Козицька Олена Геннадіївна,
заступник начальника 1-го відділення СВ Хмельницького відділу поліції ГУНП в Хмельницькій області, кандидат юридичних наук

ДАРКНЕТ З ТОЧКИ ЗОРУ КРИМІНАЛІСТИЧНОЇ НАУКИ

Створення у другій половині XX століття всесвітньої системи об'єднаних комп'ютерних мереж для зберігання, обробки та передачі інформації фактично ознаменувало початок цифрової революції. Наразі комп'ютерною мережею Інтернет користується 3,9 млрд. людей або 51,2 % населення планети (статистичні дані Міжнародного союзу електрозв'язку станом на грудень 2018 року) [4]. При цьому особливе занепокоєння викликає те, що окремі сегменти Інтернету стали ринком розповсюдження зброї, дитячої порнографії, підроблених документів, різноманітних технічних засобів для доступу до банківської таємниці, торгівлі людьми і наркотиками. Крім того, останнім часом спостерігається тенденція до збільшення кількості зламів скриньок електронної пошти, урядових ресурсів, отримання доступу до матеріалів, які містять державну таємницю [5, с. 42].

Усе це обумовлює необхідність розробки заходів, спрямованих на протидію кіберзлочинності та необхідність дослідження криміналістичною наукою тих сегментів Інтернету, які найчастіше виступають місцем і засобами вчинення злочинів.

Загалом, Інтернет-середовище умовно можна поділити на три рівні:

– «поверхневий» Інтернет – сукупність індексованих сайтів, які можна знайти за допомогою звичайних пошукових систем (Google Chrome, Safari та ін.). Користувачі поверхневого Інтернету визначаються на основі IP адреси;

– «глибинний» Інтернет (Deep web, Deep Internet), де знаходяться веб-сторінки, не пов'язані з іншими гіперпосиланнями, а також сайти, доступ до яких відкритий лише для зареєстрованих користувачів та Інтернет-сторінки, вхід до якої можливий лише у випадку введення паролю [2]. Дана частина Інтернету є недоступною для пошукових систем. Прикладом глибинних Інтернет-ресурсів є державні бази даних, електронні бібліотеки, різноманітні реєстри тощо;

– Даркнет («Тіньова мережа», «Темна павутина») – прихована мережа, з'єднання в якій встановлюються лише між довіреними пірами (рівноправними учасниками (користувачами) мережі), з використанням нестандартних протоколів та портів. До ресурсів Даркнету належить також Telegram через особливості свого шифрування, заборони використання в окремих країнах, а також функціонування зашифрованих каналів продажу заборонених речовин, координації протиправних діянь.

Термін «Даркнет» з'явився у 1970-х роках в той час, коли велася розробка мережі ARPANET (праобразу сучасного Інтернету), і використовувався для позначення мереж, які ізолювалися від загальної

мережі з метою безпеки. Широке розповсюдження даний термін отримав у 2002 році завдяки публікації працівників компанії Microsoft Пітера Біддла, Пола Інгленда, Маркуса Пейнаду та Брайана Уілмана «Даркнет і майбутнє розповсюдження інформації» [3].

Нині невидимий Інтернет налічує більше, ніж 8000 терабайт інформації (600 мільярдів окремих документів проти 20 млрд. у «поверхневому» Інтернеті) [6, с. 98], що збільшується кожного дня.

Отримання доступу до Даркнет потребує установки і використання спеціального програмного забезпечення, найбільш розповсюдженим з яких є система Tor (The Onion Router). Tor – це вільне і відкрите програмне забезпечення для реалізації так званої «цибулевої» маршрутизації другого покоління, що фактично є системою проксі-серверов, яка дозволяє встановлювати анонімне мережеве з'єднання із захистом від зняття інформації [7, с. 651].

Висока анонімність, притаманна Даркнету, обумовлює використання його ресурсів не лише для спілкування без обмежень та контролю з боку держави, але й з метою вчинення злочинів.

