Стегалин Сергей Валентинович
1 курс адъюнктура
Нижегородская академия МВД России

«ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ».

THE USE OF OPEN SOURCES OF INFORMATION IN THE DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED THROUGH THE INTERNET INFORMATION AND TELECOMMUNICATIONS NETWORK AND MOBILE COMMUNICATIONS.

Аннотация. Сложности в раскрытии и расследовании преступлений, совершенных посредством информационно-телекоммуникационной сети Интернет и средств мобильной связи, возникают в связи с отсутствием у сотрудников оперативных и следственных подразделений полноценных знаний и опыта в данном направлении, а также с недостаточной оперативностью при сборе сведений, подлежащих установлению. В статье обосновывается необходимость для субъекта выявления и расследования преступлений наличия знаний в сфере современных информационных технологий, выступающих в качестве средств совершения преступлений данной категории, и ориентирования в открытых источниках сведений, позволяющих установить оперативно значимую информацию. В статье автором рассматривается понятие OSINT и разъясняется важность практического применения разведки по открытым источникам сотрудниками

правоохранительных органов для оперативного сбора криминалистически значимой информации при раскрытии и расследовании преступлений.

Ключевые слова и словосочетания: Интернет-ресурсы, базовые станции, IMEI, интернет-сайты, IP-телефония, IP-адрес, Интернет-провайдер, хостинг-провайдеры, виртуальная частная сеть, киберпреступления, разведка по открытым источникам, OSINT, интернет-разведка, ориентирующая информация.

Annotation. Difficulties in the disclosure and investigation of crimes committed through the Internet information and telecommunications network and mobile communications arise due to the lack of full-fledged knowledge and experience in this area among the staff of operational and investigative units, as well as insufficient efficiency in collecting information to be established. The article substantiates the need for a subject to identify and investigate crimes to have knowledge in the field of modern information technologies, acting as a means of committing crimes of this category, and orientation in open sources of information that allows to establish operationally significant information. In the article, the author examines the concept of OSINT and explains the importance of the practical application of open source intelligence by law enforcement officers for the rapid collection of criminally significant information in the disclosure and investigation of crimes.

Keywords and phrases: Internet resources, base stations, IMEI, Internet sites, IP telephony, IP address, Internet provider, hosting providers, virtual private network, cybercrimes, open source intelligence, OSINT, Internet intelligence, orienting information.

Стремительное развитие информационных и телекоммуникационных технологий неизбежно повлияло на формирование современного социума и

одновременно выступило фактором возникновения новых источников угрозы его функционирования. Недостаточная упорядоченность использования сферы IT-технологий, несовершенство нормативно правовой базы, регулирующей социально-экономические отношения в киберпространстве, сформировали сложную систему криминогенных факторов, оказывающих негативное влияние на общество. Мошенничества, совершенные с использованием средств мобильной связи и сети Интернет, не первый год остаются одними из самых распространенных видов преступной деятельности в современном мире.

В теоретических исследованиях и практических рекомендациях специалистами в области криминалистики неоднократно описывались наиболее распространенные способы совершения мошенничеств с использованием средств сотовой связи: мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду; розыгрыш призов; смс-просьба; телефонная просьба содействия правоохранительным органам в фиксации фактов преступлений; платный код; штрафные санкции оператора; ошибочный перевод средств; вишинг.

Еще более многочисленными и разнообразными являются способы осуществления мошеннических действий, совершенные с использованием сети Интернет. По информации НЦБ Интерпола МВД России, к самым распространенным видам таких преступлений относятся: брачные мошенничества; приобретение товаров и услуг посредством сети Интернет; крик о помощи; фишинг; нигерийские письма; брокерские конторы.

Вопросы раскрытия и расследования интернет мошенничеств неоднократно становились объектами изучения специалистов в области криминалистики и оперативно-розыскной деятельности, которые в своих работах рассматривают различные аспекты механизма совершения преступлений подобного вида, а также проблемы организационно-правового

и информационного характера, возникающие у субъектов выявления и расследования преступлений на различных этапах работы [5, с. 146].

Так, по мнению Н. В. Яджина и В. А. Егорова, «проблема расследования и документирования преступных действий обусловлена недостаточной организацией взаимодействия между правоохранительными органами и учреждениями, опосредованно участвующими в совершении преступлений» [6, с. 164].

С позиции А. Н. Григорьева и Е. В. Титова, проблемой в раскрытии и расследовании киберпреступлений выступает «длительность получения оперативно значимой информации» [2, с. 12], что связано с существованием и использованием множества платежных систем, Интернет-провайдеров, регистраторов доменных имен и т. д.

