УДК 343.12

Рукавишникова Галина Александровна
Уральский юридический институт МВД России
Факультет подготовки следователей
Россия, Екатеринбург
9089133977@mail.ru
Титов Павел Михайлович
Уральский юридический институт МВД России
Кафедра оперативно – разыскной деятельности ОВД
Россия, Екатеринбург
titov1995@ya.ru
Rukavishnikova Galina
Ural Law Institute of the Ministry of Internal Affairs of Russia
Faculty of Investigator Training
Russia, Ekaterinburg
Titov Pavel
Ural Law Institute of the Ministry of Internal Affairs of Russia
Department of Operative Investigative Activities of the Internal Affairs Department
Russia, Ekaterinburg

ОБЩАЯ ХАРАКТЕРИСТИКА ТЕХНОЛОГИЙ OSINT НА ПЛАТФОРМЕ TELEGRAM ДЛЯ ИСПОЛЬЗОВАНИЯ В ПОЛУЧЕНИИ ЗНАЧИМОЙ ИНФОРМАЦИИ

Аннотация: в статье рассматриваются вопросы общей характеристики технологий OSINT на платформе TELEGRAM для использования в получении значимой информации. Обращается внимание на проведении оперативно-розыскных мероприятии и иных мероприятий по открытым источником информации в открытом и закрытом сегменте Интернета. Особое внимание уделяется технологии OSINT на платформе TELEGRAM, в результате

применения которой, можно получить значимую информацию для правоохранительной деятельности.

Ключевые слова: информация, OSINT, оперативно-розыскная деятельность, оперативно-розыскные мероприятия, компьютерная разведка, ориентирующая информация, сетевая разведка, правоохранительная деятельность.

GENERAL CHARACTERISTICS OF OSINT TECHNOLOGIES ON THE TELEGRAM PLATFORM FOR USE IN OBTAINING MEANINGFUL INFORMATION

Annotation: the article discusses the general characteristics of OSINT technologies on the TELEGRAM platform for use in obtaining meaningful information. Attention is drawn to the conduct of operational search activities and other activities on an open source of information in the open and closed segment of the Internet. Particular attention is paid to OSINT technology on the TELEGRAM platform, as a result of which it is possible to obtain significant information for law enforcement.

Key words: information, OSINT, operational search activity, operational search activities, computer intelligence, orienting information, network intelligence, law enforcement.

Цифровизация становится неотъемлемым элементом деятельности любого человека. Повсеместно социальные и политические процессы, а также деятельность государственных органов перемещается в цифровую среду и для того, чтобы успешно адаптироваться в обществе, люди создают различные цифровые профили на государственных порталах, ведут страницы в социальных сетях, выкладывая при этом фотографии и иную информацию о себе. Интернет в своем открытом сегменте имеет настолько обширную сеть, что обыденный человек представить не может, не говоря о закрытом сегменте Интернета.

На этом фоне, как никогда становится актуальной фраза британского банкира Натана Ротшильда: «Кто владеет информацией — тот владеет миром». Да, хотелось бы, безусловно, с данными словами согласиться. Это подтверждается и современными условиями, в которых Российская Федерация находится.

Но для того, чтобы «владеть» информацией необходимо знать, как и откуда её получать, и наиболее подходящим вариантом в этом вопросе являются общедоступные источники. Такой метод сбора, анализа и использования информации из открытых источников именуется OSINT (Open source intelligence).

OSINT – это разведывательный набор инструментов, включающий в себя такие инструменты, как поиск, выбор, сбор, анализ информации. В зависимости от целей, OSINT можно использовать по-разному. К примеру, это хороший инструмент для разведывательных служб, правоохранительных органов [1, с. 216], журналистов и исследователей. Он позволяет получить доступ к информации, которая обычно недоступна пользователям. Особенностью OSINT является то, что он основан на открытых источниках, что делает его более прозрачным и доступным для широкой аудитории. OSINT можно применять в отношении конкретных людей, событий, явлений и целей.

Как было отмечено выше, основной принцип технологии OSINT состоит в использовании общедоступных источников для сбора и анализа информации. Это включает в себя все виды данных, доступных через Интернет: новости, социальные сети, блоги, форумы, онлайн-платформы, академические исследования и многое другое. Важным отличием OSINT является использование информации, которая открыта для всех, включая не только публикации, но и скрытые данные, такие как метаданные, которые могут содержать полезные сведения.

Условно, методы сбора информации OSINT можно классифицировать на два вида: пассивные и активные. Пассивные методы – это рядовые методы,

которые доступны для любого пользователя и не предполагают глубокого анализа информации и прямого воздействия с системами. В качестве примера такого метода, можно привести использование поисковых сетей (Google, Яндекс и другие) [2, с. 133]; просмотр анкет и страниц пользователя в социальных сетях; получение геолокационных данных с помощью общедоступных ресурсов вроде «Google Maps» или «Яндекс.Карты» и тд. Активные методы – это методы, через которые оказывается влияние непосредственно на объект исследования, при этом, предполагается использование специальных систем, которые доступны лишь определенному кругу лиц. Как правило, получение доступа к таким средствам осуществляется через подписку (бесплатно или за определенную сумму денежных средств) либо посредством создание поддельных учетных записей и/или сайтов и т.д. [3, с. 8].

