис. … канд. юрид. наук. М., 2013. 243 с.

знать организацию и предложения рынка незаконного оборота наркотических средств;

уметь работать с сетевыми ресурсами, осуществлять сложный критериальный поиск информации, осуществлять коммуникацию с поставщиком, проводить финансовые онлайн-операции;

владеть методиками изготовления наркотических средств.

Производство и хранение наркотических средств:

знать методику производства и специфику обращения, синтеза и хранения наркотических средств и реагентов для их изготовления;

уметь изготавливать наркотические средства;

владеть технологиями производства и хранения наркотических средств.

Подбор торговой площадки, создание сетевого ресурса:

знать технические требования и условия функционирования информационных ресурсов, основные методы, способы и средства получения, хранения, обработки информации для решения поставленных задач, алгоритмы создания веб-сайтов;

уметь использовать средства обработки информации;

владеть навыками работы с информацией в глобальных компьютерных сетях.

Размещение рекламы:

знать психологические основы воздействия рекламной продукции на человека; основы работы с информацией;

уметь ориентироваться на рынке рекламной продукции, создавать макеты рекламных продуктов;

владеть маскировкой незаконного контента, основами программирования.

Разработка и внедрение мер конспирации:

знать алгоритмы функционирования современных программных и аппаратных средств;

уметь разрабатывать меры анонимизации;

владеть специфической терминологией, коррумпированными связями в компетентных органах.

Организация связи между участниками:

знать основы функционирования современных средств связи;

уметь использовать системы средств связи;

владеть основами эксплуатации средств связи.

Подбор финансовых инструментов:

знать основы бухгалтерского учета и финансовой деятельности; современные финансовые средства;

уметь использовать платежные инструменты;

владеть схемами вывода денежных средств.

Распределение преступных результатов:

знать основные статьи доходов и расходов преступной организации;

уметь осуществлять схемы вывода и обналичивания денежных средств;

владеть основами функционирования платежных онлайн-инструментов.

Индивидуальные

Получение и обработка заказов:

знать способы обработки информации;

уметь анализировать, аккумулировать и обрабатывать полученную информацию;

владеть навыками обработки информации.

Оплата:

знать технологии бесконтактных финансовых операций и систем;

уметь проводить финансовые онлайн-операции;

владеть основами функционирования платежных онлайн-инструментов.

Фасовка:

знать требования к условиям хранения наркотических средств;

уметь упаковывать наркотические средства.

Перемещение покупателю:

знать работу используемого программного обеспечения;

уметь скрытно перемещать наркотические средства в пространстве.

Как видно из представленных сведений, чем ближе реализуемые мероприятия к завершению преступной транзакции, тем меньше навыков, знаний и умений требуется. Предполагается, что наличие определенных знаний и умений у преступника поможет следователю определить его преступную функцию и иные характеристики личности. И, наоборот, преступная роль в незаконном

сбыте наркотических средств будет указывать на требуемые для ее реализации знания, навыки и умения, что позволит определить особенности способа совершения преступления, места поиска следов, их качественное состояние, а также выявить иные эпизоды преступной деятельности.

Связь между возрастом преступника и выбранным им способом совершения преступления.

Преступность идет в ногу со временем, и в век информационно-телекоммуникационных технологий лица возраста преступной активности (20–40 лет) активно используют его достижения. Например, их предшественники в силу реалий современности и своей преступной активности в ранний период использовали более «простые» способы незаконного сбыта наркотических средств.

Связь между возрастом преступника и выполняемой им преступной ролью в незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий.

Преступники, старшие по возрасту, в основном выполняют организационные функции в силу наличия определенного жизненного опыта, а более молодые – всю черновую работу. Причем последние в силу общего инфантилизма, склада ума и характера вряд ли могут рассчитывать на «повышение» в рамках уже функционирующей преступной организации, поскольку тонкости преступного наркобизнеса им, как правило, недоступны. Конечно, некоторые из них планируют в будущем завершить выполняемую «черновую» работу и начать собственный преступный бизнес, но, как показывает практика, молодые люди не успевают осуществить свои планы, так как попадают в поле зрения правоохранительных органов.

Кроме того, в 100% изученных уголовных дел незаконный сбыт наркотических средств осуществлялся с использованием уже существующих торговых площадок. Данный факт обусловливает необходимость упоминания обособленной составляющей рассматриваемых криминалистически значимых сведений – лиц, обеспечивающих создание, организацию и функционирование используемых преступниками информационно-телекоммуникационных технологий и систем, но имеющих опосредованное отношение к незаконному сбыту наркотических средств, так как направленность их умысла заключается в создании благоприятных условий

для его реализации либо же вовсе отсутствует (например, при создании правомерных интернет-ресурсов (торговых и информационных ресурсов), социальных сетей). Речь ведется о создателях информационных ресурсов, посредством которых и совершаются преступные деяния. Связь с наркосбытчиками будет заключаться в использовании последними их разработок как на возмездной, так и на безвозмездной основе. Особенности их личности вряд ли будут представлять интерес в рамках рассматриваемой тематики, но факт их существования и упоминание о них определяют содержание информационной составляющей рассматриваемых преступлений и обусловливают детерминирующую связь со способом и следовой картиной незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий. А установление направленности умысла и факта преступной связи с наркосбытчиками позволит правоохранительным органам выйти на более высокий, более масштабный уровень преступной наркодеятельности.

ГЛАВА 2. ОРГАНИЗАЦИЯ ПРЕДВАРИТЕЛЬНОГО И ПЕРВОНАЧАЛЬНОГО ЭТАПОВ РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. Получение первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий

Структура и качественные характеристики современной преступности обусловливают необходимость криминалистического обеспечения правоохранительной деятельности[1].

Здесь речь ведется не только о технико-криминалистических средствах, но и о разработанных в рамках криминалистической науки рекомендациях, отражающих эффективные методы и приемы работы с информацией о преступлении.

Еще в 2001 г. А.В. Дулов и А.С. Рубис отмечали, что содержание «традиционной» криминалистики не соответствует современным реалиям, и указывали на важность того, чтоб методики расследования отдельных видов преступлений не только основывались на результатах научного анализа уголовных дел и передовом практическом опыте, но и включали отдельные положения мыслительных приемов, методов получения (выявления) информации о преступлении[2].

Также 100% опрошенных нами респондентов сообщили о непосредственном влиянии таких сведений на организацию расследования уголовных дел[3].

Р.С. Белкин отмечал особое значение первоначальной криминалистически значимой информации о преступлении, определяя ее как полученную из непроцессуальных источников и не имеющую доказательственного значения информацию о преступлении,

---

[1] См.: Россинская Е.Р. Проблемы современной криминалистики и направления ее развития // Эксперт-криминалист. 2013. № 1. С. 2–6.

[2] Дулов А.В., Рубис А.С. Понятие и содержание выявления преступлений // Право и демократия: сб. науч. тр. Минск: Изд-во БГУ, 2001. Вып. 11. С. 276–280.

[3] См.: Приложение 2.

имеющую ориентирующий характер и впоследствии способную приобрести доказательственный статус[1].

Аналогичной позиции придерживаются и такие исследователи, как Н.П. Яблоков, С.Ю. Журавлева, С.К. Крепышева и др.[2]

Н.И. Савченко, ссылаясь на положения уголовно-процессуального закона (п. 9 ст. 5 УПК РФ), отмечает в качестве начала досудебного производства момент получения информации о преступлении и предлагает называть этот этап предварительным, обозначая его окончанием момент возбуждения дела[3].

Полностью разделяя представленные мнения, необходимо рассмотреть в рамках настоящей работы отдельные положения, связанные с получением (выявлением) первоначальной криминалистически значимой информации об анализируемых преступлениях как составляющей предварительного этапа расследования.

Выявить преступление – значит обнаружить и зафиксировать событие, содержащее признаки преступления, т. е. действие (бездействие), охарактеризованное в уголовном законе как преступное[4]. Фактически это означает получить первоначальные криминалистически значимые сведения о нем.

А.А. Рудых, рассматривая преступления в сфере информационных технологий, включает в содержание первоначальной криминалистически значимой информации сведения о пользователях,

---

[1] Белкин Р.С. Криминалистическая энциклопедия. 2-е изд. доп. М.: Мегатрон XXI, 2000. С. 83.

[2] См.: Яблоков Н.П. Некоторые проблемы отечественной криминалистики в свете сегодняшнего времени // Современная криминалистика: проблемы, тенденции, перспективы: материалы Междунар. науч.-практ. конф., посвященной 90-летию со дня рождения заслуженного деятеля науки РФ, заслуженного юриста РСФСР, доктора юридических наук, профессора Н. Яблокова. Москва, 22 дек. 2015 г. / ред.-сост. М.А. Лушечкина. М.: МАКС Пресс, 2015. С. 22; Журавлева С.Ю., Крепышева С.К. Криминалистическая методика и тактика: контекст современного понимания роли криминалистики в юридической деятельности и юридическом образовании // Современная криминалистика: проблемы, тенденции, перспективы: материалы Междунар. науч.-практ. конф., посвященной 90-летию со дня рождения заслуженного деятеля науки РФ, заслуженного юриста РСФСР, доктора юридических наук, профессора Н. Яблокова. Москва, 22 дек. 2015 г. / ред.-сост. М.А. Лушечкина. М.: МАКС Пресс, 2015. С. 50.

[3] Савченко Н.И. Особенности предварительного и первоначального этапов расследования получения, дачи взятки: дис. ... канд. юрид. наук. Краснодар, 2020. С. 58.

[4] См.: Гуценко К.Ф., Ковалев М.А. Правоохранительные органы: учеб. для студентов юрид. вузов и факультетов. М.: Зерцало М, 2001. С. 94.

проявлявших сетевую активность, и о событиях, произошедших в связи с ней. В частности, сюда отнесены:

сведения об используемых в преступных целях номерах мобильных телефонов;

сведения о номере банковской карты либо электронного платежного средства;

информация о доменном имени или адресе используемого преступниками интернет-ресурса;

адреса электронной почты причастных к совершению преступления лиц;

идентификационные номера страниц в социальной сети;

IP адреса и т. д.[1]

Верховный Суд РФ к первоначальным сведениям о незаконном сбыте наркотических средств относит информацию о возмездной либо безвозмездной реализации (продаже, дарении, обмене, уплате долга, даче взаймы и т. д.) наркотических средств[2].

Таким образом, в понятие первоначальной криминалистически значимой информации об анализируемых преступлениях следует включать сведения о пользователях информационно-телекоммуникационных технологий и систем, а также об их сетевой активности, связанной с реализацией наркотических средств.

Такие признаки сетевой активности могут быть разделены на две группы:

– прямо свидетельствующие об осуществлении незаконного сбыта наркотических средств (содержательная часть сообщений в мессенджерах, чатах, социальных сетях, информационный контент веб-сайтов, личных аккаунтов, push-уведомлений, баннерная реклама в сети Интернет и т. п.);

– косвенно указывающие на осуществление незаконного сбыта наркотических средств (регистрация и регулярное осуществление финансовых операций по электронным счетам, кошелькам, платежным системам, специфические перемещения

[1] Рудых А.А. Информационно-технологические обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Ростов н/Д, 2020. С. 136–137.

[2] О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ. 2006. № 14. Доступ из справ. правовой системы «КонсультантПлюс».

пользователя, отраженные в данных программ геолокации и геопозиционирования, использование программ-ботов, попытки анонимизации сетевой активности, использование мессенджеров с функциями шифрования сообщений, нецелевое использование нетипичного или специального программного и аппаратного обеспечения и т. п.).

Признаки второй группы имеют криминалистическое значение лишь в совокупности с признаками первой, позволяя конкретизировать анализируемую преступную деятельность, определить ее масштабы и круг участвующих лиц.

В общем, информация о фактах незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий поступает в правоохранительные органы из следующих источников:

оперативные источники – 51%;

сообщения, полученные от наружных служб – 27%;

сообщения от населения – 13%;

явки с повинной – 0%;

выявляется в ходе расследования иного уголовного дела –9%.

Несмотря на традиционное отнесение рассматриваемой деятельности к компетенции оперативных подразделений, источники и методы получения информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий весьма разнообразны.

Зачастую такая информация становится известной без помощи правоохранительных органов: ее сообщают лица, прямо или косвенно связанные с преступным деянием.

В некоторых же случаях требуется проведение специализированных мероприятий, направленных на получение первоначальной криминалистически значимой информации. Их содержание должно определяться источником таких сведений и иметь комплексный характер, включать в себя оперативно-розыскные мероприятия, их комбинации, следственные действия, поисковую работу в сети Интернет, представляющую особый интерес в силу новизны, эффективности и доступности.

К рассматриваемой категории специализированных мероприятий могут быть отнесены следующие.

1. *Поиск информации о фактах незаконного сбыта наркотических средств на ресурсах сети Интернет с использованием общедоступного программного обеспечения специального назначения*.

К данной группе относятся: программы-сканеры (веб-пауки, краулеры)[1], позволяющие анализировать содержимое интернет-сайтов, осуществлять целевой поиск информации о потенциальных преступниках и аккумулировать информацию о преступных фактах; программы, определяющие перечни IP-адресов и их владельцев, с которыми работал пользователь интересующей компьютерной системы; программы, распознающие индивидуальный почерк работы пользователя; программы для обнаружения скрытых процессов в компьютерной системе и др.

2. *Поиск информации в Интернете с использованием распространенных поисковых систем (Google, Rambler, Yahoo, Yandex и др.)*, обеспечивающих эффективный многокритериальный анализ сетевых информационных ресурсов, содержащих требуемые сведения. Для его оптимизации и повышения точности получаемых результатов необходимо владение специализированными для каждой поисковой системы «языками формирования запросов».

Например, при вводе в поисковую строку запроса «купить героин» система укажет ссылки на все веб-сайты, где фигурируют заданные слова «купить» и «героин». Для исключения таких сайтов и достижения требуемого результата поиска требуется уточнение запроса: «купить героин наркотик».

3. *«Серфинг» интернет-ресурсов* представляет собой поиск и просмотр различных веб-страниц интересующей пользователя тематики.

Для его оптимизации А.А. Рудых разработал для субъектов расследования универсальный криминалистический веб-обозреватель «СайберВатсон», предназначенный для поиска информации на веб-ресурсах[2].

---

[1] Интернет-бот, который систематически просматривает Всемирную паутину и обычно используется поисковыми системами с целью веб-индексации. URL: https://en.wikipedia.org/w/ index.php?title=Web_crawler&oldid=1071827490 (дата обращения: 14.02.2022).

[2] Рудых А.А. Указ. соч. С. 148.

Цель его создания состоит в обеспечении удобства поиска информации по заданным критериям в виде отображения запросной части интерфейса соответствующих веб-ресурсов. Кроме того, разработанный веб-обозреватель обеспечивает возможность поиска информации как на одной странице, так и на нескольких, выделенных согласно заданным критериям, содержащимся в интерфейсе.

Несмотря на то, что Роскомнадзор в пределах своей компетенции регулярно выявляет тематические ресурсы, содержащие запрещенную к распространению информацию, а также периодически проводит совместные с МВД мероприятия, направленные на выявление и блокирование таких веб-сайтов, их существует достаточно много.

Яркий пример работы с ресурсами сети Интернет описываемым способом наглядно был продемонстрирован в 2013 г. Э. Хиггинсом, который, будучи никак не связанным с правоохранительными органами и имея всего лишь стандартный персональный компьютер с доступом к сети Интернет, в ходе проведения так называемой «разведки по открытым источникам» овладел большим объемом информации об участвовавших в Сирийском конфликте сторонах, их вооружении, о каналах его поставки и т. п.[1]

Кроме того, данное направление активно развивается как медиагигантами (например, Yandex), так и отдельными заинтересованными пользователями (Dragstat[2]), которые активно осуществляют сбор статистических данных о запросах поисковых систем к интернет-ресурсам, публикуя отчеты в открытых источниках, что позволяет достаточно объективно оценивать количественные и качественные показатели незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий.

4. *Поиск информации с использованием ресурсов социальных сетей.* Следственным комитетом РФ приводится перечень источников информации, где следует искать сообщения о готовящихся

[1] См.: Роль больших данных в частных расследованиях и анализе. URL: https://habr.com/ru/company/asus/blog/240877/ (дата обращения: 18.04.2020).

[2] Канал социального сервиса Telegram, в рамках которого регулярно размещаются исследования различных тематических проектов, информация о трендах продаж, спросе и предложениях рынка незаконного сбыта наркотиков.

и совершенных преступлениях. В этот список вошли «ВКонтакте», «Facebook», «Twitter», «Одноклассники», «ЖЖ», «Мой мир», «Instagram», видеохостинги «YouTube», «Rutube», геосоциальный сервис «Foursquare» и др. Согласно рекомендациям Следственного комитета РФ анализ ресурсов данных социальных сетей позволит установить первоисточники сообщений и выявлять причины, которые привели к тем или иным событиям, выявлять публикации криминальной тематики[1]. Кроме того, социальные сети активно используются наркосбытчиками для подбора участников преступной деятельности, размещения специфической рекламы, создания площадки для интернет-магазина, а также в качестве средства коммуникации между сообщниками либо между продавцом и приобретателем наркотических средств.

Осознавая реальную опасность подобного использования социальных сетей, В.Г. Дикарев и А.Ю. Олимпиев предлагают законодательно закрепить возможность установления оперативного контроля за функционированием соответствующего программного обеспечения и аккумулировать полученные результаты в рамках АИС[2], руководствуясь положительным опытом регионов[3].

Также существуют различные программные комплексы, с помощью которых может быть решено множество задач: поиск пользователей в соответствии с заданными критериями; сбор из социальных сетей любой доступной информации и ее анализ с построением графиков заданных характеристик пользователей, их групп; статистический анализ действий; поиск связей между пользователями; аккумуляция информации о них, размещенной в открытых источниках (места пребывания, круг общения, круг интересов и т. п.) и др.

5. *Анализ операций с криптовалютой.*

Речь ведется об анализе и мониторинге операций, которые производятся с криптовалютой. В ряде случаев данная информация является общедоступной.

---

[1] См.: Следственный комитет намерен ввести мониторинг социальных сетей: URL: https://www.zakonia.ru/news/sledstvennyj-komitet-nameren-vesti-monitoring-sotssetej (дата обращения: 14.05.2017).

[2] Автоматизированная информационная система.

[3] Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. 2016. № 8. С. 147–152.

Например, затрагивая аналитическую работу, учитывая, что большая часть финансовых операций, связанных с незаконным сбытом наркотиков с использованием информационно-телекоммуникационных технологий, осуществляется с использованием криптовалюты, особый интерес для исследования представляет ее блокчейн-анализ[1].

Например, экс-агент ФБР Ильван Йам в ходе блокчейн-анализа отследил трансфер более 700 тыс. биткоинов с анонимной даркнет-площадки Silk Road на персональный компьютер Росса Ульбрихта – ее владельца[2].

Если лицу, осуществляющему блокчейн-анализ, удастся идентифицировать биткоин-адреса пользователя, то они могут быть использованы для последующего наблюдения за транзакциями.

Кроме того, сегодня активно ведется работа по поиску новых методов получения анализируемой информации, среди которых можно выделить следующие:

Осуществление взаимодействия с финансовыми организациями, обслуживающими электронные платежные системы. Речь идет как об оперативном информировании правоохранительных органов о подозрительных транзакциях (например, единовременный перевод больших сумм, в частности в иностранной валюте, и т. п.), так и о незамедлительном предоставлении компетентным органам регистрационных данных клиентов, а также сведений о движении денежных средств по открытым счетам;

И.С. Бедеров видит возможность решения вопроса получения и использования первоначальной криминалистически значимой информации об анализируемых преступлениях в создании единой системы криминалистического учета и идентификации на основе электронно-цифрового следа[3].

---

[1] Процесс проверки, идентификации, моделирования и визуального представления данных в криптографической распределенной книге, известной как блокчейн. В целях получения информации о различных субъектах, осуществляющих операции с криптовалютой. URL: https://en.wikipedia.org/w/index.php?title=Blockchain_analysis&oldid=1050167634 (дата обращения: 15.02.2022).

[2] Экс-агент ФБР отследил трансфер более 700 тыс. биткоинов с серверов Silk Road на ПК подозреваемого в управлении ресурсом. URL: https://www.securitylab.ru/news/470643.php (дата обращения: 14.08.2021).

[3] Цит. по: Сидоренко Елена. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений. URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia- lish-chetvert-kiberprestuplenii (дата обращения: 24.03.2020).

В подтверждение этого на государственном уровне рассматривается возможность регистрации мобильных устройств по их заводскому номеру (IMEI)[1].

Современная проблема работы с электронно-цифровыми следами состоит в отсутствии единого формализованного языка[2], посредством которого следовая картина, формируемая ими, могла бы быть описана.

Специалистами в сфере информационной безопасности в настоящее время уже накоплен определенный опыт по использованию стандартов (специальных языковых конструкций), позволяющих описывать инциденты информационной безопасности. Однако их многообразие порождает проблему единства представления и толкования одних и тех же событий.

Среди таких языков (GenCode, TEX, GML, SGML и др.) особое место занимает XML в связи с его универсальностью, простотой восприятия, возможностями восстановления данных и прочтения многими приложениями. Поэтому мы видим возможным решение обозначенной проблемы путем создания специализированного диалекта – языка XML, ориентированного на задачи, стоящие перед правоохранительными органами в сфере борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий. Компетенция криминалистики в данном вопросе заключается в формировании набора требований к этому языковому средству, обеспечивающего:

высокую функциональность;

стандартизированный вид (возможность прочтения различными системами и обычным пользователем);

автоматический контроль грамматики и синтаксиса построения сообщений;

минимизацию и единство используемых категорий и их свойств.

---

[1] См.: Тишина Юлия. Смартфоны пройдут перепись // Коммерсант. 2020. 28 апр. С. 5.

[2] Язык, состоящий из слов, буквы которых взяты из алфавита и хорошо сформированы в соответствии с определенным набором правил. URL: https://en.wikipedia.org/w/index.php? title=Formal_language&oldid=1069224063 (дата обращения: 15.02.2022).

Создание единого формализованного языка обеспечит эффективную реализацию предложений об аккумуляции и использовании баз данных электронно-цифровых следов.

Реализация предложения И.С. Бедерова[1] обусловливает необходимость постоянного накопления и предоставления оператором связи по запросу правоохранительных органов сведений, индивидуализирующих работу конкретного пользователя (устройства связи, гаджета) и отражающихся в сетевой статистике и системных журналах серверов, а также информации о признаках используемого прикладного программного обеспечения (операционной системы, браузера, приложения и др.), его режимах работы и т. п.

