ние и расследование таких противоправных деяний, обусловливая высокий уровень их латентности.

Интенсивность разработки схем мошенничеств, совершаемых при помощи информационных технологий, недостаточность опыта и сил в данном направлении борьбы с преступностью, еще не позволяет в достаточной мере противостоять данному виду преступлений.

Современные преступники, разрабатывая различные схемы совершения мошенничеств, совершаемых с использованием информационных технологий, используют достижения научно-технического прогресса, активно используются знания в области компьютерной техники и программирования. Для получения большей выгоды и применения более изощренных способов совершения мошенничеств криминальные субъекты объединяются в устойчивые преступные группы, носящих часто транснациональный характер, при этом жертвой преступных деяний может стать любое физическое или юридическое лицо, государственная и негосударственная организация.

В настоящее время оперативные сотрудники применяют рекомендации по выявлению мошенничества, которые по своей структуре сходны с мошенничествами, совершаемыми с использованием информационных технологий, однако имеют иную специфику. Данные обстоятельства определенным образом сказываются на снижении способности правоохранительных органов своевременно выявлять и раскрывать факты совершенного преступления.

Борьба с мошенничеством, совершенным с использованием информационных технологий, будет возможна лишь тогда, когда правоохранительные органы будут вооружены научными положениями и разработанными на их основе практическими рекомендациями по выявлению и расследованию данного вида преступлений.

Очевидно, что случаи мошенничества, совершенного с использованием информационных технологий, были зафиксированы и ранее, тем не менее совершалось оно не так часто, как в настоящее время. Различные исследователи осуществили попытки изучения данной темы, однако рассматривали только отдельные элементы проблем выявления мошенничеств, совершаемых с использованием информационных технологий. Таким образом, актуальность темы обусловливается рядом проблем теоретического и прикладного характера. В настоящее время необходимо решить много научно-практических задач совершенствования деятельности органов внутренних дел Республики Беларусь, направленных на выявление мошенничеств, совершенных с использованием информационных технологий:

требуется более полное изучение анализа правовых основ и современного состояния практики;

необходимо разработать криминалистическую характеристику данного вида преступлений;

рассмотреть способы совершения;

выделить организационные и тактические особенности;

разработать научно-практические рекомендации по проведению (организации) следственных действий, оперативно-розыскных и иных мероприятий при выявлении и раскрытии преступлений.

УДК 004 + 343

В.А. Кудинов, кандидат физико-математических наук, доцент, профессор кафедры информационных технологий и кибербезопасности Национальной академии внутренних дел (г. Киев, Украина)
kafedra@i.ua

СОВРЕМЕННЫЕ ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ АНАЛИЗА ЦИФРОВЫХ ФОТОГРАФИЙ, КОТОРЫЕ МОГУТ ИСПОЛЬЗОВАТЬСЯ В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Сегодня мы наблюдаем высокий уровень использования гражданами возможностей современных информационных технологий в своей повседневной деятельности, в частности, активное создание ими цифровых фотографий и их публикацию в соцсетях, сохранение в своих средствах мобильной связи и вычислительной техники. Работники правоохранительных органов для эффективного противодействия компьютерной преступности могут использовать ряд современных программных средств для анализа цифровых фотографий, а именно: подлинности, даты, времени и месте создания, технического устройства съемки и сведений о человеке.

Цифровая фотография, по сути, – это программный файл, в котором, кроме информации о самом изображении, сохраняется информация о том, как оно было сделано. Эта информация называется метаданные фотографии. Метаданные размещаются в своих специальных разделах, как, например, «Свойства файла», EXIF, IPTC и других, необходимых при хранении фотографий. Метаданные фото – информация, полезная в обычном случае, но опасная для тех, кто хочет обеспечить себе максимальную анонимность. Так называемые EXIF-данные могут рассказать не только о параметрах фотоаппарата/смартфона, из которого бы-

ла сделана фотография, но и многое другое (дату создания, геолокацию, информацию о владельце фото и т. д.).

Существует множество способов выяснить EXIF-данные фотографии, независимо от того, кто ее владелец и где ее местонахождение. Среди этих способов наибольшей популярностью пользуются варианты с браузером, средствами Windows и онлайн-сервисами. Рассмотрим их более подробно.

