Введенская Ольга Юрьевна,
старший преподаватель кафедры криминалистики
Краснодарского университета МВД России,
кандидат юридических наук

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОЛУЧЕНИЯ ПЕРВОНАЧАЛЬНОЙ ИНФОРМАЦИИ О НЕЗАКОННОМ СБЫТЕ НАРКОТИЧЕСКИХ СРЕДСТВ

Понятие первоначальной информации весьма широкое и включает в себя любые сведения (как процессуальной природы, так и не процессуальной), имеющие значение для раскрытия и расследования преступлений, раскрывающие признаки определенного состава преступлений, определяющие наличие, либо же отсутствие преступного факта.

А.А. Рудых, рассматривая преступления в сфере информационных технологий, включает в содержание первоначальной информации о них: сведения о пользователях, 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].

---

[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».

Таким образом, в понятие первоначальной 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.

На наш взгляд, 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 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.

Говоря о получении первоначальной информации следует отметить ее специфику, определяемую использованием информационно-телекоммуникационных технологий: первичным должно явиться исследование информационной плоскости преступлений, связанных с незаконным сбытом наркотических средств, и, следуя по пути преступника, появляется возможность восполнить все информационные пробелы криминальной картины.

В ранее проведенном исследовании[1] были рассмотрены основные группы методов получения такой информации. Однако, как очевидно, преступность не стоит на месте, регулярно расширяя свой преступный арсенал, в противовес принимаемым контрмерам. В связи с чем предлагаем рассмотреть ряд актуальных для этой сферы подходов.

Рассматривая данную категорию уголовных дел, основной объем доступной правоохранительным органам первоначальной информации о незаконном сбыте наркотических средств будет находиться именно в информационном пространстве, тем самым и определяется содержание методов ее получения:

---

[1] Введенская О.Ю. Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2022. 201 с.

Интернет-анализ контента – это процесс исследования содержания сетевой активности пользователей информационно-телекоммуникационных систем и технологий для выявления подозрительного поведения и идентификации угроз. Специалисты по цифровой криминалистике используют различные инструменты и методы, такие как анализ трафика, поиск аномалий и обнаружение вторжений, для выявления и расследования преступлений, связанных с сетевой активностью и сетевым поведением. Его можно проводить как точечно, целенаправленно, так и с использованием систем искусственного интеллекта:

– регистрационные данные – для абсолютного большинства сетевых ресурсов логина и пароля доступа к ним оказывается недостаточно. И пользователи, желающие посещать этот ресурс, вынуждены указывать персональные данные. Например, дата рождения, имя и т.п., вполне могут не соответствовать действительности, то номер телефона или адрес e-mail, зачастую, приходится указывать реальный, потому что этого требует алгоритм проверки и персонификации. Результат сопоставления регистрационных данных нескольких ресурсов вполне вероятно откроет доступ к третьему.

– из вышеописанного вытекает еще один аспект – мультиник – использование одного и того же ника (логина) на разных информационных площадках.

– стили и характеристики письменной речи – лингвистический анализ криминалистически значимых сведений позволяет определить пол, приблизительный возраст, образовательный уровень, хобби, профессиональную принадлежность и т.п. Причем, учеными-лингвистами выявлено, что для идентификации человека достаточно весьма небольшого объёма текста.

– профессиональная тематика – знания о способах изготовления, культивирования и иных действий с наркотическими средствами представляют весьма узкую направленность и постоянно обновляются, в связи с чем представляется актуальным анализ соответствующих тематических сетевых ресурсов, являющихся площадкой общения заинтересованных пользователей.

– кросспосты – публикация на различных интернет-ресурсах однотипных постов. Данный факт может явиться основанием для объединения этих ресурсов и их последующего совокупного анализа.

– общие друзья – анализ контента социальных сетей в совокупности с комментариями на различных тематических интернет-ресурсах, по типу: «см. у NiKa…» поможет вполне точно определить круг общения

– и др.

