БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Зачем власти блокируют Tor и можно ли это сделать [Электронный ресурс]. – Режим доступа: https://www.forbes.ru/tekhnologii/448961-zacem-vlasti-blokiruut-tor-i-mozno-li-eto-sdelat (дата обращения: 17.11.2022).

2. Следователем МВД России возбуждено уголовное дело о легализации более 2 млрд рублей [Электронный ресурс]. – Режим доступа: http://www.mvd.ru (дата обращения: 17.11.2022).

3. Состояние преступности в России за январь-октябрь 2022 года [Электронный ресурс]. – Режим доступа: http://www.mvd.ru (дата обращения: 17.11.2022).

УДК 343.985.4:[343.575:004.77](470)

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ОСМОТРА СРЕДСТВ СОТОВОЙ СВЯЗИ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

Нугаева Э.Д.,
кандидат юридических наук
(Уфимский юридический институт МВД России)

Аннотация: автором в статье изложены тактические рекомендации по проведению осмотра и процессуальной фиксации сведений, расположенных в электронной памяти сотового телефона на стадиях статистического и динамического осмотра.

Ключевые слова: тактика, осмотр, сотовый телефон, специалист, следователь, наркотические средства, психотропные вещества, информация.

CRIMINALISTIC ASPECTS OF THE INSPECTION OF CELLULAR COMMUNICATION FACILITIES IN CRIMINAL CASES IN THE FIELD OF ILLICIT TRAFFICKING OF NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES

Nugaeva E.D.,
Candidate of Law
(Ufa Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the author of the article presents tactical recommendations for conducting an inspection and procedural fixation of information located in the electronic memory of a cell phone at the stages of statistical and dynamic inspection.

Keywords: tactics, inspection, cell phone, specialist, investigator, narcotic drugs, psychotropic substances, information.

Незаконный оборот наркотических средств (далее – НС) и психотропных веществ (далее – ПВ) и его последствия продолжают сегодня оставаться одной из наиболее острых общемировых проблем. На территории Российской Федерации ежегодно правоохранительными органами выявляются порядка 200 тыс. преступлений, связанных с незаконным оборотом НС и ПВ [1]. Одна из тенденций современной преступности в сфере незаконного оборота НС и ПВ заключается в появлении транснациональных и трансграничных организованных групп и преступных сообществ (организаций), объединяющих людей из разных регионов или стран мира, взаимодействующих друг с другом посредством сети Интернет. Использование удаленной передачи данных обеспечивает высокую степень конспирации, обусловленную отсутствием непосредственного контакта между продавцами и покупателями наркотиков, позволяет быстро передавать информацию, одновременно увеличивает количество посетителей, обеспечивает простоту сбора информации при небольших финансовых издержках. Согласно статистическим данным Главного информационного центра МВД России в 2020 году на 90,7% возросло число выявленных фактов сбыта наркотиков, совершенных с использованием IT-технологий [2, с. 44]. В 2021 году отмечается увеличение удельного веса преступлений, совершенных дистанционно, в том числе с использованием IT-технологий, на 7,7% по сравнению с 2020 годом [3, с. 47].

С целью выявления транзитной цепи наркопреступлений и всех лиц, причастных к их совершению, требуется комплексная работа органов дознания во взаимодействии со следователями, сотрудниками экспертно-криминалистических подразделений МВД России, Интерполом, специалистами в области компьютерных технологий, Росфинмониторингом и прочими специализированными департаментами. Ярким тому примером является функционирующая в период с 2015 по апрель 2022 г. на территории Российской Федерации торговая площадка Hydra, на базе которой более 19 000 виртуальных магазинов осуществляли криминальную деятельность, оказывая услуги по продаже наркотиков,

фальшивых банкнот, поддельных документов, нелегальных технических средств и иную противозаконную деятельность. Годовой оборот транзакций, совершаемых на платформе, превышал миллиард рублей. В результате грамотно организованной международной полицейской операции правоохранительными органами Федеративной Республики Германии и сотрудниками МВД России 5 апреля 2022 г. было обнаружено и изъято серверное оборудование, обеспечивающее работу криминального маркетплейса и принадлежащие наркоторговцам криптовалютные средства в сумме, эквивалентной 25 млн долларам США, а 10 апреля 2022 г. следователем управления по расследованию организованной преступной деятельности в сфере незаконного оборота наркотических средств Следственного департамента МВД России в порядке ст. 91 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) был задержан, а в последующем заключен под стражу гр. П., выполнявший преступную роль по поддержке работоспособности платформы Hydra путем администрирования размещенных на ней интернет-ресурсов и предоставления серверного оборудования для ее функционирования. На сегодняшний день противоправная деятельность указанной платформы пресечена [4]. В настоящее время в России в сети Интернет функционируют торговые площадки, расположенные на псевдо-доменах верхнего уровня onion, созданные для обеспечения доступа к анонимным или псевдо-анонимным адресам сети Tor, где представлено множество магазинов с различными видами товаров, производство и (или) реализация которых запрещены законодательством Российской Федерации. На этих площадках подробно разъясняются вопросы организации незаконного бизнеса, в некоторых случаях – осуществления приема на «работу». Для стимулирования пользователей нередко проводятся различные викторины и конкурсы, где в качестве приза используются наркотические средства и криптовалюта. Получаемые денежные средства дают возможность организаторам привлекать к своей деятельности высококлассных специалистов в области технологий и информационной безопасности, врачей, наркологов, юристов и пр. [5, с. 25]. Подобные интернет-ресурсы используются и для распространения информации о новых видах потенциально опасных психоактивных веществ (аналогов и производных наркотических средств, психотропных веществ), которые могут употребляться с целью достижения наркотического опьянения. Доступность в сети Интернет сведений о химических формулах таких веществ способствует синтезированию все новых их разновидностей, которые до установления мер государственного контроля над их оборотом могут реализовываться фактически беспрепятственно [6, с. 4].

