УДК 004.62

СПЕЦИФИКА СБОРА ЦИФРОВЫХ СЛЕДОВ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Комерцов В.В.
(Ростовский юридический институт МВД России)

Аннотация: в данной статье рассматриваются методы и способы, используемые сотрудниками полиции для раскрытия и расследования преступлений, связанных с нелегальным оборотом наркотиков и иных психотропных веществ при помощи информационно-коммуникационной сети Интернет и иных компьютерных технологий.

Ключевые слова: цифровые следы, собирание доказательств, следственная экспертиза, наркотические средства, противодействие преступлениям, связанным с наркотическими веществами.

THE SPECIFICS OF COLLECTING DIGITAL TRACES WHEN COMMITTING CRIMES IN THE FIELD OF ILLICIT DRUG TRAFFICKING WITH THE USE OF COMPUTER TECHNOLOGY

Komertsov V.V.
(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: this article discusses the methods and methods used by police officers to uncover and investigate crimes related to illegal trafficking of drugs and other psychotropic substances using the Internet information and communication network and other computer technologies.

Keywords: digital traces, evidence collection, investigative expertise, narcotic drugs, countering crimes related to narcotic substances.

Распространение наркотических и психотропных веществ в нашей стране – актуальная проблема, об этом свидетельствует статистика уголовных дел, возбужденных по статьям, связанным с незаконным оборотом наркотических средств, психотропных веществ или их аналогов, сильнодействующих веществ. По данным Министерства внутренних дел Российской Федерации [1] в 2004 году их количество было равно 139345, спустя 10 лет количество преступлений стало значительно выше, в 2014 году составило 254730, в 2021 году было возбуждено 172092, из которых 51444 были совершенны с использованием информационно-коммуникационной сети Интернет и иных компьютерных технологий.

Часто на улицах городов и других населенных пунктов можно обнаружить граффити с предложением высокооплачиваемой работы, для получения которой необходимо перейти по ссылке. Также подобные предложения приходят пользователям социальных сетей. Переходя по указанному адресу в сети Интернет, попадают в один из популярных мессенджеров, где «менеджер компании» рассказывает суть работы и заработную плату, чаще всего она заключается в распространении «закладок» [2], то есть наркотических средств в небольшой упаковке, спрятанной в каком-либо определенном месте.

Зачастую работа «закладчиков»-распространителей также координируется через эти мессенджеры кураторами, которые указывают места нахождения наркотических веществ, а также те координаты, куда их нужно доставить. Этим же способом покупатель связывается с наркодилером, узнает стоимость, производит оплату и узнает координаты «закладок».

Другим способом приобретения наркотических веществ являются сайты (большинство таких сайтов имеют домен .onion) в так называемом «даркнете» - часть всемирной паутины, для попадания в которую необходимы специальные браузеры, самым часто используемым из которых является «Tor». Также с помощью таких сайтов возможно проводить оплату. Самыми популярными способами провести оплату за наркотические вещества являются перевод криптовалюты между криптокошельками участников сделки или с помощью неверифицированных онлайн-кошельков, для создания которых достаточно иметь сим-карту, зарегистрированную на любого человека.

Данные способы распространения наркотиков обрели большую популярность из-за относительной «безопасности» участников сделки и затрудненной их идентификацией.

В связи с развитием информационных технологий и роста количества преступлений, совершенных с их помощью, законодатель внес поправки в уголовное законодательство, а именно внес в 2012 году в Уголовный кодекс Российской Федерации [3] ст. 228.1 «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», а именно часть 2 данной статьи, которая предусматривает наказание за распространение наркотиков именно с помощью сети Интернет.

Для борьбы с данным родом преступлений, совершенных с помощью информационных технологий, существуют специальные методы собирания «цифровых следов». В современной юридической литературе под «цифровыми следами» понимают связанные с преступлением результаты создания либо изменения компьютерной информации в различных формах, а также корректировку физических характеристик носителей.

Во время проведения экспертиз, связанных с «цифровыми следами», необходимо соблюдать общепринятые принципы, к ним относятся:

1. В следственные действия, связанные с компьютерной информацией, не должны вноситься какие-либо изменения.

2. Все действия, проводимые с информацией, должны осуществляться специалистом, компетентным в данной области.

