Бедеров И.С.[1] DOI 10.51980/2021_4_60

Отдел специальных разработок Технопарка Санкт-Петербурга

Новая система идентификации электронно-цифровых следов в оперативно-розыскном противодействии наркопреступности

В современных исследованиях предпринимаются безуспешные попытки дать определение такому понятию, как «киберпреступность», обозначить его границы. Мы будем оперировать таким термином, как «преступления, совершенные с использованием информационно-телекоммуникационных технологий» (далее – ИТП), который был введен в обиход в 2017 г. с подачи бывшего генпрокурора России Юрия Чайки. Термин этот является собирательным и охватывает различные виды противоправных действий преступников. Но общим критерием его является то, что преступление совершается с использованием программно-аппаратных средств и телекоммуникационных сетей различных типов.

За последние 7 лет число ежегодно регистрируемых ИТП выросло в 45 раз с 11 тыс. в 2013 г. до 500 тыс. в 2020 г. Доля таких преступлений от общего числа регистрируемых преступлений в стране сегодня достигает 30%. Однако это еще не предел. По мнению сотрудников правоохранительных органов, ИТП имеют значительный потенциал к дальнейшему росту, а реальное их число может быть больше официальных данных в 3 раза. Раскрываемость ИТП постоянно падает и на этот год не превышает 22%, а по отдельным видам ИТП, таким как кибермошенничество или виртуальный терроризм, не превышает 9%.

Торговля наркотиками в сетевом пространстве в настоящее время является основным видом преступной торговли. Представители правоохранительных органов Евросоюза отметили в последние годы значительное увеличение количества дел, связанных с наркоторговлей. В России, по данным МВД, в 2020 г. рост числа преступлений, связанных с незаконным оборотом наркотиков, увеличился на 66% по сравнению с 2019 г.

Сеть предоставляет колоссальные возможности для глобальной экономики и социального процветания. Однако она одновременно создает и существенные проблемы для правоохранительной

[1] Основатель и владелец российской компании Интернет-Розыск, создатель ряда аналитических продуктов, предназначенных для предупреждения и расследования преступлений, совершаемых посредством использования информационно-телекоммуникационных технологий.

деятельности. Сеть представляет собой новый вид реальности – киберпространство, в котором классическая криминалистика уже не работает. В киберпространстве невозможно собрать отпечатки пальцев или образцы ДНК, провести трасологическую или иную экспертизу. Современный уклад жизни требует создания в стране принципиально новой системы криминалистического учета и идентификации, предназначенной для использования в киберпространстве.

В качестве объекта криминалистической регистрации следует использовать те идентификаторы электронных устройств пользователей, которые остаются при посещении ими любого интернет-ресурса (модель устройства, версия операционной системы и браузера, языковые и экранные параметры, IP-адрес и иные параметры соединения, авторизованные аккаунты электронной почты и социальных сетей, рекламные и иные идентификаторы). В своей совокупности эти идентификаторы позволяют установить и выделить уникальное устройство не менее чем из 40 млн прочих. На базе ОСР Технопарка Санкт-Петербурга в начале 2020 г. петербургской компанией «Интернет-Розыск» был создан прототип такой разработки, а также целая линейка других продуктов, использующихся сегодня в правоохранительной деятельности и имеющих соответствующие рекомендации.

Новая система криминалистической идентификации может стать основой для организации государственного предприятия – бюро криминалистической регистрации и учета электронно-цифровых следов, которое станет основным поставщиком информации для всех субъектов оперативно-розыскной деятельности. Потенциал изучения электронно-цифровых следов пользователей представляется значительным: от идентификации киберпреступников и составления портретов пользователей сети до формирования информационного среза общества, его интересов и ожиданий. Их использование позволит создать эффективный инструментарий для расследования широкого спектра правонарушений, совершаемых с использованием высоких технологий, а применение сквозной аналитики данных сделает его доступным для широкого спектра сотрудников правоохранительных органов. Расследование ИТП с применением новой системы идентификации будет лишено таких существенных проблем, как затянутость сроков получения данных от операторов связи и владельцев интернет-ресурсов, урезанность предоставляемой ими информации, отсутствие возможности перекрестного анализа.

