УДК 004.056:341.48

ГУЦАЛЮК М.В., *доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.,*
провідний науковий співробітник Міжвідомчого центру з проблем боротьби з організованою злочинністю при РНБО України

ПРОТИДІЯ ВИКОРИСТАННЮ УЧАСНИКАМИ ЗЛОЧИННИХ УГРУПОВАНЬ МЕРЕЖІ “ДАРКНЕТ”

Анотація. *В статті досліджуються питання протидії кіберзлочинності, зокрема використання мережі “Даркнет”. Пропонуються напрями вдосконалення чинного законодавства.*

Ключові слова*: кіберзлочинність, “Даркнет”, міжнародне співробітництво.*

Summary. *The article deals with the issues of cyber crime, and using the Darknet in particular. The improvements of the legislation in this area are proposed.*

Keywords: *cyber crime, Darknet, international cooperation.*

Аннотация. *В статье исследуются вопросы противодействия киберпреступности, в частности использование сети “Даркнет”. Предлагаются направления совершенствования действующего законодательства в данной сфере.*

Ключевые слова: *киберпреступность, “Даркнет”, международное сотрудничество.*

Постановка проблеми. Поширення діяльності в Інтернеті найрізноманітніших верств населення по всьому світу та використання ними новітніх інформаційних технологій останнім часом відзначається значним зростанням кіберзлочинності.

Відповідно до звіту однієї з провідних компаній з інформаційної безпеки “Herjavec Group” активність кіберкриміналітету у найближчі десятиліття стане одним з найбільших викликів для людства. У 2021 році передбачається зростання щорічних збитків від кіберзлочинності в розмірі 6 трлн доларів США (порівняно з 3 трлн. у 2016 році). Це більше ніж прибуток від усієї глобальної незаконної торгівлі наркотиками [1].

Закон України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 р. № 2163-VIII визначає кіберзлочинність як сукупність кіберзлочинів. У свою чергу кіберзлочин або комп’ютерний злочин визначено як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

До таких злочинів слід віднести правопорушення, передбачені розділом XVI КК України “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” (ст. 361-363). Також до даної категорії слід віднести і інші злочини, наприклад, передбачені ч. 3 ст. 190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки); ст. 200 (використання підроблених електронних засобів доступу до банківських рахунків); ч. 4 ст. 301 (збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки) КК України. На нашу думку, законодавець повинен надати чіткий перелік таких злочинів, що дасть можливість проведення якісного аналізу статистичних даних з метою вироблення стратегії і тактики протидії кіберзлочинності.

Інформаційні ресурси, як державні, так і приватного сектору, а також громадян, постійно піддаються різноманітним кіберзагрозам. Однією з найнебезпечніших кіберзагроз є кібератаки. В європейському законодавстві діє Директива щодо кібератак на інформаційні системи (Directive 2013/40/EU Of The European Parliament And Of The Council, of 12 August 2013) [3], у якій зазначається, що кібератаки на інформаційні системи, зокрема, пов’язані з організованою злочинністю, є зростаючою загрозою в Європейському Союзі та у всьому світі. Це, в свою чергу, призводить до зростання занепокоєння з приводу потенційних терористичних або політично мотивованих нападів на інформаційні системи, які є частиною критичної інфраструктури держав-членів Союзу.

Водночас організовані злочинні угруповання у своїй діяльності широко використовують мережу “Даркнет” (Darknet), веб-сайти якої не індексуються і на них не можливо потрапити через Google чи Yahoo. Ця частина Інтернету ніяк не врегульована законодавчо, діяльність у ній майже неможливо проконтролювати, а тому криміналітет на основі цієї мережі постійно створює і удосконалює протиправну діяльність.

Результати аналізу наукових публікацій. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська, П.Д. Біленчук., К.І. Бєляков, В.М. Бутузов, В.Д. Гавловський, М.А. Погорецький, В.Г. Хахановський, В.П. Шеломенцев, О.М. Юрченко та інші. Проте стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі спонукає для подальших досліджень.