Например, к IP-адресу пользователя привязаны используемая операционная система, наименование браузера, разрешение экрана используемого устройства и целый ряд других параметров. Такие сведения могут быть использованы для идентификации сетевого устройства в дополнение к IP и MAC-адресу.

Совпадение электронно-цифровых следов, обнаруженных в связи с совершенным преступлением и хранящихся в базе данных, по мнению И.С. Бедерова, будет равнозначно идентификации личности пользователя[2].

Какое количество этих признаков необходимо, определяется лицом, оценивающим полученные сведения с точки зрения достаточности, исходя из их содержания и качественных характеристик.

Для фиксации оператором связи максимального количества индивидуализирующих сетевые устройства признаков возможно создание и массовое внедрение специально разработанных приложений общего назначения (например, платежных, информационных и др.), использование которых требует получения доступа к информации сетевого устройства (к камере, к микрофону, к списку контактов, к геопозиции и т. п.), что обеспечит возможность сбора и хранения статистической следовой информации, позволяющей идентифицировать пользователя гаджета на основе комплекса признаков используемого сетевого устройства и типичной для конкретного пользователя сетевой активности.

---

[1] См.: Сидоренко Елена. Указ. соч.

[2] См.: Сидоренко Елена. Указ. соч.

Подобные решения в настоящее время разрабатываются компаниями, работающими в сфере информационной безопасности, и активно внедряются в практическую деятельность[1].

Значительная часть криминалистически значимой информации может быть почерпнута из массивов данных, образованных коммуникационными сервисами[2], например функционирующих на основе технологии Web RTC API[3], облачной технологии VoxImplant[4], OktellR2[5] и др.

Такие технологии могут быть использованы как в браузерах, так и в иных прикладных программах (например, в командных играх) и представляют собой благодатную почву для коммуникации преступников, совершающих незаконный сбыт наркотических средств анализируемым способом.

В данном случае, помимо метаданных[6], открывается возможность доступа к информационному контенту, привязанному к ним.

Несмотря на то, что сведения весьма неустойчивы и могут быть преднамеренно изменены, их значительное количество и комплексное использование, а также возможность перекрестной проверки обеспечивают необходимый уровень достоверности.

Однако, несмотря на широкий круг мероприятий (оперативные разработки, средства и методы, деятельность наружных служб, следственные и процессуальные действия), направленных на получение криминалистически значимой информации о преступлении, очевидно, что число сотрудников компетентных органов и масштабы киберпреступности несоизмеримы.

---

[1] См.: Крылов П.В., Сачков И.К. Способ и система выявления удаленного подключения при работе на страницах веб-ресурса: патент 2649793. Группа АйБи. URL: https://patentdb.ru/patent/2649793 (дата обращения: 22.05.2020).

[2] Сервисы, предназначенные для общения между пользователями.

[3] Проект с открытым исходным кодом, предназначенный для организации передачи потоковых данных между браузерами или другими поддерживающими его приложениями по технологии точка–точка. URL: https://ru.wikipedia.org/?curid= 3320124 &oldid=118766852 (дата обращения: 21.12.2021).

[4] Аналогичная технология, которая может быть использована в мобильных приложениях.

[5] Программа, предназначенная для расширения функциональных возможностей бизнес-приложений.

[6] Раскрывают сведения о признаках и свойствах, характеризующих какие-либо сущности, позволяющие автоматически искать и управлять ими в больших информационных потоках. URL: https://ru.wikipedia.org/?curid=16316&oldid=115626917 (дата обращения: 23.07.2021).

В связи с этим государство, признавая актуальность проблемы борьбы с преступностью, использующей информационно-телекоммуникационные технологии, в частности с незаконным оборотом наркотических средств, активно рассматривает вопрос создания киберполиции – ведомства в структуре МВД по борьбе с киберпреступлениями[1]. Это абсолютно оправданно, поскольку бороться с такой преступностью можно только на основе достижений технической революции[2].

Вместе с тем инициативное выявление правоохранительными органами анализируемых преступных фактов может попасть под определение понятия «провокация», т. е. подстрекательство, склонение, побуждение в прямой или косвенной форме к совершению противоправных действий, направленных на передачу наркотических средств сотрудникам правоохранительных органов (или лицам, содействующим им)[3].

Речь ведется о том, что умысел преступника на незаконный сбыт наркотического средства должен возникнуть до начала проведения оперативно-розыскного мероприятия в его отношении. При этом первоначальная информация должна быть получена из независимых от правоохранительных органов источников.

Решение данного вопроса нам видится первоначально в разработке криминалистикой предложений, касающихся создания прикладного программного обеспечения, функционирующего на основе технологий искусственного интеллекта, и его внедрения в деятельность правоохранительных органов.

Под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека[4].

---

[1] См.: Патруль выходит в сеть // Рос. газ. 2019. Федер. вып. 252(8010). 7 нояб.

[2] См.: Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. С. 20.

[3] См.: Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ: утв. Президиумом Верховного Суда РФ 27 июня 2012 г. Доступ из справ.-правовой системы «Гарант».

[4] См.: О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 окт. 2019 г. № 490. Доступ из справ. правовой системы «КонсультантПлюс».

Э.М. Пройдаков предлагает считать искусственным интеллектом системы, проявляющие поведение, свойственное человеку[1].

В.В. Путин называет такие технологии рывком всего человечества вперед, который будет охватывать все сферы жизни, сочетая их между собой[2].

Сферы применения искусственного интеллекта весьма разнообразны: осуществление функции распознавания лиц, голоса, отпечатков пальцев, реализация таких сервисов, как голосовые помощники, программирование[3], принятие различных решений согласно заложенным алгоритмам и т. п.

Ю.Н. Жданов и В.С. Овчинский отмечают активное использование технологий искусственного интеллекта правоохранительными органами США, Великобритании, Нидерландов и Китая для сбора, классификации, обработки и хранения информации[4].

О.А. Решняк и С.А. Ковалев также обозначают использование технологий искусственного интеллекта как перспективное направление в деятельности правоохранительных органов по борьбе с преступностью [5].

Информационную основу для такого программного обеспечения могут создать существующие и активно разрабатываемые в настоящее время SIEM-системы[6].

---

[1] Пройдаков Э.М. Современное состояние искусственного интеллекта // Науковедческие исследования. 2018. С. 129.

[2] См.: Дискуссия «Искусственный интеллект - главная технология XXI века» // AI Journey 2020. Полное видео. - URL: https://www.youtube.com/watch?v=mW2LvLu-p04 (дата обращения: 20.07. 2021).

[3] См.: Маношин Д.А. Программирование искусственного интеллекта // Colloquium-journal. №12 (36). 2019. С. 115.

[4] Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. С. 42.

[5] Решняк О.А., Ковалев С.А. Предпосылки использования искусственного интеллекта в расследовании преступлений // Расследование преступлений: проблемы и пути их решения. 2021. № 3(22). С. 105.

[6] Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба. URL: https://ru.wikipedia.org/?curid=5231905&oldid=118279902 (дата обращения: 02.12.2021).

Задачами таких систем являются[1]:

обеспечение возможности учета анализа различных событий;

обработка и корреляция событий по заданным параметрам;

сбор и хранение событий из различных источников и их последующая консолидация и группировка;

оповещение о зафиксированных инцидентах и обеспечение удобного инструментария для последующей работы с информацией о них.

Однако для реализации стоящих перед ней задач необходимы полезные источники подлежащих обработке данных.

На сегодняшний день такими источниками являются следующие.

1. Сведения, аккумулируемые распространителем информации в сети Интернет, который в соответствии с действующим законодательством обязан обеспечить хранение данных о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий. А также текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки[2]. Аналогичные обязанности возложены и на операторов связи[3].

2. Массивы данных оператора связи, который обязан своевременно обновлять и хранить в течение трех лет информацию об абонентах и оказанных им услугах (фамилия, имя, отчество (наименование – для юридического лица), место жительства (место нахождения – для юридического лица), реквизиты основного

---

[1] См.: Быков А.А. SIEM-система – универсальный инструмент службы безопасности // Современные инновации. 2017. № 6(20). С. 47.

[2] См.: О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 6 июля 2016 г. № 374-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[3] См.: Там же.

документа, удостоверяющего личность, данные о расчетах за оказанные услуги связи, о соединениях и платежах абонента)[1].

3. В случае реализации вышеозвученных предложений о регистрации электронно-цифровых следов и мобильных устройств в качестве источника рассматриваемого вида могли бы быть использованы эти базы данных.

Объем, структура и содержание таких сведений относит их к категории больших данных (Bigdata).

Информационное содержание таких данных без специальной обработки недоступно для восприятия человека. К настоящему времени по вопросам аккумуляции, хранения и использования методов обработки больших данных проведено достаточное количество исследований[2].

Таким образом, наиболее оптимальным способом получения первоначальной криминалистически значимой информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий является автоматизированный анализ больших данных, аккумулируемых в соответствии с действующим законодательством Российской Федерации операторами связи, осуществляемый специальным программным обеспечением, функционирование которого основано на технологиях искусственного интеллекта.

В случае обнаружения в массивах анализируемых данных признаков, указывающих на осуществление незаконного сбыта наркотических средств названным способом, информируется уполномоченное лицо правоохранительных органов.

В целом, исходя из природы и содержания такой деятельности, ее следует осуществлять уже действующим или планируемым

---

[1] См.: Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление Правительства РФ от 27 авг. 2005 г.; О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] См.: Булычев А.В. Системный подход к анализу скрытых закономерностей в больших массивах слабоструктурированных данных: дис. ... канд. юрид. наук. М.: Ин-т систем анализа РАН, 2010. 91 с.; Болбаков Р.Г. Большие данные в информационных науках // Образовательные ресурсы и технологии. 2017. № 1(18). С. 30–35; Шаль А.В. Технологии больших данных в статистике // Учет и статистика. 2017. № 2(46). С. 81–88 и др.

к созданию оперативным подразделениям органов внутренних дел Российской Федерации. Также представляется целесообразным наделение сотрудников органов предварительного расследования правом оперативного доступа к полученной информации в рамках расследования конкретного уголовного дела. Например, в части установления новых эпизодов преступной деятельности, для повышения эффективности анализа материалов уголовных дел и формирования логических связей между лицами и событиями, в рамках планирования и проведения следственных действий.

Например, Ю.Н. Жданов и В.С. Овчинский предлагают осуществлять деятельность по получению первоначальной криминалистически значимой информации о преступлениях посредством разработок робототехники[1]. Однако очевидно, что такая деятельность должна осуществляться централизованно и быть строго регламентирована законом.

Поскольку современные источники аккумулируют как содержание (смысловую нагрузку) информации информационно-телекоммуникационных сетей, так и метаданные, многокритериальный поиск должен осуществляться в первую очередь по содержательной части, а метаданные должны быть использованы для уточнения событий, идентификации автора и т. п.

При разработке критериев поиска информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий из общей массы данных целесообразно использовать знания криминалистической характеристики, отраженные в ее закономерностях (табл. 2.).

[1] Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. С. 42.

Таблица 2

Критерии поиска информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий

Критерий	Содержание
Подозрительный или аномальный трафик	Наличие в статистике попыток обхода блокировки тематических ресурсов; факты посещения тематических ресурсов; факты, свидетельствующие о попытках анонимизации работы, пробелы в трафике; наличие запросов HTTP от спам-бота; Использование прикладных программ повышенной анонимности; использование платежных инструментов, частые поступления на счет равных сумм; регистрация на одном сетевом ресурсе разных аккаунтов и доступ к ним с одного и того же сетевого устройства.
Содержание переписки	Наличие часто пересылаемых геометок (в летнее время года – точек открытой местности, в зимнее – строений, заброшенных помещений), в частности между пользователями разных регионов; активное использование специальной терминологии (жаргона), в частности, характерной для региона: кайф, дурь, скорость и т. п; размещенные объявлений на соответствующих ресурсах о вакансиях с ключевыми словами: анонимный курьер, разносчик и др., характерные для региона.

Представленные критерии, обусловленные криминалистическими закономерностями анализируемой категории преступлений, не являются исчерпывающими, так как криминалистические знания о преступлениях, связанных с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий, регулярно расширяются, корректируются, дополняются и совершенствуются. В связи с этим при появлении новых знаний о рассматриваемых преступлениях выделенные признаки и их взаимозависимости должны постоянно дополняться.

Полученная таким образом информация прямо не может свидетельствовать о совершении преступления, в частности незакон-

ного сбыта наркотиков. Для принятия решения о ее проверке требуется совпадение нескольких критериев (их точное количество должно определяться в зависимости от характера полученных сведений) и последующее уточнение при помощи метаданных, сопутствующих анализируемой информации.

Полагается, что с развитием криминалистических знаний о закономерностях исследуемого вида преступлений предложенные критерии могут и должны быть дополнены, соответствуя реалиям современности и специфике конкретного региона.

Полученные результаты в их завершенном, проработанном и соответствующим образом оформленном виде следует предоставлять в распоряжение следователя в порядке, установленном законодательством Российской Федерации[1].

Конечно, идеализировать такой способ получения первоначальной криминалистически значимой информации о преступлении не стоит.

Например, Г.И. Колесникова отмечает в качестве недостатка программ, функционирующих на основе технологий искусственного интеллекта, невозможность воссоздания мыслительных процессов человека[2].

Также нельзя не учитывать противодействие, оказываемое преступниками: использование технологий, трафик которых недоступен для традиционных мер контроля (в частности, VPN, технологии малого радиуса действия и т. д.).

Кроме того, полученная таким образом информация в своей первоначальной форме доказательством не является и носит лишь ориентирующий характер, что определяет необходимость ее дальнейшей проверки уголовно-процессуальными средствами.

Вместе с тем получение первоначальной криминалистически значимой информации об анализируемых преступлениях таким

---

[1] См.: Об утверждении Инструкции о порядке передачи результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сент. 2013 г. № 776/703/509/507/1820/42/535/398/68. Доступ из справ. правовой системы «КонсультантПлюс».

[2] Колесникова Г.И. Искусственный интеллект: проблемы и перспективы // Видеонаука. 2018. № 2(10). С. 34–39.

путем может разрешить широкий круг стоящих перед правоохранительными органами задач. Полученная информация может:

явиться основанием для проведения оперативно-розыскных мероприятий;

быть положена в основу прогнозирования, т. е. создания прогностической информации за счет еще не выявленных причинных связей, отношений, которые станут потенциальными в познании будущего;

выступить объектом аналитического поиска, ориентированного на глубокую разведку среды, в которой действуют и общаются участники, позволяющего выявить целые группы преступных деяний и лиц, их совершающих[1];

быть положенной в основу совместного планирования расследования;

включая в себя отдельные признаки сетевой активности лиц, а также сведения об их деятельности (геометки, сфера интересов, локации перемещений и т. п.), стать ориентирующей информацией при формировании круга причастных к преступлению лиц (выделенных по общности полученных признаков);

оказать содействие следователю в формировании картины конкретного преступления, выделить типичные правила, действия, признаки, присущие ему, и в соответствии с этим наиболее эффективно осуществлять расследование.

[1] См.: Овчинский С.С. Оперативно-розыскная информация / под ред. А.С. Овчинского, В.С. Овчинского. М.: ИНФРА-М, 2000. С. 285–309.

2.2. Предварительная проверка и оценка первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий

В соответствии с требованиями уголовно-процессуального законодательства дознаватель, орган дознания, следователь, руководитель следственного органа обязаны принять, проверить сообщение о любом совершенном или готовящемся преступлении[1].

То есть проведение предварительной проверки сообщения о преступлении – обязанность, а не право дознавателя, органа дознания, следователя. Однако в более ранних научных трудах содержатся рекомендации проведения такой проверки лишь в случае недостаточности первичной информации о признаках состава преступления[2].

Например, В.Н. Яшин предлагает считать предварительной проверкой сообщения о преступлении регламентированную уголовно-процессуальным законом деятельность уполномоченных на то должностных лиц правоохранительных органов по сбору дополнительных сведений по первичному материалу о преступлении[3].

Однако проверка первоначальной информации о преступлении – обязательный элемент в структуре предварительного расследования, и ее назначение состоит в аккумуляции информации (признаков), свидетельствующей о наличии состава преступления.

А.С. Лизунов называет такую проверку сообщения о преступлении «доследственная проверка»[4].

В то же время, несмотря на то, что ученые активно используют этот термин, мы разделяем мнение А.Н. Калюжного, кото-

---

[1] См.: Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 177-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] См.: Селиванов Н.А. Справочная книга криминалиста. М.: Норма, 2001. С. 190; Степанов В.В. Предварительная проверка первичных материалов о преступлениях. Саратов: Саратов. юрид. ин-т, 1972. С. 10–11.

[3] Яшин В.Н. Предварительная проверка первичных материалов о преступлении: дис. … канд. юрид. наук. М., 1999. С. 10.

[4] Лизунов А.С. Понятие и форма производства доследственной проверки // Бизнес в законе. Экономико-юридический журнал. 2012. № 3. С. 80.

рый считает, что он является «некорректным по отношению к рассматриваемой деятельности, так как ее проведение не всегда оканчивается возбуждением уголовного дела и проведением предварительного расследования»[1]. В настоящем исследовании нами будет использован термин «предварительная проверка».

Стоит отметить современную тенденцию включения рекомендаций по проведению предварительной проверки в положения методик расследования отдельных видов преступлений.

А.Г. Филиппов, например, выделяет предварительную проверку как новый раздел в криминалистике, аргументируя это тем, что именно ее положения вооружают следователя арсеналом средств установления достаточности данных, необходимых для возбуждения уголовного дела[2].

Л.А. Савина также говорит о существовании тактики проведения предварительной проверки сообщений о преступлениях и относит к компетенции криминалистики изучение конкретных средств и приемов такой проверки[3].

Н.И. Савченко называет предварительную проверку сообщений о преступлениях основным элементом предварительного этапа расследования уголовных дел[4].

Однако исследования ученых в области криминалистики и уголовного процесса, как и результаты проводимых предварительных проверок, свидетельствуют о наличии многочисленных нарушений закона, ошибках и иных недостатках при проверке сообщений о преступлениях[5].

Только 6% опрошенных сотрудников органов предварительного расследования высоко оценивают поступившие им матери-

---

[1] Калюжный А.Н. Предварительная проверка сообщений о преступлениях: понятие и этапы производств // Юридическая наука. 2013. № 1. С. 61.

[2] Криминалистика: учеб. / под ред. А.Г. Филиппова. 2-е изд., перераб. и доп. М.: Спарк, 2000. С. 342.

[3] Савина Л.А. Организация и тактика предварительной проверки сообщений об экономических преступлениях на железнодорожном транспорте: дис. ... канд. юрид. наук. М., 2005. 228 с.

[4] Савченко Н.И. Указ. соч. С. 58.

[5] См.: Ильин А.Н. Тактика предварительной проверки сообщения о преступлении: автореф. дис. … канд. юрид. наук. М., 2009. С. 2, 3.

алы предварительных проверок о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий, считая, что в них установлены все признаки состава преступления; 62% – оценивают их удовлетворительно, отмечая наличие в них некоторых незначительных пробелов; 32% – как неудовлетворительные, поскольку представленные материалы не отвечали предъявляемым к ним требованиям либо вследствие некачественного проведения предварительной проверки часть доказательственной базы была утрачена.

В связи с этим А.Н. Ильин указывает на необходимость решения вопроса о месте положений тактики предварительной проверки в системе криминалистики и о разработке и внедрении соответствующего учебного курса. Свое предложение автор обосновывает тем, что исследование системы научных знаний о средствах и методах проверки сообщений о преступлениях и выработка рекомендаций по совершенствованию этой деятельности представляются весьма актуальными как для науки криминалистики, так и для практики правоохранительных органов[1].

Результаты проведенного анализа уголовных дел позволяют сделать вывод, что большая часть (78%) материалов предварительной проверки информации об анализируемых преступлениях разрешаются оперуполномоченными, 15% – участковым уполномоченным полиции и только 7% – следователями.

То есть в разрешении первоначальной информации о рассматриваемых преступлениях участвуют сотрудники правоохранительных органов разных направлений деятельности. Тем не менее в большинстве случаев предварительная проверка поручается органу дознания, а подразделения, осуществляющие расследование уголовных дел, получают уже готовые материалы.

Методы и средства проверки заявлений и сообщений о преступлениях традиционно делятся на две группы:

1. Непроцессуальные, т. е. мероприятия, предусмотренные федеральными законами «О полиции» и «Об оперативно-розыскной деятельности»[2].

---

[1] Ильин А.Н. Указ. соч.

[2] См.: Ильин А.Н. Указ. соч. 24 с.

Например, А.Л. Осипенко и П.В. Миненко считают основным средством документирования информации о незаконном сбыте наркотических средств с использованием телекоммуникационных устройств такое оперативно-розыскное мероприятие, как проверочная закупка[1].

2. Мероприятия, порядок проведения которых закреплен уголовно-процессуальным законодательством:

следственные действия, проведение которых возможно до возбуждения уголовного дела: осмотр, освидетельствование, эксгумация трупа, получение образцов для сравнительного исследования, назначение экспертизы;

процессуальные средства проверки сообщения о преступлениях: истребование необходимых материалов; производство документальных проверок и ревизий, исследований и иные.

Методы и средства избираются в зависимости от процессуальных полномочий субъекта предварительной проверки. Однако очевидно, что чем больше мероприятий, направленных на установление признаков преступления, выполнено, тем более полно и объективно будет проведена проверка.

Относительно анализируемых преступлений А.В. Шебалин отмечает, что предварительная проверка информации о них должна проводиться посредством проведения оперативно-розыскных мероприятий «Оперативный эксперимент» и «Проверочная закупка», называя используемые в данном случае процессуальные средства неэффективными[2].

Проведенное же нами исследование опровергает это утверждение и свидетельствует об активном использовании процессуальных средств предварительной проверки. Например, осмотр места происшествия был проведен в 100% изученных уголовных дел. В качестве его специфики можно отметить, что таких мест может

---

[1] Осипенко А.Л., Миненко П.В. Оперативно-розыскное противодействие незаконному обороту наркотических средств, совершаемому с использованием телекоммуникационных устройств // Вестник Воронежского института МВД России. 2014. № 1. С. 151–154.

[2] Шебалин А.В. Особенности этапа предварительной проверки материалов о незаконном сбыте наркотических средств, совершенном бесконтактным способом // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2015. № 15-1. С. 150.