Говоря о сложности расследования преступлений рассматриваемой категории, указанные специалисты отмечают «недостаточно высокий уровень информационной подготовки у сотрудников следственных и оперативных подразделений, а также отсутствие устоявшейся практики расследования таких преступлений и направления уголовных дел в суд» [2, с. 13].

Практически всеми исследователями отмечается, что существующая в наше время штатная численность и материально-техническое обеспечение специализированных подразделений МВД России, противодействующих киберпреступлениям, не позволяют эффективно бороться с ними [3, с. 26].

Изучение проблемных вопросов, связанных с дефицитом информационного обеспечения при раскрытии и расследовании мошенничеств, совершенных с использованием средств сотовой связи и сети Интернет, позволяет утверждать, что субъект расследования должен уверенно владеть следующими видами компетенций:

– четким пониманием и умением оперировать ключевыми терминами, такими как сотовая связь, базовые станции, IMEI, IP-адрес, VPN

(виртуальная частная сеть), интернет-сайт, IP-телефония, Интернет-провайдер;

– обладанием сведениями о возможностях современных информационных технологий, используемых в качестве средств совершения преступлений данной категории;

– умением ориентироваться в открытых источниках установления оперативно значимой информации с учетом критериев запрашиваемых сведений.

Вместе с тем субъект выявления и расследования рассматриваемых преступлений должен четко представлять и реализовывать алгоритм действий, позволяющий зафиксировать факт мошенничества, совершенного с использованием средств сотовой связи либо сети Интернет, и собрать необходимый перечень первоначальных сведений.

Сбор преимущественной части информации, значимой для раскрытия и расследования интернет мошенничеств, происходит, во-первых, посредством подробного допроса потерпевшего и свидетелей обо всех обстоятельствах происшествия; во-вторых, путем направления необходимых запросов операторам сотовой связи, банковским организациям, в случае необходимости — Интернет-провайдерам и хостинг-провайдерам. На оперативность получения сведений, подлежащих установлению, и их объем непосредственно влияют своевременность направления запросов, а также понимание сотрудником правоохранительных органов критериев запрашиваемой информации в зависимости от способа совершенного преступления. Исходя из сказанного нам представляется актуальным изучение вопроса использования сотрудниками правоохранительных органов отдельных Интернет-ресурсов как вспомогательного средства раскрытия и расследования телефонных и интернет-мошенничеств.

В ходе совершения рассматриваемых преступлений для осуществления звонков потерпевшим либо отправки sms-сообщений в целях получения

конфиденциальных данных, необходимых для хищения денежных средств с банковских счетов и карт, злоумышленники используют различные абонентские номера. Регистрация этих номеров происходит путем оформления абонентского договора, для чего оператору мобильной связи нужно предоставить персональную информацию: Ф. И. О., пол, возраст, дата рождения, место рождения, место регистрации, полные паспортные данные. Указанные данные отображаются в карточке клиента, на которой фиксируются сведения о включении и выключении мобильного устройства, информация о расходах и пополнениях лицевого счета, направлении вызовов, смс-сообщений, их содержании, посещенных интернет-сайтах, скачанных файлов, используемых приложениях, совершенных онлайн-покупках, месторасположении и IMEI мобильного устройства, номер sim-карты и ID-соты. Эти сведения предоставляются оператором сотовой связи субъекту — инициатору проверки.

Рассматривая мобильный телефон в качестве наиболее распространенного средства совершения интернет-преступлений, субъекту расследования следует принимать в расчет особенности его эксплуатации. Сотовая связь представляет собой разновидность радиосвязи, а сотовый телефон выступает средством, отправляющим и принимающим сигнал с другого устройства, при этом на пути данного сигнала расположены базовые станции, ретранслирующие сигнал и помогающие сохранять непрерывную связь на больших расстояниях. В то же время в биллинге оператора сотовой связи, предоставившего услуги, происходит сбор информации об использовании телекоммуникационных услуг, их тарификации, выставлении счетов абонентам, обработка платежей, сохраняется информация о времени и продолжительности вызова, номер базовой станции.

Истребовав у оператора сотовой связи сведения о координатах базовых станций отдельного абонента с помощью интернет-ресурса xinit.ru (https://xinit.ru/bs/), сотрудник правоохранительных органов может

воспользоваться сервером «Координаты базовых станций» и установить зону действия той или иной станции.

Наиболее перспективным является анализ сведений, содержащих данные о сеансах связи абонента с различными базовыми станциями. Установление этой информации дает возможность определить схему перемещений абонента, его местонахождение в определенное время, личность субъекта, с которым происходила встреча (если другой человек пользовался сотовым телефоном), относительная и абсолютная продолжительность встречи, ее территориальность (близость от места совершения преступления).