Наиболее распространенным объектом осмотра по делам рассматриваемой категории выступает сотовый телефон, с которого осуществлялся обмен данными о месте и способе производства, синтезирования, приобретения, хранения, сбыта, перевозки, хищения или иного незаконного порядка обращения с НС и ПВ. Сложность осмотра сотового телефона обусловлена, во-первых, отсутствием знаний, необходимых для описания аппаратного и программного обеспечения сотового телефона из-за сложности устройств; во-вторых, отсутствием навыков и умений извлечения криминалистически значимой информации

с использованием аппаратно-программных комплексов, например, «мобильного криминалиста» и т.п. Дополнительные трудности при осмотре сотового телефона возникают в связи с необходимостью определения процессуального порядка доступа к тем или иным сведениям, поскольку в ряде случаев при помощи телефона сотрудники получают доступ к сведениям, расположенным на удаленном сервере, что не позволяет именовать такое следственное действие осмотром предмета; кроме того, в отдельных случаях требуется получение судебного решения в связи с ограничением тайны связи [7, с. 75]. Ограничиваясь объемом работы, авторы данной статьи ставят задачу изложить тактику осмотра и процессуальной фиксации сведений, расположенных в электронной памяти сотового телефона.

Осмотр необходимо производить совместно со специалистом в области технологий или информационной безопасности.

Следует помнить, что алгоритм действий приглашенного специалиста и следователя при внешнем осмотре телефона обусловлен состоянием телефона. Так, если на момент осмотра он выключен, то включать его не рекомендуется, так как в нем возможно установлена программа типа «антивор», способная к удалению криминалистически значимой информации и (или) полной блокировке работы телефона. В случае нахождения телефона во включенном состоянии, в последующих действиях следует руководствоваться «Рекомендациями по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров», разработанными ЭКЦ МВД России, Следственным департаментом МВД России и ГУНК МВД России, в которых отражен следующий алгоритм действий:

1) перевести устройство в «авиарежим» для недопущения удаленного стирания информации с устройства;

2) подключить устройство к сети питания (по возможности);

3) установить (со слов задержанного либо иным способом) и внести в протокол пароль доступа к устройству;

4) провести в присутствии понятых сброс паролевой защиты для обеспечения дальнейшего свободного входа в мобильное устройство (в настройках);

5) проверить наличие на устройстве дополнительных «рабочих пространств», предварительно определив расположение в них мессенджеров и прочих сервисов;

6) осуществить проверку сервисов и мессенджеров, находящихся на момент осмотра во включенном состоянии. Отключить в настройках функцию автоматического удаления сообщений. При обнаружении защищенных паролем сервисов и мессенджеров установить пароль и внести его в протокол;

7) зафиксировать переписку и другую значимую информацию путем создания скриншотов (снимков экрана) или фотосъемки изображений на экране осматриваемого устройства;

8) проверить историю установленных на устройстве браузеров в целях определения посещаемых интернет-ресурсов;

9) при выявлении наркоориентированных интернет-ресурсов установить и зафиксировать в протоколе пользовательские логин и пароль для доступа к ним (опции заполнения могут содержаться в настройках устройства);

10) осуществить проверку устройств на наличие так называемых программ-шпионов. В случае обнаружения принять меры для их отключения;

11) осмотреть содержание программ, фиксирующих заметки пользователя, календарей, ежедневников и сервиса «документы» на наличие в них логинов и паролей, а также другой значимой информации. Уделить внимание навигационным программам в целях выявления возможных мест хранения наркотиков (в том числе координат «закладок»);

12) проверить хранилище графических изображений («галерея») на предмет наличия фотографий мест «закладок» и тайников, а также иной информации, способствующей изобличению задержанного в противоправной деятельности [8, с. 17].

При описании внешнего вида телефона в протоколе осмотра следует отразить: наименование, марку, размеры, цвет, конструкцию, материал, из которого изготовлен, модель, характеристику клавиатуры, фоновый рисунок, имя владельца на дисплее, наличие повреждений, украшений или наклеек.