3. Оформление всех процессуальных действий соответствующими актами, установленными законом.

4. Ответственность сотрудников, работающих с информацией, за ее сохранность.

Все данные, которые могут стать доказательствами совершения преступления, возможно разделить на основные группы: сетевые и локальные.

К локальным данным относится вся информация, которая содержится на компьютерах, переносных устройствах и других гаджетах пользователя, к ним относят: имя и формат файла, даты его создания и (или) изменения, идентификационные номера ЭВМ и прочие.

К сетевым данным причисляют информацию, доступ к которой осуществляется удаленно через устройства связи, к данной категории относят: IP- и MAC-адреса устройства, а также поисковые запросы, загрузка файлов в память устройства, данные, указываемые пользователем при регистрации профилей в различных социальных сетях и форумах.

Чаще всего при расследовании используют локальные следы, оставшиеся у пользователей на мобильных устройствах, а также персональных и других видах компьютеров.

Для получения данных с портативных устройств в органах внутренних дел существует ряд программного обеспечения, позволяющего извлечь различные сведения об использовании гаджета, включая сведения о входящих и исходящих голосовых звонках, текстовых (СМС) и мультимедийных (ММС) сообщениях, использовании сторонних приложений, а также данные о подключении данного устройства к сети Интернет. К такому ПО относят следующие средства извлечения информации: «Cellebrite UFED», «Мобильный криминалист», «Belkasoft Evidence Center Ultimate» и другие. Большинство из них способны выполнять вышеуказанные действия с средствами мобильной связи разных производителей и под управлением различных операционных систем. Основанием для использования данных программ является Уголовно-процессуальный кодекс Российской Федерации [4], а именно следующие следственные действия: ст. 186 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», ст. 176 УПК РФ «Получение информации в ходе следственного осмотра мобильного устройства» и ч. 7 ст. 185 УПК РФ «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка».

Также при исследовании «содержимого» мобильного устройства эксперты могут обнаружить очень полезный для следствия вид данных – геолокационные данные – благодаря тому, что большинство телефонов и других переносных устройств оснащены модулями Global Positioning System (GPS) (и) или государственной автоматизированной информационной системы (ГЛОНАСС), а в случаях если подключение к таким системам не происходило, местоположение можно определить с помощью вышек сотовой связи, к которым подключалось устройство. Данная информация может являться доказательством нахож-

дения лица в определенном месте, устанавливать маршруты передвижения пользователя устройства и другие.

Для получения данных с персонального или другого вида компьютеров существуют другие экспертизы. Они состоят из двух этапов: предварительный и основной. Каждый из них проводится по определенному алгоритму:

Предварительный:

1. Установление и формальная фиксация даты и времени проводимого исследования.

2. Соблюдение «фактора неожиданности» в момент изъятия оборудования.

3. Установление контроля за всеми помещениями, в которых могут находиться ЭВМ и другие необходимые для экспертиз устройства.

4. Отключение устройства от всех возможных подключений к сети.

5. Обеспечение ограниченного доступа к исследуемым устройствам.

6. Другие действия, направленные на обеспечение безопасности и первоначального вида данным, хранящимся на устройстве (устройствах).

Основной:

1. Производится внешний осмотр устройства на предмет повреждения и наличия внешних устройств.

2. На оборудование для проведения исследования включается режим, защищающий изучаемое устройство от изменений находящихся на нем данных, а после осуществляется изучение свойств хранимой на устройстве информации.

3. Производится копирование содержимого объекта исследования на иной информационный носитель. Данное действие в органах внутренних дел производится с помощью утилиты «Оттиск», которая позволяет получить доступ к большинству всех возможных файлов, а также осуществить скоростное копирование. Дальнейшие исследования происходят со скопированными данными.

4. Экспериментальный запуск программ и иной информации, находящейся на изучаемом устройстве. Данная стадия включает в себя различные действия:

а) восстановление удаленных с устройства данных;

б) проверка файлов на наличие вредоносного программного обеспечения при помощи антивирусных программ;

в) обнаружение и анализ ПО, установленного на устройстве, а также того, которое не установлено, но его данные имеются в памяти объекта изучения;

г) поиск информации, связанной с вопросами, поставленными следователем перед экспертом;

д) другие необходимые для ответа на поставленные вопросы действия.

