Назаренко И.С.

Белгородский юридический институт МВД России имени И.Д. Путилина

Актуальные вопросы поиска цифровых следов при раскрытии преступлений в сфере незаконного оборота наркотиков

В ходе исследования изъятой компьютерной техники и терминалов связи необходимо уделять пристальное внимание средствам шифрования и сетевой анонимизации. Чаще всего злоумышленниками используется специализированное программное обеспечение для сокрытия персональных данных и активных цифровых следов в сети Интернет.

Как показывает практика, в большинстве случаев злоумышленники используют специализированное программное обеспечение анонимизации «TheOnionRouter» (далее – «Tor»), представляющее собой специально настроенную систему прокси-серверов, направленную на создание анонимного шифрованного сетевого соединения, имеющего защиту от «сетевого прослушивания», следовательно, не позволяющее проводить такие виды оперативно-розыскных мероприятий, как «снятие информации с технических каналов связи» и «получение компьютерной информации». «Tor» представляет собой специальный веб-браузер (созданный на основе «Mozilla Firefox»). При грамотном использовании «Tor» злоумышленники сохраняют анонимность при посещении и администрировании информационных ресурсов, учетных записей социальный сетей, каналов, использовании мессенджеров и электронной почты, в том числе при работе со специальными приложениями, использующими трафик сети Интернет. К данной группе также относятся программы, обеспечивающие защищенный обмен сообщениями, использующие криптографические технологии. Например, «Telegram» и «Jabber» (при использовании расширений OTR2). Стоит отметить, что помимо обеспечения анонимности в сети Интернет злоумышленники активно используют средства криптографии для того, чтобы затруднить или сделать невозможным доступ к информации, хранящейся на персональном компьютере, для сотрудников правоохранительных органов. Наиболее распространенным криптографическим программным обеспечением является «PGP» (имеются версии для операционных систем семейств «Windows» и «Mac OS») и ее свободный аналог «GPG» (для большинства распространенных операционных. В быту часто используется термин «мессенджеры», а также «VeraCrypt» или «TrueCript» (для организации шифрованного раздела на жестком диске или флэш-накопителе, в том числе скрытого).

Цифровые следы являются совокупностью уникальных цифровых артефактов, обнаруженных в процессе исследования информации, содержащейся в памяти технического устройства, которые в дальнейшем могут быть использованы в качестве доказательств в рамках следствия, дознания, а также судебного разбирательства. Исследование технических устройств в рамках как доследственной проверки, так и в рамках возбужденных уголовных дел позволяет обнаруживать и фиксировать цифровые следы рассматриваемых компьютерных инцидентов и различных правонарушений. Грамотно спланированное и проведенное исследование информации позволит восстановить хронологию инцидента информационной безопасности, установить причины его возникновения, а самое главное – получить необходимую оперативно-значимую информацию, позволяющую установить злоумышленника (MAC-адреса, IP-адреса сетевого интерфейса, используемые сервера, адреса электронной почты, доменные имена, возможные учетные записи и т.д.).

Процесс криминалистического исследования компьютерных систем включает в себя ряд типовых этапов:

– идентификация (получение информации об инциденте, определение скомпрометированных цифровых устройств и наилучших источников потенциальных цифровых доказательств);

– изъятие цифровых носителей, связанных с расследованием; создание образов (копий) изъятых носителей информации;

– верификация неизменности свидетельств в процессе сбора (расчет хэш-значений);

– анализ – поиск артефактов, которые могут подтвердить или опровергнуть поставленные расследованием вопросы, в ходе анализа должна обеспечиваться неизменность цифровых свидетельств);

– формирование отчета, содержащего сделанные в ходе анализа выводы;

– сохранение (защита собранных свидетельств их от любых изменений или удаления)[1].

По рассматриваемой категории преступлений возникает необходимость в производстве как осмотра места происшествия (места закладок, места расположения терминалов оплаты, рабочего места оператора, кассира и т.д.), так и осмотра различных предметов (наркотических средств, компьютеров, сотовых телефонов, планшетов и иной компьютерной техники), что объясняется спецификой рассматриваемой категории дел. В связи с тем, что данные преступления совершаются посредством использования информационно-коммуникационных технологий, в ходе осмотра места происшествия необходимо предпринимать усилия к обнаружению технических устройств, компьютерной техники, периферийного оборудования, терминалов связи, интегрированных и съемных носителей информации (накопителей на жестких магнитных дисках, оптических и флеш-накопителей). Осмотр и изъятие вышеуказанных технических устройств и накопителей информации следует осуществлять с участием специалиста в области информационных технологий или информационной безопасности. В рамках осмотра места происшествия, следственных действий, а также хранения не следует подвергать осматриваемые электронные носители информации воздействию высоких или низких температур, сильных электромагнитных полей. Их источниками могут быть сильные магниты, магнитные дактилоскопические порошки и кисточки, линии электропередач, микроволновые печи с поврежденным корпусом, рентгеновские устройства (например, досмотровые или поисковые). Носители информации, признанные вещественными доказательствами по уголовному делу, необходимо хранить в защищенных хранилищах и упакованными способом, исключающим доступ к ним без нарушения целостности упаковки.

В рамках совершенствования деятельности по противодействию организованным преступным группам, совершающим преступления в сфере незаконного оборота наркотиков, необходимо:

– совершенствовать деятельность специализированных следственно-оперативные групп по раскрытию данного вида преступлений, в том числе активно использовать новые методы поиска и документирования цифровых следов;

– совершенствовать методы мониторинга социальных сетей, различных каналов и сообществ, а также иных сегментов сети Интернет, во взаимодействии с подразделениями Роскомнадзора блокировать информационные активы злоумышленников;

– совершенствовать методы борьбы с анонимизацией сетевого трафика.

Дальнейшее развитие технологического потенциала сотрудников органов внутренних дел и внедрение новейших информационных технологий в области обнаружения и изъятия цифровых доказательств станет важным шагом к предупреждению и пресечению наркопреступлений, которые на протяжении многих лет являются одной из главных проблем безопасности не только Российской Федерации, но и мирового сообщества.

Натейкина Н.А.

Бурятский государственный университет имени Доржи Банзарова (г. Улан-Удэ)

Инновационные подходы к проверке версий о невиновности по делам о присвоении и растрате

Проверка версий о невиновности обвиняемого по делам о присвоении или растрате (ст. 160 УК РФ) является важнейшим элементом расследования, обеспечивающим действие презумпции невиновности (ст. 14 УПК РФ). Традиционно органы предвари-

[1] Васильева И.Н. Обеспечение готовности организации к инцидентам информационной безопасности в условиях цифровой экономики // Инновационные технологии и вопросы обеспечения безопасности реальной экономики : сборник научных трудов по итогам всероссийской научно-практической конференции, Санкт-Петербург, 27 марта 2020 г. / под ред. Г.В. Лепеша, О.Д. Угольниковой, С.Ю. Александровой. СПб. : Санкт-Петербургский государственный экономический университет, 2020. С. 267-276.