При проведении следственного действия следует установить:

а) IMEI-код устройства, набрав комбинацию клавиш «*#06#»;

б) абонентский номер, однозначно определяющий (идентифицирующий) оконечный элемент сети связи или подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленным в ней (в нем) идентификационным модулем, набрав комбинацию клавиш, определенную оператором связи, либо осуществив звонок на другой абонентский номер, имеющийся в распоряжении, непосредственно во время производства следственного действия;

в) информацию о соединениях между абонентскими устройствами путем создания личного кабинета абонентского номера, используя приложение для мобильных устройств либо веб-версию личного кабинета абонента с целью извлечения детализации разговоров и обмена сообщениями (с письменного согласия владельца);

г) анализ сохраненных Wi-Fi данных устройства (в разделе расширенных свойств имеются данные о MAC-адресе устройства, с которого происходила раздача и выделенный IP-адрес);

д) в разделе «Общая информация» о телефоне, как правило, имеются данные об IP-адресе, MAC-адресе, количестве слотов для sim-карты, видах операторов, определенных устройством, и IMEI-кодах;

е) в приложениях, мессенджерах данные об аккаунте и привязанных банковских картах, в том числе виртуальных электронных кошельках.

Установленный IMEI-код сразу же в ходе осмотра можно перепроверить путем использования специального сервиса на сайте https://www.imei.info/ru. Широкий спектр возможностей позволяет не только удостовериться в действи-

тельности IMEI-кода технического устройства, в отсутствии постороннего вмешательства в программное обеспечение, но и перепроверить в базах данных информацию об утере или его хищении. Полученная информация отражается в протоколе с описанием процедуры получения сведений.

Информация о соединениях между абонентами может быть получена как в ходе осмотра сотового телефона путем использования подключенного личного кабинета, так и направления запроса оператору связи. При направлении запроса следует затребовать дополнительно информацию о базовых станциях с указанием азимутов обслуживания абонента. Кроме того, возможно использование сайтов по предоставлению возможности установления координат базовых станций и определения с помощью карт, размещенных в сети Интернет, расположение абонента на местности, например, www.xinit.ru. Сайт 2ip.ru позволяет определить производителя технического устройства, используемого в преступной деятельности или представляемого доказательственное значение в рамках расследования уголовного дела по факту незаконного сбыта НС и ПВ. Данные об IP-адресе или доменном имени устройства или сайта способствуют получению сведений о провайдере, для получения которых можно использовать, например, сервис, расположенный по адресу https://2ip.ru/lookup.

Аналогичным образом возможно установление и иных данных: модели телефона, производителя, IP-адреса, с которых осуществлялся выход в сеть Интернет, наименования провайдера, осуществляющего доступ в сеть Интернет и обеспечивающего средством связи и др.

На заключительном этапе лицо, производящее следственное действие, подводит его итоги, представляет участникам изъятые предметы и объекты в упакованном виде, обозначает время и дату окончания следственного действия, устанавливает возникшие вопросы, замечания, ходатайства жалобы по ходу, способу и организации проведения осмотра, знакомит с протоколом и результатами фиксации хода следственного действия, устанавливает замечания, ходатайства, заявления, жалобы к качеству и порядку составления протокола.

В завершении отметим, что следователь при производстве осмотра сотового телефона не должен полностью полагаться на помощь специалиста в вопросе обнаружения криминалистически значимой информации. Именно следователь является должным лицом, ответственным за конечный результат осмотра и обеспечение полной сохранности информации при ее извлечении в неизменном виде.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Стратегия государственной антинаркотической политики Российской Федерации на период до 2030 г.» // СПС «КонсультантПлюс» (дата обращения: 01.08.2022).

2. Комплексный анализ состояния преступности в Российской Федерации по итогам 2020 года и ожидаемые тенденции ее развития: аналитический обзор. – Москва: ВНИИ МВД России, 2021. – 72 с.

3. Комплексный анализ состояния преступности в Российской Федерации по итогам 2021 года и ожидаемые тенденции ее развития: аналитический обзор. – Москва: ВНИИ МВД России, 2022. – 76 с.

4. Сотрудники ФСБ задержали наркодилеров с торговой площадки Hudra в даркнете [Электронный ресурс]. – Режим доступа: https://lenta.ru/news/2020/01/17/hydra/ (дата обращения: 12.04.2022).

5. Земцова С.И., Галушин П.В., Карлов А.Л. Участие специалиста и эксперта в расследовании преступлений в сфере незаконного оборота наркотических средств, совершенных с использованием криптовалюты: учебное пособие. – Красноярск: СибЮИ МВД России, 2020. – 88 с.

6. Жданова Е.В., Малиенко А.А., Кузнецов А.Г. и др. Противодействие преступлениям, связанным со сбытом наркотиков, совершаемым бесконтактным способом с использованием информационных, телекоммуникационных и высоких технологий на территории государств – участников СГ: аналитический обзор с предложениями. – Москва: ВНИИ МВД России, 2019. – 36 с.

7. Земцова С.И., Суров О.А., Галушин П.В. Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий. – Москва: Юрлитинформ, 2019. – 208 с.

8. Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров: рекомендации. – Москва: ЭКЦ МВД России, следственный департамент МВД России, ГУНКМВД России, 2020. – 18 с.