Секция «Криминалистика»

Криминалистическое исследование информации пользователей, содержащейся в облачных хранилищах

Научный руководитель – Жидков Дмитрий Николаевич

Вайберт Наталия Антоновна
Студент (специалист)
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Санкт-Петербург, Россия
E-mail: tasha.vaybert@mail.ru

Преступления, совершаемые в киберпространстве, уже не считаются редкими, процент таких деяний с каждым годом возрастает. Исходя из официальных статистических данных, содержащихся в «Сведениях о состояния преступности в России за январь-ноябрь 2018 года», размещенных на сайте МВД России, преступлений с использованием компьютерных и телекоммуникационных технологий было зарегистрировано 156 307, из них раскрыто 38 773, преступлений в сфере компьютерной информации - 2 357, раскрыто - 525, преступлений экономической направленности, совершенных с использованием компьютерных и телекоммуникационных технологий зарегистрировано 9 416, раскрыто - 3 514, преступлений на транспорте, совершенных с использованием компьютерных и телекоммуникационных технологий зарегистрировано 2 977, из них было раскрыто 1 651. [1]

Проведенный нами анализ статистических данных по рассматриваемой категории преступлений, позволяет сделать вывод о стремительном, повсеместном, росте регистрации таких преступлений и все более меньшему уровню их раскрываемости. Раскрываемость преступлений исследуемой группы в процентном соотношении с количеством зарегистрированных таких преступлений в 2015 составила - 50,9 %, в 2016 - 51,6 %, в 2017 - 22,5%, в 2018 - 24,8% .

Сегодня, по нашему мнению, перед всей российской правоохранительной системой стоит очень важная задача - научиться выявлять, раскрывать и пресекать наступление исследуемых событий. В условиях развития доказательственного значения судебных экспертиз, огромную роль в этих процессах правоприменители возлагают на различные ведомственные судебно-экспертные учреждения.

Судебная компьютерная экспертиза сейчас находится в пике своего развития, несомненно, существует масса экспертных задач требующих скорейшего разрешения. В нашей статье нам бы хотелось остановиться на такой актуальной экспертной задаче как «извлечение данных из облачного хранилища». В настоящее время такие технологии хранения информации стали достаточно популярными. На сегодняшний день самыми востребованными на рынке облачных хранилищ являются Dropbox, Google Drive, Яндекс. Диск, iCloud, OneDrive, Облако@mail.ru. Стремительное развитие облачных сервисов, увеличение их количества и улучшение качества свидетельствуют о том, что эти технологии будут использоваться продолжительное время. Удобной моделью использования хранилища является та, при которой первично данные размещаются на накопителе (в памяти устройства), затем синхронизируются с облачным хранилищем, после чего удаляются с устройства, сохраняясь в облаке.

Облачное хранилище данных — модель онлайн-хранилища, в котором файлы хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. [3]

Из-за огромной популярности использования облачных сервисов как средств хранения данных, в том числе и о совершенных либо планируемых преступлениях, возникла необходимость в подробном анализе этих технологий. В мире в последние годы стала активно развиваться облачная криминалистика, где цифровая криминалистика начинает сливаться с онлайн-расследованиями и криминалистическими исследованиями программного обеспечения с открытым исходным кодом. При быстром и эффективном доступе облачные доказательства оказываются единственной «зацепкой» в цифровом расследовании уголовных и гражданских дел. Однако в нашем государстве на данный момент юридически правоотношения по исследованию информации, содержащейся в облачных сервисах, не сформированы, механизмов использования полученных при таких исследованиях сведений нет.

В международной практике использование данных из облачных хранилищ является одним из самых популярных методов расследования следующих групп преступлений: мошенничество, изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, террористический акт.

Неопытные преступники при совершении преступления оставляют следы в так называемом облаке. Например, в практике известен случай, когда мужчина занимался изготовлением и распространением файлов детской порнографии, удалив фото и видео с мобильного устройства, забыв, что они были сохранены в облачном хранилище, при этом же были обнаружены диалоги, в которых он прикреплял файлы детской порнографии за перевод ему на карту денежных средств. Эта ошибка помогла правоохранительным органам раскрыть преступление и привлечь гражданина к уголовной ответственности согласно п. «г» ч. 2 ст. 242.1 УК РФ.

Некоторые из программ, позволяющих экспертам-криминалистам извлекать и анализировать информацию из облачных хранилищ, мы рассмотрим более подробно в этой статье и раскроем их функционал.