Конкретный пример активного метода – боты в мессенджере Telegram. Боты – это интернет-сервисы, то есть специализированные онлайн-платформы и инструменты, которые предоставляют доступ к открытым источникам информации. Эти сервисы обеспечивают удобный и эффективный способ сбора и анализа данных, а также предоставляют различные функции для фильтрации, обработки и визуализации информации.

В Telegram существует разнообразие ботов, которые предоставляют различную информацию о людях, в зависимости от их целей и функций. Некоторые боты могут предоставлять информацию о публичных профилях в социальных сетях, контактных данных, результаты поиска по базам данных или даже более конкретную информацию о личности.

Однако, стоит быть осторожным с ботами, предоставляющими информацию о людях, так как они могут использоваться в незаконных целях или нарушать права на конфиденциальность. Важно учитывать, что сбор, хранение и распространение личных данных без согласия владельца данных может быть незаконным и нарушать права на конфиденциальность.

При использовании подобных ботов важно убедиться, что они соблюдают законодательство и не нарушают приватность и безопасность личных данных.

Как правило, все информация, предоставляемая ботами, является персональными данными, то есть, фактически, само создание и использование таких ботов, нарушает права на конфиденциальность, так как они собирают личные данные о людях и без их согласия предоставляют доступ к данным третьим лицам.

Рассмотрим наиболее популярные боты и кратко проанализируем их возможности, предварительно квалифицировав их по объекту поиска:

Сервисы для сбора данных по номеру абонента. Так, например - @Usersbox. Бот предоставляет возможность только по номеру абонента получить следующую информацию: ФИО, дата рождения, адрес прописки, номер СНИЛС, номер ИНН, паспортные данные, Email, информация о объявлениях на Avito, и т.д. Пользователю дается 5 бесплатных дней использования сервиса, далее цена подписки начинается от 49 рублей. Примерно аналогичную информацию предоставляют @Zernerda_bot, @Quick OSINT, @egrul_bot.

Сервисы для сбора данных по фотографии. Рассмотрим данный вид сервисов на примере @VkUrlbotBot. После загрузки изображения сервис находит ссылки на аккаунты из социальных сетей с похожими фотографиями, помимо этого, возможно осуществлять: поиск телефона по ссылке на страницу VK; поиск телефона по Username Telegram; пробив ID по Username Telegram; поиск по ФИО; проверка номера авто; поиск телефона по Username Telegram; поиск телефона по ссылке на страницу Facebook; поиск предыдущих никнеймов Telegram; проверка почты; поиск по номеру телефона. Также, поиск по фотографии осуществляют такие боты как: @FFace_bot, @FCfind_bot; @Poiskovichokbot и др.

Сервисы для сбора информации об электронной почте. SmartSearch_Bot – благодаря электронной почте бот также позволяет получить информацию в виде

ссылок на социальные сети, адреса проживания, дата рождения и других данных. У этого бота есть и другие функции, так, например, можно отправьте стикер, чтобы найти создателя или отправить точку на карте, чтобы найти людей, которые сейчас там, так же с помощью голосовых команд также можно выполнять поисковые запросы.

Сервисы для сбора данных о номере транспортного средства. В этой сфере рассмотрим бот @AVinfoBot, который осуществляет проверку по госномеру, VIN и телефону продавца. Пользователю предоставляется возможность получить сведения об участии автомобиля в ДТП, кредитах, пробеге и другие существенные сведения. Кроме того, информацию о транспортном средстве можно узнать в ботах @AntiParkonBot и @avtocodbot.

Помимо вышерассмотренных ботов, существуют и другие, например, функционал бота @TeleSINT позволяет выполнять поиск по нику в Telegram и определить, в каких группах состоит тот или иной интересующий пользователь.

Как видно из краткого анализа, Telegram-боты, позволяют при наличии минимальных данных узнать многие персональные данные третьего лица, своего рода это и есть технология OSINT, однако, такой, весьма легкий способ получения конфиденциальной информации имеет двойственную природу.

Так, одним из основных направлений применения OSINT является сфера безопасности. Разведка, правоохранительные органы и частные детективные агентства активно используют технологию OSINT для сбора информации о преступниках, ликвидации угроз и предотвращения преступлений. Благодаря OSINT можно идентифицировать потенциальных преступников, проанализировать схемы их действий, а также предоставить релевантные данные в судебные процессы. Кроме того, в целях реализации принципа «публичности», применение технологии OSINT также находит свое место в сфере журналистики: основываясь на открытых источниках информации, журналисты могут проверять факты, подтверждать достоверность новостей, выявлять манипуляции с информацией и разоблачать фейки. То есть, OSINT становится мощным

инструментом, который помогает журналистам предоставлять актуальную и достоверную информацию общественности. И, наконец, OSINT является важным средством для обычных пользователей, которые имеют доступ к огромному количеству информации в сети. Благодаря этой технологии, любой человек может провести собственное расследование, изучить интересующую тему, проверить достоверность информации или просто оставаться в курсе событий. Таким образом, технология OSINT способна выполнить почти все задачи, которые ставятся перед «частными детективами». Для разведок всего мира нужность OSINT очевидна. Однако кого-то может удивить, что методики и инструменты открытой разведки не только не засекречены, но, напротив, совершенно общедоступны.