быть несколько: место задержания наркосбытчика, обнаружения наркотических средств, их изготовления и т. п. Осмотры предметов (мобильного телефона, оборудования, используемого для изготовления и фасовки наркотиков, и т. п.) и документов в рамках предварительной проверки сообщения о преступлении проводились также в 100% случаев. Весьма распространено (95%) такое проверочное действие, как получение образцов для сравнительного исследования (по данной категории дел получают образцы срезов карманов одежды задержанного, смывы с его рук и т. д.). В 100% случаев проводились судебные физико-химические экспертизы, что обусловлено особенностью уголовных дел, связанных с незаконным оборотом наркотиков: только проведение специального исследования может определить, относится обнаруженное вещество к наркотическим или нет. Как правило, остальные экспертизы проводятся уже после возбуждения уголовного дела, что обусловлено рядом процессуальных вопросов (сохранность объектов для проведения дополнительных и повторных экспертиз, соблюдение прав участников уголовного процесса и т. п.).

Необходимо особое внимание уделить судебной компьютерной экспертизе. Действительно, трудоемкость исследования, технические сложности, а также большие очереди на исследование, обусловленные ее узкой направленностью, делают невозможным проведение такой экспертизы в рамках предварительной проверки.

В этом случае для обеспечения требуемого качества и возможности ее проведения после возбуждения уголовного дела на проверочном этапе следует уделить особое внимание детальному осмотру компьютерной техники и программного обеспечения. Он должен быть проведен максимально подробно в целях фиксации следов и индивидуальных особенностей объектов осмотра.

Кроме того, в рамках такого осмотра могут быть установлены наименование и алгоритмы работы используемых информационно-телекоммуникационных систем и ресурсов, на основании чего может быть реконструирована криминальная ситуация.

100% изученных материалов уголовных дел содержали объяснения, полученные в ходе предварительной проверки, 100% –

результаты иных проверочных мероприятий (изъятия, результаты оперативно-розыскных мероприятий и т. п.).

Основная цель предварительной проверки – восполнение информационных пробелов в имеющейся первоначальной информации, что необходимо для отнесения деяния к определенному преступному, установив признаки его состава.

Рекомендации по проведению предварительных проверок информации о незаконном сбыте наркотических средств, совершаемом как традиционными способами[1], так и анализируемым[2], содержатся в ранее проведенных исследованиях.

Однако изучение представленных рекомендаций по проведению предварительных проверок первоначальной информации об анализируемых преступлениях свидетельствует о том, что ни одна из них не отражает особенности протекания криминальных процессов как в материальном, так и в информационном пространстве одновременно.

По результатам проведенного анализа уголовных дел о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий, в части проведения проверки первоначальной информации о преступлении могут быть сделаны следующие выводы.

Объем, вид и субъект проводимых проверочных мероприятий определены содержанием и источником первоначальной информации о преступлении.

Для анализируемой категории преступлений характерны следующие проверочные ситуации:

---

[1] См.: Черняков М.М. Проверка сообщений о незаконном обороте наркотических средств и психотропных веществ // Вестник Сибирского юридического института МВД России. 2016. № 1(22). С. 46–48; Григорьев О.Г., Кривощеков Н.В.Особенности расследования преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ и их аналогов: учеб.-практ. пособие. Тюмень: Тюмен. юрид. ин-т МВД России, 2010. 104 с.; Ошлыкова Е.А. Указ. соч. 243 с. и др.

[2] См.: Шебалин А.В. Указ. соч. С. 150–154; Гончарова Н.С. Проблемы криминалистической деятельности на этапе проверки сообщения о незаконном сбыте наркотических средств бесконтактным способом // Организационное, процессуальное и криминалистическое обеспечение уголовного судопроизводства: материалы VI Междунар. науч. конф. студентов и магистрантов. Симферополь, 2017. С. 22–24; Решняк О.А. Указ. соч. С. 87–120 и др.

1. Незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий совершен в очевидных условиях – 27%. В этом случае речь идет о деятельности организованных преступных групп. Установлены все либо основные звенья преступной цепи, что дает возможность полностью прекратить противоправную деятельность конкретной преступной организации.

Такая проверочная ситуация является наиболее благоприятной и требует грамотного и максимально полного документирования в материалах проверки объема криминального поведения каждого из задержанных лиц (разрешается совокупностью процессуальных и непроцессуальных проверочных мероприятий таких, как опросы, экспертизы, осмотры, получение компьютерной информации и др., в зависимости от особенностей конкретной проверочной ситуации и субъекта предварительной проверки).

2. Незаконный сбыт наркотических средств анализируемым способом совершен в условиях неочевидности – 73%. Термин «неочевидность» применен условно. Эта проверочная ситуация может иметь следующие типичные вариации:

задержан «закладчик», не располагающий сведениями ни о первоисточнике наркотических средств, ни о лицах, связанных с ними, и т. п.;

в правоохранительные органы поступила информация о функционировании сетевого ресурса, посредством которого осуществляется незаконный сбыт наркотических средств.

То есть объем информации о преступлении крайне ограничен: не выявлены следы преступления, особенности способа незаконного сбыта наркотиков, не установлены все лица, причастные к его совершению, в связи с чем их противозаконная деятельность не пресечена.

Проверочные мероприятия должны проводиться как в материальной плоскости, так и в информационной. Помимо традиционных (опросы, осмотры, криминалистические экспертизы, проверочные закупки и т. п.), необходимо тщательно проработать информационную составляющую: осмотры изъятых средств связи,

производство судебных компьютерных экспертиз, получение компьютерной информации, прослушивание телефонных переговоров и др. Например, О.А. Решняк говорит о наблюдении за местами сетевого общения наркопотребителей и наркосбытчиков[1].

Также проверочные ситуации могут быть сформированы и в зависимости от источника информации о преступлении, что определит лиц, осуществляющих проверку, и используемые ими средства и методы в рамках своей компетенции.

Двойственная (материальная и информационная) природа способов совершения преступлений, связанных незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных систем, требует применения различных методик проведения предварительной проверки первоначальной информации о них.

Традиционные (процессуальные и непроцессуальные) алгоритмы и методики проведения проверочных мероприятий в большей части направлены на установление признаков материальной составляющей способа совершения преступления: источники и способы непосредственного получения и изготовления наркотических средств и реагентов для их изготовления, хранение, фасовка, перемещение, распределение преступных ролей, использование некоторых мер конспирации и т. п.

Специфика же информационной составляющей способа совершения анализируемого преступления требует особого подхода. Порядок деятельности по установлению ее признаков отражен в алгоритмах функционирования используемых в преступных целях информационно-телекоммуникационных систем и технологий. То есть уполномоченному лицу, проводящему проверку, необходимо проследовать по «пути» их функционирования.

Вид используемых преступниками информационно-телекоммуникационных систем и их программного обеспечения обусловлен спецификой торговой площадки, посредством которой осуществлялся незаконный сбыт наркотических средств.

Очевидно, что обнаружение наркотического средства в «закладке» не является прямым свидетельством незаконного сбыта

[1] Решняк О.А. Указ. соч. С. 99.

наркотических средств с использованием информационно-телекоммуникационных технологий. Для того чтобы вести речь о рассматриваемом преступлении, на момент предварительной проверки должно быть установлено лицо, связанное с обнаруженными наркотическими средствами (сбывающее или же приобретающее их). Соответственно, оно и выступит источником сведений об организации торговой площадки, посредством которой наркотические средства и были приобретены. Необходимые сведения могут быть получены путем проведения оперативно-розыскных мероприятий, получения объяснений, осмотра используемых средств связи, производства экспертиз и т. п.

После установления порядка организации торговой площадки, помимо традиционных для проверки сообщений о незаконном сбыте наркотических средств мероприятий[1]*, с учетом специфики анализируемых преступлений целесообразно проведение проверочных мероприятий согласно определенным алгоритмам (табл. 3).*

Применительно к представленным в таблице 3 данным следует указать, что конкретное наименование мероприятий, посредством которых могут быть реализованы представленные алгоритмы, будет зависеть от полномочий субъекта предварительной проверки.

При наличии доступа к телекоммуникационным системам хотя бы одного из лиц, причастных к совершению преступления, можно установить достаточно большой объем сведений об информационной составляющей способа совершенного преступления, раскрывающей криминальную деятельность. Анализ этих сведений в условиях ограниченного объема информации о преступлении поможет установить механизм и, возможно, иных участников преступного процесса.

[1] См.: Черняков М.М. Указ. соч. С. 46-48; Григорьев О.Г., Кривощеков Н.В. Указ. соч. 104 с.; Ошлыкова Е.А. Указ. соч. 243 с. и др.

Таблица 3

Алгоритмы предварительной проверки первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий

Организация торговой площадки, используемой для сбыта наркотических средств с использованием информационно-телекоммуникационных технологий					
Даркнет	Стандартные интернет-соединения			Перспективные телекоммуникационные технологии	
	Социальные сети	Интернет-сайты			
		Очевидное	Неочевидное	Очевидное	Неочевидное
Осмотр и анализ используемых преступниками средств связи, в частности на предмет установления наличия VPN, TOR, биткоин-кошельков, иных платежных инструментов, средств анонимизации; установление и изучение регистрационных данных, используемых на платформе; установление связей с другими аккаунтами	Анализ информационного контента аккаунта; установление регистрационных данных; установление контактов, связей и активности пользователя; анализ Cookie[1]; получение и анализ трафика; анализ журнала Log-файлов[2].	Получение сведений: о регистрации домена, об оплате хостинга; анализ запросов к серверу; получение трафика; получение и анализ сведений сетевых журналов (подключений, активности и т. п.); определение настроек браузера; анализ связей установленного на компьютерном устройстве преступника	Получение и анализ трафика; обнаружение, фиксация и анализ: следов использования платежных инструментов, сведений сетевых журналов (подключений, активности и т. п.); изучение настроек браузера, установленного программного обеспечения и следов его использования.	Изучение и анализ средств связи; анализ алгоритмов и следов работы установленного прикладного программного обеспечения; используемых технических устройств и технологий организации связи.	Изучение и анализ средств связи; анализ алгоритмов и следов работы установленного прикладного программного обеспечения.

[1] Фрагменты данных, отправленные сервером на устройство, откуда был совершен вход в Интернет. Служат для аутентификации (проверки подлинности) пользователя, сохранении его настроек и персональных предпочтений.

[2] Файлы подключений.

и активности пользователя в целом; анализ установленных прикладных программ (возможно использование одних и тех же сведений о пользователе или же не отключенные Javascript [1] в браузере).		программного обеспечения и информационного контента сайта; обнаружение, фиксация и анализ следов подключения и настройки платежных инструментов.			

Благодаря коммуникативной сущности деятельности в информационно-телекоммуникационном пространстве при проведении должных аналитических мероприятий сетевая деятельность одного пользователя, даже несмотря на предпринятые им меры анонимизации, позволит установить другого, с которым последний контактировал.

В случае использования Даркнета актуальна проверка уязвимостей TOR, Javascript и др., позволяющая установить IP-адреса пользователей и провести анализ их реквизитов, регистрационных данных, выявить связь с аккаунтами других пользователей сети.

Например, личность создателя SilkRoad, несмотря на все предпринятые меры анонимизации, была установлена в процессе аналитической работы: было обнаружено использование им реальных регистрационных данных на одном из интернет-ресурсов, весьма опосредованно связанных с SilkRoad[4].

В случае осуществления незаконной деятельности с использованием социальных сетей необходимо иметь в виду, что владелец аккаунта при регистрации мог указать не соответствующую

[1] Браузерная технология для оптимизации работы.

[4] См.: Розыск и поимка владельца Silk Road. Отчет агента ФБР. URL: https://habr.com/ru/post/196464/ (дата обращения: 09.01.2020).

действительности информацию о себе[1]. Мероприятия, проводимые на этапе предварительной проверки, должны быть направлены на установление и отработку его сетевой активности, причем не только связанной с выявленным преступным фактом, но и осуществляемой до и после совершения преступления, а также контактов пользователя и его взаимодействия с ними.

При осуществлении незаконного сбыта наркотических средств посредством веб-сайтов анализ сетевой активности пользователя может указать на незаконный интернет-ресурс. В то время как работа с лицом, стоящим во главе этого ресурса, позволит установить клиентуру сайта.

Специфика еще не используемых для незаконного сбыта наркотиков, но в скором времени предположительно весьма популярных для этих целей телекоммуникационных технологий состоит в их обособленности от интернет-провайдеров. Если у наркокурьера (закладчика) или у лиц, приобретающих наркотические средства, интересующие сведения могут быть получены в ходе осмотра используемого телекоммуникационного устройства и его программного обеспечения, то у непосредственных организаторов анализируемого преступления дополнительно должны быть подвергнуты детальному изучению и осмотру технические средства, задействованные в установлении связи.

В рамках изучения информационных ресурсов стоит обратить внимание и на их организаторов, поскольку их деятельность также может быть противоправной, заключаться в создании условий для совершения преступления (за исключением функционирования легальных интернет-площадок) и, соответственно, должна быть пресечена.

Изучение трафика платежных инструментов позволит установить факты оплаты услуг маркетплейса[2] (витрина, реклама, продвижение) и в ходе дальнейшей аналитической работы выявить

---

[1] См.: Цимбал В.Н., Цимбал Н.Г. Использование информации социальных сетей Интернет в ходе предварительного расследования // Теория и практика общественного развития. 2013. Вып. 10. С. 426.

[2] Платформа электронной коммерции, онлайн-магазин электронной торговли, предоставляющий информацию о продукте или услуге третьих лиц. URL: https://ru.wikipedia.org/?curid=7367740&oldid=114630219 (дата обращения: 02.06.2021).

возможные контакты владельцев и посетителей интернет-площадки.

В основу тактических рекомендаций по проведению предварительной проверки первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий должен быть положен принцип «ожидания».

Он заключается в недопустимости пресечения преступной деятельности в момент получения сведений о ней. То есть лицом, проводящим предварительную проверку выявленного преступного факта, должен быть установлен максимальный объем потенциальной доказательственной информации, контактов, геопозиций, активности заподозренного в совершении преступления, до момента пресечения его преступной деятельности. Естественно, нельзя допустить совершения нового преступления.

Целесообразность избрания такой тактики обусловлена высокой степенью анонимности анализируемой преступной деятельности, в связи с чем объем первоначальной информации, как правило, весьма ограничен.

Например, *Б. и не установленное следствием лицо занимались незаконным сбытом наркотических средств с использованием информационно-телекоммуникационной сети Интернет при следующих обстоятельствах: через сайт «***», зарегистрированный в сети Интернет, не установленное следствием лицо размещало объявления о продаже наркотиков и получало заказы. Далее через программу «***» передавало Б. информацию о заказе. Б. расфасовывала наркотические средства в соответствии с заказом, делала их «закладку», о местонахождении которой посредством программы «***» передавала информацию не установленному следствием лицу*[1].

Уголовное дело было возбуждено по оперативным материалам. На момент предварительной проверки правоохранительные органы располагали сведениями о предмете и способе незаконного сбыта наркотиков, а также о лице, непосредственно их сбывавшем, чья незаконная деятельность была немедленно пресечена. Вместе

[1] См.: Архив Ленинского районного суда г. Новороссийска Краснодарского края. Уголовное дело № 1-44/2018 по ч. 4 ст. 228.1, ч. 2 ст. 228 УК РФ.

с тем сама преступная организация осталась функционировать, и, вполне вероятно, вскоре место Б. будет занято другим лицом.

Ключевая же информация (сведения о личности неустановленного лица, а также о первоисточнике наркотических средств), способная обеспечить эффективную борьбу с данным видом преступности при соблюдении соответствующих тактических рекомендаций и грамотно проведенных проверочных мероприятий, могла и должна была быть получена еще на этапе ее проверки. Так, столь раннее пресечение противоправной деятельности Б. при получении только первичной информации о ней было нецелесообразно. Куда больший успех в рамках сложившейся проверочной ситуации принесла бы организация оперативного наблюдения за телекоммуникационной сетью и функционированием изъятого средства связи, получение и последующий анализ его трафика и транслируемой компьютерной информации.

Совокупность полученных в ходе проверки сообщения о преступлении результатов оценивается уполномоченным на то лицом с точки зрения достаточности признаков, указывающих на преступление, и по результатам оценки принимается одно из предусмотренных уголовно-процессуальным законом решений[1].

Подводя итог вышесказанному, можно заключить, что специфика предварительной проверки первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий определяется характеристиками информационной составляющей способа анализируемого преступления. Порядок и содержание деятельности по их установлению содержится в алгоритмах функционирования используемых в преступных целях информационно-телекоммуникационных систем и технологий.

То есть установление признаков рассматриваемого преступления лицу, проводящему проверку первоначальной криминалистически значимой информации о нем, необходимо начинать с анализа особенностей функционирования используемых в преступных целях телекоммуникационных устройств и их программ-

[1] См.: Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 177-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

ного обеспечения. При этом следует учитывать, что их вид определяется спецификой организации торговой интернет-площадки, используемой для незаконного сбыта наркотических средств. В дальнейшем, используя тактику «ожидания», нужно установить максимальное необходимое для формирования полного представления о предмете доказывания количество фактов, восполнив имеющиеся информационные пробелы.

Таким образом, учет сформулированных выводов, а также проведение перечисленных проверочных мероприятий обеспечат качество и полноту проведения предварительной проверки первоначальной информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий. Следователь, зная о специфике анализируемого преступления, а также об алгоритмах, обеспечивающих эффективное проведение проверочных мероприятий, будет иметь возможность объективно оценить полученные материалы, а также грамотно спланировать как согласованную деятельность в рамках предварительной проверки, так и дальнейшее расследование в целом.

2.3. Особенности первоначального этапа расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Расследование преступлений – это сложная разнонаправленная деятельность, осуществляемая уполномоченными на то должностными лицами правоохранительных органов совместно с иными участниками расследования, по полному и объективному установлению истины по уголовному делу.

Традиционно криминалистика разделяет процесс расследования преступлений на три этапа: первоначальный, последующий и заключительный[1]. В дополнении к этому Н.И. Савченко говорит о существовании предварительного этапа расследования[2]. Однако единства представлений о границах этих этапов расследования нет.

---

[1] См.: Белкин Р.С. Курс советской криминалистики. М.: Акад. МВД СССР, 1979. Т. 3. С. 259.

[2] Савченко Н.И. Указ. соч. С. 4.

По мнению некоторых авторов, первоначальный этап расследования преступлений начинается с момента получения информации о совершенном или готовящемся преступлении и до принятия решения о возбуждении уголовного дела[1]. Однако не все поступившие сообщения о преступлениях разрешаются возбуждением уголовного дела.

С.В. Кисляков называет началом первоначального этапа расследования преступлений проведение осмотра места происшествия[2].

Осмотр места происшествия – одно из процессуальных средств проверки сообщения о преступлении, которая, как отмечено выше, не всегда оканчивается возбуждением и дальнейшим расследованием уголовного дела.

О.В. Цуканова обозначает границы первоначального этапа расследования с момента поступления сообщения о преступлении до предъявления обвинения лицу, его совершившему[3].

Мы также не можем согласиться с этим мнением, поскольку не каждое расследование включает в себя предъявление обвинения (например, нераскрытые преступления). И это исключает деятельность следователя на последующем этапе.

В.И. Лунгу очерчивает границы первоначального этапа расследования вокруг выполнения неотложных следственных действий. И называет его началом принятие уголовного дела к производству лицом, проводящим расследование[4]. Однако некоторые следственные действия могут быть выполнены до принятия уго-

---

[1] См.: Звезда И.И. Характеристика первоначального этапа расследования мошенничества в банковской сфере // Деятельность правоохранительных органов в современных условиях: сб. материалов 20-й Междунар. науч.-практ. конф. Иркутск, 2015. С. 328.

[2] Кисляков С.В. Некоторые проблемы первоначального этапа расследования ДТП, с причинением вреда здоровью человека // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. материалов Всерос. науч.-практ. конф. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 191.

[3] Цуканова О.В. Понятие, структура и задачи первоначального этапа расследования преступлений, совершенных на объектах железнодорожного транспорта // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. материалов Всерос. науч.-практ. конф. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 353–356.

[4] Лунгу В.И. Первоначальный этап расследования преступлений: автореф. дис. … канд. юрид. наук. Киев, 1991. 25 с.

ловного дела следователем к производству. Кроме того, расследование уголовного дела могут осуществлять различные следователи, каждый раз принимая его к своему производству.

В некоторых научных трудах, посвященных первоначальному этапу расследования, его границы так и не обозначены[1].

Обобщая существующие взгляды исследователей и опыт расследования уголовных дел, можно прийти к выводу, что границы первоначального этапа расследования преступлений могут быть обозначены от принятия решения о возбуждении уголовного дела до момента сбора достаточного количества доказательств, позволяющих заподозрить конкретное лицо в совершении расследуемого преступления.

Причем достаточность таких доказательств, как и момент перехода к следующему этапу расследования, оценивает следователь.

То, что именно в рамках анализируемого этапа расследования происходит сбор основной доказательственной информации по делу, неоспоримо, это придает ему особое значение.

А.М. Моисеев и С.В. Кондратюк называют основной задачей анализируемого этапа расследования выявление уличающих преступника фактов[2].

В результате проведенного нами исследования установлено, что поводами к возбуждению уголовных дел о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий являются:

1) заявление о преступлении (13%) – такие заявления исходят, как правило, от заинтересованных лиц;

2) явка с повинной (0%) – отсутствие такого повода к возбуждению уголовных дел свидетельствует об умышленном и заранее спланированном характере совершаемых преступных действий;

---

[1] См.: Гончарова Т.А. Первоначальный этап расследования терроризма: автореф. дис. … канд. юрид. наук. М., 2006. 24 с.; Папышева Е.С. Методика первоначального этапа расследования убийств, совершенных несовершеннолетними: автореф. дис. … канд. юрид. наук. М., 2010. 30 с.

[2] МоисеевА.М., Кондратюк С.В. Криминалистические признаки наркосбыта посредством Интернет // Балканско-научное собрание. №1. 2017. С. 44.

3) сообщение о преступлении, полученное из иных источников (87%) – сюда отнесены оперативные материалы, рапорта следователя, сотрудников наружных служб и т. п.;

4) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании (0%).

Поводы к возбуждению уголовного дела, помимо формальных оснований, должны содержать набор признаков, необходимых для принятия процессуального решения о начале расследования.

Специфика анализируемых преступлений в части определения наиболее оптимального момента для возбуждения уголовных дел определена двойственной природой способа совершения преступления и состоит в том, что, помимо общих обстоятельств, указывающих на признаки состава преступления (объект, субъект, объективная сторона, субъективная сторона), на момент принятия решения о возбуждении уголовного дела должен быть установлен ряд фактов, связанных с информационной составляющей способа его совершения, что, в свою очередь, позволит определить основные особенности способа совершения преступления, места нахождения и виды следов его совершения и организовать эффективное расследование уголовного дела.

