Волков А.В. DOI 10.51980/2021_4_56

Автономная некоммерческая организация «Центр судебных экспертиз и научно-технических исследований» (г. Челябинск)

Лужнов В.С.

Автономная некоммерческая организация «Центр судебных экспертиз и научно-технических исследований» (г. Челябинск)

Мобильная криминалистика и своевременная фиксация цифровых следов преступлений

Актуальность своевременной фиксации цифровых следов преступлений обусловлена активным использованием при совершении преступлений, связанных с незаконным оборотом наркотических средств, технологий, предназначенных для дистанционной коммуникации, в рамках которой взаимодействие лиц осуществляется посредством программ для мгновенного обмена сообщениями – мессенджеров[1]. В связи с тем, что современные устройства позволяют использовать ряд паролей и скрытые либо защищенные пространства и папки, необходимо понимать, что существуют несколько видов паролей:

1) шифрование файловой системы устройства (при включении устройства до загрузки операционной системы требуется ввести пароль);

2) блокировка устройства (пароль разблокировки экрана);

3) блокировка приложений устройства (пароль установлен на какое-либо приложение, запрашивается у пользователя при его открытии);

4) сокрытие приложений, файлов и папок (файл, папка или приложение скрыты с рабочего стола и (или) из меню приложений или замаскированы под какое-либо другое приложение (например, «Калькулятор»), посредством специализированного программного обеспечения, установленного на устройстве);

[1] Instant messaging market, 2015-2019 / The Radicati Group, 2015. Available at: http://www.radicati.com/wp/wp-content/uploads/2015/02/ Instant-Messaging-Market-2014-2018-Executive-Summary.pdf (accessed 25 September 2018); Roberts J.J. Here are the most popular apps for secure messages / 2017. Available at: http://fortune.com/2017/01/17/most-popular-secureapps/ (accessed 27 September 2018).

5) использование «вторых пространств» (у некоторых устройств, например у смартфонов Xiaomi, имеется стандартное программное обеспечение, именуемое «вторым пространством», которое активируется с помощью ввода определенного пароля при разблокировке экрана устройства).

Таким образом, сразу после задержания подозреваемого лица необходимо уточнить пароли, используемые задержанным лицом для разблокирования устройства, приложений, установленных на устройстве, и другие пароли безопасности.

Все пароли, которые уточняются в ходе отработки задержанного лица, необходимо фиксировать в письменном виде как в протоколах изъятия, так и в отбираемых объяснениях, рапортах отработки и других материалах ОРД. Также с целью упрощения поиска паролей в ходе следствия рекомендуется фиксировать все пароли на отдельном листе бумаги и прикреплять его к устройству посредством клеевых лент. В будущем такой способ облегчит работу следователя и дополнительно зафиксирует парольные фразы устройства.

Кроме того, в ходе проведения досмотров, осмотров и обысков не стоит пренебрегать различными записками, блокнотами и иными записями, так как в них могут содержаться как оперативно значимые сведения, так и следственно значимые сведения, необходимые для изобличения лиц, причастных к преступной деятельности, в том числе и к ранее совершенным преступлениям.

В 2020 г. ЭКЦ МВД России, Следственный департамент МВД России и ГУНК МВД России издали 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».

Одним из вопросов, рассмотренных в рекомендациях, является «Памятка о порядке действий при обнаружении у подозреваемых лиц коммуникационных устройств». Поскольку от правильного и своевременного сбора информации зависит возможность полноценного и всестороннего проведения оперативных и следственных мероприятий, направленных на раскрытие преступлений, как текущих, так планируемых и ранее совершенных, необходимо раскрыть ее содержание в данной работе.

Таким образом, при проведении изучения мобильных устройств необходимо придерживаться следующего алгоритма.

1. Перевести устройство в «авиарежим», для недопущения удаленного стирания информации с устройства.

2. Подключить устройство к сети питания и до окончания фиксации цифровых следов не дать устройству выключиться.

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

4. Провести в присутствии понятых сброс защиты паролем для обеспечения дальнейшего свободного входа в мобильное устройство (в настройках мобильной операционной системы устройства).

5. Проверить наличие на устройстве дополнительных «рабочих пространств» («рабочих столов»), 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 интернет-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 автоматического заполнения могут содержаться в настройках устройства или интернет-браузера).

10. Осуществить проверку устройства 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.

При невозможности установить парольные фразы устройств требуется незамедлительно направлять такие устройства в ЭКЦ ГУ МВД России для проведения компьютерно-технической экспертизы, в рамках которой специалисты ЭКЦ с большей вероятностью смогут осуществить получение всей информации с мобильного устройства.

В случае если специалисты ЭКЦ не могут получить доступ к мобильному устройству, остается возможность получения всей интересующей информации из устройства при привлечении сторонних организаций, деятельность которых направлена на проведение компьютерно-технических экспертиз. Так, сотрудники АНО (Автономная некоммерческая организация) «ЦНТИ» (Центр судебных экспертиз и Научно-Технических Исследований) неоднократно осуществляли подобные экспертизы, в рамках которых была получена следственно и оперативно значимая информация, которая применялась как в виде доказательной базы, так и для дальнейшего проведения ОРМ.

В качестве заключения необходимо отметить, что при правильном и своевременном фиксировании имеющейся информации, цифровых следов, метаданных, использовании открытых источников для их анализа и поиска информации в совокупности с комплексами оперативно-розыскных мероприятий значительно повышаются шансы на деанонимизацию пользователей, ведущих противоправную деятельность в сети Интернет.

Сбор информации и формирование баз данных будут способствовать эффективному раскрытию как текущих преступлений, так и преступлений из числа прошлых лет. Сведения, полученные из рапортов, формируются в единую базу и используются в служебной деятельности. От качества изложенной в них информации зависит качество базы. Соответственно, рапорта отработки должны содержать исчерпывающую информацию, а именно:

– информацию об используемых задержанным лицом интернет-мессенджерах (данные аккаунта, пароли доступа, данные аккаунтов лиц, с которыми задержанный контактировал при осуществлении преступной деятельности);

– фотохостинги, используемые для передачи изображений (при наличии полные ссылки с полученными и отправленными тайниками с наркотических средств);

– используемые средства анонимизации (VPN, Proxy, удаленные серверы, сервисы шифрованной передачи данных);

– финансовые инструменты, используемые для получения (отправки) оплаты за противоправную деятельность (с указанием банковских карт, используемых криптовалютных кошельков и их адресов, аккаунтов электронных кошельков и различных электронных чеков).