Инновации, безусловно, не позволят отразить абсолютно все угрозы. Однако они могут помочь полиции отражать угрозы более эффективно, быстро и с меньшими финансовыми потерями. Полицейским сегодня необходимо не просто идти в ногу со временем, а

опережать преступников в инновационном развитии. Это не представляется возможным без организации систем сбора и анализа больших данных. Но именно анализ бигдата[1] позволит им отойти от деструктивной системы реагирования на уже совершенные преступления к их предиктивной аналитике, профилактике и предупреждению.

Электронно-цифровой след (англ. digital fingerprint) является относительно новым явлением для расследования ИТП. Он представляет собой совокупность данных о конечном электронном устройстве правонарушителя, которые автоматически сохраняются при посещении любого ресурса в сети Интернет. Эти данные включают в себя сведения об IP-адресе, операторе услуг связи, примерной геолокации, используемом устройстве, его операционной системе, браузере, языковых и иных настройках. Кроме того, цифровой след может включать в себя идентификаторы пользователя для автоматического входа в социальные сети, электронную почту или иные онлайн-сервисы, которые содержатся в файлах cookie. Централизованный сбор электронно-цифрового следа в целях криминалистического учета позволяет эффективно и быстро идентифицировать большинство пользователей сети Интернет, в том числе пользователей тех сервисов и посетителей сайтов, которые не предоставляют их данные правоохранительным органам Российской Федерации.

Самостоятельное получение электронно-цифрового следа устройства пользователя осуществляется посредством перенаправления его трафика на тот web-ресурс, код и лог которого является открытым для сотрудника полиции. Таким ресурсом может являться сайт в сети Интернет, на котором были заранее размещены специальные скрипты, предназначенные для идентификации посетителей. В целях экономии времени можно воспользоваться одним из общедоступных логгеров, таких как iplogger.ru или grabify.link. Они позволяют пользователю создать уникальную ссылку на тот или иной объект в Интернете, проходя по которой пользователь оставит данные о своем устройстве. Такие ссылки часто демаскируются антивирусными программами, установленными на устройства злоумышленников. В связи с этим производится маскировка логгируемых ссылок при помощи сервисов по сокращению ссылок (clck.ru, bit.do, lnnkin.com) или путем ретрансляции через одну из социальных сетей.

Иной функционал предлагают логгеры, которые позволяют внедрять свой код в состав офисных документов. Примеры таких логгеров: canarytokens.org/generate, mailtracking.com/mailtracking/

[1] Big Data – это инструменты и способы обработки большого количества структурированной и не очень информации. Информация собирается в центры обработки информации – data-центры.

pmdoctrack.asp и locklizard.com/track-pdf-monitoring. Сформированный с их помощью документ можно переслать адресату и, если он запустит на своем устройстве полученный файл, его данные также станут доступными для изучения. Отдельная категория логгеров – это те, которые позволяют встраивать себя в код электронного письма: getnotify.com, readnotify.com/readnotify и didtheyreadit.com.

Более широкие возможности для идентификации возникают в случае создания собственного интернет-ресурса, включающего в свой состав самописные средства логгирования устройств пользователей, а также системы идентификации пользователей по их рекламным и иным идентификаторам (аналогично тому, как сайты торговых компаний идентифицируют контакты своих посетителей). Это может быть классический «соцфишинг»: kr-tracker.ru, socfishing.com, pogodiwidget.com, trackerrus.ru или более серьезные модули, использующие дампы данных социальных сетей: ltracker.ru, dmp.one, getsale.io. В результате использования такого «заряженного» сайта или ханипота можно не только получить данные об устройстве и соединении пользователя, но и выявить список социальных профилей, электронных адресов или телефонов, имеющих авторизацию в его браузере.