УДК 343.985

Р. А. Дерюгин
начальник кафедры криминалистики
Уральского юридического института МВД России,
кандидат юридических наук
В. Ю. Иванов
преподаватель кафедры криминалистики
Уральского юридического института МВД России

ИСПОЛЬЗОВАНИЕ «РАЗВЕДКИ» ПО ОТКРЫТЫМ ИСТОЧНИКАМ (OSINT) ДЛЯ ПОЛУЧЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ИЗ СЕТИ ИНТЕРНЕТ

В настоящее время цивилизованный мир невозможно представить без современных технологий. Практически у каждого человека в личном пользовании имеются компьютерные устройства (смартфон, ноутбук и др.) с доступом к сети Интернет. У большинства людей также имеются личные страницы в социальных сетях, аккаунты на интернет-сайтах, в мессенджерах и т. д.

Цифровизация жизнедеятельности человека не могла не отразиться на таком негативном социальном явлении, как преступность. Согласно статистическим данным МВД России, происходит неуклонный рост количества преступлений, совершенных с использованием IT-технологий. Если в 2016 году было зарегистрировано 66 тыс. киберпреступлений, в 2019 – 180 тыс., то в 2022 году их количество превысило 500 тыс. [1]. Согласно данным Генеральной прокуратуры Российской Федерации, за последние 5 лет общее количество зарегистрированных преступлений, совершенных с использованием IT-технологий, увеличилось более чем в 11 раз, их доля составила 25 % от общего числа зарегистрированных преступлений [2].

Информационно-телекоммуникационные технологии возможно использовать и в правоохранительных целях. Так, криминалистически значимую информацию, характеризующую личность преступника, можно найти в сети Интернет. Для ее поиска в открытых источниках необходимо обладать определенными навыками и знаниями в области OSINT.

В настоящее время область применения OSINT используется не только в гражданской деятельности служб безопасности предприятий по борьбе с инцидентами кибербезопасности, но и в правоохранительной деятельности по противодействию преступности.

Под понятием OSINT следует считать разведывательную деятельность, связанную с поиском и анализом информации из общедоступных источников, включая сеть Интернет, о конкретном человеке или событии. Надо полагать, что невозможно установить конкретные рамки понятия OSINT, соответствующим инструментом можно считать даже поисковые системы «Яндекс», Google и т. п.

Ключевое отличие OSINT от других форм поиска информации заключается в обследовании только открытых источников данных без нарушения законодательства [3, с. 133].

Анализ информации, содержащейся в социальных сетях и на иных сайтах, хранящих персональные данные, открывает большие возможности для сбора информации о конкретном лице. Действительно, информация о злоумышленнике и о совершенном им деянии, добытая благодаря OSINT, имеет важное значение для эффективного расследования преступления, выдвижения версии, грамотного применения тактических приемов при производстве следственных действий, планировании и организации подготовки проведения тактических операций (комбинаций), а также для правильного выстраивания алгоритма действий следователя [4, с. 68].

Для данных целей следователю, оперативным работникам и иным сотрудникам правоохранительных органов целесообразно использовать OSINT-сервисы, которые имеются в открытом доступе в сети Интернет.

Все сервисы можно классифицировать по объекту поиска:

− сервисы для сбора информации по Ф. И. О.: Nomer.org (nomer.center и зеркала), Yandex.people, Mmnt.ru, Spra.vkaru.net, Fio.stop-list.info, Zitely.rosfirm.info, byratino.info, боты в ТГ (@ewic3feccpbot);

− сервисы для сбора информации по номеру телефона: веб-сайты Nomer.org (nomer.center и зеркала), боты в мессенджерах (@AVInfoBot, @SmartSearch_Bot, @mailsearchbot, @get_kontakt_bot);

