конфіденційної та іншої інформації про об'єкти зацікавленості в умовах загострення воєнно-політичної обстановки.

В останні роки для отримання інформації активно використовуються латентні ресурси мережі Інтернет та спеціальне програмне забезпечення. Це дозволяє користуватися ресурсами низки прихованих веб-сайтів через віртуальні канали замість прямого зв'язку. Так, для доступу до прихованих ресурсів Інтернету використовуються спеціальні програмні продукти «Tor», «I2P» та інші. А за допомогою спеціальних сайтів (наприклад, www.bitcoin.org) може здійснюватися фінансування джерел інформації.

Програмний продукт «Tor» формує ланцюжок зашифрованих з'єднань таким чином, що при переході на певний сайт фіксація такої дії не здійснюється. Вузли мережі поділяються на такі, через які проходить трафік (релеї), а також такі, через які здійснюється вихід до заблокованих сайтів відкритого Інтернету. Адресами прихованих сторінок в мережі «Tor» є криптографічні комбінації букв і чисел з доменним ім'ям «.onion», які постійно змінюються. Сама мережа формується користувачами, які встановлюють точки виходу та надають приховані дані для доступу до необхідних сайтів. Внутрішні сайти «Tor» приховані на веб-серверах та є ресурсами псевдо-домену .onion. Тому, інформація, що отримується із таких ресурсів, має подвійний рівень захисту: унеможливлює відстеження власника сайту; унеможливлює (ні власником, ні будь-ким іншим) відстеження користувача (шукача) інформації.

За результатами дослідження офіційних статистичних даних за період з січня по вересень 2017 року встановлено, що загальна кількість щоденних користувачів «Tor» на території України займає п'яте місце світового обсягу. А кількість виявлених правоохоронними органами України груп користувачів, причетних до незаконної діяльності із використанням ресурсів прихованого Інтернету, складає лише 16, що є незначним порівняно із загальним обсягом користувачів.

Наступним способом отримання інформації є використання файлообмінних латентних мереж, таких як «P2P». Тут за допомогою спеціальних трекерів отримується необхідна інформація, яка через технічні ресурси (комп'ютери) декількох користувачів Інтернету акумулюється та узагальнюється. Однією із умов такого способу отримання інформації є обов'язкове знання електронної адреси джерела інформації та цифрового сертифікату.

Інший спосіб дозволяє отримати інформацію за допомогою «Freenet», що використовує існуючу мережу відкритого Інтернету та технічні ресурси інтернет-провайдерів, але унеможливлює ідентифікацію дій користувача в загальній мережі (не фіксує URL-адреси).

Всередині мережі «Freenet» функціонує спеціальний програмний продукт «Frost» (режим доступу: www.freenetproject.org/frost.html),

який дозволяє анонімного отримувати інформацію на форумах або через окремі файли.

Клоном «Freenet» є «I2P» (Invisible Internet Project). Дана мережа створена з метою забезпечення анонімного доступу до різноманітних послуг, пов'язаних, наприклад, з обміном миттєвими повідомленнями через спеціальну електронну пошту, сайти, сервіси передачі файлів тощо. Передана по мережі інформація зашифровується, а сама мережа залишається децентралізованою. До I2P-мереж зловмисники підключаються не тільки через комп'ютери, але й смартфони та планшети з операційною системою «Android».

«Hyperboria» являє собою експериментальну децентралізовану мережу, засновану на мережевому протоколі «cjdns». Передача даних на фізичному рівні може здійснюватися як з використанням інфраструктури Інтернету, так і безпосередньо між маршрутизаторами, що дозволяє створити повністю незалежну від Інтернету глобальну мережу з комірчастою топологією. Трафік, що використовується в «Hyperboria», зашифровується, однак адреси відправника та одержувача залишаються відкритими.