Несмотря на то что метод установления местонахождения абонента путем использования данных, полученных через сеансы связи с различными базовыми станциями, не дает абсолютно точных сведений, подпадая под влияние ряда факторов (топография местности, помехи от зданий и т. д.), данный способ может быть эффективен при доказывании совершения преступления группой лиц и установлении соучастников преступных действий.

Кроме того, большинство авторов, изучающих рассматриваемую тему, отмечают, что значительная часть интернет-мошенничеств совершается лицами, отбывающими наказание в исправительных учреждениях [4]. Поэтому, если в зоне действия установленной базовой станции будет находиться конкретное исправительное учреждение, целесообразно направить поручение о проведении отдельных оперативно-разыскных мероприятий в рамках расследуемого уголовного дела об отработке на причастность к совершенному преступлению лиц, отбывающих наказание на его территории, а также запросить сведения о лицах, судимых за совершение преступлений указанной категории, что может помочь в установлении дополнительных эпизодов преступной деятельности и возможных соучастников преступных действий.

Располагая информацией об IMEI (серийном номере) сотового телефона, которым пользуется мошенник, сотрудник правоохранительных органов, используя Интернет-ресурс IMEI.info (www.imei.info), может установить марку и модель указанного мобильного устройства, его местонахождение, даже в случае замены sim-карты, осуществленной с целью сокрытия следов преступления.

В случае установления сведений о нахождении мобильного телефона, с которого осуществлялись преступные действия, в другом государстве сотрудник правоохранительных органов может подготовить и направить международное поручение через НЦБ Интерпол на установление местонахождения лица, использующего данный мобильный телефон.

Отдельно следует отметить, что с развитием цифровых технологий мошенники стали использовать для совершения преступлений в сфере информационных технологий IP-телефонию, которая выступила альтернативой мобильной связи и городскому телефону, при этом позволяет осуществлять звонки не только в пределах Российской Федерации, но и по всему миру. Вместо автоматической телефонной станции при использовании IP-телефонии выступают серверы SIP-провайдеров, которые соединяются с серверами других SIP-провайдеров телефонными сетями общего пользования или станциями мобильной связи через интернет-канал.

При расследовании преступлений, совершенных с использованием IP-телефонии, субъекту расследования следует знать, что подключение данной технологии предусматривает необходимость выбора провайдера, среди которых наиболее востребованными являются «Задарма», Telphin, Sipnet. Для регистрации у конкретного провайдера необходимо предоставить в его адрес свои установочные данные: имя, адрес электронной почты, пароль и номер мобильного телефона. Каждому Интернет-провайдеру при этом выделяется определенное количество IP-адресов в конкретном диапазоне. IP-адрес представляет собой уникальный идентификационный номер, который

получает пользователь для идентификации технического устройства, с помощью которого осуществляется выход в Интернет, — это своего рода адрес компьютера в сети. Расследование мошенничеств, связанных с использованием средств сотовой связи и сети Интернет, предусматривает необходимость установления сотрудником правоохранительных органов IP-адреса пользователя и Интернет-провайдера, что возможно при использовании Интернет-ресурса 2IP (www.2ip.ru).

Владение сведениями об Интернет-провайдере позволит сотруднику правоохранительных органов направить в его адрес запрос о предоставлении установочных данных физического либо юридического лица, зарегистрировавшего конкретный IP-адрес. Анализ полученной информации даст возможность установить местонахождение мошенника либо технического устройства, с которого осуществлялись преступные действия.

Однако отметим, что получение сведений по IP-адресам усложняется использованием в ходе совершения преступления средств анонимизации в сети, которые называются VPN (виртуальная частная сеть). Данный вид связи предусматривает одно или несколько сетевых соединений поверх другой сети. VPN используется для различных задач: защиты персональных данных и конфиденциальности, виртуализации местоположения, разблокировки доступа для ускорения соединений, совершения интернет-покупок, а также для сокрытия следов преступления, совершенного в сети Интернет. В результате лицо, совершающее преступление, использует сервер третьего лица, которое чаще всего локализуется преимущественно за пределами Российской Федерации. Этот сервер нередко принадлежит иностранным Интернет-провайдерам, которым весьма затруднительно направить запрос в рамках российского правового поля.

Основной задачей сотрудника правоохранительных органов при раскрытии и расследовании мошенничеств, связанных с использованием интернет-сайтов, выступает установление регистратора домена, поэтому

целесообразно использовать следующие Интернет-ресурсы: whois.ru (https://whois.ru/), регистратор доменных имен (www.reg.ru).