5. Переформатирование полученных данных в форму, понятную для человека, не обладающего данными в сфере информационных технологий.

6. Составление отчета об исследовании, ответы на поставленные перед экспертом вопросы, фиксация их на бумажных или электронных носителях. Требования к результатам, предоставленным на электронных носителях: данные на них вносятся без каких-либо изменений, а сами носители должны быть CD- или DVD-диски, без возможности перезаписи. На нерабочей стороне носителя специальным маркером наносятся дата и номер экспертизы, номер приложения, заверенные подписью эксперта, осуществлявшего экспертизу.

Получение сетевых данных, которые включают в себя IP- и MAC-адреса, номер sim-карты, с которой осуществлялся доступ к сети Интернет, Log-файлы и прочие необходимы для следствия данные, сотрудники полиции и иные следственные органы могут получить от операторов связи. Они, согласно Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи» [5], обязаны собирать следующие данные:

1. Данные человека, который заключил договор с оператором мобильной связи.
2. О входящих и исходящих звонках на номер, закрепленный за sim-картой.
3. О пополнениях и списаниях денежных средств на счете абонента (балансе).
4. Об индивидуальных идентификационных номерах мобильных устройств (IMEI).
5. Об иных sim-картах, которые использовались совместно в устройстве.
6. О геолокации устройства, согласно подключениям к сотовым вышкам (станциям).
7. Иные сведения, установленные федеральным законом.

Данные сведения позволяют своевременно осуществлять мероприятий, которые включены в стадии оперативно-разыскной деятельности.

Также проводятся исследования, не связанные с информацией, которая хранится на устройстве, а именно трасологические, которые включают в себя исследования потожировых следов, остывших на различных частях устройств, различных частиц, следы вскрытия устройства и многие другие «классические» экспертизы.

Использование методов и средств установления «электронных следов», а также соблюдение особенностей их применения позволяет сотрудникам правоохранительных органов, осуществляющих следствие по делам в сфере незаконного оборота наркотических средств, выполнять необходимые следственные действия в кратчайший срок, собирать важнейшие доказательства для привлечения к уголовной ответственности лиц, совершивших преступление, а также предупреждения дальнейших нарушений закона.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Состояние преступности [Электронный ресурс]. – Режим доступа: https://мвд.рф/ (дата обращения: 20.10.2022).

2. Закладчика с половиной килограмма наркотиков поймали в Разметелево [Электронный ресурс]. – Режим доступа: https://www.mk-lenobl.ru/ (дата обращения: 26.10.2022).

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.10.2022) // СПС «КонсультантПлюс».

4. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.10.2022) // СПС «КонсультантПлюс».

5. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (ред. от 30.12.2021) // СПС «КонсультантПлюс».

6. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2-х ч. – Москва: Академия управления МВД России, 2019. Ч. 1. – 208 с.

7. Чекунов И.Г., Рядовский И.А., Иванов М.А. [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие / под ред. И. Г. Чекунова. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2018. – 106 с.

УДК 004.85

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИКОВ В СЕТИ ИНТЕРНЕТ

Лемайкина С.В.
(Ростовский юридический институт МВД России)

Аннотация: статья посвящена анализу незаконного оборота наркотических веществ с использованием рынка DarkNet (Даркнет), а также проблемам, возникающим у правоохранительных органов при расследовании таких преступлений. В статье также определены методы выявления незаконного оборота наркотиков с использованием искусственного интеллекта.

Ключевые слова: незаконный оборот наркотиков, DarkNet (Даркнет), искусственный интеллект, онлайн, анонимность, веб-сайты.

THE USE OF ARTIFICIAL INTELLIGENCE TO INVESTIGATE CRIMES RELATED TO DRUG TRAFFICKING ON THE INTERNET

Lemaikina S.V.
(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article is devoted to the analysis of illicit drug trafficking using the DarkNet market, as well as problems that arise for law enforcement agencies in the investigation of such crimes. The article also defines methods for detecting drug trafficking using artificial intelligence.

Keywords: drug trafficking, darknet, artificial intelligence, online, anonymity, websites.