УДК 004

СЕТЬ ИНТЕРНЕТ И КИБЕРПРЕСТУПНОСТЬ

Д. Д. Новик
курсант 2 курса факультета милиции
Могилевского института МВД Республики Беларусь
Научный руководитель: ***М. Н. Хуторова****,*
преподаватель кафедры оперативно-розыскной деятельности
факультета милиции
Могилевского института МВД Республики Беларусь,
магистр педагогических наук

Тема киберпреступности является очень актуальной и интересной, но в то же время сложной, потому что компьютерная преступность развивается с большой скоростью и сотрудникам правоохранительных органов необходимо успевать усваивать новые знания.

В статье предлагается познакомиться с таким понятием, как OSINT (open-source intelligence), то есть поиск информации по открытым источникам — это методология сбора и анализа данных, находящихся в открытом доступе. OSINT является особенно актуальным и широко используется оперативными сотрудниками. Это может быть обычный поиск по социальным сетям, поиск по новостным сообщениям и многое другое. Если оперативные сотрудники не будут использовать специальные программы, поиск информации займет довольно много времени.

Методология OSINT различает активную и пассивную разведку.

В ходе ведения пассивной разведки сотрудник не выходит на прямой контакт с интересующим его объектом, никак себя не обнаруживает. К пассивной разведке относится поиск информации в поисковых системах, таких как Google или Yandex, изучение баз данных на предмет возможных утечек информации и др.

Активная разведка включает в себя произведение заметных действий со стороны сотрудника лицами, находящимися под наблюдением. Это может быть непосредственное исследование инфраструктуры организации через сканирование портов, осуществление перебора директорий, проверка всех доменных имен на серверах и др.

Самое первое, что может применить сотрудник правоохранительных органов из перечисленного выше, это проверить доменные имена. Для этих целей функционирует множество утилит (в качестве примера использовался yandex.ru): Nslookup (linux\windows nslookup yandex.ru), Ping (linux\windows

ping yandex.ru), Host (linux host yandex.ru), getent (linux getent hosts yandex.ru), resolveip (linux resolveip-s yandex.ru) и др.

Используя данные утилиты, мы можем узнать IP-адрес субъекта, на кого зарегистрирован домен, адрес владельца домена и др.