Причем, анализ активности в сети Интернет покажет максимальную эффективность лишь при работе с множеством источников. Точное их количество, как и степень верификации полученной информации, должен определить человек, осуществляющие его. Для чего активно разрабатывается и внедряется программное обеспечение специального назначения.

Например, на основе технологий искусственного интеллекта создана нейросеть «Товарищ майор». Важнейшей ее функцией является определение владельцев анонимных Telegram-каналов. Кроме того, возможности программы позволяют устанавливать подписи к мультимедиа (сообщениям, в том числе во встроенном чате, стикерпаках, документах и видеороликах, загруженных в сообщество); анализировать контент с информацией о привязанных к профилю пользователя номерах мобильных телефонов, адресах и других цифровых следах; проводить анализ других идентификаторов, а также получать данные из блогах, веб-сайтах и социальных сетей; проверять юридических лиц по их ИНН, аккумулируя из различных источников общую информацию о компании и др.

Очевидно, что платформы Telegram-каналов имеют особую популярность в среде наркосбытчиков. В связи с чем использование подобных программных решений в деятельности правоохранительных органов поднимет результаты противодействия наркопреступности на новый уровень.

Кроме того, ГРЧЦ активно использует систему искусственного интеллекта «Окулус»: автоматическое обнаружение и выделение в общем потоке сведений экстремистского характера, наносящие вред детям, пронаркотический контент, призывы к массовым незаконным мероприятиям, суициду и пропаганду ЛГБТ.[1]

Согласно Ведомственной программе цифровой трансформации МВД России на 2023-2025 годы[2] разработаны проекты технических заданий для подготовки и тестирования систем искусственного интеллекта для нужд МВД.

В данной Программе речь ведется о системах «Клон» (для выявления фактов фальсификации видеоизображений) и «Конъюнктура» (составление прогнозов появления негативных событий и чрезвычайных ситуаций, а также моделирование сценарии реагирования на них). Их внедрение в практическую деятельность планируется уже в 2025 г. Подобные тенденции позволяют ожидать разработки и внедрения систем, задачей функционирования которых будет являться борьба с отдельными видами преступлений. В частности, с незаконным сбытом наркотических средств, совершаемом рассматриваемым способом.

Извлечение данных – в данном случае речь ведется как об извлечении отдельных данных, части системы так и об ее полном извлечении из цифровых устройств: персональных компьютеров, средств мобильной связи, иных

---

[1] В России запустили систему поиска запрещенного контента в интернете «Окулус»: Известия от 13 февраля 2023 г. – URL https://iz.ru/1469322/2023-02-13/v-rossii-zapustili-sistemu-poiska-zapreshchennogo-kontenta-v-internete-okulus (дата обращения: 10.10.2024).

[2] Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023-2025 годы: Распоряжение МВД России от 25 января 2023 г. № 1/649. Доступ из справочной правовой системы «Гарант».

цифровых устройств – ключевых инструментов рассматриваемой преступной деятельности, и, соответственно, носителей первоначальной криминалистически значимой информации о них.

Для IOS наиболее перспективным представляется использование уязвимостей, например, в цикле обновления операционной системы, а также агентов-экстракторов – специальных приложений, после установки которых открывается доступ к файловой системе, например Elcomsoft iOS Forensic Toolkit.

Способы извлечения данных из устройств Android гораздо шире. Особый интерес представляет собой использование уязвимостей системы. Современная практика открывает обширные возможности извлечения полной файловой системы через Android KeyStore, применения специализированных инструментов для получения root-доступа[1] и извлечения данных и др.

Стоит отметить альтернативный метод – Chip-off, заключающийся в извлечении из одного устройства чипа памяти и в его установке в другое. Как правило, таким образом проводится работа по получению криминалистически значимой информации их неработающих устройств.