Разработчик Cellebrite UFED Cloud Analyzer заявляет в своих функциональных возможностях следующее: программа предоставляет компьютерным экспертам мгновенное извлечение, сохранение и анализ учетных записей, социальных сетей и облачных хранилищ, извлечение данных с мобильных устройств; обеспечение сохранности криминалистических данных; визуализаю данных в едином формате; создание отчетов об использовании и экспорте интересуемых данных.[2]

Помимо этого он позволяет унифицировать и организовывать разрозненные данные в единую форму, передавать и интегрировать данные для последующего анализа. В настоящее время программа позволяет извлекать информацию из следующих источников: Google Drive; Dropbox; Данные о местоположении Google; Gmail; Twitter; Facebook; Kik Messenger.

Указанный аппаратно-программный комплекс позволяет автоматически собирать существующие облачные данные и метаданные и упаковывать их таким образом, чтобы впоследствии они могли быть использованы в суде. Благодаря этой программе ускоряется сам процесс расследования киберпреступлений, с ее помощью следователь может получить ответы на многие вопросы, интересующие следствие.

До недавнего времени было сложно извлекать данные из облачного хранилища мобильных устройств Apple. Ни для кого не секрет, что эта американская компания постоянно работает над усилением безопасности своей мобильной платформы, а также сервиса iCloud. С появлением российской программы Elcomsoft Phone Breaker и обходом систем двухфакторной аутентификации стало возможно извлечение информации из «облака» подозреваемого в совершении преступления.

«Мобильный криминалист» способен извлекать и анализировать данные из различных

облачных сервисов. Экспертам-криминалистам для доступа к информации необходима аутентификация. Программа позволяет работать с iCloud, Google, Microsoft, мобильные хранилища, почтовые сервисы и дроны, всего она имеет доступ к 55 облачным сервисам.

Например, «Яндекс. Почта», распространенный среди российских интернет-пользователей облачный сервис. Здесь доступ к информации осуществляется с помощью следующих методов: по логину и паролю, по OAuth-токену, по прохождению двухфакторной аутентификации.

Комплекс может извлекать следующие данные из «Яндекс. Почты»: имя и ID пользователя, логин, адрес почты, является ли аккаунт сотрудника Яндекса, страна и регион, а также их телефонные коды, страна регистрации аккаунта, время регистрации, день рождения пользователя, информация о контактах, помимо этого данные из полученных писем.

Все эти программы способны взламывать почти любые телефоны, добираться до облачного хранилища и анализировать его. К сожалению, в России данные технологии ещё не нашли своего широкого применения. На сегодняшний день все так же сложно проникнуть в мобильный телефон, не зная пароля от него. Все это влияет на процент раскрываемости подобных преступлений. В ходе интервьюирования с начальником отделения 6 отдела СЧ по РОПД ГСУ ГУ МВД России по Санкт-Петербургу и Ленинградской области майором юстиции Лисенковым Дмитрием Евгеньевичем была получена информация: «из-за невозможности доказать, что именно этот человек видоизменял или загружал документ в облако, извлечённые данные из серверного хранилища чаще выступают косвенными доказательствами».

Подводя итог вышесказанному, хочется отметить, что киберпреступления являются популярными, но в то же время трудно раскрываемые. Хотя доказательства могут лежать перед нами, мы не можем ими завладеть, так как современное оборудование не позволяет экспертам проникнуть в заблокированный телефон или облачное хранилище. Поэтому считаю немаловажным изобрести новые подходы к извлечению информации из мобильных устройств.

При видимости наличия реальных возможностей по использованию, указанных в статье аппаратно-программных комплексов на практике у сотрудников экспертно-криминалистических подразделений России, в связи международной санкционной политикой ограничивающей права Российской Федерации, существует огромное количество как организационных проблем по закупке такого оборудования, так и масса правовых проблем по регламентации использования полученной такими комплексами информации.

Источники и литература

1) МВД России ФКУ «Главный информационно-аналитический центр»: Состояние преступности в России за январь-ноябрь 2018 года.

2) Исследование облачных хранилищ при расследовании преступлений: https://www.anti-malware.ru/analytics/Technology_Analysis/analysis_cloud_storage_investigation_of_crimes#part2

3) Облачное хранилище данных: https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D0%B0%D1%87%D0%BD%D0%BE%D0%B5_%D1%85%D1%80%D0%B0%D0%BD%D0%B8%D0%BB%D0%B8%D1%89%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85