

DARKNET ЯК ДЖЕРЕЛО ПРОТИПРАВНОГО КОНТЕНТУ

Даркнет – це підпільний Інтернет, який існує на базі основного [1]. Даркнет або ще як його називають «DarkNet», «DeepWeb», «глибокий Інтернет», «темний Інтернет» – вищий за ступенем анонімності сегмент Інтернету, до якого неможливо підключитися через звичайний браузер. У ньому сконцентровані спільноти, що займаються незаконною діяльністю, в тому числі торгівлею зброєю, банківськими картами, наркотиками і т.д., але так само існує й безліч цілком легальних і нешкідливих проєктів – бібліотеки, літературні журнали [2]. Іншими словами – Інтернет мережа, яка містить контент, який в певні мірі при його застосуванні/використанні може бути незаконним. При цьому, зберігається анонімність (приватність) користувачів. Отже «DarkNet» – це мережа, яка містить контент, який є виключно протизаконним (торгівля зброєю, наркотики, порнографічна продукція, насильство тощо); частково відноситься до протизаконним (данні платіжних карток, особисті данні тощо); відкритого доступу але з певним обмеженням передбаченого законодавством про захист авторських прав (бібліотека, журнали, музика, відео тощо), а також різноманітні форуми без обмежень свободи слова.

Відмінність «темного» Інтернету від звичайного, в тому, що у невидимому для більшості користувачів існують сотні сайтів, де можна безперешкодно купити заборонену або обмежену продукцію зброєю або скористатися послугами хакерів [3]. Зайти в нього можна тільки за допомогою спеціальних програм, здебільшого це програми, які поширюються некомерційними організаціями. Як приклад, одною з таких програм є Tor, яка об'єднує програму та браузер разом – все це підноситься як Tor-браузер, тобто, цілий пакет програм: маршрутизатор, який дозволяє увійти в даркнет, і спеціальна версія Firefox, де відключені або обмежені всі можливості, що дозволяють ідентифікувати особу [1]. Тобто, стати користувачем можна тільки

після встановлення спеціального програмного забезпечення.

Сьогодні, в мережі Інтернет досить широко розписано покроковість дій користувачів, які мають намір стати учасниками «тасмного» Інтернету. Також, необхідно зазначити, що сайти в мережі Tor, мають свої особливості, зокрема, багато сайтів в цій мережі виглядають подібним чином: not Evil – пошук по мережі Tor; oneirun – каталог посилань; TORCH – ще один пошук; CoinMixer – міксер біткоїни; Флибуста – книжкова бібліотека; Hidden Answers – сервіс анонімних запитань і відповідей; rutrackeripnext.onion – дзеркало rutracker.org; rutorc6mqdinc4cz.onion – дзеркало rutor.info тощо [2].

На перший погляд, можна припустити, що користувачів «Даркнет» не можна притягнути до кримінальної відповідальності. Утім, зарубіжна практика свідчить про притягнення осіб, які здійснювали торгівлю зброї, наркотиків через даркнета. Це стосується також виявлення та закриття таких сайтів, але здебільшого виявляються такі злочини під час роботи під прикриттям [4]. Також, Tor-браузера не є гарантією анонімності вироблених вами дій. Відповідно інформація та пропозиції в цій мережі можуть бути помилковими, шахрайськими [2]. Тобто користувач може бути жертвою шахрайських дій. І відповідно, анонімність обох користувачів унеможливить встановлення факту вчинення шахрайства та осіб причетних до нього.

Підсумовуючи наведене, зазначимо, «Darknet» – це мережа, яка містить контент, який в більшості випадків заборонений (або наслідки його використання є забороненими) у вільному обігу. При цьому, користувачі даною мережі залишають в анонімності свої дані, і вони не є «захищеними» та недосяжним для правоохоронної системи.

Список використаних джерел

1. На власному досвіді: що можна купити в даркнеті та як забрати товар. Українська правда. <https://bzh.life/ua/lyudi/ludi-opyt-darknet>.
2. Как попасть в «Даркнет». <http://9net.ru/191-darknet-kak-voyti.html>.
3. Очень темные дела. Lenta.ru. <http://darknet.lenta.ru/>.
4. Joseph Cox The dark web as you know it is a myth. 18.06.2015. <https://www.wired.com/2015/06/dark-web-know-myth/>.