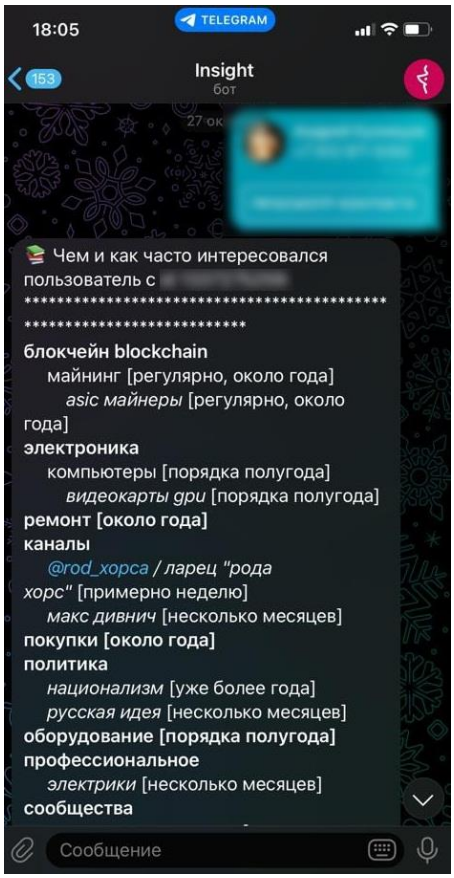

Рисунок 1. **Телеграм-бот, позволяющий выявлять интересы пользователя исходя из его подписок на телеграм-каналы**

− сервисы для сбора информации об электронной почте и никнеймах: веб-сайты (Haveibeenpwned.com, Leakedsource.ru, Dehashed.com, Email.rep, Intelx.io, instantusername.com, Namechk.com, Yasni.com), боты в мессенджерах (@SmartSearch_Bot, @mailsearchbot);

− сервисы для сбора информации по фотографии: Findclone.ru, Vk.watch, Search4faces.com, @AVInfobot, @Falcone_FaceID_bot;

− сервисы для сбора информации по адресу: Nomer.org (nomer.center и зеркала), Rosreestr.ru, Address.stop-list.info, Photomap.ru, Wigle.net (по BSSID точек Wi-Fi), боты ТГ (@Friends-FindBot);

− сервисы для сбора информации о домене: Archive.org (сохраненные архивные версии страниц сайтов), Cashedview.com (сохраненные архивные версии страниц сайтов), Ru.smart-ip.net (гео-IP, трассировка писем), Whois.domaintools.com, Virustotal.com, Xinit.ru, Urlscan.io, Censys.io, Shodan.io, Atsameip.intercode.ca;

− сервисы для анализа СМИ: веб-сайты («Медиалогия», Brand Analytics, Nownews.com); боты (@tgstat, @buzzim_alerts_bot, @MotherSearch_Bot).

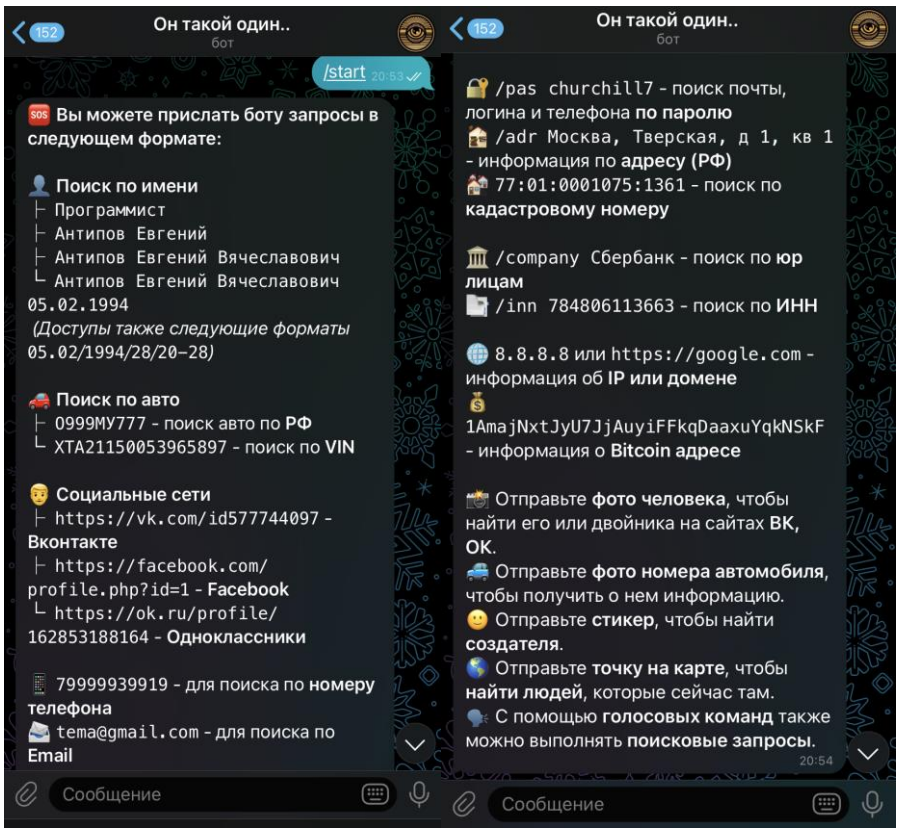

Рисунок 2. **Возможности телеграм-бота «Глаз Бога»**

Наиболее профессиональным инструментом OSINT следует считать дистрибутив Kali Linux, разработанный для IT-специалистов. Дистрибутив содержит множество инструментов, связанных с безопасностью и сетями, которые ориентированы на экспертов в компьютерной безопасности.