На этом фоне возникает проблемы развития преступности. Так, например, преступники могут использовать OSINT для выявления перспективных мишеней и слабых мест в защите потенциальной жертвы, подготовки к целевым атакам с использованием социальной инженерии, а также в целях доксинга (сбор и публикация персональной информации о человеке, часто из соображений мести). С помощью полученных данных могут моделировать угрозу и разрабатывать план атаки. Кибератака, как, впрочем, и все атаки начинается с разведывательной аналитической операции, для начала происходит пассивное получение разведданных, что и позволяет сделать технология OSINT.

Также, помимо возможности совершения кибератак, благодаря данной технологии, беспрепятственно доступ к паспортным данным некоторых гражданин, могут получить и мошенники. В дальнейшем, полученная информация может быть использована для различных целей.

Перечислим некоторые основные способы использования:

1. Открытие фальшивых счетов: Мошенники могут использовать чужие паспортные данные для открытия фальшивых банковских счетов или кредитных карт. Это позволяет им получить доступ к финансовым средствам или совершать транзакции от имени других лиц.

2. Подделка личности: Используя паспортные данные, мошенники могут подделывать личность жертвы. Они могут оформить кредиты, арендовать недвижимость, открывать счета и совершать другие действия, выдаваясь за других людей.

3. Финансовые мошенничества: Мошенники могут использовать паспортные данные, чтобы получить доступ к банковским счетам жертвы, совершать финансовые операции или переводы денежных средств. Они могут также использовать эти данные для получения доступа к чужим электронным кошелькам или платежным системам [4, с. 72].

4. Мошенничество по телефону: Паспортные данные могут быть использованы мошенниками при звонках, где они выдают себя за представителей банков, государственных учреждений или других организаций. Они могут просить жертву предоставить паспортные данные для проверки личности или для осуществления финансовых операций.

Таким образом, преступления, совершение которых возможно посредством использования технологий OSINT, весьма разнообразны, именно этим и обусловлена двойственная природа существования данной технологии, выраженная непосредственно в ботах мессенджера Telegram, так как, именно с их помощью у злоумышленников появляется возможность наиболее оптимальным путем получить всю интересующую их информацию в максимально короткий промежуток времени.

Подводя итоги, необходимо отметить, что технология OSINT имеет огромный потенциал и продолжает развиваться, изменив и улучшив нашу способность искать и анализировать информацию. Она позволяет нам видеть мир с новой перспективы, расширяет границы наших знаний и способствует развитию различных областей, от правоохранительной деятельности, в том числе и оперативно-розыскной [5, с. 317], до журналистики и обычного интернет-пользователя. Необходимо осознать и использовать возможности, которые технология OSINT предоставляет, чтобы эффективно работать с

информацией в нашей современной информационной эпохе. Для этого, в том числе и в вузах, должны изучаться такие возможности, в первую очередь в правоохранительных целях [6, с. 105].

Список литературы:

1. Титов П. М. Оперативно-розыскные мероприятия, проводимые оперативными сотрудниками при выявлении и раскрытии преступлений в экономической сфере / П. М. Титов // Технологии XXI века в юриспруденции : Материалы Пятой международной научно-практической конференции, Екатеринбург, 19 мая 2023 года. – Екатеринбург: АНО «Центр содействия развитию криминалистики «КримЛиб»», 2023. – С. 216-220.

2. Янгаева М. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева, Н. О. Павленко // Алтайский юридический вестник. – 2022. – № 2(38). – С. 131-135.

3. Дворянкин О.А. OSINT, PENTEST и нетсталкинг - информационные технологии интернета // Национальная ассоциация ученых (НАУ) – № 84. – 2022. – С. 6-13.

4. Титов П. М. Проверка по сообщениям о дистанционном мошенничестве и краже с банковских счетов либо электронных денежных средств / П. М. Титов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2023. – № 9. – С. 70-77.

5. Титов П. М. Получение компьютерной информации / П. М. Титов // 25 лет на службе Отечеству : Сборник научных трудов, посвященный деятельности научных школ Санкт-Петербургского университета МВД России и приуроченной к 25-летию со дня его образования / Сост.: О.И. Городовая, О.С. Кравченко, А.А. Жаворонкова. – Санкт-Петербург : Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. – С. 316-318.

6. Качалов А. Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А. Г. Качалов, М. М. Лантаев // Юридическая наука: история и современность. – 2021. – № 9. – С. 98-106.