Итак, уголовно-процессуальный закон позволяет принять решение о возбуждении уголовного дела, основываясь только на общих признаках, а остальные могут быть установлены в ходе процессуальной деятельности следователя. Однако необходимо иметь в виду, что противодействие расследованию, предпринятые меры анонимизации и т. п. затруднят их установление, а также не позволят определить верные направления и основные этапы работы следователя. В таком случае преступная деятельность в максимально возможном объеме пресечена не будет, что явно противоречит целям расследования.

Преступная деятельность рассматриваемого вида во многом определяется алгоритмами работы используемого программного и аппаратного обеспечения, функциональные возможности которого зависят от формы организации торговой площадки, на которой осуществляется незаконный сбыт наркотических средств.

В связи с этим для принятия своевременного решения о возбуждении уголовного дела в первую очередь необходимо установить форму организации торговой площадки, используемой для сбыта наркотических средств, что позволит отграничить преступления, совершенные анализируемым способом, от иных.

Вместе с этим к моменту возбуждения уголовного дела целесообразно определить еще ряд признаков:

форму организации электронной торговой площадки, используемой для сбыта наркотических средств;

факт использования, характеристики и роль в преступном процессе программного обеспечения и телекоммуникационных технологий, а также обстоятельства их функционирования;

содержание сопровождающего контента;

факт использования способов и средств анонимизации преступной деятельности и их особенности;

объем и особенности рекламы контента электронной торговой площадки, отражающей масштабы преступной деятельности и круг причастных и заинтересованных лиц;

особенности ведения преступной финансовой деятельности.

Перечисленные признаки не являются исчерпывающими и могут быть дополнены. Однако они являются основными, характеризующими информационную составляющую преступления.

Сам процесс расследования преступлений протекает в конкретных условиях, времени и месте, во взаимосвязи с другими процессами, под влиянием определенных факторов, содержание и воздействие которых зачастую не известны следователю.

Такой синтез результатов поисково-познавательной деятельности следователя, отражающий информационное состояние процесса расследования, образует определенную обстановку, в которой действуют субъекты расследования, называемую в криминалистике следственной ситуацией.

Умение следователя правильно анализировать и оценивать сложившуюся следственную ситуацию играет существенную роль для объективного, полного и всестороннего расследования уголовного дела[1].

[1] См.: Звезда И.И. Указ. соч. С. 332.

При изучении особенностей расследования незаконного сбыта наркотических средств, совершаемого анализируемым способом, выделяют следующие следственные ситуации первоначального этапа:

лицо, подозреваемое в совершении преступления, задержано;

в правоохранительные органы поступила информация о лицах, занимающихся незаконным сбытом наркотиков[1].

Последняя ситуация, по сути, является проверочной, поскольку известный правоохранительным органам факт незаконного сбыта наркотических средств, не подкрепленный иными сведениями, указывающими на событие преступления, не может являться основанием для возбуждения уголовного дела.

В.С. Удовиченко и В.К. Зникин формируют следственные ситуации в зависимости от способа непосредственной передачи наркотических средств[2]:

приобретатель и продавец наркотиков знакомы лично и передают наркотические и денежные средства друг другу;

цепочка «продавец – покупатель» разрывается посредниками, одним или несколькими, хотя факт их знакомства полностью не исключается;

между продавцом и покупателем передача наркотических и денежных средств осуществляется без личного контакта.

Представленные следственные ситуации не отражают в полном объеме всю информацию, с которой приходится сталкиваться следователю на первоначальном этапе расследования преступления.

А.В. Шебалин и А.В. Польгерт представляют анализируемые следственные ситуации таким образом[3]:

имеются следы наркотических средств и предметы, контактировавшие с ними;

---

[1] См.: Герасимова С.О. Методика расследования бесконтактного способа сбыта наркотиков // Развитие общественных наук российскими студентами: сб. науч. тр. Краснодар, 2017. С. 72.

[2] Удовиченко В.С., Зникин В.К. Способ совершения преступления как тактико-образующий элемент ситуации допроса подозреваемого и обвиняемого при незаконном сбыте наркотических средств // Известия Балканского государственного университета. 2013. № 2-1(78). С. 124–125.

[3] Шебалин А.В., Польгерт А.В. Первоначальный и последующий этап расследования незаконного сбыта наркотических средств, совершенного посредством телекоммуникационных сетей // Вестник Томского государственного университета. Право. 2017. № 24. С. 119–125.

имеются следы рукописных записей (адреса закладок, номера мобильных, банковские реквизиты);

имеется компьютерная техника, являющаяся средством совершения преступлений, обнаружены их электронно-цифровые следы;

обнаружены электронно-цифровые следы, содержащиеся в компьютерной технике, которая не является средством совершения преступления.

Мы также не можем согласиться с таким представлением объема информации первоначального этапа расследования рассматриваемых преступлений, поскольку она не отражает всех сведений, которые должны быть известны следователю.

Считается, что следственные ситуации первоначального этапа расследования формируются по результатам разрешения проверочных ситуаций, а содержание и порядок производства необходимых оперативно-следственных мероприятий определяются особенностями конкретной следственной ситуации.

Таким образом, в зависимости от эффективности преодоления информационных пробелов предварительной проверки сообщений об анализируемых преступлениях возможны следующие типичные следственные ситуации первоначального этапа расследования.

1. Задержан сбытчик наркотических средств в момент либо после совершения преступления. Установлен способ его совершения, выявлены следы, а также сведения, позволяющие установить личности причастных к его совершению.

Основной целью деятельности следователя в данной ситуации будет как доказывание вины задержанного, так и установление первоисточника наркотических средств и лиц, причастных к их незаконному сбыту.

В ходе разрешения данной ситуации могут быть проведены такие мероприятия:

осмотр места происшествия;

получение образцов для сравнительного исследования;

допросы задержанного и свидетелей;

криминалистические экспертизы;

обыск по месту проживания задержанного;

следственные осмотры предметов и документов, в частности, особое внимание уделяется осмотру мобильного телефона и иных средств связи;

получение информации о соединениях между абонентами и абонентскими устройствами;

прослушивание телефонных переговоров;

оперативное наблюдение;

получение компьютерной информации;

другие оперативно-следственные мероприятия, содержание и последовательность которых определяются особенностями конкретной следственной ситуации.

2. Задержан сбытчик наркотических средств, установлены способ и следы совершенного преступления. Первоисточник наркотических средств, а также личности причастных к совершенному преступлению не известны.

Данная следственная ситуация является наиболее распространенной и в то же время наиболее сложной в связи с небольшим объемом имеющейся информации о преступлении.

Для проверки такой следственной ситуации может быть выдвинут целый ряд версий, среди которых основными можно назвать следующие:

преступление совершено лицами, страдающими наркоманией и проживающими на территории осуществления расследования;

преступление совершено лицами, заранее объединившимися для незаконного сбыта наркотических средств на территории Российской Федерации;

преступление совершено и организовано задержанным лицом единолично.

Учитывая двойственную природу способа совершения анализируемых преступлений, для проработки его информационной составляющей представляется перспективным выдвижение в рассматриваемой следственной ситуации версии, конкретизирующей способ незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, о виде торговой площадки, посредством которой он и был совершен.

Содержание такой версии будет определяться результатами проведения проверочных мероприятий. Например: незаконный сбыт наркотических средств совершен посредством коммуникационного сервиса Telegram.

В ходе осмотра изъятых аппаратных средств особое внимание уделяется установленному программному обеспечению. В ходе проверки такой версии необходимо иметь в виду, что подозреваемый мог опередить сотрудников правоохранительных органов и удалить анализируемую прикладную программу. В случае отсутствия ярлыка Telegram на рабочем столе, но наличии данных, указывающих на ее использование, следует подвергнуть осмотру системную папку «загрузки», а также приложения «AppStore», «Google Play» или аналогичные (в зависимости от функционирующей операционной системы), где будут отражены установленные на устройство в настоящем времени, а также ранее прикладные программы, что позволит зафиксировать факт их использования, войдя в аккаунт приложения. В случае невозможности самостоятельного входа в приложение под регистрационными данными владельца аккаунта этот вопрос может быть разрешен в ходе проведения судебной компьютерной экспертизы. Осмотр содержимого вкладки «конфиденциальность» позволит определить заданные условия анонимизации. Telegram автоматически синхронизирует контакты из адресной книги. Таким образом может быть установлен круг пользователей, с которыми возможно осуществление контактов посредством рассматриваемого программного обеспечения. Введя в строке поиска наименования установленных информационных каналов, можно ознакомиться с их содержимым, а также установить других подписчиков из списка контактов задержанного и следы активности владельца аккаунта. Сопоставление установленных таким образом сведений с адресной книгой, результатами допросов, полученной компьютерной информацией и результатами иных оперативно-следственных мероприятий, проводимых в рамках разрешения выдвинутой следственной версии, позволит установить как личность пользователей, стоящих за никами в Telegram, так и множество иных промежуточных фактов: особенности информационного контента по продаже наркотических средств, наименование используемых сетевых устройств, соединений и др., что будет способствовать установлению всех элементов преступной картины.

Успех разрешения такой следственной ситуации достигается грамотной координацией оперативно-тактических средств, следственных действий, компетенцией привлеченного к их проведению специалиста и результатами анализа полученных результатов.

3. Установлен факт функционирования сетевого информационного ресурса, посредством которого осуществляется незаконный сбыт наркотических средств.

Версии выдвигаются по поводу личности организаторов такого ресурса, масштабов их деятельности и будут сформулированы в зависимости от особенностей конкретной ситуации и содержания материалов проверки. Например, информационный ресурс функционирует на территории региона либо создателями сетевого информационного ресурса являются лица, ранее судимые за совершение аналогичных преступлений и проживающие в регионе его функционирования.

В данной следственной ситуации уже известен вид и порядок функционирования торговой площадки, посредством которой осуществляется незаконный сбыт наркотических средств. В связи с этим, помимо «традиционных» мероприятий первоначального этапа расследования (допросы, осмотры, экспертизы и т. п.), следователю надлежит двигаться в соответствии с алгоритмами функционирования торговой площадки.

Например, в случае незаконного сбыта наркотиков посредством интернет-сайта устанавливается оперативный контроль за сетью, производятся запросы на сервер, обслуживающий незаконный веб-ресурс, для установления пользователя хостингом[1], анализируются следы оплаты домена, по результатам чего могут быть сделаны запросы в финансовые организации для установления контактных данных клиента, запрашивается статистика обращений к веб-ресурсу, устанавливаются регистрационные данные выявленных IP-адресов. Целесообразно проведение проверочной закупки, компьютерной экспертизы сайта. В случае установления лиц, причастных к расследуемому преступлению, могут быть проведены допросы, очные ставки, обыски, осмотры, получение информации о соединениях между абонентами и иные следственные действия, а также оперативно-розыскные мероприятия по аналогии с первой следственной ситуацией.

Знание типичных следственных ситуаций и версий, умение следователя ориентироваться в них, анализировать и разрешать их позволяют наиболее полно и обоснованно определять дальнейшие

[1] Услуга по предоставлению ресурсов для размещения информации на сервере, постоянно имеющем доступ к сети (обычно Интернет). URL: https://ru.wikipedia.org/?curid =24706&oldid=120050112 (дата обращения: 15.02.2022).

направления расследования, намечать и продумывать систему первоначальных следственных действий и оперативно-розыскных мероприятий, тем самым преодолевать существующую информационную неопределенность, характерную для рассматриваемого этапа расследования[1].

Таким образом, определение оптимального момента для возбуждения уголовного дела и грамотные действия следователя в рамках имеющегося объема информации позволят наиболее эффективно организовать первоначальный этап расследования и реализовать все стоящие перед следователем на анализируемом этапе задачи. Для этого следователь должен в совершенстве владеть знаниями криминалистической характеристики и методики расследования анализируемых преступлений, следственной и судебной практики, норм законодательства, регулирующих информационно-телекоммуникационную сферу, основ работы в сети Интернет, особенностей и порядка функционирования телекоммуникационных технологий.

2.4. Использование специальных знаний на первоначальном этапе расследования преступлений, совершаемых посредством информационно-телекоммуникационных технологий

Быстрое и полное установление всех обстоятельств совершенного преступления, привлечение виновных к уголовной ответственности невозможны без слаженной и согласованной работы участников уголовного судопроизводства.

Расследование незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, а в особенности его первоначальный этап, проходят в условиях тесного взаимодействия с оперативными подразделениями.

Транснациональный характер используемой в преступном процессе сети Интернет и телекоммуникационных технологий обусловливает необходимость международного взаимодействия в части использования зарубежных информационно-телекоммуникационных ресурсов.

---

[1] См.: Мирошников В.В. Особенности первоначального этапа расследования незаконной миграции // Пробелы в российском законодательстве. 2010. № 3. С. 182.

Специфика предмета и способа совершения преступлений анализируемого вида состоит в том, что без знаний химии, физики, компьютерной техники, программирования, сетевых коммуникаций эффективное расследование рассматриваемого вида преступлений невозможно. В связи с этим особый интерес представляет взаимодействие следователя с лицом, обладающим такими знаниями.

С.И. Земцова[1] и Д.С. Кодиров[2] отмечают необходимость привлечения в ходе расследования преступлений, связанных с незаконным оборотом наркотиков, специалистов различных областей знаний: химика и взрывотехника (при осмотре нарколабораторий), агротехника и ботаника, специалиста в области информационных технологий (при производстве осмотра электронных носителей информации), а также специалистов из других областей специальных знаний: медицины, наркологии, педагогики, психологии, филологии, лингвистики, кинологии и т. д.

По мнению Р.С. Атаманова, специальные знания, используемые при расследовании преступлений, совершаемых с использованием сети Интернет, – это углубленные систематизированные знания в области высоких информационных технологий и компьютерной техники, доступные относительно узкому кругу профессионалов, а также практические навыки использования этих знаний, выработанные в процессе профессиональной деятельности[3].

В федеральном законодательстве имеется упоминание «специальных знаний»[4] как знаний в области науки, техники, искусства или ремесла.

---

[1] Земцова С.И. Участие специалиста в раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных и сильнодействующих веществ: автореф. дис. ... канд. юрид. наук. М., 2017. С. 11.

[2] Кодиров Д.С. Незаконный оборот наркотических средств: особенности методики расследования: по материалам Республики Таджикистан: автореф. дис. ... канд. юрид. наук. М., 2017. С. 11.

[3] Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. … канд. юрид. наук. М., 2012. С. 10.

[4] См.: О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31 мая 2001 г. № 73-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

Современными исследователями активно разрабатывается тематика «специальных знаний»[1]. Плюрализм мнений относительно формулировки рассматриваемого понятия позволяет выделить признаки специальных знаний, затрудняющие доктринальную разработку единого определения:

комплексный характер – в едином понятии обобщены знания о различных сферах жизни, что обусловливает их неоднородность;

отсутствие определенных границ, что затрудняет их разделение с иными видами знаний (например, с общедоступными);

субъективизм в оценке – отсутствие единых критериев, определяющих достаточность и глубину знаний их носителя.

Отдельные авторы называют такие знания «профессиональными»[2], однако уголовно-процессуальный закон не предъявляет требований к тому, чтобы специальные знания их носителя являлись предметом профессиональной деятельности[3].

Мы разделяем позицию В.В. Клевцова, который определяет анализируемое понятие как знания, навыки и умения, приобретенные путем специальной подготовки и профессионального опыта, используемые на основе современных достижений в соответствующей области науки, техники, искусства или ремесла, применяемые при раскрытии и расследовании преступлений в целях установления обстоятельств, подлежащих доказыванию, в случаях и порядке, определенных действующим законодательством[4].

Привлечение лиц, обладающих специальными знаниями, к расследованию преступлений рассматриваемой категории обусловлено как требованиями законодательства, регламентирующего уголовное судопроизводство, так и протеканием преступных процессов

---

[1] См.: Захохов З.Ю. Понятие и сущность специальных знаний в уголовном судопроизводстве // Пробелы в российском законодательстве. Юридический журнал. 2011. № 2. С. 208–211; Соколов А.Ф., Ремизов М.В. Использование специальных знаний в уголовном судопроизводстве: учеб. пособие. Ярославль: Изд-во Ярослав. гос. ун-та им. П.Г. Демидова, 2010. 128 с.

[2] См.: Захохов З.Ю. Указ. соч.

[3] См.: Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 174-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[4] См.: Клевцов В.В. Использование специальных знаний при расследовании преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ: автореф. дис. … канд. юрид. наук. Орел, 2010. С. 8

в телекоммуникационных системах, закрытых и недоступных к восприятию несведущим лицом.

В подтверждение сказанному Я.С. Карпов отмечает, что следственные и оперативные знания недостаточны для расследования преступлений о незаконном обороте наркотических средств. В связи с этим для определения направлений расследования, постановки вопросов эксперту, исследования особенностей функционирования информационно-телекоммуникационных систем и ресурсов, оценки доказательственной информации, полученной в ходе проведения следственных действий, требуется привлечение иных лиц, обладающих глубокими знаниями о них[1].

Специалист – лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном уголовно-процессуальным законом России, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию[2].

Основное требование, предъявляемое к специалисту, – наличие специальных знаний. Причем действующее законодательство не определяет их глубину и объем. Предполагается, что это должен сделать следователь, привлекающий к участию специалиста, с учетом стоящих перед ним задач.

Таким образом, в качестве специалиста могут быть привлечены любые лица, сведущие в нужной сфере, не заинтересованные в исходе дела.

В частности, в качестве специалиста может быть привлечен и эксперт[3].

Взаимодействие с экспертно-криминалистическими подразделениями может осуществляться как в процессуальной форме

---

[1] Карпов Я.С. Методика расследования незаконного оборота прекурсоров наркотиков на первоначальном этапе: автореф. дис. …канд. юрид. наук. М., 2018. 34 с.

[2] См.: Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 174-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[3] См.: О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 4 июля 2003 г. № 92-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

(участие эксперта в производстве следственных действий, проведение криминалистических экспертиз и т. п.), так и в непроцессуальной (консультационная деятельность, выполнение поручений технического характера и т. п.). Участие специалиста в рамках расследования преступлений протекает в тех же формах.

Для оказания содействия в расследовании незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий в большинстве случаев в качестве специалистов привлекаются сотрудники экспертных подразделений МВД. В ряде случаев для поиска необходимого специалиста прибегают к помощи оперативных сотрудников, которые, в свою очередь, привлекают их из числа гражданских лиц в соответствии с Федеральным законом «Об оперативно-розыскной деятельности»[1].

На любого специалиста, участвующего в уголовном процессе, распространяются общие требования, предусмотренные действующим законодательством.

Обладая специальными знаниями, эксперты способны внести неоценимый вклад в деятельность следователя по установлению истины при расследовании преступлений.

Практически все опрошенные следователи (99%) отмечают потребность в помощи специалиста в ходе расследования уголовных дел рассматриваемой категории.

Несмотря на то, что обязанность поиска и закрепления доказательств лежит на следователе, эффективность производства таких следственных действий, как осмотр места происшествия, обыск, выемка и др., проводимых при расследовании незаконного сбыта наркотических средств, во многом зависит от уровня знаний специалистов, вовлеченных в их проведение[2].

Таким образом, специфика информационно-телекоммуникационных технологий, используемых в процессе совершения преступления, физические свойства и обусловленные ими особенности работы с наркотическими средствами, изощренность и техно-

---

[1] См.: Об оперативно-розыскной деятельности: федер. закон от 12 авг.1995 г. № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] См.: Шаевич А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: автореф. дис. … канд. юрид. наук. Иркутск, 2007. С. 3–4.

логичность современных способов незаконного сбыта наркотических средств, а также высокая латентность анализируемых преступлений определяют необходимость и целесообразность создания на первоначальном этапе расследования рассматриваемых преступлений специализированных следственно-оперативных групп. При этом представляется обязательным:

включение в их состав специалиста, обладающего глубокими специальными криминалистическими знаниями в области информационно-телекоммуникационных технологий, для оказания квалифицированного содействия следователю, в производстве у которого находится уголовное дело с вещественными доказательствами, образованными в результате IT-инцидентов, произошедших в связи с совершением преступления;

назначение судебных экспертиз и интерпретации полученных результатов для обеспечения их доступности для всеобщего восприятия;

оказание консультативной помощи следователю в рамках своей компетенции в случае необходимости.

Помимо специальных знаний в области IT-технологий, специалисты должны иметь глубокую правовую подготовку, обеспечивающую наиболее полную и эффективную работу с вещественными доказательствами, образованными в результате IT-инцидентов, произошедших в ходе расследуемых преступлений, а также грамотное закрепление полученных доказательств.

Такие специалисты могут как находиться в штате следственных или экспертно-криминалистических подразделений ОВД, так и быть привлечены из других правоохранительных органов для расследования преступлений, связанных с использованием информационно-телекоммуникационных технологий.

Их подготовка возможна на базе образовательных организаций МВД России, обучающих по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, либо в других специализированных учебных заведениях.

Очевидно, что персональная ответственность за результаты предварительного расследования, следственных действий, качество и полноту собранных доказательств должна лежать на следователе. Специалист в рамках работы соответствующей следственно-оперативной группы должен заниматься подготовкой и

оказанием помощи в проведении следственных действий, связанных с использованием, проверкой и оценкой собранных вещественных доказательств в информационной составляющей расследуемого преступления.

По окончании первоначального этапа расследования, когда основной объем информации, позволяющей заподозрить конкретное лицо в совершении преступления, собран, проводятся совместное сопоставление, интерпретация, процессуальное оформление и оценка полученных в ходе такой работы доказательств. Разрешение всех возникающих на последующем и заключительном этапах вопросов и ходатайств возможно в рамках консультативной помощи.

Необходимость создания таких специализированных следственно-оперативных групп обусловлена существующими реалиями правоохранительной практики: активная информатизация и технологизация преступности обусловливают необходимость работы с новыми, неизвестными следователю объектами. Реальное количество компетентных лиц, способных решать задачи специалиста в рамках расследования рассматриваемых преступлений, крайне ограничено. Поэтому для проведения следственных действий, связанных с информационной составляющей преступления, за период расследования привлекается несколько специалистов одного направления. Очевидно, что данный факт негативно отражается на интерпретации полученных результатов и единстве восприятия информационной составляющей преступления.

Значительная часть опрошенных следователей (64%) отмечают, что высказанное нами предложение о создании соответствующих специализированных следственно-оперативных групп улучшит качество расследования преступлений рассматриваемой категории.

