Секция «Криминалистика»

Особенности поиска информации о пользователях в открытых источниках

Научный руководитель – Жидков Дмитрий Николаевич

Иванов Евгений Игоревич

Студент (специалист)

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Санкт-Петербург, Россия

E-mail: ivanovjenya2000@mail.ru

В нынешнее время информация является неотъемлемой частью нашей жизни. «Кто владеет информацией, тот владеет миром» эти слова актуальны и сейчас. Сегодня бытует мнение, что государство получает более 80% необходимой информации из открытых источников. По нашему мнению сейчас, когда все коммуникации перешли в интернет, возможностей поиска с открытых источников стало намного больше. Указанные процессы ни обходят и преступников, которые в связи развитием технологий все чаще при коммуникации используют интернет.

В интернете пользователи оставляют о себе много информации: связи с другими людьми, профили в социальных сетях, интересы, геолокацию, семейное положение и т.д. Использование таких источников для сбора информации в международном пространстве называется OSINTом.

Полученные данные из открытых источников являются результатом OSINTа. Поэтому OSINT, по нашему мнению является неотъемлемой частью профессиональной деятельности современного сотрудника органов внутренних дел. Попробуем разобраться в том, что же такое OSINT.

OSINT[1] это результат работы систем и приложений, о назначении которых знает далеко не каждый человек. Таких систем и приложений большое множество и все они разнообразные, но есть и такие, которые схожи по некоторым выполняемым признакам. Сегодня у сотрудника правоохранительных органов имеется возможность по произведению указанных мероприятий без использования специализированного программно-аппаратного комплекса и программного обеспечения. Далее в нашей статье мы рассмотрим основные системы и приложения и их назначение.

Robtex - система, предоставляющая информацию о домене, о IP-адресе, на котором находится ресурс, о владельце домена, а также о том, какие еще домены используют это же серверное пространство[1].

InfoSniper - это поисковик с «геолокацией» для IP адресов и доменов, который может указать где сервер находится физически. Такой поиск становится важным в случае расследований[2].

Maltego - это метапоисковая система и графическая утилита для анализа базы данных. С помощью каждодневных обновлений, можно получить множество данных, которые могут быть обработаны вплоть до готового результата. Однако интерфейс Maltego не доступен в браузере, чего нельзя сказать о аналоге SpiderFoot[3].

Casefile приложение, которое производит визуализацию на основе имеющейся информации. То есть создает интерфейс, включающую в себя имеющиеся данные, чем облегчает восприятие информации[4].

Geotweet является приложением для отслеживания записей в twitter, а также в instagram. Найденные координаты тут же можно отобразить на google-картах для составления схемы перемещений владельца аккаунта[5].

Find Face - приложение, которое позволяет найти человека в интернете по фотографии[6].

Поскольку невозможно установить чёткие рамки понятия OSINT, соответствующим инструментом можно считать даже Google, однако узкоспециализированный OSINT-софт существует. Наибольшей известностью в нетсталкерских[2] кругах пользуется программа Intrigue.

Сервис позволяет изучать какой-либо сетевой объект и по результатам этого собирать досье (Dossier) на него либо на связанного с ним человека или организацию. Содержит множество функций, от masscan по айпи и брутфорса[3] URI до краулера[4] заданной вебстраницы или результатов поисковика.

Подводя итог выше изложенному, можно отметить, что OSINT это некая комбинация систем и приложений, которая глобально облегчает работу агентуры, так как эта комбинация позволяет не только собрать информацию об объекте, но и структурировать ее, а после выдать в удобном виде. Из-за того, что информация является важнейшим ресурсом, возрастает значимость OSINTa в наши дни. В скором времени все силовые структуры перейдут на OSINT, ввиду прогресса и изобретений нынешнего века.

---

[1] OSINT (англ. Open source intelligence)- В переводе с английского «Разведка на основе открытых источников»

[2] Нетсталкеры - это люди, которые ищут малоизвестную, малодоступную информацию

[3] Брутфорс (с англ. brute force) переводится как «полный перебор» или еще известен как метод «грубой силы» . С точки зрения взлома систем безопасности — банальный перебор всех возможных комбинаций пароля с целью выявления верного.

[4] Караулер - программа, являющаяся составной частью поисковой системы и предназначенная для перебора страниц Интернета с целью занесения информации о них в базу данных поисковик

Источники и литература

1 Рустам Абдулин, OSINT. Сбор информации на основе открытых источников,2014г,08.01.2019, http://rustam-abdullin.blogspot.com/2014/06/osint.html

2 Рустам Абдулин, OSINT. Сбор информации на основе открытых источников,2014г,08.01.2019, http://rustam-abdullin.blogspot.com/2014/06/osint.html

3 Рустам Абдулин, OSINT. Сбор информации на основе открытых источников,2014г,08.01.2019, http://rustam-abdullin.blogspot.com/2014/06/osint.html

4 Рустам Абдулин, OSINT. Сбор информации на основе открытых источников,2014г,08.01.2019, http://rustam-abdullin.blogspot.com/2014/06/osint.html

5 mr_agafonov, Применение некоторых средств автоматизации Open Source Intelligence (OSINT),2016г,08.01.2019 ,https://defcon.ru/penetration-testing/2692/

6 mr_agafonov, Применение некоторых средств автоматизации Open Source Intelligence (OSINT),2016г,08.01.2019 ,https://defcon.ru/penetration-testing/2692/