Для організації спеціальної анонімної мережі використовується програмне забезпечення «Veiled». Даний продукт функціонує без завантаження й встановлення на таких пристроях, як «iPhone» та комп'ютери з операційними системами Windows, Mac і Linux. «Veiled» дозволяє зашифровувати інформацію та здійснювати приховане спілкуватися в чаті.

Використання можливостей турецького програмного продукту «GetContact» для ідентифікації осіб дозволило зібрати зловмисникам значний обсяг інформації про телефонні номери та імена користувачів мобільних пристроїв зв'язку.

Іншим способом збору інформації про дії користувачів Інтернету є використання спеціальних лічильників, віджетів та інших пристроїв і трекерів. За інформацією німецького додатку «Ghostery» на кожному десятому ресурсі одночасно працює більше десяти таких інструментів, що охоплює майже 80 % всіх сайтів світового Інтернету. Російська Федерація займає у світі третє місце по використанню прихованих датчиків інтернет-поведінки користувачів (cookies). Так, наприклад, у березні 2018 року лише на сайті Gismeteo використовувалось близько дев'яти трекерів для збору конфіденційної інформації, зокрема, щодо силових структур України. Так, тільки одна російська DMP-компанія (DMP – Data management platform – платформи зі збору, сегментації та передачі конфіденційних даних про користувачів) за допомогою інструментів «Aidata» і «Openstat» акумулювала близько декількох сотень мільйонів cookies.

Наступним способом є отримання інформації через інтернет-провайдерів за допомогою «clickstream» (потоку кліків). З цією метою використовується спеціальне обладнання для автоматичної передачі інформації, зокрема, конфіденційного https-трафіка.

Використання засобів сканування Wi-Fi мереж для отримання та систематизації інформації про активність користувачів Інтернету. За сукупністю отриманих показників визначалися місця дислокації підрозділів збройних формувань України, їх географічні координати, розраховувалися параметри вогневого ураження. Так, з використанням зазначеного способу на початку 2015 року артилерією противника було здійснено обстріл місць дислокації прикордонних підрозділів та штабу АТО в м. Кроматорськ.

Дослідження зв'язків он-лайн активності клієнтів окремих банків (через розрахунки електронними картками) з їх діяльністю в режимі оф-лайн дозволяє чітко встановити місце знаходження, отримати персональні дані та конфіденційну інформацію про об'єкт зацікавленості.

Використання масивів даних ріелторських компанії, супермаркетів та інших постачальників послуг за умов активації через номер мобільного телефону. Так, наприклад, у 2016 році за результатами активного розквартирування військовослужбовців та аналізу масивів даних фірм-постачальників таких послуг була зібрана майже вся інформація про укомплектованість та склад збройних формувань і правоохоронних органів України в місцях їх дислокації.

Використання інформації про активність мобільних телефонів надає можливість відслідковувати переміщення військових колон та особового складу, їх маневр та кількісний склад. Крім того, за допомогою «привабливих» SMS повідомлень (наприклад, рекламних) користувач мобільного пристрою добровільно завантажує спеціальний додаток, який за окремими параметрами отримує доступ майже до всіх аудіо, фото й відео даних.

З використання інструменту скоринга збирається конфіденційна інформації з соціальних мереж та загальнодоступних сайтів і масивів даних.

Таким чином, розглянуто окремі прийми та способи, за допомогою яких спецслужби іноземних держав та зацікавлені організації і особи можуть отримувати конфіденційну та іншу необхідну інформацію в умовах загострення воєнно-політичної обстановки.

З метою протидії зазначеній протиправній діяльності пропонується прийняття нових процесуальних норм, які регламентують використання програмно-технічних комплексів для здійснення моніторингу кіберпростору та встановлення фактичних даних про осіб, причетних до правопорушень. Разом із тим, слід зосередити увагу на реалізацію заходів із використанням методів розвідувальної та контрозвідувальної діяльності, боротьби з кіберзлочинністю.

Одержано 31.10.2018