Практическими сотрудниками в ходе рассматриваемой деятельности по получению первоначальной криминалистически значимой информации из цифровых устройств активно используется «Мобильный криминалист» [2]. Инструменты весьма универсальны и предназначены для работы с широким спектром мобильных устройств, персональных компьютеров и облачных сервисов. Возможности работы со средством мобильной связи представлены на рисунке.

Функционал данного программного обеспечения представляет весьма широкий спектр возможностей: это не только экспертный анализ цифровых данных, но и аналитические возможности. Например, «Мобильный криминалист Десктоп» предоставляет возможность извлечения данных из систем Windows, macOS, Linux и их последующего анализа посредством разнообразных интегрированных утилит.

Также, имеется ряд альтернативных программных инструментов (Magnet AXIOM, Belkasoft Evidence Center и др.), предоставляющих схожие возможности по извлечению данных из мобильных устройств и жестких дисков.

Анализ метаданных – речь ведется о данных, описывающих непосредственное содержание файла.

Современная классификация метаданных весьма обширна: внутренние, административные, по характеристикам внешних признаков и др.

---

[1] Возможность получить полный доступ к системным процессам и утилитам на устройстве с операционной системой Android.

[2] МКО системы. URL.: https://mko-systems.ru/ (дата обращения 3.10.2014).

Также различаются их форматы: DCMI, MARC, vCard, XML и др., в зависимости от содержания. Упорядочивание метаданных позволяет структурировать информацию, придавая ей целостный вид, провести ее анализ.

Например, веб-приложение DataHub представляет собой открытую платформу для поиска и обнаружения метаданных.

К сожалению, современная практика свидетельствует о недостаточном внимании метаданным, в то время как их анализ окажет содействие в идентификации пользователя информационных систем и технологий, а также позволит составить весьма полное представление о масштабах и участниках преступной деятельности, после проведенного логического анализа полученной информации.

Восстановление удаленных данных – наркосбытчики стремятся к максимальному сокрытию следов своей преступной деятельности. В связи с чем весьма наивно полагать что цифровое устройство, ставшее носителем первоначальной криминалистически значимой информации, сохранит интересующие правоохранительные органы сведения в первозданном виде. В связи с чем приобретает особую актуальность восстановление удаленных данных. На самом деле, процесс элементарного удаления цифровой информации, как правило, не всегда предполагает его физическое удаление. А представляет собой выполнение команды «del» в каталоге файла. Кроме того, существует ряд физических причин: от неисправности контроллера до выхода из строя блока магнитных головок (БМГ). В связи с чем современные технологии открывают широкие возможности для восстановления удаленных данных – то есть извлечения удаленных, недоступных, утерянных, поврежденных или форматированных данных из вторичного хранилища, съемных носителей или файлов, когда к хранящимся на них данным невозможно получить доступ обычным способом[1]. Для получения первоначальной криминалистически значимой информации о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий разработан и активно используется целый ряд как бесплатного и общедоступного, так и коммерческого программного обеспечения, решающего вопросы разной природы и сложности (Феникс, Recuva, Disk Drill, Pandora recovery, ФотоДОКТОР и др.). Также, зачастую, требуется проведение работ по приведению в рабочее состояние носителя информации.

Получение первоначальной информации из иных источников – деятельность по незаконному сбыту наркотических средств, как было отмечено выше, протекает как в информационном, так и в физическом пространстве, тем самым расширяя перечень носителей криминалистически значимой информации о рассматриваемых преступлениях: видеорегистраторы, БПЛА, камеры наружного наблюдения и др. В связи с чем могут использоваться

[1] Восстановление данных. URL.: https://en.wikipedia.org/wiki/Data_recovery (дата обращения 3.10.2024).

результаты применения иных комплексов, например, разработанных для нужд Министерства Обороны и др.

Например, для контроля аномальных передвижений в наземной и надводной обстановке разработаны мобильные комплексы «Зверобой», «Ратник», «Амулет» – также предполагает и работу с источниками мобильной связи и др.