При установлении регистратора домена и обладая знаниями о предоставляемых для регистрации домена сведениях, сотрудник органов внутренних дел может направить запрос для истребования данных о физическом либо юридическом лице (лицах), осуществляющих оплату доменного имени. Анализ полученной информации позволит организовать дальнейшее расследование, направленное на установление лиц, причастных к совершению преступления.

При раскрытии и расследовании преступлений необходимо оперативно получать данные для их своевременного анализа и использования в служебной деятельности. При этом могут применяться специальные средства и методы с целью получения информации о замыслах, планах и мероприятиях преступника, а также для изучения его (их) личности. К таким методам относится интернет-разведка (OSINT – Open Source Intelligence) [1, с. 64].

На сегодняшний день США занимают лидирующую позицию в области разведки, огромные денежные ресурсы, выделяемые их правительством, позволяют создавать программное обеспечение для сбора и анализа большого объема цифровых данных (например, Palantir).

Необходимо отметить, что конкурентная разведка в России принципиально отличается от мировой разведки по открытым источникам. В мире конкурентная разведка – часть деятельности маркетинга. Специалист по маркетингу осуществляет бечмаркинг. В России конкурентную разведку (OSINT) можно сравнить с контрразведкой, и ее осуществляют службы безопасности.

OSINT – это разведывательная дисциплина, включающая в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ. Источники OSINT отличаются от других форм разведки,

поскольку они должны быть легально доступны общественности без нарушения каких-либо законов или конфиденциальности.

90% полезной информации, получаемой спецслужбами, поступает из открытых источников. Сегодня социальные сети и иные сайты, содержащие персональные данные, открывают большие возможности для сбора информации о лице. Например, можно получить много данных о человеке по всему миру, просто проверив личную страницу этого человека в Facebook, «ВКонтакте» и других социальных сетях.

С помощью OSINT можно не только проводить сбор данных в социальных сетях, но также использовать расширенные запросы поисковых систем для предоставления наиболее точных результатов поиска, осуществлять поиск удаленных версий веб-сайтов, отслеживать людей и их деятельность в Интернете с помощью общедоступных баз данных и эффективных инструментов поиска, просматривать спутниковые изображения любой улицы мира, искать геолокацию лица и многое другое.

OSINT применяется не только для сбора данных из онлайн-источников. Бумажные издания при необходимости также могут исследоваться в рамках процесса сбора данных, однако онлайн-источники составляют самый большой сегмент OSINT.

Если раньше, чтобы получить какие-то данные о лице, необходимо было посетить некоторое количество Интернет-ресурсов, то на сегодняшний день для автоматизации OSINT существуют различные интегрированные интернет-ресурсы и программные средства (например, Maltego, FOCA, Creepy, NameChk. com, Yateda.com). Сервисы представляют из себя платформы, на которых можно сразу провести комплекс действий: и поиск информации, и анализ результатов, и мониторинг дальнейших изменений.

Резюмируя вышеизложенное, отметим, что сотрудники полиции, особенно подразделений следствия, дознания и уголовного розыска, должны изучить и в дальнейшем применять в своей профессиональной деятельности

приемы и методы OSINT. Так как благодаря разведке по открытым источникам можно получить криминалистически значимую информацию ориентирующего характера, которая может быть использована для выдвижения версий, определения направлений расследования, планирования следственного действия, прогнозирования возможной линии поведения участников уголовного процесса и возможного противодействия расследованию.

Список используемой литературы и используемых источников

1. Бельдеубаева Д.Р. Применение OSINT-технологий в качестве повышения эффективности деятельности органов внутренних дел // Правопорядок в России: проблемы совершенствования. XV Всероссийская конференция: сборник статей. М., 2021. С. 64-70.

2. Григорьев А. Н., Титов Е. В. Проблемы выявления, раскрытия и расследования интернет мошенничества // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2018. № 2 (52). С. 11-14.

3. Иванова А. А. Методика расследования незаконного изготовления, распространения и оборота порнографических материалов или предметов: дис. ... канд. юрид. наук. Псков: ПЮИ ФСИН России, 2011. 301 с.

4. Литвинов Н. Д., Федотов А. Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения. URL: https://cyberleninka.ru/article/n/ moshennichestvo-s-ispolzovaniem-sredstv-mobilnoysvyazi-distantsionnoe-ponyatie-i-osobennosti-sover sheniya/viewer (дата обращения: 15.07.2024).

5. Осяк В. В., Ковалева А. В., Фролова Е. Ю. «Мобильные» мошенничества: способы совершения и алгоритмизация расследования // ЮристПравоведъ. 2020. № 3 (94) С. 145-150.

6. Яджин Н. В., Егоров В. А. Организационно-правовое и информационное обеспечение расследования преступлений, совершаемых с использованием средств мобильной связи // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 163-169.