ня СЭД – сістэмна высокатэхналагічны працэс атрымання комплекснай доказнай інфармацыі з матэрыяльна адлюстраваных следавых сістэм у выглядзе аптымізаванай судова-экспертнай інфармацыі.

У перспектыве развіццё тэхніка-крыміналістычнага забеспячэння павінна перайсці з матэрыяльнага на інтэлектуальны ўзровень працэсу атрымання і апрацоўкі КЗІ. Яно павінна выглядаць не як сістэма асобных набораў і камлектацыйных сродкаў, а як комплекс тэхналагічных сістэм, дзе тэхнічнымі сродкамі атрымання КЗІ павінны быць не тэхніка-крыміналістычныя сродкі суб'ектыўнага выбару, а тэхналагічныя сістэмы зняцця КЗІ ў залежнасьці ад суб'ектаў, кірункаў і ўзроўню іх дзейнасці з улікам сітуацыйнага змянянення характару вырашэння крыміналістычна абумоўленых задач.

Пераход ад аналагавага да лічбавага этапу фарміравання высокатэхналагічнага працэсу атрымання доказнай інфармацыі будзе прадугледжваць не толькі менш выдатковую сістэму выкарыстоўваемых сіл і сродкаў, але і якасна іншую ступень яе даказнасці і паўнаты, дасць магчымасць аўтаматызацыіі працэсу атрымання КЗІ і распрацоўкі метадалагіна абгрунтаванай сістэмы першапачатковай яе апрацоўкі, уніфікацыі гэтага працэсу з сістэмай экспертнага ўзроўню атрымання доказнай інфармацыі [2, с. 85–87].

Гэта дазволіць у найбольшай ступені наблізіцца да інфармацыйнага ўзроўню атрымання, апрацоўкі і выкарыстання КЗІ. Лакальная і комплексная апрацоўка і выкарыстанне КЗІ ў сеткавым фармаце (у тым ліку і для вырашэння вышуковых задач і пры ўмове прававога замацавання гэтага працэсу) магчыма на аснове аўтаматызаванай інфармацыйна-вышуковай сістэмы паўнавартнага аўтаматызаванага атрымання КЗІ. Вынаснымі сродкамі сістэмы атрымання КЗІ будуць працуючыя ў сеткавым фармаце ноўтбукі з пераферыйнымі сродкамі зняцця, аналізу, апрацоўкі, перадачы і атрымання інфармацыі ў патрэбных аб'ёмах і формах. Гэта дазволіць не толькі ўдасканаліць працэсс на метадалагічна абгрунтаванай аснове атрымання КЗІ, але і на тэхналагічным узроўні забяспечыць магчымасць інфармацыйнага ўзроўню выкарыстання доказнай значнасці ўсіх відаў КЗІ ў вышуковым і ў доказным іх значэнні як інфармацыйна насычаных сістэм.

1. Ренер Н.А. Тенденции развития криминалистики в XXI веке: об итогах некоторых научных дискуссий // Эксперт-криминалист. 2014. № 2.

2. Гучок А.Я. Кірункі ўдасканалення тэхніка-крыміналістычнага забеспячэння дзейнасці праваахоўных органаў // Уголовный процесс и криминалистика: история и современность : Криминалистические чтения памяти заслуженного деятеля науки, доктора юридических наук, профессор Н.И. Порубова : материалы Междунар. науч.-практ. конф. (Минск, 3 дек. 2015 г.) : в 2 ч. Ч. 2 / редкол.: М.П. Шруб (отв. ред.) [и др.]. Минск : Акад. МВД, 2015.



УДК 343.985

***И.Г. Мухин***

## СОВРЕМЕННЫЕ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИЕ СРЕДСТВА ИССЛЕДОВАНИЯ ИНФОРМАЦИИ, РАЗМЕЩЕННОЙ В ОБЛАЧНЫХ ХРАНИЛИЩАХ

Облачные технологии нередко называют технологиями будущего. Однако пока неясно, насколько это будущее будет «безоблачным» для правоохранительных органов.

Новые компьютерные технологии постоянно внедряются в жизнь современного общества. Они призваны облегчить использование информации и обмен ей. Такие технологии, оптимизируя деятельность обычного пользователя в интернет-среде, часто осложняют работу правоохранительных органов по раскрытию и расследованию преступлений. Так, например, графическая и биометрическая системы блокировки смартфонов повысили их безопасность и одновременно затруднили их криминалистическое исследование.

Аналогичной видится ситуация с активным использованием современными пользователями облачных технологий.

Облачное хранилище данных (англ. cloudstorage) – модель хранения данных в компьютерных сетях, при которой размещение контента осуществляется на различных серверах (сети взаимосвязанных между собой серверов), определенный объем пространства которых предоставляется в пользование клиенту. Для того чтобы начать пользоваться облачным хранилищем данным, необходимо установить на свое средство компьютерной техники программу-клиент, зарегистрироваться на сайте поставщика облачных услуг (наиболее популярные: Яндекс. Диск, облако@mail.ru, GoogleDrive, Dropbox, OneDrive, iDrive), выбрать себе имя пользователя и пароль, указать, какую информацию необходимо загрузить в облачное хранилище.