1. *С помощью браузера*. Поиск информации по фотографии с помощью браузера, пожалуй, самый простой и доступный способ. Чтобы узнать нужные данные про фото, можно использовать: 1) для Google Chrome – нужно установить расширение Exponator или Exif Viewer; 2) для Internet Explorer – нужно скачать приложение IExif. После установки расширения достаточно лишь навести курсор на любое фото, чтобы получить необходимую информацию; 3) для Mozilla Firefox – браузер поддерживает удобные расширения Exif Viewer или FxIF для распознавания метаданных фото.

2. *С помощью средств Windows.* Необходимо кликнуть правой кнопкой мыши по фото, выбрать команду «Properties» и найти в окне вкладку «Details», где можно узнать параметры фото, ее геолокацию, дату и другие данные.

3. *С помощью онлайн-сервисов.* Они позволяют быстро узнать EXIF-данные фото. Достаточно лишь загрузить фотографию на сервис или указать прямую ссылку на нее, а все остальное он сделает сам.

Findexif.com – бесплатный сервис. Минимум функционала и простота в использовании (в нем нет возможности загрузить фотографии, сервис работает только со ссылками). Предоставляет EXIF-данные.

Fotoforensics.com – сайт, который может обнаружить error level analysis (ELA), т. е. «дорисованные» области на изображении или вставленные в него при редактировании. После обработки программа выдает фотографию, где редактируемые фрагменты будут выделяться на фоне других. Кроме того, программа также предоставляет EXIF-данные фотографии.

Jeffrey's Exif Viewer – бесплатный сервис, который позволяет определить происхождение фотографий и изображений. С его помощью можно узнать EXIF-данные. Преимущество сервиса в том, что он позволяет изучить изображение как по ссылке из сети Интернет, так и загрузив его с компьютера.

Google Search by Image – обратный поиск изображений: загрузив фото, можно отследить первоисточник, а также выяснить, где она еще публиковалась.

TinEye – этот инструмент работает по принципу Google Search by Image.

JPEGSnoop – программа, которая устанавливается на компьютер (работает только в Windows) и позволяет смотреть метаданные не только изображений, но и форматов AVI, DNG, PDF, THM. Программу можно использовать для многих целей: позволяет увидеть, редактировалось ли изображение, выявить ошибки в поврежденном файле и т. п.

Рассмотрим особенности установления места съемки. Если информация о геолокации есть в метаданных, то она может помочь с предельной точностью установить место съемки. Но в то же время наличие данных о геолокации зависит от нескольких факторов. Во-первых, от устройства, которым была сделана фотография. В некоторых камерах или мобильных устройствах может не быть GPS-датчика, который фиксирует координаты. Во-вторых, от желания пользователей мобильных устройств – они могут отключить геолокацию из соображений приватности или уменьшения нагрузки на аккумулятор. В-третьих, наличие таких данных зависит от ресурса, на котором фотография была опубликована. Социальные сети Facebook, Twitter или Instagram удаляют метаданные из самих фотографий во время загрузки на серверы этих ресурсов. Но в то же время они могут непосредственно показывать информацию о местонахождении автора фотографии, если он дал доступ к GPS-датчику своего мобильного устройства.

Иногда возникает необходимость в изменении EXIF-данных фото. Самый простой способ удалить скрытые данные в фото – использовать системные инструменты Windows. Для этого необходимо кликнуть правой кнопкой мыши по фотографии, выбрать команду «Properties» и найти в окне вкладку «Details». Кликнуть внизу пункт «Удаление свойств и личной информации». После этого на вкладке можно самостоятельно выбрать данные, которые нужно удалить. Если нежелательно потерять эти данные, то можно создать копию фотографии с удаленными EXIF-данных, сохранив при этом оригинал.

Наименее требователен к профессиональным навыкам способ – использовать онлайн-сервисы. Хорошим примером такого сервиса является *IMGonline*, который позволяет быстро выбрать нужные данные и заменить их необходимыми параметрами. Копирование всех встроенных метаданных из одной фотографии в другую происходит без сжатия и потери качества.

Таким образом, нами проведен анализ современных программных средств для анализа метаданных цифровых фотографий, которые могут использоваться в борьбе с компьютерной преступностью.