Найбільш поширеними злочинами, які вчиняються за допомогою Даркнету, є:

– злочини, пов'язані з незаконним обігом наркотичних засобів, психотропних речовин (у мережі не лише можна придбати будь-який наркотичний засіб чи психотропну речовину, але й знайти детальну інструкцію їх виготовлення),

– злочини, пов'язані з незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами;

– розповсюдження порнографічної продукції, а також втягнення у заняття проституцією та звідництво;

– торгівля людьми;

– злочини, предметом посягання яких є інформація (в Даркнеті можна відшукати і придбати практично будь-яку інформацію, в тому числі з обмеженим доступом (наприклад, інформацію, яка містить персональні дані інших осіб, або ж банківську чи державну таємницю), а також замовити злам чужої електронної пошти, сайту, бази даних;

– злочини, пов'язані з порушенням авторських та суміжних прав (у Даркнеті розміщені бібліотеки, відеотеки, наповнені незаконним контентом);

– шахрайства з фінансовими ресурсами, несанкціонований доступ до електронних платіжних систем.

Також у Даркнеті легко можна відшукати особу, яка погодиться стати виконавцем вбивства, підпалу, терористичного акту, доведення до самогубства тощо.

Підходи до державного контролю і правового регулювання Даркнету можна поділити на три групи:

а) державна позиція, відповідно до якої Даркнет повинен бути забороненим, оскільки він використовується у злочинних цілях і не дозволяє ідентифікувати злочинців;

б) позиція прихильників вільного Інтернету, які виступають проти будь-якого втручання і контролю з боку держави;

в) підхід, який враховує неможливість заборони Даркнету і нейтральність оцінки самої анонімної технології соціальної комунікації. При цьому в межах останнього підходу відмічається необхідність як технічного, так і правового реагування на загрози, які несе Даркнет. Вказана позиція є найбільш збалансованою, оскільки в ній Даркнет позиціонується як інструмент, який набуває суспільної небезпеки в зв'язку зі злочинною метою користувачів, а не сам по собі. Крім того, поточний рівень розвитку не дозволяє державам блокувати використання Даркнету. Разом з цим необхідно розробляти правові і технічні засоби боротьби з його небезпечними проявами [1, с. 11].

У зв'язку з викладеним, можемо дійти висновку, що Даркнет як місце і засіб вчинення злочинів потребує детального дослідження криміналістичною наукою. Зокрема, актуальними є наукові розвідки щодо способу вчинення злочинів у Дарнеті, їх слідової картини, особливостей виявлення цих злочинів на стадії готування, вчинення та приховання, тактики проведення окремих слідчих та негласних слідчих (розшукових) дій.

Список використаних джерел:

1. Васильев А., Ибрагимов Ж., Васильева О. Даркнет как ускользающая сфера правового регулирования. *Юрислингвистика*. 2019. № 12 (23). С. 10–12. URL: https://doi.org/10.14258/leglin(2019)1202(2019).
2. Глубокая сеть. *Википедия – свободная энциклопедия* : вебсайт. URL: https://ru.wikipedia.org/wiki/Глубокая_сеть.
3. Даркнет. *Википедия – свободная энциклопедия* : вебсайт. URL: https://ru.wikipedia.org/wiki/Даркнет#cite_note-14.
4. Интернет-доступ (мировой рынок). Tadviser. Государство. Бизнес. ИТ, 06.03.2019 : вебсайт. URL: http://www.tadviser.ru/index.php/Статья:Интернет-доступ_(мировой рынок).
5. Каримов В. Х. Актуальные вопросы выявления и расследования преступлений, совершаемых с использованием средств шифрования данных в сети интернет. *Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами* : сборник научных статей. Барнаул : Изд-во Алт. ун-та, 2017. Вып. XIV. С. 40–48.
6. Ткачук Т. Ю. Тіньовий Інтернет: співвідношення можливостей і загроз. *Інтернет речей: проблеми правового регулювання та впровадження* : матеріали наук.-практ. конф., 24 жовт. 2017 р. Київ : Політехніка, 2017. С. 94–100.
7. Узденов Р. М. Новые границы киберпреступности. Всероссийский криминологический журнал. 2016. № 4, т. 10. С. 649–655.