Казалось бы, не имеющие отношение к правоохранительной деятельности по противодействию незаконному сбыту наркотических средств с использованием информационно-телекоммуникационных технологий сведения, могут быть успешно использованы правоохранительными органами. Полагается, фильтрация такой информации должна происходить согласно заранее разработанным критериям соответствия, определяемым содержанием криминалистической характеристики рассматриваемых преступлений, актуальной в текущий момент с учетом оперативной обстановки в заданном регионе, а их предоставление в рамках межведомственного взаимодействия.

Получение данных наружной фото- видеофиксации (например, в рамках взаимодействия с подразделениями ГИБДД и др., данные системы распознавания лиц и автомобилей – «Следопыт», ПАРСИВ), также позволит, согласно заранее разработанным критериям, получить максимальный объем первоначальной уголовно-релевантной информации о рассматриваемых преступлениях.

Анализ больших данных. Скорость информационного обмена не вызывает сомнений. Структуированную или неструктуированную информацию большого объема недостаточно просто получить, вопрос заключается в ее обработке и в выделении в общем массиве криминалистически значимой. Такая работа требует специальных навыков. Которые, к сожалению, имеются далеко не у всех сотрудников правоохранительных органов. Сегодня данный вопрос настолько актуален, что успешно функционируют отдельные программные продукты и даже целые платформы (например, PolyAnalyst), позволяющие осуществлять анализ больших данных даже непрофессионалам. Посредством передовых алгоритмов машинного обучения и технологий искусственного интеллекта открываются широкие возможности извлечения из объема больших данных криминалистически значимой информации и структуирование полученных результатов в веб-отчеты. Критерии, предъявляемые к полезности информации должны определяться актуальностью криминалистических знаний, так же, как и алгоритмы обучения искусственного интеллекта.

Касаемо введения полученных результатов в процессуальную деятельность вызывают интерес предложения[1] о дополнении перечня мероприятий для документирования исследованием информации, содержащейся в технологических системах ее передачи.

Организационная составляющая – Например, в США действуют такие ведомства, как United States Emergency Computer Readiness Team (Компьютерная команда экстренной готовности США), US Cyber Command (подразделение вооруженных сил, осуществляющее деятельность в киберпространстве), Computer Intellectual and Crime Property Section (подразделение уголовного отдела Министерства юстиции США) и др. – то есть, подразделения, занимающиеся IT-безопасностью и инцидентами, осуществляют свою деятельность в составе большей части силовых ведомств США. В России же относительно недавно создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий в структуре Министерства внутренних дел РФ. Очевидно, введение подобных подразделений в структуру и других силовых ведомств позволит оказывать всестороннее противодействие преступности рассматриваемого вида.

Очевидно, что описанные методы не исчерпывающие и лишь раскрывают в доступной для неспециалиста в данном вопросе форме современные направления получения первоначальной криминалистически значимой информации о рассматриваемых преступлениях.

Широкие возможности работы с цифровой информацией, в форме которой и существует значительная часть первоначальной криминалистически значимой информации о рассматриваемых преступлениях, безусловно, созданы соответствующими специалистами, тем не менее, их использование может быть вполне адаптировано и для непрофессионалов в IT-сфере.

К сожалению, на практике складывается ситуация, что преступность идет в ногу со временем, а правоохранительные органы по ее следам. В связи с чем необходимо постоянное совершенствование криминалистических знаний, внедрение передовых разработок в практическую деятельность, а также аналитическая работа, позволяющая разрабатывать эффективные контрмеры, направленные на опережение преступников.

[1] URL.: https://www.vedomosti.ru/society/articles/2023/08/16/990319-mvd-rasshiryaet-perechen-operativno-rozisknih-meropriyatii-dlya-dokumentirovaniya-kiberprestuplenii (дата обращения 13.09.2024).