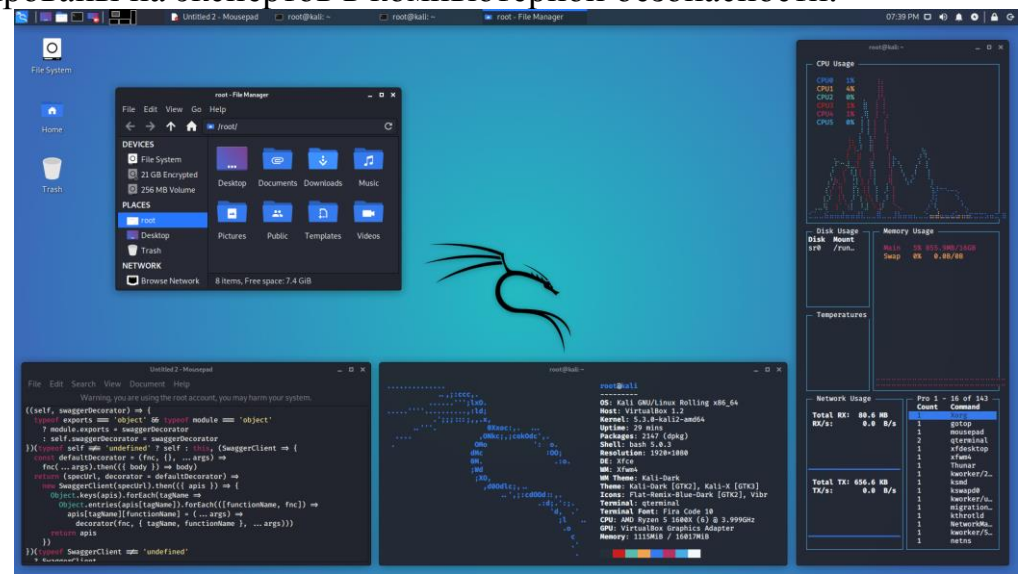

Рисунок 3. **Вычислительная деятельность дистрибутива Kali Linux**

Список инструментов Kali Linux довольно обширен и разбит на несколько категорий, например, возможность сетевого сканирования, перехвата трафика и т. д. Утилиты выделены в категорию сбора информации, среди которых:

− Maltego, Recon-ng, MassMine — приложение для добычи и архивирования данных из социальных медиа;

− OSRFramework — это набор библиотек для выполнения задач по разведке на основе открытых источников;

− SpiderFoot — это инструмент с открытым исходным кодом для автоматизированной разведки;

− theHarvester — это инструмент для сбора e-mail-адресов, имен доменов, виртуальных хостов, открытых портов/баннеров и имен работников из различных открытых источников и т. д. [5, с. 57].

Подводя итог, отметим, что сотрудникам правоохранительных органов, особенно следственных подразделений, необходимо владеть навыками поиска криминалистически значимой информации в сети Интернет. Такая информация имеет важное значение для выдвижения версий, планирования конкретного следственного действия и всего процесса расследования уголовного дела, прогнозирования возможного противодействия участников уголовного судопроизводства.

Список основных источников

1. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 20.01.2023). Перейти к источнику Вернуться к статье

2. Сведения о состоянии преступности [Электронный ресурс] // Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/activity/crimestat (дата обращения: 20.01.2023). Перейти к источнику Вернуться к статье

3. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юрид. вестн. 2022. № 2 (38). С. 131–135. Вернуться к статье

4. Бельдеубаева Д. Р. Применение OSINT-технологий в качестве повышения эффективности деятельности органов внутренних дел // Правопорядок в России: проблемы совершенствования : сб. ст. М., 2021. С. 64–70. Вернуться к статье

5. Поликарпов Е. С. Основы компьютерной разведки : учеб. пособие. М. : Москов. ун-т МВД России им. В. Я. Кикотя, 2020. 321 с. Вернуться к статье