Следует учитывать, что некоторые данные о пользователе загружаются в облако автоматически, без уведомления пользователя.Так, например, при использовании некоторых программных продуктов от компании Google от пользователя требуется согласие на синхронизацию его устройства (смартфон, планшет, ноутбук) с системой GoogleLocation. После этого указанная система автоматически собирает и хранит информацию о местонахождении пользователя (отметки на карте Google – каждые 5 мин) и о выполняемых им действиях (исходящие звонки, использование камеры смартфоны и т. д.). Казалось бы, такая деятельность поставщиков облачных услуг помогает правоохранительным органам, однако это не совсем так. Остановимся на про-

блемах, связанных с расследованием преступлений, при условии использования подозреваемыми облачных технологий.

1. Проблема определения владельца информации. Организации – владельцы облачных хранилищ не несут ответственности за контент (информацию), размещенный на их серверах третьими лицами, т. е. не являются ее владельцами, несмотря на то, что владеют накопителями, на которых эта информация хранится. Если подозреваемый не даст признательных показаний о том, что та или иная информация размещена в облаке им самим, доказать обратное практически невозможно. Теоретически сотрудники правоохранительных органов могут запросить у владельца облачного ресурса информацию о том, с какого IP-адреса загружены в облако интересующие их данные и таким образом доказать, что это сделал именно подозреваемый. Но на практике ждать такого ответа приходится от полугода до двух лет либо не приходится вовсе.

Даже если эксперт обнаруживает информацию, аналогичную размещенной в облаке, доказать, что такая информация загружена подозреваемым, а не третьим лицом, имеющим доступ к облачному хранилищу, по причинам, указанным выше, весьма затруднительно.

2. Проблема получения доступа к облачному хранилищу. В настоящее время возможны два способа получения доступа к чужому облачному хранилищу: ручной и автоматический. Для осуществления ручного доступа сотруднику правоохранительного органа необходимо знать логин (имя пользователя или адрес его электронной почты) и пароль. Получить указанные реквизиты можно как непосредственно у самого подозреваемого (например, в ходе допроса), так и в процессе осмотра принадлежащего ему средства компьютерной техники, с которого осуществляется доступ к облаку. Извлечение данных из облачного хранилища можно также производить как вручную, так и автоматически, т. е. либо самостоятельно копировать все обнаруженные в облаке файлы на служебный компьютер, либо воспользоваться специально разработанным программным продуктом, например таким как «Мобильный криминалист» от компании Oxygen. Второй способ выглядит более предпочтительным, так как позволяет извлекать скрытые и удаленные файлы. Возможностью же полностью автоматического доступа к информации, хранящейся в облачном хранилище, в настоящее время обладают аппаратно-программные комплексы UFED (UFEDTouch, UFEDTK – аппаратно-программные; UFED 4PC – программный) от компании Cellebrite. Указанные комплексы самостоятельно обнаруживают на изъятом у подозреваемого мобильном устройстве (смартфон, планшет) реквизиты доступа к облаку, подключаются к нему и извлекают всю информацию.



Таким образом, используя возможности доступа к облачным хранилищам, правоохранительные органы могут получить информацию о местонахождении и деятельности подозреваемого в конкретное время, а также извлечь и исследовать данные, которые подозреваемый пытался скрыть путем размещения их на удаленном сервере. В то же время доказывать принадлежность указанной информации подозреваемому придется, скорее всего, традиционными криминалистическими средствами.

УДК 343.985

***М.Г. Серпучёнок***

## АКТУАЛЬНЫЕ ВОПРОСЫ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ОТТИСКОВ ПЕЧАТЕЙ

Оттиск печати – неотъемлемый реквизит документа, требующего особого удостоверения его подлинности. Она является одним из наиболее эффективных средств защиты документа от подлога.

В большинстве случаев преступления в экономической и других сферах деятельности совершаются с использованием подложных документов, содержащих оттиски печатей.

Стремительное проникновение компьютерной техники практически во все сферы деятельности человека (в том числе и противоправную), ее общедоступность и постоянное совершенствование, расширение возможностей современных технологий по изготовлению удостоверительных печатных форм (фотополимерная технология, гравирование лазером по резине и т. д.), позволяют даже в домашних условиях, при наличии несложного оборудования, изготовлять без особого труда и в кратчайший срок печатные формы, в том числе копии клише с подлинных оттисков. Данные обстоятельства существенно упрощают возможность изготовления высокоточных дубликатов клише печатей с воспроизведением как общих (форма, размер, содержание), так и частных признаков оригинала клише (искривления, изломы, утолщения элементов, особенности микрорельефа печатающей поверхности) и усложняют работу экспертов при решении идентификационных задач, основанных на таких положениях, как «познание индивидуального (случайного) основано на исследовании закономерного. Чтобы выявить случайные, а потому и индивидуализирующие данный предмет свойства, нужно отграничить их от свойств, обусловленных закономерностями данного явления» [1, с. 270]. Это приводит к снижению значимости удостоверительных печатных форм как средств защиты от подлога.