Ю.В. Гаврилин также описывает положительный практический опыт создания специализированных следственно-оперативных групп для расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий[1].

[1] Гаврилин Ю.В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Труды Академии управления МВД России. 2018. № 4(48). С. 145–150.

Таким образом, станет возможным обеспечить оперативность, качество и тщательность проработки IT-инцидентов, произошедших в связи с совершенным преступлением, что позволит наиболее глубоко, полно и максимально компетентно проработать технологическую составляющую анализируемых преступлений.

В свою очередь, экспертно-криминалистические подразделения составляют мощнейшую систему научно-технического обеспечения следствия и органов дознания[1].

По анализируемой категории уголовных дел проводятся физико-химические экспертизы – 100%, фоноскопические – 27%, судебные компьютерно-технические – 64%, иные (экспертизы документов, дактилоскопические, трасологические, материалов, веществ, изделий и др.) – 100%.

К их производству привлекаются как государственные, так и негосударственные экспертные учреждения.

Результаты проведенного исследования свидетельствуют о том, что физико-химические, а также некоторые традиционные криминалистические экспертизы были проведены по 100% дел. Данный факт обусловлен как организационными моментами, так и тем, что в ходе проведения следственных действий ключевым, но недостаточно традиционным объектам криминалистического исследования не было уделено необходимое внимание, как следствие, они не стали объектами экспертного исследования.

Решение этого вопроса возможно путем разработки и применения критериев оценки следовоспринимающих объектов.

Если следователь оценивает обнаруженный следовоспринимающий объект как потенциальное доказательство с точки зрения требований, предъявляемых уголовно-процессуальным законом (относимость, допустимость, достоверность и достаточность), то для специалиста основным критерием оценки такого объекта как потенциального для дальнейшей работы должна послужить его способность запечатлевать и отражать события совершенного преступления, описывая его сущность.

---

[1] См.: Кучерук С.А. Типовые ситуации организации взаимодействия и тактики в особо сложных условиях раскрытия и расследования преступлений: метод. рекомендации. Краснодар: Краснодар. акад. МВД России, 2005. С. 16.

Такая способность следовоспринимающих объектов может быть определена как *«криминалистическая емкость»*. То есть *способность объекта воспринимать, хранить и отражать объем информации о преступном деянии, в ходе совершения которого он был задействован, тем самым описывая совершенное преступление.*

Полагается, что на это свойство могут влиять как субъективные, так и объективные факторы.

Субъективные факторы: количественная составляющая (соотношение реально существующего и необходимого для исследования объемов), которая зависит от условий их фиксации и изъятия; существующие возможности исследования (что определяется современным технико-криминалистическим обеспечением, специальными знаниями и технологиями).

Объективные факторы: качественная составляющая (обусловленная характеристиками следобразующего и следовоспринимающего объектов) – способность объекта запечатлевать в себе следы конкретного вида; информационная составляющая (объем информации о преступном деянии, который следовоспринимающий объект способен запечатлеть).

Кроме того, криминалистическая емкость может быть как потенциальной, так и реальной. Говоря о потенциальной криминалистической емкости, мы рассматриваем способность объекта запечатлевать, хранить и отражать следы совершенного преступления в общем, соответственно его физическим свойствам. Знания об этих свойствах следовоспринимающих объектов могут быть почерпнуты из физики, химии, кибернетики и других наук.

Реальная криминалистическая емкость – объем используемой на практике информации, обусловленный качеством образования следа, обнаружения, фиксации, изъятия следовоспринимающих объектов, используемыми и существующими возможностями их исследования.

Значение потенциальной криминалистической емкости постоянно и представляет собой отражение уровня развития технологий, позволяющих изучать свойства объекта, а также глубины знаний человека о свойствах исследуемых объектов.

Реальная же криминалистическая емкость определяется особенностями совершения конкретного преступления, механизма

следообразования, компетентностью лиц, работающих с данными объектами.

Объективно оценить объект с точки зрения его «криминалистической емкости» специалист может непосредственно на месте в момент его обнаружения, принимая во внимание особенности совершенного преступления, руководствуясь личными знаниями и опытом.

Сопоставление потенциальной криминалистической емкости обнаруженного следовоспринимающего объекта с реальной позволяет объективно оценить его возможную информационную нагрузку.

На основании этого специалист может определить необходимость изъятия конкретного следовоспринимающего объекта, возможность, целесообразность и очередность проводимых исследований, а также прогнозировать содержание полученного в ходе их проведения результата. Параллельно следователь оценивает такие объекты с точки зрения их потенциальной относимости, допустимости, достоверности и достаточности, после чего принимается совместное обоснованное решение об их изъятии, и определяется порядок работы с ними.

Учитывая информационную составляющую способа совершения анализируемых преступлений, необходимо в ходе их расследования уделять особое внимание специфичным для такой категории преступлений следовоспринимающим объектам. Для этого целесообразно оценивать их с точки зрения «криминалистической емкости» с учетом воздействия на них элементов способа совершения конкретного преступления, которое они и отражают. В данном случае речь ведется об использовании информационно-телекоммуникационных технологий, что обусловит необходимость изъятия и исследования соответствующих объектов.

На основании результатов анализа уголовных дел рассматриваемой категории наглядно представим соотношение потенциальной криминалистической емкости основных следовоспринимающих объектов, связанных с использованием информационно-телекоммуникационных технологий, отраженной в вопросах, которые могут быть разрешены в ходе экспертного исследования, с реальной, отраженной в материалах экспертиз (табл. 4).

Таблица 4

Основные объекты экспертного исследования по уголовным делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, частота их исследования, разрешаемые в ходе экспертиз группы вопросов, отражающие потенциальную криминалистическую емкость исследуемых следовоспринимающих объектов, и их реальная криминалистическая емкость

Вид объекта	Частота исследования	Потенциальная криминалистическая емкость	Реальная криминалистическая емкость
Аппаратные средства (мобильный телефон, ноутбук, компьютер, периферийные устройства и комплектующие, сетевое оборудование, аксессуары и т. п.)	64%	Следы эксплуатации	100%
		Следы работы в сети Интернет	100%
		Следы и тип установленного программного обеспечения	100%
		Следы внесения изменений	60%
Программное обеспечение (системное, прикладное)	64%	Следы эксплуатации	100%
		Назначение	100%
		Следы отклонения от нормальных параметров функционирования	10%
		Следы использования приемов алгоритмизации и программирования	0%
		Следы использования для решения конкретных задач	90%
		Следы вредоносного ПО	10%
		Следы использования средств защиты	55%
		Следы внесения изменений	15%

Окончание таблицы

Вид объекта	Частота исследования	Потенциальная криминалистическая емкость	Реальная криминалистическая емкость
Информационные объекты (электронные документы, мультимедийные файлы, базы данных, приложения и т. п.)	64%	Следы форматирования	0%
		Следы монтажа	10%
		Следы, свойства и характеристики размещения данных	90%
		Содержимое данных	100%
		Следы использования средств защиты	40%
		Следы преодоления средств защиты	10%
		Следы изменения состояния данных	5%
		Следы решения определенных функциональных задач	85%
		Следы пользователя	100%
Компьютерные сети и их компоненты	0%	Следы функционирования	0%
		Следы работы в сети Интернет	0%
		Следы отклонения от заданных параметров функционирования	0%
		Количество и функционирование пользовательских режимов	0%
		Следы работы пользователя	0%
Компьютерные сети и их компоненты	0%	Следы и характеристики средств защиты и их преодоления	0%
		Следы подключения и использования оборудования	0%
		Следы решения конкретных задач	0%
		Следы внесения изменений	0%
		Следы и содержание установок удаленного доступа и протоколов подключений	0%

Как видно из приведенной таблицы, криминалистическая емкость специфичных для незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий следовоспринимающих объектов, связанных со способом и механизмом преступления, на практике используется не в полном объеме. То есть реальная криминалистическая емкость «традиционных» следовоспринимающих объектов значительно выше криминалистической емкости объектов, отображающих информационную составляющую анализируемого преступления.

С позиций криминалистики единственным путем, следуя которому можно воссоздать минувшее событие, является движение по следам, которые оно образует. Однако в ходе предварительного расследования нередко складывается ситуация, когда должное внимание ключевым следовоспринимающим объектам не уделено. Это может быть обусловлено невозможностью объективной оценки следовой информации, заключенной в объекте, в силу потенциальной формы ее существования[1].

Предложенный нами подход призван способствовать рациональному расходованию сил и средств, а также повышению эффективности раскрытия и расследования преступлений.

Таким образом, для повышения качества производства следственных действий и расследования преступлений в целом необходимо особое внимание уделить вопросам оптимизации и совершенствования использования специальных знаний на ключевом, первоначальном этапе расследования преступлений.

[1] См.: Поздеев И.А. Организация взаимодействия следователя со сведущими лицами в ходе расследования разрушений строительных объектов: автореф. дис. … канд. юрид. наук. Челябинск, 2011. 25 с.

2.5. Установление пространственно-временных характеристик незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий

Особенностью первоначального этапа расследования является его проблемно-ситуационный характер. Ограниченный объем информации о преступлении определяет многовариантность деятельности, осуществляемой в его рамках, что означает возможность проведения по одной и той же категории преступлений различных следственных действий, оперативных мероприятий, наличие различных их совокупностей.

Н.В. Олиндер объясняет пристальное внимание ученых-криминалистов к производству следственных действий первоначального этапа расследования тем, что именно в его рамках происходит накопление и закрепление основного объема доказательственной информации[1].

В связи с этим исследователи активно разрабатывают рекомендации по совершенствованию производства следственных действий с учетом особенностей определенных видов преступлений.

По делам, связанным с незаконным оборотом наркотических средств, достаточно полно и подробно описана тактика производства осмотра места происшествия, допросов, обыска, получения образцов для сравнительного исследования и других следственных действий[2]. Предложены методики работы с наркотическими средствами, объектами, связанными с ними, с лицами, совершающими их незаконный оборот, позволяющие наиболее полно установить и представить в форме доказательств события совершенного преступления.

---

[1] Олиндер Н.В. Следственные ситуации на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем // Юридический вестник СамГУ. 2015. Т. 1. № 4. С. 87.

[2] См.: Игнатенко Е.А. Методика расследования незаконной пересылки наркотических средств: дис. ... канд. юрид. наук. Благовещенск, 2015. 208 с.; Чернышенко Е.В. Расследование незаконного оборота наркотических средств и психотропных веществ в исправительных учреждениях ФСИН России: дисс. ... канд. юрид. наук. М., 2015. 235 с.; Земцова С.И. Указ. соч. и др.

Однако способы совершения преступлений в целом и незаконного сбыта наркотических средств в частности постоянно совершенствуются, что требует регулярного уточнения порядка производства и содержания следственных действий.

Глобальное внедрение в жизнь общества информационно-телекоммуникационных технологий побуждает ученых-криминалистов активно изучать особенности следственных действий по делам о преступлениях, совершенных с их использованием, на основании чего разрабатываются передовые тактические рекомендации[1].

В части расследования незаконного оборота психоактивных веществ, совершенного с использованием компьютерных технологий, О.А. Решняк подробно рассматривает тактику отдельных следственных действий первоначального этапа расследования, таких, как следственный осмотр, обыск, выемка, назначение экспертиз и др.[2]

Однако несмотря на достаточную разработанность вопросов, связанных с проведением следственных действий по делам о незаконном обороте наркотиков, в частности путем его сбыта, а также о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, в рекомендациях по проведению следственных действий на первоначальном этапе расследования анализируемых преступлений имеются значительные пробелы. Их существование обусловлено относительной обезличенностью пользователя информационно-телекоммуникационных технологий и сложностями его идентификации.

Вместе с тем эффективное решение идентификационных задач возможно путем установления и анализа пространственно-временных характеристик рассматриваемого вида преступлений – сведений о месте нахождения конкретного лица в определенный

---

[1] См.: Дусева Н.Ю. Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: дис. ... канд. юрид. наук. Волгоград, 2015. 193 с.; Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук. М., 2016. 29 с.; Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. … канд. юрид. наук. Ростов н/Д, 2017. 188 с.; Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук. М., 2018. 199 с.

[2] Решняк О.А. Указ. соч. С. 133–156.

отрезок времени в период использования им информационно-телекоммуникационных систем и технологий в преступных целях, о хронологической последовательности преступных действий, о местонахождении объектов, задействованных в криминальном процессе.

Криминалистическая теория пространственно-временных связей места, времени совершения преступления с личностью преступника не является новой. Еще в 90-х гг. XX столетия В.М. Мешков[1] говорил, что выявление взаимосвязей между двумя или более установленными пространственно-временными характеристиками преступного события позволит доказать их принадлежность к одной хронологической шкале либо к разным, а также обеспечит возможность установить тождество произошедших криминальных событий с личностью преступника. Именно установление этих связей и будет иметь первостепенное значение для доказывания.

Такие сведения, полученные в ходе проведения следственных действий, будут являться отражением связей информационной и материальной составляющих способа совершения преступления, также посредством этих сведений могут быть конкретизированы и доказаны масштабы расследуемой преступной деятельности, идентифицирована личность преступника, установлено его тождество с криминальными событиями.

Ровно половина опрошенных нами респондентов сообщила, что установление пространственно-временных характеристик определенных событий, произошедших в ходе незаконного сбыта наркотических средств анализируемым способом, будет иметь значение на первоначальном этапе расследования и позволит идентифицировать личность пользователя информационно-телекоммуникационных систем и установить иные обстоятельства совершенного преступления.

А.В. Шампаров по результатам проведенного исследования делает вывод, что на фоне стремительно снижающейся достоверности «традиционных» источников доказательств (показаний свидетелей, подозреваемого, обвиняемого и др.) судьи более склонны

[1] Мешков В.М. Основы криминалистической теории временных связей. М., 1994. 128 с.

доверять доказательствам, полученным посредством технических средств[1].

В связи с изложенным нами предприняты попытки внести уточнения в уже существующие рекомендации по производству отдельных следственных действий в ходе расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, направленных на установление пространственно-временных характеристик преступного события.

Использование в криминальном процессе технических устройств с функциями осуществления коммуникации абонентов при помощи каналов связи обусловило возможность проведения такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ).

Традиционно в следственной практике предметом рассматриваемого следственного действия является информация операторов мобильной связи[2].

Уголовно-процессуальный закон к таким сведениям относит: дату, время, данные о продолжительности соединений между абонентами или абонентскими устройствами, номерах абонентов, другие данные, позволяющие идентифицировать абонентов, а также сведения о номерах и месте расположения приемопередающих базовых станций.

В.Ю. Стельмах отмечает, что предметом анализируемого следственного действия является именно информация, существующая в установленной законом форме, а не сами устройства связи[3]. Таким образом, сведения о сетевой активности абонентов сети Интернет и телекоммуникационных технологий также могут являться его предметом, что обусловлено как их содержанием, так и общностью технического обеспечения, необходимого для производства рассматриваемого следственного действия.

---

[1] Шампаров А.В. Установление пространственно-временных характеристик механизма преступления: от теории к практике // Труды Академии управления МВД России. 2014. № 4(32). С. 122.

[2] См.: Вазюлин С.А., Васюков В.Ф. Получение информации о соединениях между абонентами: специфика процедуры // Уголовный процесс. 2014. № 1. С. 10–21.

[3] Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами // LesRussia. 2017. № 3(124). С. 142.

В случае использования IP-телефонии или мобильного Интернета информация будет представлена в виде телефонных номеров с указанием регистрационных данных владельца абонентского номера и сведений биллинговых служб. При использовании же иных видов интернет-соединений представленные сведения будут содержать информацию об используемых абонентами IP-адресах, данные об этих абонентах, о регионе, наименование провайдера, а также информацию о MAC-адресе используемого сетевого устройства.

Обычно такие сведения получают следственным путем в организации-провайдере по запросу либо путем проведения оперативно-розыскных мероприятий.

Однако так может быть получена лишь информация, находящаяся в ведении оператора связи. Транслируемая же в режиме онлайн охватывается понятием «тайна связи»[1].

Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» предусмотрено такое оперативно-розыскное мероприятие, как снятие информации с технических каналов связи, предметом которого и являются рассматриваемые сведения, в частности транслируемые онлайн. Однако очевидно, что в процессе расследования уголовного дела целесообразно получение информации о преступлении путем проведения следственных действий, в ходе которых формируются доказательства, а также для выявления и контроля новых инцидентов преступной деятельности или для раскрытия преступления следственным путем[2].

С.А. Вазюлин и В.Ф. Васюков отмечают возможность получения сведений об осуществляемых в режиме реального времени интернет-соединениях аналогичным образом[3].

Следует уточнить, что в рамках настоящего параграфа речь идет не столько о физической форме получения рассматриваемой информации, сколько о способе незамедлительного придания ей доказательственного статуса, т. е. о варианте кратчайшего

---

[1] См.: О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] См.: Цветков Ю.А. Раскрытие преступлений следственным путем // Уголовный процесс. 2015. № 10. С. 56–65.

[3] Вазюлин С.А., Васюков В.Ф. Указ. соч.

пути введения уголовно-релевантной информации в уголовный процесс.

Рассматриваемое следственное действие имеет сложную структуру и включает в себя подготовку, непосредственное получение требуемой информации и последующий осмотр полученных материалов, порядок и условия проведения которых описаны в законе[1].

Процесс получения такой информации (в рамках следственного действия) проводится оператором связи, в это время присутствие следователя не представляется целесообразным. Его основная работа состоит в подготовке анализируемого следственного действия, в том числе и в получении судебного решения, а также в придании доказательственной формы полученным результатам путем их осмотра и закрепления в соответствующем протоколе.

При расследовании уголовных дел о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий возможности анализируемого следственного действия будут определяться особенностями следственной ситуации первоначального этапа.

В случае задержания сбытчика (закладчика/наркокурьера) наркотических средств, когда основной объем информации о преступлении известен и задача следователя состоит в доказывании вины задержанного, основной целью производства такого следственного действия будет являться установление первоисточника наркотиков, а также лиц, связанных с их незаконным распространением.

Путем анализа протоколов допроса подозреваемого либо в ходе производства иных следственных действий или оперативных мероприятий следует установить оказывающего услуги доступа в сеть Интернет оператора связи, как мобильного, так и обслуживающего абонентов по месту жительства подозреваемого. Следует получать информацию о соединениях в двух этих точках. По адресу проживания может быть получена информация об интернет-трафике задержанного, которая может содержать сведения о сеан-

[1] См.: Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 177-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

сах интернет-связи с организаторами преступления, после чего вызвавшие подозрения данные абонентов сети должны быть взяты под контроль.

Информация оператора мобильного Интернета представляет особый интерес благодаря сведениям биллинговых служб, а в случае использования WI-FI соединений будет содержать IP-адреса, присвоенные пользователю. Их изучение может указать на оператора, обслуживающего данную сеть, у которого и могут быть получены сведения о личности абонента и др.

Такая информация свидетельствует о том, что в определенное время и в определенном месте абонент использовал связь (подключался к сети Интернет), а его личность может быть идентифицирована после сопоставления с другими доказательствами.

Например, использование полученных таким путем пространственно-временных характеристик места и времени нахождения задержанного наркосбытчика в результате должной аналитической работы может позволить установить «склад» наркотических средств (место хранения или местонахождение человека, хранящего их), что, очевидно, откроет достаточно масштабные перспективы как для следователя, так и для правоохранительной деятельности в целом.

В следственной ситуации, когда установлены основные члены преступной организации, осуществляющей незаконный сбыт наркотических средств, а также способ и следы, свидетельствующие об этом, роль полученной информации будет определяться особенностями доказывания сплоченности и функционирования преступной организации[1], а также возможностью установления еще неизвестных преступных связей.

В случае установления факта функционирования сетевого информационного ресурса, посредством которого осуществляется незаконный сбыт наркотических средств, может быть очерчен круг причастных к совершению рассматриваемых преступлений лиц, получены доказательства связи с незаконным сетевым информационным ресурсом, а также в совокупности с результатами

[1] См.: Белова Н.В. Доказывание организованного характера преступной группы на досудебных стадиях уголовного процесса: дис. ... канд. юрид. наук. Воронеж, 2002. 187 с.

иных следственных действий и оперативно-розыскных мероприятий идентифицирована личность наркосбытчиков.

Осмотр электронных носителей с полученной информацией предпочтительно проводить в специализированной криминалистической лаборатории в целях обеспечения сохранности и исключения возможности ее модификации. Обязательным участником такого осмотра является специалист. Также необходимо участие специалиста и в случае нахождения информации на бумажном носителе для ее расшифровки.

Особое значение будет иметь осмотр носителей информации совместно следователем и специалистом, это поможет обеспечить глубокий и всесторонний анализ полученной информации, а также возможность планирования дальнейших направлений расследования.

Представляется, что это наиболее оптимальный способ получения следственным путем онлайн-информации об абонентской активности лиц, связанных с незаконным сбытом наркотических средств анализируемым способом.

Также в ходе анализа полученных сведений могут быть определены круг лиц, причастных к преступлению, особенности реализации его способа, восполнены многие информационные пробелы имеющейся модели преступления. При необходимости могут быть даны поручения органу дознания, а возможно, и по каналам Интерпола об установлении личности владельцев IP-адресов либо телефонных номеров, об их отработке на причастность к совершенному преступлению. Кроме того, в случае установления личностей, причастных к преступлению, по информации баз данных, например ИБД «Регион» и т. п., могут быть получены более обширные сведения о них и составлена ориентировка.

В подтверждение этого О.А. Решняк отмечает, что полученная таким путем информация о пространственно-временных характеристиках расследуемого преступления помогает следователю в выдвижении следственных версий, в установлении круга общения подозреваемого, его местоположения, а также возможных соучастников преступления[1].

Кроме того, высокий тактико-криминалистический потенциал получения информации о соединениях между абонентами и

[1] Решняк О.А. Указ. соч. С. 152–153.

(или) абонентскими устройствами актуализирует возможность его разностороннего использования в целом ряде сфер, связанных с доказыванием[1].

Тем не менее, по мнению М.В. Старичкова[2], не стоит преувеличивать значение анализируемого следственного действия, так как информация, являющаяся отражением функционирования устройства связи, не индивидуализирует конкретного пользователя.

А.Ю. Шапошников отмечает, что для использования в доказывании полученной информации необходимо установить и доказать множество промежуточных фактов, например, что в тот или иной момент устройством пользовалось конкретное лицо и т. п., обозначая косвенное доказательственное значение полученных сведений[3].

Предполагается, что с помощью таких доказательств при условии должного внимания к ним и проверки, осуществляемой путем проведения иных следственных и оперативно-следственных мероприятий, может быть установлено максимальное количество лиц, причастных к совершению преступления, доказана вина задержанных, а также выявлены иные промежуточные факты.

Информационная составляющая способов совершения анализируемых преступлений определяет активный процесс коммуникации и, как следствие, существование такого криминалистического объекта, как электронные сообщения.

Н.А. Архипова электронными сообщениями называет любые сообщения, передаваемые посредством информационно-телекоммуникационных сетей, а также сообщения SMS, EMS, MMS, мессенджеров, электронной почты и др.[4], что особенно актуально для анализируемого вида преступлений.

---

[1] См.: Цыкора А.А. Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи: автореф. дис. … канд. юрид. наук. Ростов н/Д, 2013. С. 9.

[2] Старичков М.В. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия // Юристъ-правовед. 2018. № 4(87). С. 199–203.

[3] Шапошников А.Ю. Ходатайство о получении информации об абонентах должно быть обоснованным // Уголовный процесс. 2010. № 10. С. 43.

[4] Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. № 6. С. 132.

Причем такие сообщения в ходе проведения их осмотра стоит рассматривать с двух точек зрения:

как содержание, имеющее смысловую нагрузку (об источниках наркотических средств, о способах их производства, фасовки, хранения, об организации их распространения, о процессе коммуникативного взаимодействия участников преступной организации между собой, с покупателями и т. п.), т. е. как информацию, переданную или полученную пользователем информационно-телекоммуникационной сети;

как форму, отражающую обстановку (место, время, используемое программное и аппаратное обеспечение и т. п.) процесса коммуникации пользователей, т. е. как любые излучения, передачу или прием знаков, сигналов, звуков, изображений и т. п. по любой электромагнитной системе.

Информация, содержащаяся в электронных сообщениях, по мнению ученых, позволяет:

напрямую изобличить лицо в совершении преступления в случае, если преступный процесс был запечатлен на фото/видео, или в случае обнаружения прямо свидетельствующей о совершении преступления переписки;

косвенно указать на преступное поведение лица или на его причастность к совершенному преступлению;

способствовать установлению фактов и обстоятельств, имеющих значение для уголовного дела[1].

Тактика осмотра электронных сообщений подробно описана в более ранних работах[2].

---

[1] См.: Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 24.

[2] См.: Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи. С. 132–135; Она же. Организационно-тактические особенности получения и использования содержания текстовых сообщений в процессе раскрытия и расследования преступлений // Вестник Алтайского государственного университета. 2012. № 2-1(74). С. 71–73; Павлов В.В., Золотов М.А., Калентьева Т.А. Проблемы получения и фиксации информации, содержащейся на электронных устройствах лиц, задержанных по делам о незаконном обороте наркотических средств с использованием ресурсов сети Интернет // Вестник Волжского университета им. В.Н. Татищева. 2019. № 2, т. 1. С. 216–225 и др.

Фактическим основанием рассматриваемого следственного действия являются достаточные основания полагать, что информация, имеющая значение для уголовного дела, содержится в сообщениях, передаваемых по сетям электросвязи.

Юридическое основание осмотра электронных сообщений зависит от способа их получения: если речь ведется об электронных сообщениях, находящихся в ведении организатора распространения информации в сети Интернет[1] либо передаваемых по каналам связи в режиме онлайн, требуется получение судебного решения. В то же время на осмотр сообщений, оказавшихся в распоряжении следователя путем производства их выемки (вне следственного действия осмотр и выемка электронных сообщений) либо в ходе удовлетворения ходатайства об их приобщении к уголовному делу, т. е. по инициативе или с ведома их владельца, судебное решение не требуется. Тем не менее в случае исходящей от участников предварительного расследования инициативы приобщения электронных сообщений к уголовному делу представляется целесообразным провести их осмотр с участием предоставившего их лица. Его инициатива предоставить осматриваемые сообщения и согласие на их осмотр следователем должны быть зафиксированы в протоколе следственного действия и заверены его подписью.

Н.А. Архипова предлагает производить на месте «поверхностный» осмотр электронных сообщений, а детальный – после их выемки, проведенной путем копирования на электронный носитель[2].

Однако учитывая способность компьютерной информации легко модифицироваться, в частности в ходе копирования на электронный носитель, вряд ли это предложение можно назвать обоснованным. Так, целесообразно проводить детальный осмотр таких сообщений на месте.

В подтверждение этого Ю.В. Гаврилин и А.А. Балашова говорят о необходимости изъятия такой информации посредством

[1] См.: О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 6 июля 2016 г. № 374-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

[2] Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. № 6. С. 132–135.

копирования на электронный носитель, однако после ее детального осмотра с участием специалиста на месте[1].

Кроме того, нельзя исключать ситуацию, когда такие сообщения, хранящиеся в памяти устройства связи, удалены. Если имеются достаточные основания полагать, что такие сообщения наличествуют, то в случае их фактического отсутствия нельзя обойтись без помощи соответствующего специалиста или даже судебной компьютерно-технической экспертизы. Удаление сообщений может быть произведено разными способами. В случае использования системной команды «удалить» это действие можно назвать условным, поскольку оно заключается лишь во внесении соответствующей метки в файловой системе электронного носителя информации. Такое сообщение может быть легко восстановлено.

Если же удаление было проведено с использованием специальных программ (Например, AngryUser и др.) или систем уничтожения информации (например, Раскат, Универсал, Импульс-7У, Импульс-кейс и др.), электронные сообщения, как и их носители, восстановлению не подлежат.

В этом случае необходимо зафиксировать в протоколе осмотра наличие таких программ (аппаратных систем) или допросить специалиста, зафиксировавшего факт их использования. Все это будет свидетельствовать о возможном существовании электронных сообщений, по мнению следователя, имеющих значение для расследования уголовного дела.

По делам о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий, помимо той части электронных сообщений, которая раскрывает содержание преступных действий, особый интерес представляет среда их нахождения (приложения, мессенджеры, чаты, блоги, социальные сети и т. п.), а также метаданные сообщений (дата, время, расширение, используемое для их создания программное обеспечение, информация об учетных записях пользователей, которые их создали, и др.), раскрывающие пространственно-временные характеристики совершенного преступления.

---

[1] См.: Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1(13). С. 134.

Все эти сведения будут иметь значение как в доказывании, так и в проведении аналитической работы, направленной на идентификацию пользователей телекоммуникационных устройств связи.

Типичным для расследования уголовных дел о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий является осмотр средств мобильной связи, который был проведен в 100% изученных уголовных дел.

В связи с повсеместным использованием мобильных телефонов тактика их осмотра описана многими исследователями[1].

Применительно к расследованию уголовных дел о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий такое следственное действие имеет особую актуальность в связи с его неотложностью. То есть с возможностью его проведения в случаях, не терпящих отлагательств, до возбуждения уголовного дела.

Кроме того, в соответствии с разъяснениями Конституционного Суда Российской Федерации проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения специального судебного решения[2].

---

[1] См.: Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной мобильной связи: дис. ... канд. юрид. наук. М., 2009. 252 с.; Шебалин А.В. Расследование хищений средств сотовой связи: дис. ... канд. юрид. наук. Барнаул, 2009. 224 с.; Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. ... канд. юрид. наук. СПб., 2011. 26 с.; Бутенко О.С. Криминалистические и процессуальные аспекты осмотра мобильных телефонов в рамках предварительного следствия // Lex Russia. 2016. № 4(113). 49–60; Грибунов О.П. Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4(83). С. 137–142 и др.

[2] См.: Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 25 янв. 2018 г. № 189-О. URL: http://doc.ksrf.ru/decision/KSRFDecision314926.pdf (дата обращения: 19.03.2020).

Типовые способы совершения рассматриваемых преступлений предусматривают отправку лицом, стоящим во главе организации, занимающейся незаконным сбытом наркотических средств, геометки места хранения расфасованной партии наркотиков в адрес закладчика посредством используемого мессенджера. Закладчик, осуществив «закладку», отправляет в ответ геометку, согласно которой конечный потребитель их может забрать.

Таким образом, в ходе осмотра используемого в преступном процессе мобильного телефона особое значение будет иметь осмотр приложений с функциями навигации, посредством которого могут быть установлены пространственно-временные характеристики совершенного преступления.

На сегодняшний день популярны такие прикладные программы, как «Яндекс-карты», «Яндекс-навигатор», «Google maps», «Навител-навигатор», «Maps.me», «2gis» и др.

Ю.В. Гаврилин отмечает, что в анализируемом преступном процессе они являются основными для обнаружения мест «закладок»[1].

Как правило, такие программные продукты могут использоваться любыми операционными системами по единому принципу функционирования. Обычно доступ к таким приложениям, а также к сохраненной истории поисков возможен как онлайн, так и офлайн. Навигационные возможности, а также точность координат обеспечиваются подключением к сервисам GPS, встроенным в современных гаджетах, установленным соединением WI-FI либо подключением к вышке сотовой связи.

Эти приложения прокладывают пешеходные, автомобильные и маршруты общественного транспорта от одной точки к другой; содержат сведения о расположении различных объектов, их ландшафтных особенностях, организациях, расположенных в них, и т. п. А также сохраняют данные обо всех посещениях в истории и входят в комплекс средств получения криминалистически значимой пространственно-временной информации о преступлении.

[1] См.: Гаврилин Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях. С. 44.

Такие сведения занимают одно из центральных мест в массиве криминалистически значимой информации[1].

Проведенный анализ следственной практики случаев получения такого рода сведений в ходе осмотра мобильного телефона, а также в рамках проведения криминалистических экспертиз не выявил.

Нам же представляются обязательными документирование и исследование таких криминалистически значимых сведений. Причем эти действия должны выполняться незамедлительно. Оптимальным процессуальным способом получения информации из навигационных прикладных программ является осмотр изъятого мобильного телефона как неотложное следственное действие.

Далее, исходя из способа подключения, могут быть запрошены сведения о геолокациях пользователя за ранние периоды. Обязательным участником такого осмотра должен являться специалист для решения вопросов получения доступа к прикладным программам, установления вида используемого навигационного приложения (путем изучения открытых вкладок смартфона, геометок, отправленных его владельцу в мессенджерах), просмотра истории его работы (точки, поиски, маршруты и т. п.), а также для установления способа подключения прикладной навигационной программы к сервису GPS и сетевых реквизитов, присвоенных используемому устройству.

В ходе допроса должен быть установлен срок осуществления противоправной деятельности в качестве закладчика. Анализируемый период должен охватывать все время преступной деятельности, а также несколько недель до ее начала. Изучение «допреступного» периода позволит определить типичные локации и маршруты передвижения пользователя, отклонения от которых в период осуществления преступной деятельности могут указывать на места получения наркотических средств или производства закладок.

Кроме того, представляет особый интерес проведение экспертного исследования навигационных программ, сервисов и их аппаратного обеспечения в рамках производства судебной компьютерно-технической экспертизы. В изученной нами следственно-

[1] См.: Дусева Н.Ю. Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: автореф. дис. ... канд. юрид. наук. Волгоград, 2015. С. 3.

судебной практике сведения о проведении таких экспертиз отсутствуют. Объектами рассматриваемой экспертизы могут явиться средства компьютерной техники, обеспечивающие функционирование рассматриваемых программ, а также сами программы, утилиты и сервисы, являющиеся носителями пространственно-временных характеристик совершенного преступления. Таким образом могут быть разрешены задачи поиска, сбора и исследования сведений об особенностях их функционирования в преступном процессе. В частности, восстановлена удаленная история запросов, история заданных маршрутов и геоточек, выделены часто используемые, а также разрешены некоторые идентификационные вопросы.

Путем проведения вышеописанных следственных действий могут быть установлены пространственно-временные характеристики совершенного преступления.

Ученые, исследующие вопросы идентификации пользователя[1], отмечают, что идентификация 95% людей возможна по 4 пространственно-временным точкам. По 2 точкам можно идентифицировать половину пользователей, а по 11 точкам 100%.

В ходе вышеописанных следственных действий может быть установлен значительный объем информации о преступлении. Установленные пространственно-временные характеристики преступления будут иметь особое значение в идентификации преступника и лиц, причастных к криминальному деянию. Подробным изучением этих вопросов занимается новая отрасль науки – аналитическая разведка.

[1] См.: Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen, Vincent D. Blondel Unique in the Crowd: The privacy bounds of human mobility . URL: https://www.nature.com/articles/srep01376 (дата обращения: 17.03.2020).

Заключение

По результатам изучения проблемы незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, а также практики противодействия ему, следует сделать ряд выводов и предложений.

1. Незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий представляет собой совокупность действий в реальном (физическом) пространстве и транзакций, направленных на совершение множественных фактов рассматриваемого деяния, чем и определена двойственность его содержания (материальная и информационная составляющие).

2. Среди современных информационно-телекоммуникационных технологий для незаконного сбыта наркотических средств наиболее удобным представляется использование информационных технологий (push-уведомлений в качестве дополнительной опции в браузерах, приложениях, мессенджерах и т. п. специально разработанных приложений), а также телекоммуникационных технологий (сетей малого радиуса действия, сетей близкоконтактного взаимодействия, микроконтроллерных аппаратных средств), что обусловлено сложностями в осуществлении уполномоченными органами контроля за их функционированием.

3. В основе работы информационно-телекоммуникационных систем и технологий лежат строгие алгоритмы, обусловливающие их технологическую составляющую.

4. Криминалистическая характеристика незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий – это абстрактная модель, разработанная в результате изучения процессов функционирования информационно-телекоммуникационном технологий и систем, в которой обобщены типичные сведения об основных элементах незаконного сбыта наркотических средств, а также об особенностях сбыта наркотических средств, совершаемого с их использованием.

5. Состав и сущность криминалистической характеристики преступления обусловлены его двуединой природой (материальной и информационной). Помимо элементов, характеризующих

материальную составляющую криминалистической характеристики (место, время, предмет преступного посягательства, способ совершения преступления, формируемые им следы и др.), она включает в себя информационные элементы, существование которых определено технологической сущностью используемых при совершении преступлений автоматизированных информационных систем. Строгие алгоритмы функционирования элементов автоматизированных систем предопределяют возможность выявления жестких взаимосвязей между всеми элементами криминалистической характеристики.

6. Типичные способы незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий представляют собой совокупность действий в физическом пространстве и транзакций, осуществляемых асинхронно друг с другом. Их структура связана не временной (подготовка, совершение, сокрытие), а логической последовательностью действий. То есть мероприятия, направленные на достижение преступного результата, выполняются по мере их необходимости. Достижение положительного результата одного из них не влечет за собой реализацию следующего конкретного мероприятия, а определяет необходимость проведения целого ряда других, зачастую разнородных, но связанных с предшествующими аналогичным преступным умыслом и обусловленных заданными алгоритмами функционирования информационно-телекоммуникационных систем, технологий и ресурсов.

Действия, входящие в состав способа совершения преступления и связанные с использованием информационно-телекоммуникационных технологий, определяют содержание его информационной составляющей.

7. Используемые при совершении преступлений рассматриваемого вида информационно-телекоммуникационные системы и технологии определяются формой организации торговых площадок, посредством которых осуществляется незаконный сбыт наркотиков: Даркнет; стандартные интернет-соединения; с использованием ранее обозначенных, еще не используемых для незаконного сбыта наркотических средств, но перспективных для достижения анализируемых преступных целей информационно-телекоммуникационных технологий.

8. Незаконный сбыт наркотических средств, совершенный рассматриваемым способом, формирует следовую картину, включающую все известные современной криминалистике виды следов: материальные, идеальные и «виртуальные». Если место нахождения и механизм следообразования «традиционных» (материальных и идеальных) следов преступления будут определены содержанием способа изготовления и перемещения наркотических средств, то место нахождения и механизм следообразования «виртуальных» определит порядок функционирования торговых площадок по продаже наркотических средств. Последовательность обнаружения следов заключена в алгоритмах функционирования используемых информационно-телекоммуникационных технологий и систем.

9. Анализируемые преступления носят групповой характер и классифицируются в зависимости от уровня организации преступных групп. «Высокоорганизованные» преступные группы характеризуются распределением ролей, включающих «организаторов», «изготовителей», «закладчиков» и некоторых других в зависимости от их преступной роли и содержания осуществляемой незаконной деятельности.

В преступных группах более низкого уровня организации возможно четкое выделение лишь роли «организатора», преступные обязанности иных участников разнообразны и определены недостаточно ясно. Реализация противоправных функций в совершении рассматриваемых преступлений в условиях строгой алгоритмизации функционирования информационно-телекоммуникационных систем становится возможной за счет знаний, умений и навыков, требуемых для их использования. Это детерминирует связь сведений о личности типичного преступника со следами и способом совершенного преступления. Чем обширнее навыки, знания и умения преступника, тем более высокотехнологичный способ совершения преступления им будет выбран, тем затруднительнее окажется процесс обнаружения и фиксации следов преступления. Также выявлены связи между возрастом преступника и способом совершения преступления, между возрастом преступника и его криминальной ролью. В совершении незаконного сбыта наркотических средств анализируемым способом выделена пре-

ступная роль лиц, не связанных общим умыслом с наркосбытчиками, но косвенно обеспечивающих возможность совершения незаконного сбыта наркотических средств рассматриваемым способом. Это, в первую очередь, создатели и организаторы виртуальных торговых площадок, используемых преступниками для незаконного сбыта наркотических веществ.

10. В понятие первоначальной криминалистически значимой информации об анализируемых преступлениях следует включать сведения о пользователях информационно-телекоммуникационных технологий и систем, а также об их сетевой активности, связанной с реализацией наркотических средств. Такие признаки могут как прямо свидетельствовать о совершении рассматриваемого преступления (содержательная часть сообщений в мессенджерах, чатах, социальных сетях; информационный контент веб-сайтов, личных аккаунтов; push-уведомления; баннерная реклама в сети Интернет и т. п.), так и косвенно (регистрация и регулярное осуществление финансовых операций по электронным счетам, кошелькам, платежным системам; нетипичные перемещения пользователя, отраженные в данных программ геолокации и позиционирования; использование программ-ботов; попытки анонимизации сетевой активности; использование мессенджеров с функциями шифрования сообщений; нецелевое использование нетипичного или специального программного и аппаратного обеспечения (в контексте вышеупомянутых перспективных для реализации рассматриваемой преступной деятельности телекоммуникационных технологий) и т. п.). Признаки второй группы имеют криминалистическое значение лишь в совокупности с признаками первой, позволяя конкретизировать анализируемую преступную деятельность, определить ее масштабы и круг участвующих лиц.

11. Источники и методы получения первоначальной криминалистически значимой информации о незаконном сбыте наркотических средств с использованием информационно-телекоммуникационных технологий разнообразны. И носят как оперативно-розыскную, так и процессуальную природу. Оптимальным способом получения первоначальной криминалистически значимой информации об анализируемых преступлениях является автоматизированный анализ больших данных, аккумулируемых в соответствии

с действующим законодательством Российской Федерации операторами связи. Такой анализ осуществляется с использованием специального программного обеспечения, функционирующего на основе технологий искусственного интеллекта, согласно заданным критериям, отраженным в признаках, указывающих на осуществление незаконного сбыта наркотических средств анализируемым способом. Такие признаки должны быть почерпнуты из современных знаний криминалистической характеристики об анализируемом виде преступлений и охватывать как содержательную часть информационных массивов, так и метаданные.

12. Для предварительной проверки первоначальной информации об анализируемом преступлении типичны следующие проверочные ситуации:

1) незаконный сбыт наркотических средств с использованием информационно-телекоммуникационных технологий совершен в очевидных условиях – 27%; в этом случае речь идет о деятельности организованных преступных групп, установлены все или основные звенья преступной цепи;

2) незаконный сбыт наркотических средств анализируемым способом совершен в условиях неочевидности – 73% (термин «неочевидность» применен условно); эта проверочная ситуация может иметь следующие типичные вариации:

задержан «закладчик», не располагающий сведениями ни о первоисточнике наркотических средств, ни о лицах, связанных с ними, и т. п.;

в правоохранительные органы поступила информация о функционировании сетевого ресурса, посредством которого осуществляется незаконный сбыт наркотических средств.

13. Двойственная (материальная и информационная) природа способов совершения преступлений, связанных с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных систем, требует применения различных методик проведения предварительной проверки первоначальной информации о них. Специфика информационной составляющей способа совершения преступления определяет особый подход к работе с первоначальной криминалистически значимой информацией, подлежащей проверке: порядок деятельности по установлению признаков преступления отражен в алгоритмах

функционирования используемых в преступных целях информационно-телекоммуникационных систем и технологий, особенности которых могут быть установлены на основе специфики торговой площадки, посредством которой осуществлялся сбыт наркотиков. Содержание проверочных мероприятий практически полностью определяется алгоритмами, обеспечивающими функционирование электронных торговых площадок, посредством которых осуществляется незаконный сбыт наркотических средств.

14. Поводами к возбуждению уголовных дел о незаконном сбыте наркотических средств рассматриваемым способом являются:

заявление о преступлении – 13%;

явка с повинной – 0%;

сообщение о преступлении, полученное из иных источников – 87%;

постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании – 0%.

15. Специфика анализируемых преступлений в части определения оптимального момента возбуждения уголовных дел состоит в том, что, помимо общих обстоятельств (указывающих на признаки состава преступления – объект, субъект, объективная сторона, субъективная сторона), на момент принятия решения о возбуждении уголовного дела должен быть установлен ряд важных фактов (признаков), связанных с информационной составляющей способа преступления:

форма организации электронной торговой площадки, используемой для сбыта наркотических средств;

факт использования, характеристики и роль в преступном процессе программного обеспечения и телекоммуникационных технологий, а также обстоятельства их функционирования;

содержание сопровождающего контента;

факт использования способов и средств анонимизации преступной деятельности и их особенности;

объем и особенности рекламы контента электронной торговой площадки, отражающей масштабы преступной деятельности и круг причастных и заинтересованных лиц;

особенности ведения преступной финансовой деятельности.

Перечисленные признаки не являются исчерпывающими и могут быть дополнены, однако, это основные признаки, характеризующие информационную составляющую преступления.

16. В зависимости от эффективности преодоления информационных пробелов предварительной проверки сообщений об анализируемых преступлениях формируются следующие типичные следственные ситуации и версии первоначального этапа расследования:

Задержан сбытчик наркотических средств, в момент либо после совершения преступления, установлен его способ, выявлены следы, а также сведения, позволяющие установить личность иных лиц, причастных к его совершению.

Задержан сбытчик наркотических средств, установлены способ и следы совершенного преступления. Первоисточник наркотических средств, а также личности иных лиц, причастных к совершенному преступлению, не известны. Для проверки такой следственной ситуации могут быть выдвинуты следующие версии:

преступление совершено лицами, страдающими наркоманией и проживающими на территории осуществления расследования;

преступление совершено лицами, заранее объединившимися для незаконного сбыта наркотических средств на территории Российской Федерации;

преступление совершено и организовано задержанным лицом единолично.

Учитывая двойственную природу способа преступлений, для проработки его информационной составляющей перспективно выдвижение в рассматриваемой следственной ситуации версии, конкретизирующей способ незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий, о наименовании торговой площадки, посредством которой он и был совершен.

Содержание такой версии будет определяться результатами проведения проверочных мероприятий. Также будет установлен факт функционирования сетевого информационного ресурса, посредством которого осуществляется незаконный сбыт наркотических средств.

Версии выдвигаются по поводу личности организаторов такого ресурса, масштабов их деятельности и формулируются в зависимости от особенностей конкретной ситуации и содержания материалов про-

верки. Например, информационный ресурс функционирует на территории региона или создателями сетевого информационного ресурса являются лица, ранее судимые за совершение аналогичных преступлений и проживающие в регионе его функционирования.

17. Внесено предложение о создании на первоначальном этапе расследования рассматриваемых преступлений специализированных следственно-оперативных групп. В их состав представляется обязательным включить специалиста, обладающего как специальными криминалистическими знаниями в области информационно-телекоммуникационных технологий, так и правовой подготовкой.

В рамках специализированной следственно-оперативной группы специалист должен оказывать квалифицированное содействие следователю в расследовании уголовного дела в части работы с вещественными доказательствами, образованными в результате IT-инцидентов, произошедших в связи с совершением преступления. Кроме того, специалист необходим для назначения судебных экспертиз и интерпретации полученных результатов, обеспечения их доступности для восприятия широким кругом лиц, оказания консультативной помощи следователю в рамках своей компетенции. По окончании первоначального этапа расследования, когда основной объем информации, позволяющей заподозрить конкретное лицо в совершении преступления, собран, проводятся совместное сопоставление, интерпретация, процессуальное оформление и оценка полученных в ходе такой работы доказательств. Разрешение всех возникающих на последующем и заключительном этапах вопросов и ходатайств возможно в рамках консультативной помощи.

18. Даны рекомендации по оптимизации совместной деятельности следователя и специалиста на первоначальном этапе расследования рассматриваемых преступлений, в рамках которых им предложено в пределах своей компетенции оценивать следовоспринимающие объекты, подлежащие изъятию, с точки зрения их относимости, допустимости, достоверности, достаточности и криминалистической емкости, т. е. способности объекта воспринимать, хранить и отражать объем информации о преступном деянии, в ходе совершения которого он был задействован.

19. Несмотря на достаточную разработанность вопросов, связанных с проведением следственных действий по делам о незаконном сбыте наркотиков, а также о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, в рекомендациях по их производству имеются значительные пробелы, в частности обусловленные затруднениями в идентификации личности пользователей информационно-телекоммуникационных технологий. Их устранение представляется возможным путем установления пространственно-временных характеристик совершенного преступления в ходе специфических следственных действий, таких как получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ), следственные осмотры (электронных сообщений, средств мобильной связи использующих навигационные программы), назначения компьютерной экспертизы. Для этого сформированы соответствующие рекомендации по их проведению.

Литература

Нормативные правовые акты, официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г. Доступ из справ. правовой системы «КонсультантПлюс».

2. Бангкокская декларация «Партнерство во имя будущего» (Бангкок, 21 окт. 2003 г.) // Дипломатический вестник. 2003. № 11.

3. Конвенция о преступности в сфере компьютерной информации ETS No. 185 (Будапешт, 23 нояб. 2001 г.). Доступ из справ. правовой системы «КонсультантПлюс».

4. Единая конвенция о наркотических средствах 1961 года с поправками, внесенными в нее в соответствии с Протоколом 1972 года о поправках к Единой конвенции о наркотических средствах 1961 года. Доступ из справ. правовой системы «КонсультантПлюс».

5. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (заключена в г. Вене 20 дек. 1988 г.). Доступ из справ.правовой системы «КонсультантПлюс».

6. Окинавская хартия глобального информационного сообщества (о. Окинава, 22 июля 2000 г.) // Дипломатический вестник. 2000. № 8. С. 51–56.

7. Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

8. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 дек. 2001 г. № 177-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

9. Кодекс Российской Федерации об административных правонарушениях: федер. закон от 30 дек. 2001 г. № 195-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

10. Гражданский кодекс Российской Федерации от 18 дек. 2006 г. № 230-ФЗ. Ч. 4. Доступ из справ. правовой системы «КонсультантПлюс».

11. Об оперативно-розыскной деятельности: федер. закон от 12 авг. 1995 г. № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

12. О наркотических средствах и психотропных веществах: федер. закон от 8 янв. 1998 г. № 3-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

13. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31 мая 2001 г. № 73-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

14. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 4 июля 2003 г. № 92-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

15. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

16. Об информации, информационных технологиях и о защите информации: федер. закон от 20 июля 2006 г. № 149-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

17. О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

18. О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон от 29 дек. 2010 г. № 436-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

19. О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации: федер. закон от 28 июля 2012 г. № 139-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

20. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей: федер. закон от 5 мая 2014 г. № 97-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

21. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер

противодействия терроризму и обеспечения общественной безопасности: федер. закон от 6 июля 2016 г. № 374-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

22. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

23. О некоторых вопросах информационной безопасности Российской Федерации: указ Президента РФ от 22 мая 2015 г. № 260. Доступ из справ. правовой системы «КонсультантПлюс».

24. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 дек. 2016 г. № 646. Доступ из справ. правовой системы «КонсультантПлюс».

25. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справ. правовой системы «КонсультантПлюс».

26. О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 окт. 2019 г. № 490. Доступ из справ. правовой системы «КонсультантПлюс».

27. О стратегии национальной безопасности Российской Федерации: указ Президента РФ от 2 июля 2021 г. № 400. Доступ из справ. правовой системы «КонсультантПлюс».

28. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утв. Президентом РФ 12 дек. 2014 г. № К 1274) // Официальный сайт Совета Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/131.html. (дата обращения: 02.07.2017).

29. Концепция государственной политики по контролю за наркотиками в Российской Федерации: постановление Верховного Совета РФ от 22 июля 1993 г. № 5494-1. Доступ из справ. правовой системы «КонсультантПлюс».

30. Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации: постановление Правительства РФ от 30 июня

1998 г. № 681. Доступ из справ. правовой системы «КонсультантПлюс».

31. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление Правительства РФ от 27 авг. 2005 г. № 538. Доступ из справ. правовой системы «КонсультантПлюс».

32. О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено»: постановление Правительства РФ от 26 окт. 2012 г. № 1101. Доступ из справ. правовой системы «КонсультантПлюс».

33. Об утверждении правил оказания услуг по передаче данных: постановление Правительства РФ от 23 февр. 2006 г. № 32. Доступ из справ. правовой системы «КонсультантПлюс».

34. Об утверждении «Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации»: постановление Правительства РФ от 31 июля 2014 г. № 743. Доступ из справ. правовой системы «КонсультантПлюс».

35. Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: утв. постановлением Правительства РФ от 16 марта 2009 г. № 228. Доступ из справ. правовой системы «КонсультантПлюс».

36. Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет»: приказ ФСБ России от 19 июля 2016 г. № 432. Доступ из справ. правовой системы «КонсультантПлюс».

37. Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет»: приказ ФСО России от 7 сент. 2016 г. № 443. Доступ из справ. правовой системы «КонсультантПлюс».

38. Об утверждении Инструкции о порядке приема, регистрации и разрешении в территориальных органов Министерства внутренних дел Российской Федерации заявлений и сообщений о преступления, об административных правонарушениях: приказ МВД России от 29 авг. 2014 г. № 736. Доступ из справ. правовой системы «КонсультантПлюс».

39. Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий: приказ Минкомсвязи России от 16 апр. 2014 г. № 83. Доступ из справ. правовой системы «КонсультантПлюс».

40. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 окт. 2006 г. Доступ из справ. правовой системы «КонсультантПлюс».

41. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ от 15 июня 2006 г. № 14. Доступ из справ. правовой системы «КонсультантПлюс».

42. Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ: утв. Президиумом Верховного Суда РФ 27 июня 2012 г. Доступ из справ. правовой системы «КонсультантПлюс».

43. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 25 янв. 2018 г. № 189-О. URL:

http://doc.ksrf.ru/decision/KSRFDecision314926.pdf (дата обращения 19.03.2020).

Учебная и научная литература

1. Аверьянова Т.В. и др. Криминалистика: учеб. под ред. А.И. Бастрыкина. М.: Экзамен, 2014. 511 с.

2. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. 3-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2012. 990 с.

3. Аносов А.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, телекоммуникационных и высоких технологий: учеб. пособие: в 2 ч. М.: Акад. управления МВД России, 2019. 208 с.

4. Антонян Ю.М., Кудрявцев В.Н., Эминов В.Е. Личность преступника. СПб.: Юридический Центр пресс, 2004. 366 с.

5. Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2001. 288 с.

6. Бастрыкин А.И. Расследование преступлений повышенной общественной опасности (криминалистические аспекты): практ. пособие. М.: Известия, 2010. 160 с.

7. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: НОРМА, 2001. 240 с.

8. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике. М.: Юрид. лит., 1988. 456 с.

9. Белкин Р.С. Криминалистическая энциклопедия. 2-е изд. доп. М.: Мегатрон XXI, 2000. 333 с.

10. Белкин Р.С. Курс криминалистики: учеб. пособие. М.: ЮНИТИ-ДАНА: Закон и право, 2001. 867 с.

11. Белкин Р.С. Курс советской криминалистики. М.: Акад. МВД СССР, 1979. Т. 3. 407 с.

12. Булыжкин А.В., Бадиков Д.А. Некоторые особенности расследования преступлений, связанных с незаконным оборотом наркотических средств с использованием информационно-телекоммуникационных систем «Интернет»: практ. рекомендации. Орел: Орлов. юрид. ин-т МВД России им. В.В. Лукьянова, 2019. 31 с.

13. Васюков В.Ф., Панферов Р.Г. Расследование контрабанды наркотических средств в международных почтовых отправлениях: учеб. пособие. М., Прометей, 2021. 332 с.

14. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие. 2-е изд., доп. и испр. М.: ЦИнНМОКП МВД России, 2000. 64 с.

15. Вышинский А.Я. Теория судебных доказательств в советском праве. М.: Гос. изд. юрид. лит., 1950. 308 с.

16. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Изд-во Томского ун-та, 1985. 333 с.

17. Гаврилин Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: учеб. пособие. М.: Акад. управления МВД России, 2021. 71 с.

18. Григорьев О.Г., Кривощеков Н.В. Особенности расследования преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ и их аналогов: учеб.-практ. пособие. Тюмень: Тюмен. юрид. ин-т МВД России, 2010. 104 с.

19. Гуценко К.Ф., Ковалев М.А. Правоохранительные органы: учеб. для студентов юрид. вузов и факультетов. М.: Зерцало-М, 2001. 440 с.

20. Дремлюга Р.И. Интернет-преступность. Владивосток: Дальневост. ун-т, 2008. 240 с.

21. Еникеев М.И. Юридическая психология: учеб. для вузов. М.: НОРМА, 2001. 439 с.

22. Ермолович В.Ф. Криминалистическая характеристика преступлений. Минск: Амалфея, 2001. 304 с.

23. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт. М.: Международные отношения, 2020. 288 с.

24. Закатов А.А., Смагоринский Б.П. Криминалистика: учеб. Волгоград: Волгоград. акад. МВД России, 2000. 472 с.

25. Земцова С.И., Галушин П.В., Карлов А.Л. Участие специалиста и эксперта в расследовании преступлений в сфере неза-

конного оборота наркотических средств, совершенных с использованием криптовалюты: учеб. пособие. Красноярск: СибЮИ МВД России, 2020. 88 с.

26. Земцова С.И., Суров О.А., Галушин П.В. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов: учеб. пособие. 2-е изд., перераб. и доп. Красноярск: СибЮИ МВД России, 2019. 184 с.

27. Использование информации, содержащейся на электронных носителях в уголовно-процессуальном доказывании: учеб. пособие / под ред. Ю.В. Гаврилина и А.В. Победкина. М., 2021. 140 с.

28. Ищенко Е.П. Виртуальный криминал. М.: Проспект, 2012. 232 с.

29. Ищенко Е.П., Топорков А.А. Криминалистика: учеб. для вузов. 2-е изд., испр., доп. и перераб. М.: Контракт: ИНФРА-М, 2010. 784 с.

30. Ковалев С.А., Вехов В.Б. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: монография. М.: Буки-Веди, 2015. 182 с.

31. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия-Телеком, 2002. 336 с.

32. Колесниченко А.Н. Общие положения методики расследования отдельных видов преступления. Харьков, 1965. 47 с.

33. Колмаков В.П. Следственный осмотр. М.: Юрид. лит., 1969. 196 с.

34. Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учеб. пособие. М.: Проспект, 2022. 200 с.

35. Корухов Ю.Г. Трасология и трасологическая экспертиза: учеб. / отв. ред. И.В. Кантор. М: ИМЦ ГУК МВД России, 2002. 376 с.

36. Криминалистика: информационные технологии доказывания: учеб. для вузов / под ред. В.Я. Колдина. М.: Зерцало-М, 2007. 752 с.

37. Криминалистика: учеб. / под ред. А.Г. Филиппова. 2-е изд., перераб. и доп. М.: Спарк, 2000. 670 с.

38. Криминалистика: учеб. для вузов / под ред. проф. А.Ф. Волынского. М.: Закон и право, ЮНИТИ-ДАНА, 1999. 615 с.

39. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования / под ред. Р.С. Белкина, Т.В. Аверьяновой. М.: Новый юрист, 1997. 167 с.

40. Кузнецов А.А., Муленков Д.В., Пропастин С.В., Соколов А.Б. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей и информации на них: учеб. пособие. Омск: Омск. акад. МВД России, 2015. 116 с.

41. Кучерук С.А. Типовые ситуации организации взаимодействия и тактики в особо сложных условиях раскрытия и расследования преступлений: метод. рекомендации. Краснодар: Краснодар. акад. МВД России, 2005.147 с.

42. Мешков В.М. Основы криминалистической теории временных связей. М., 1994. 128 с.

43. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронеж. гос. ун-т, 2001. 255 с.

44. Новик В.В. Способ совершения преступления. Уголовно-правовой и криминалистический аспекты. СПб., 2002. 92 с.

45. Овчинский С.С. Оперативно-розыскная информация / под ред. А.С. Овчинского, В.С. Овчинского. М.: ИНФРА-М, 2000. 365 с.

46. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск: Омск. акад. МВД России, 2009. 372 с.

47. Прозументов Л.М., Шеслер А.В. Личность преступника: криминологический аспект: учеб. пособие. Томск: Томск. филиал РИПК МВД России, 1995. 238 с.

48. Селиванов Н.А. Справочная книга криминалиста. М.: Норма, 2001. 240 с.

49. Сергеев Л.А. Сущность и значение криминалистических характеристик преступлений: руководство для следователей. М.: Юрид. лит., 1971. 752 с.

50. Соколов А.Ф., Ремизов М.В. Использование специальных знаний в уголовном судопроизводстве: учеб. пособие. Ярославль: Изд-во Ярослав. гос. ун-та им. П.Г. Демидова, 2010. 128 с.

51. Стельмах В.Ю., Ефремова О.М., Васюков В.Ф. Производство следственных действий, направленных на получение и использование компьютерной информации: монография / под общ. ред. А.Г. Волеводза. М.: Проспект, 2021. 480 с.

52. Степанов В.В. Предварительная проверка первичных материалов о преступлениях. Саратов: Саратов. юрид. ин-т, 1972. 142 с.

53. Турчин Д.А. Теоретические основы трасологической идентификации в криминалистике. Владивосток: Дальневост. ун-т, 1983. 188 с.

54. Хайруллова Э.Т. Особенности расследования незаконного сбыта наркотических средств и психотропных веществ, совершенного бесконтактным способом: учеб. пособие. Казань: КЮИ МВД России, 2020. 96 с.

55. Шмонин А.В. Методология криминалистической методики: монография. М.: Юрлитинформ, 2010. 415 с.

56. Яблоков Н.П. Криминалистика: учеб. М., 2012. 371 с.

57. Яблоков Н.П. Криминалистика: учеб. М.: Юриспруденция, 2003. 781 с.

Научные статьи

1. Абдусаламов Р.А., Арсланов Ш.Д. Специфика и способы совершения преступлений в сети Интернет // Юридический вестник ДГУ. 2014. № 1. С. 116–118.

2. Абрамова П.В. К вопросу о структуре криминалистической характеристики преступлений, совершенных против правосудия // Научный журнал КубГАУ. 2014. № 104(10). С. 1606–1618.

3. Агафонов В.В., Чистова Л.Ю. Способы совершения преступлений в сфере незаконного оборота наркотиков с использованием Интернета и электронных средств связи // Вестник Московского университета МВД России. 2011. № 3. С. 116–121.

4. Архипова Н.А. Тактика осмотра и выемки электронных сообщений, передаваемых по сетям электросвязи // Закон и право. 2018. № 6. С. 132–135.

5. Архипова Н.А. Организационно-тактические особенности получения и использования содержания текстовых сообщений в процессе раскрытия и расследования преступлений // Вестник

Алтайского государственного университета. 2012. № 2-1(74). С. 71–73.

6. Аскольская Н.Д. Виртуальные следы как элемент криминалистической характеристики компьютерных преступлений // Закон и право. 2020. № 5. С. 173–175.

7. Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 22–27.

8. Бочкин Д.В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. Государство и право. Юридические науки. 2016. № 5(13). С. 40–46.

9. Бутенко О.С. Криминалистические и процессуальные аспекты осмотра мобильных телефонов в рамках предварительного следствия // LexRussia. 2016. № 4(113). С. 49–60.

10. Быков А.А. SIEM-система – универсальный инструмент службы безопасности // Современные инновации. 2017. № 6(20). С. 46–48.

11. Вазюлин С.А., Васюков В.Ф. Получение информации о соединениях между абонентами: специфика процедуры // Уголовный процесс. 2014. № 1. С. 10–21.

12. Васюков В.Ф. Изъятие электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Вестник Томского государственного университета. Право. 2020. № 37. С. 32–39.

13. Васюков В.Ф. Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты // Уголовный процесс. 2019. № 9. С. 44–49.

14. Васюков В.Ф., Чумакова О.В., Афанасьев И.В., Комиссарова Я.В. Противодействие преступлениям в сфере высоких технологий в конце XX – начале XXI века // Вопросы истории. 2021. № 7-2. С. 259–265.

15. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 209–216.

16. Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики // Судебная экспертиза. Волгоград: Волгоград. акад. МВД России, 2016. Вып. 2. 168 с.

17. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4–12.

18. Вьюнов А.В. Общественная опасность преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ // Уголовное право и криминология. 2006. № 11(62). С. 24–27.

19. Гаврилин Ю.В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Труды Академии управления МВД России. 2018. № 4(48). С. 145–150.

20. Гаврилин Ю.В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4(56). С. 122–129.

21. Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1(13). С. 129–137.

22. Гаврилин Ю.В. Технологии обработки больших объемов данных в решении задач криминалистического обеспечения правоохранительной деятельности // Российский следователь. 2019. № 7. С. 3–8

23. Гаврилин Ю.В., Нуянзина С.В. Обеспечение законности при приеме, регистрации и разрешении сообщений о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2020. № 4(13). С. 70–73.

24. Гараев С.Т. Сущность информационно-телекоммуникационных технологий // Инновационная наука. 2016. № 6-2. С. 52–56.

25. Гавло В.К., Клочко В.Е., Ким Д.В. Криминалистическая характеристика преступлений как направление познания и систематизации криминалистически значимой информации о преступной деятельности, необходимой для решения криминалистических задач в складывающихся судебно-следственных ситуациях // Судебно-следственные ситуации: психолого-криминалистические

аспекты / под ред. В.К. Гавло. Барнаул: Алтай. ун-т, 2006. С. 115–119.

26. Гармаев Ю.П. Мультимедийные межотраслевые средства предупреждения преступности: перспективы разработки и внедрения // Криминологический журнал Байкальского государственного университета экономики и права. 2014. № 3. С. 71–80.

27. Герасимова С.О. Методика расследования бесконтактного способа сбыта наркотиков // Развитие общественных наук российскими студентами: сб. науч. тр. Краснодар, 2017. С. 71–74.

28. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 2. С. 45–53.

29. Голубчикова А.А. Криминалистическая характеристика незаконного сбыта наркотических средств – курительных смесей, совершенного бесконтактным способом // Молодежь и XXI век – 2018: материалы VIII Междунар. молодеж. науч. конф. / Юго-Запад. гос. ун-т. Курск, 2018. Т. 3. С. 348–351.

30. Гончарова Н.С. Проблемы криминалистической деятельности на этапе проверки сообщения о незаконном сбыте наркотических средств бесконтактным способом // Организационное, процессуальное и криминалистическое обеспечение уголовного судопроизводства: материалы VI Междунар. науч. конф. студентов и магистрантов. Симферополь, 2017. С. 22–24.

31. Грибунов О.П. Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4(83). С. 137–142.

32. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. 2016. № 8. С. 147–152.

33. Дондуков Б.Г. Криминалистическая характеристика времени незаконного сбыта наркотических средств, психотропных веществ или их аналогов // Вестник Сибирского юридического института МВД России. Право. 2010. № 1(5). С. 176–179.

34. Дудников А.Л. Криминалистическое понятие «способ преступления» // Проблемы законности. 2012. № 120. С. 232–242.

35. Дулов А.В., Рубис А.С. Понятие и содержание выявления преступлений // Право и демократия: сб. науч. тр. Минск: Изд-во БГУ, 2001. Вып. 11. С. 276–280.

36. Ефремова О.М., Васюков В.Ф. Нуждаются ли в корректировке правила производства следственных действий, направленных на изъятие электронных носителей информации и копирование компьютерной информации? // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4(26). С. 69–74.

37. Журавлева С.Ю., Крепышева С.К. Криминалистическая методика и тактика: контекст современного понимания роли криминалистики в юридической деятельности и юридическом образовании // Современная криминалистика: проблемы, тенденции, перспективы: материалы Междунар. науч.-практ. конф., посвящ. 90-летию со дня рождения заслуженного деятеля науки РФ, заслуженного юриста РСФСР, доктора юридических наук, профессора Н. Яблокова, Москва, 22 дек. 2015 г. / ред.-сост. М.А. Лушечкина. М.: МАКС Пресс, 2015. 480 с.

38. Захохов З.Ю. Понятие и сущность специальных знаний в уголовном судопроизводстве // Пробелы в российском законодательстве. Юридический журнал. 2011. № 2. С. 208–211.

39. Звезда И.И. Характеристика первоначального этапа расследования мошенничества в банковской сфере // Деятельность правоохранительных органов в современных условиях: сб. материалов 20-й Междунар. науч.-практ. конф. Иркутск, 2015. С. 328–332.

40. Зотов Я.А. Наркотики: историческая ретроспектива // Экономика и образование. 2013. № 1. С. 174–177.

41. Юргенс Игорь. Деньги массового поражения // Рос. газ. 2008. 24 окт.

42. Калюжный А.Н. Предварительная проверка сообщений о преступлениях: понятие и этапы производств // Юридическая наука. 2013. № 1. С. 60–62.

43. Кисляков С.В. Некоторые проблемы первоначального этапа расследования ДТП, с причинением вреда здоровью человека // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. материалов Всерос. науч.-практ. конф. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 191–195.

44. Клевцов В.В. Особенности криминалистической характеристики преступлений, связанных с распространение «дизайнерских» наркотиков с использованием сети Интернет // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. тр. Всерос. науч.-практ. конф., 29 мая 2015 г. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 195–199.

45. Клевцов К.К., Васюков В.Ф. Получение электронной информации по уголовным делам в рамках международного сотрудничества // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12. № 1. С. 36–51.

46. Климачков А.В. Оперативно-розыскная характеристика личности участников незаконного сбыта наркотических средств, совершаемого с использованием сети Интернет // Алтайский юридический вестник. 2017. № 3(19). С. 111–116.

47. Князьков А.С. Криминалистическая характеристика преступления в контексте его способа и механизма // Вестник Томского государственного университета. Право. 2011. № 1. С. 51–64.

48. Ковалев С.А., Вехов В.Б. Особенности построения типовой компьютерной модели преступлений в сфере незаконного оборота новых опасных психоактивных веществ // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сб. ст. Межведомственного круглого стола и Всерос. круглого стола, 16 окт. 2019 г. Орел: Орлов. юрид. ин-т МВД России, 2019. С. 118–122.

49. Колесникова Г.И. Искусственный интеллект: проблемы и перспективы // Видеонаука. 2018. № 2(10). С. 34–39.

50. Коржев М.А. Криминалистическое значение следов человека // Инновационная наука. 2015. № 7. С. 74–76.

51. Кошелева И.С., Михальчук А.Е. Еще раз к вопросу о значении криминалистической характеристики преступлений // Проблемы противодействия преступности в современных условиях: материалы междунар. науч.-практ. конф. Уфа: РИО БашГУ, 2004. Ч. III. С. 130–131.

52. Крайнова П.Ю. Особенности отдельных элементов криминалистической характеристики сбыта наркотических средств и психотропных веществ на территории учреждений ФСИН России // Юридическая наука и практика: альманах науч. тр. Самар. юрид. ин-та ФСИН России. Самара, 2016. С. 135–137.

53. Куранова Э.Д. Об основных положениях методики расследования отдельных видов преступлений // Вопросы криминалистики. М.: Госюриздат, 1962. Вып. 6–7. С. 152–167.

54. Кусмарцев Н.А. Основные элементы криминалистической характеристики незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов // Государство и право в условиях гражданского общества: сб. ст. Междунар. науч.-практ. конф. 2015. С. 48–50.

55. Кустов А.М., Мурзагалиева О.К., Шимановская К.Е. Типичная информация о личности преступника при расследовании преступлений в сфере оборота наркотических средств // Успехи в химии и химической технологии. Т. XXXI. 2017. № 7. С. 48–50.

56. Кушпель Е.В., Кулешов Е.П. Криминалистическая характеристика и особенности организации первоначального тапа расследования незаконного сбыта наркотиков бесконтактным способом // Защитник закона. 2018. № 2. С. 105–114.

57. Лизунов А.С. Понятие и форма производства доследственной проверки // Бизнес в законе. Экономико-юридический журнал. 2012. № 3. С. 80–83.

58. Маношин Д.А. Программирование искусственного интеллекта // Colloquium-journal. 2019. № 12(36). С. 115–117.

59. Мещеряков В.А. «Виртуальные следы» под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1(4). С. 28–33.

60. Мирошников В.В. Особенности первоначального этапа расследования незаконной миграции // Пробелы в российском законодательстве. 2010. № 3. С. 180–182.

61. Моисеев А.М., Кондратюк С.В. Криминалистические признаки наркосбыта посредством сети Интернет // Балканский юридический вестник. 2017. № 1. С. 43–46.

62. Морозова Е.И. Электронные след личности: вынужденная публичность // Знак: проблемное поле медиаобразования. 2015. № 3(17). С. 42–45.

63. Мошков А.Н. Новые информационные угрозы требуют идти в ногу со временем // Вопросы кибербезопасности. 2014. № 3(4). С. 2–6.

64. Олиндер Н.В. Следственные ситуации на первоначальном этапе расследования преступлений, совершенных с использованием электронных платежных средств и систем // Юридический вестник СамГУ. 2015. Т. 1. № 4. С. 87–91.

65. Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. 2012. № 3. С. 10–16.

66. Осипенко А.Л. Снятие информации с технических каналов связи в сети Интернет // Оперативник (сыщик). 2010. № 2(23). С. 36–39.

67. Осипенко А.Л., Миненко П.В. Оперативно-розыскное противодействие незаконному обороту наркотических средств, совершаемому с использованием телекоммуникационных устройств // Вестник Воронежского института МВД России. 2014. № 1. С. 151–154.

68. Павлов В.В., Золотов М.А., Калентьева Т.А. Проблемы получения и фиксации информации, содержащейся на электронных устройствах лиц, задержанных по делам о незаконном обороте наркотических средств с использованием ресурсов сети Интернет // Вестник Волжского университета им. В.Н. Татищева. 2019. № 2. Т. 1. С. 216–225.

69. Патруль выходит в сеть // Рос. газ. 2019. 7 нояб.

70. Пройдаков Э.М. Современное состояние искусственного интеллекта // Науковедческие исследования. 2018. С. 129–153.

71. Решняк О.А., Ковалев С.А. Предпосылки использования искусственного интеллекта в расследовании преступлений // Расследование преступлений: проблемы и пути их решения. 2021. № 3(33). С. 102–106.

72. Решняк О.А. Ковалев С.А. Проблемы расследования преступлений, совершенных с использованием современных компьютерных технологий // Обеспечение прав и законных интересов граждан в деятельности органов предварительного расследования: сб. ст. Межведомств. круглого стола и Всерос. круглого стола, 16 окт. 2019 г. Орел: Орлов. юрид. ин-т МВД России, 2017. С. 206–208.

73. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 109–117.

74. Россинская Е.Р. Проблемы современной криминалистики и направления ее развития // Эксперт-криминалист. 2013. № 1. С. 2–6.

75. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 44–45.

76. Старичков М.В. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия // Юристъ-правовед. 2018. № 4(87). С. 199–203.

77. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами // LesRussia. 2017. № 3(124). С. 141–152.

78. Стороженко О.Ю. Понятие и структура криминалистической характеристики преступлений, совершаемых в российском сегменте сети Интернет // Казанская наука. 2014. № 11. С. 196–200.

79. Субботина М.В. Расследование преступления на базе криминалистической методики // Роль и значение деятельности Р.С. Белкина в становлении современной криминалистики: материалы Междунар. науч. конф. (к 80-летию со дня рождебния Р.С. Белкина). М., 2002. С. 176–179.

80. Удовиченко В.С., Зникин В.К. Способ совершения преступления как тактико-образующий элемент ситуации допроса подозреваемого и обвиняемого при незаконном сбыте наркотических средств // Известия Балканского государственного университета. 2013. № 2-1(78). С. 123–127.

81. Харлов А.С. Способ совершения преступления как элемент криминалистической характеристики хищений сотовых телефонов // Бизнес в законе. 2010. № 1. URL: http://cyberleninka.ru/article/n/sposob-sovershenіya-prestupleniya-kak-element-kriminalisticheskoy-harakteristiki-hischeniy-sotovyh-telefonov (дата обращения: 17.10.2018).

82. Цветков Ю.А. Раскрытие преступлений следственным путем // Уголовный процесс. 2015. № 10. С. 56–65.

83. Цимбал В.Н., Цимбал Н.Г. Использование информации социальных сетей Интернет в ходе предварительного расследования // Теория и практика общественного развития. 2013. Вып. 10. С. 425–427.

84. Цуканова О.В. Понятие, структура и задачи первоначального этапа расследования преступлений, совершенных на объектах железнодорожного транспорта // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. материалов Всерос. науч.-практ. конф. Орел: Орлов. юрид. ин-т МВД России, 2015. С. 353–356.

85. Черняков М.М Проверка сообщений о незаконном обороте наркотических средств и психотропных веществ // Вестник Сибирского юридического института МВД России. 2016. № 1(22). С. 46–48.

86. Чечетин А.Е. Правовой режим доступа правоохранительных органов к информации операторов связи // Вестник Воронежского института МВД России. 2014. № 3. С. 98–104.

87. Шебалин А.В. Особенности этапа предварительной проверки материалов о незаконном сбыте наркотических средств, совершенном бесконтактным способом // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2015. № 13-1. С. 150–154.

88. Шебалин А.В., Польгерт А.В. Первоначальный и последующий этап расследования незаконного сбыта наркотических средств, совершенного посредством телекоммуникационных сетей // Вестник Томского государственного университета. Право. 2017. № 24. С. 119–125.

89. Шампаров А.В. Установление пространственно-временных характеристик механизма преступления: от теории к практике // Труды Академии управления МВД России. 2014. № 4(32). С. 121–124.

90. Шапошников А.Ю. Ходатайство о получении информации об абонентах должно быть обоснованным // Уголовный процесс. 2010. № 10. С. 42–43.

91. Тишина Юлия. Смартфоны пройдут перепись // Коммерсантъ. 2020. 28 апр. С. 5.

92. Яблоков Н.П. Некоторые проблемы отечественной криминалистики в свете сегодняшнего времени // Современная криминалистика: проблемы, тенденции, перспективы: материалы Междунар. науч.-практ. конф., посвящ. 90-летию со дня рождения заслуженного деятеля науки РФ, заслуженного юриста РСФСР, доктора юридических наук, профессора Н.П. Яблокова. Москва, 22 дек. 2015 г. / ред.-сост. М.А. Лушечкина. М.: МАКС Пресс, 2015. С. 20–25.

Диссертации и авторефераты диссертаций

1. Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. ... канд. юрид. наук. СПб., 2011. 26 с.

2. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. … канд. юрид. наук. М., 2012. 28 с.

3. Безруких Е.С. Особенности взаимодействия следователя и оперативного работника на первоначальном этапе расследования преступлений в сфере незаконного оборота наркотиков: дис. … канд. юрид. наук. Калининград, 2003. 224 с.

4. Белова Н.В. Доказывание организованного характера преступной группы на досудебных стадиях уголовного процесса: дис. ... канд. юрид. наук. Воронеж, 2002. 187 с.

5. Вехов Б.В. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дис. … канд. юрид. наук. Волгоград, 1995. 282 с.

6. Гармаев Ю.П. Теоретические основы формирования криминалистических методик расследования преступлений: автореф. дис. … д-ра юрид. наук. М., 2003. 39 с.

7. Гончарова Т.А. Первоначальный этап расследования терроризма: автореф. дис. … канд. юрид. наук. М., 2006. 24 с.

8. Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы): дис. … канд. юрид. наук. М., 2008. 177 с.

9. Дремлюга Р.И. Интернет-преступность: дис. … канд. юрид. наук. Владивосток, 2007. 248 с.

10. Дусева Н.Ю. Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: дис. ... канд. юрид. наук. Волгоград, 2015. 193 с.

11. Дусева Н.Ю. Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: автореф. дис. ... канд. юрид. наук. Волгоград, 2015. 31 с.

12. Земцова С.И. Участие специалиста в раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных и сильнодействующих веществ: автореф. дис. ... канд. юрид. наук. М., 2017. 27 с.

13. Игнатенко Е.А. Методика расследования незаконной пересылки наркотических средств: дис. ... канд. юрид. наук. Благовещенск, 2015. 208 с.

14. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет: автореф. дис. … канд. юрид. наук. Волгоград, 2008. 31 с.

15. Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет: дис. … канд. юрид. наук. Волгоград, 2008. 233 с.

16. Ильин А.Н. Тактика предварительной проверки сообщения о преступлении: автореф. дис. … канд. юрид. наук. М., 2009. 24 с.

17. Карпов Я.С. Методика расследования незаконного оборота прекурсоров наркотиков на первоначальном этапе: автореф. дис. …канд. юрид. наук. М., 2018. 34 с.

18. Кесареева Т.П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. … канд. юрид. наук. М., 2002. 195 с.

19. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной мобильной связи: дис. ... канд. юрид. наук. М., 2009. 252 с.

20. Клевцов В.В. Использование специальных знаний при расследовании преступлений, связанных с незаконным оборотом

наркотических средств и психотропных веществ: автореф. дис. … канд. юрид. наук. Орел, 2010. 26 с.

21. Ковалев С.А. Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Волгоград, 2012. 221 с.

22. Кодиров Д.С. Незаконный оборот наркотических средств: особенности методики расследования: по материалам Республики Таджикистан: автореф. дис. ... канд. юрид. наук. М., 2017. 28 с.

23. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. дис. … канд. юрид. наук. М., 2019. 25 с.

24. Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: дис. ... канд. юрид. наук. Екатеринбург, 2012. 212 с.

25. Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: автореф. дис. … канд. юрид. наук. Челябинск, 2012. 30 с.

26. Крыгин С.В. Расследование преступлений, совершаемых в сфере компьютерной информации: дис. … канд. юрид. наук. Н. Новгород, 2002. 200 с.

27. Лунгу В.И. Первоначальный этап расследования преступлений: автореф. дис. … канд. юрид. наук. Киев, 1991. 25 с.

28. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: автореф. дис. … канд. юрид. наук. М., 2007. 24 с.

29. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. … канд. юрид. наук. Ростов н/Д, 2017. 188 с.

30. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... д-ра юрид. наук. Воронеж, 2001. 33 с.

31. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.

32. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: дис. … канд. юрид. наук. М., 2004. 204 с.

33. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф. дис. … канд. юрид. наук. М., 2004. 21 с.

34. Ошлыкова Е.А. Методика расследования незаконного сбыта наркотических средств и поддержания государственного обвинения по уголовным делам данной категории: дис. … канд. юрид. наук. М., 2013. 243 с.

35. Папышева Е.С. Методика первоначального этапа расследования убийств, совершенных несовершеннолетними: автореф. дис. … канд. юрид. наук. М., 2010. 30 с.

36. Рудых А.А. Информационно-технологические обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Ростов н/Д, 2020. 239 с.

37. Поздеев И.А. Организация взаимодействия следователя со сведущими лицами в ходе расследования разрушений строительных объектов: автореф. дис. … канд. юрид. наук. Челябинск, 2011. 25 с.

38. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. ... канд. юрид. наук. Омск, 2008. 238 с.

39. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук. Омск, 2008. 22 с.

40. Решняк О.А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота психоактивных веществ: дис. ... канд. юрид. наук. Волгоград, 2019. 220 с.

41. Савина Л.А. Организация и тактика предварительной проверки сообщений об экономических преступлениях на железнодорожном транспорте: дис. ... канд. юрид. наук. М., 2005. 228 с.

42. Савченко Н.И. Особенности предварительного и первоначального этапов расследования получения, дачи взятки: дис. ... канд. юрид. наук. Краснодар, 2020. 209 с.

43. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: автореф. дис. … канд. юрид. наук. М., 2015. 24 с.

44. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации (сравнительный анализ): дис. … канд. юрид. наук. М., 2005. 168 с.

45. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток, 2005. 235 с.

46. Цыкора А.А. Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи: автореф. дис. … канд. юрид. наук. Ростов н/Д, 2013. 32 с.

47. Чекунов И.Г. Криминологические и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. … канд. юрид. наук. М., 2013. 22 с.

48. Чернышенко Е.В. Расследование незаконного оборота наркотических средств и психотропных веществ в исправительных учреждениях ФСИН России: дисс. ... канд. юрид. наук. М., 2015. 35 с.

49. Шаевич А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: автореф. дис. … канд. юрид. наук. Иркутск, 2007. 23 с.

50. Шаповалова Г.М. Возможно сть использования информационных следов в криминалистике (вопросы теории и практики): автореф. дис. … канд. юрид. наук. Владивосток, 2006. 21 с.

51. Шебалин А.В. Расследование хищений средств сотовой связи: дис. ... канд. юрид. наук. Барнаул, 2009. 224 с.

52. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук. М., 2016. 249 с.

53. Шиловский С.В. Способ совершения преступления как признак уголовно наказуемого деяния и дифференцирующее средство: автореф. дис. … канд. юрид. наук. Саратов, 2014. 28 с.

54. Щурова А.С. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети

Интернет): уголовно-правовое и криминологическое исследование: дис. … канд. юрид. наук. СПб., 2017. 256 с.

55. Яшин В.Н. Предварительная проверка первичных материалов о преступлении: дис. … канд. юрид. наук. М., 1999. 210 с.

Интернет-ресурсы

1. Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen, Vincent D. Blondel Unique in the Crowd: The privacy bounds of human mobility. URL: https://www.nature.com/articles/srep01376 (дата обращения: 17.03.2020).

2. UNODC: Всемирный доклад ООН о наркотиках 2018: резюме, выводы и политические последствия. URL: https://www.unodc.org/unodc/ru/frontpage/2018/ June/world-drug-report-2018_-opioid-crisis--prescription-drug-abuse-expands-cocaine-and-opium-hit-record-highs.html (дата обращения: 19.09.2019).

3. UNODC: Всемирный доклад о наркотиках 2020. URL: http://vngoc.org/wpcontent/uploads/2020/08/WDR_2020_Presentatoin_Booklet_1.pdf (дата обращения: 07.04.2021).

4. Википедиа: свободная энциклопедия. URL: https://ru.wikipedia.org.

5. Дискуссия «Искусственный интеллект – главная технология XXI века» // AI Journey 2020. Полное видео. URL: https://www.youtube.com/ watch?v=mW2LvLu-p04 (дата обращения: 20.07. 2021).

6. Сидоренко Елена. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений. URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii (дата обращения: 24.03.2020).

7. Крылов П.В., Сачков И.К. Способ и система выявления удаленного подключения при работе на страницах веб-ресурса: патент 2649793. Группа АйБи. URL: https://patentdb.ru/patent/2649793 (дата обращения: 22.05.2020).

8. Результаты анализа сведений о выполнении мероприятий плана деятельности Роскомнадзора за 1 полугодие (2 квартал) 2019 года. URL: https://rkn.gov.ru/docs/docP_2550.pdf (дата обращения: 19.09.2019).

9. Дейвенпорт-Хайнс Ричард. В поисках забвения. Всемирная история наркотиков 1500–2000 / пер. А. Савинова. URL: https://clck.ru/auAJe (дата обращения: 06.09.2019).

10. Роль больших данных в частных расследованиях и анализе. URL: https://habr.com/ru/company/asus/blog/240877/ (дата обращения: 18.04.2020).

11. Краткая характеристика состояния преступности в России за январь – декабрь 2020 г. // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 04.02.2021).

12. Стоп зависимость. Статистические сведения: сервис поиска реабилитационных центров и наркологических клиник. URL: https://stopz.ru/informaciya/narkomaniya/statistika-po-narkozavisimym-v-rossii/ (дата обращения 09.02.2021).

13. Состояние преступности. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 25.01.2022).

14. Толковый словарь Ожегова. URL: https://slovarozhegova.ru (дата обращения: 13.09.2020).

15. Экс-агент ФБР отследил трансфер более 700 тыс. биткоинов с серверов Silk Road на ПК подозреваемого в управлении ресурсом. URL: https://www.securitylab.ru/news/470643.php (дата обращения: 14.08.2021).

Судебная практика

1. Приговор Первореченского районного суда г. Владивостока Приморского края от 4 июля 2017 г. № 1-134/2017 по ч. 5 ст. 228.1 УК РФ в отношении Гришина Е.А. URL: http://sud-praktika.ru/precedent/399272.html (дата обращения: 11.09.2019).

2. Архив Красноармейского районного суда Краснодарского края. Уголовное дело № 1-238/2018 по п. «г» ч. 4 ст. 228.1 УК РФ, ч. 1 ст. 228 УК РФ.

3. Архив Ленинского районного суда г. Новороссийска Краснодарского края. Уголовное дело № 1-44/2018 по ч. 4 ст. 228.1, ч. 2 ст. 228 УК РФ.

4. Архив Белореченского районного суда Краснодарского края. Уголовное дело № 1-263/19 по ч. 3 ст. 30, пп. «а», «г» ч. 4 ст. 228.1 УК РФ.

5. Архив Ленинского районного суда г. Краснодара. Уголовное дело № 1-47/2017 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

6. Архив Прикубанского районного суда г. Краснодара. Уголовное дело № 1-168/2020 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

7. Архив Прикубанского районного суда г. Краснодара. Уголовное дело № 1-324/20 по ч. 1 ст. 228.1 УК РФ.

8. Архив Прикубанского районного суда г. Краснодара. Уголовное дело № 1-91/2020 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

9. Архив Первомайского районного суда г. Краснодара. Уголовное дело № 1-86/2020 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

10. Архив Ленинского районного суда г. Краснодара. Уголовное дело № 1-916/2019 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

11. Архив Прикубанского районного суда г. Краснодара. Уголовное дело № 1-1180/2019 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ.

12. Архив Прикубанского районного суда г. Краснодара. Уголовное дело № 1-436/2019 по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ, ч. 3 ст. 30, п. «б» ч. 3 ст. 228.1 УК РФ.

Оглавление

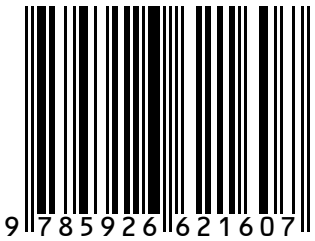
Учебное издание

Введенская Ольга Юрьевна

ОСОБЕННОСТИ ПРЕДВАРИТЕЛЬНОГО И ПЕРВОНАЧАЛЬНОГО ЭТАПОВ РАССЛЕДОВАНИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Редактор *А. И. Таранова*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2160-7



Подписано в печать 02.04.2025. Формат 60x84 1/16.
Усл. печ. л. 10,0. Тираж 50 экз. Заказ 342.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.