Метою статті є визначення проблем протидії використання організованими угрупованнями мережі “Даркнет”, а також напрацювання відповідних пропозицій для ефективної протидії кіберзлочинності.

Виклад основного матеріалу. Міжнародна спільнота розпочала активну протидію кіберзлочинності, включаючи міжнародну, наприкінці минулого століття. Тоді в різних країнах були прийняті перші закони, в яких передбачена кримінальна відповідальність за відповідні правопорушення, створені спеціалізовані правоохоронні підрозділи. У 2001 році у Будапешті була прийнята Конвенція про кіберзлочинність [4], яка була ратифікована Верховною Радою України із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.05 р. Конвенцією визначено декілька груп правопорушень, які відносяться до кіберзлочинів. Це зокрема:

– правопорушення проти конфіденційності;

– правопорушення, пов’язані з комп’ютерами;

– правопорушення, пов’язані зі змістом;

– правопорушення, пов’язані з порушенням авторських та суміжних прав.

Крім прийняття відповідного законодавства в багатьох країнах створюються спеціалізовані правоохоронні органи. Крім цього виникла необхідність тісного міжнародного співробітництва у цій галузі – адже кіберзлочинність не має кордонів. Зокрема дані питання розглядалися на Першому міжнародному конгресі з кіберзлочинності E-Crime London 2002 [5].

Слід зазначити, що організованість хакерів постійно зростає. Так, за оцінками деяких дослідників, ще 7 років тому 80 % хакерів діяли самостійно, а вже сьогодні 80 % їх входять до складу злочинних угруповань, які мають переважно транснаціональний характер.

У своїй діяльності такі групи широко використовують криптографічні технології мережевої анонімності і онлайн-розрахунків, які дозволили злочинцям створити чорний ринок, де продають і купують наркотики, крадені і контрафактні товари, дитячу

порнографію, зброю тощо. Такий електронний ринок в Інтернеті має назву “Даркнет”. Сам термін з’явився ще до появи Інтернету і означав високу ступінь анонімності в комп’ютерній мережі, яка досягалася завдяки використанню нестандартних протоколів та портів. Також злочинцями широко використовується “Діпвеб” (Deep Web) – мережа сайтів, які не індексуються пошуковими системами.

У “Даркнеті” існує велика кількість хакерських спільнот, які спеціалізуються у своїй діяльності за конкретними напрямами, наприклад, неправомірний доступ до комп’ютерних систем, продаж шкідливого програмного забезпечення (далі – ШПЗ), організація кібератак, викрадення та продаж персональних даних тощо.

Водночас сьогодні активно формується ринок хакерських послуг, завдяки якому відбувається поєднання традиційної злочинності, включаючи організовані її форми, з кіберзлочинністю – адже немає потреби бути фахівцем в сфері інформаційних технологій – достатньо замовити відповідні послуги через Інтернет та розрахуватися за послуги криптовалютою. Даний кіберринок постійно зростає завдяки анонімності на основі спеціальних протоколів зв’язку, реалізованих в цьому інтерфейсі.

Найбільш популярними у “Даркнеті” є так звані “Служби злому”, у яких хакера можна найняти для проникнення до облікових записів Gmail або Facebook чи іншого виду кібершпигунства.

Згідно розслідування “Business Insider” [6], вартість проникнення в аккаунт Gmail коштує близько 90 доларів. Вартість злому Facebook-акаунта становить 350 доларів

Іншими поширеними товарами у Діпвеб є курси хакера, які продаються за 20 доларів. В них розповідається про пошук основних уразливостей сайтів, DDoS атаки або методи пошкодження веб-сайтів.

Популярними також є навчальні посібники, що надають інструкції для злочинців та хакерів, які хочуть отримати знання з кардингу, інформацію про запуск комплектів експлойтів, керівництво по організації спаму та фішингу тощо. Хакерські спільноти дуже активно займаються продажем викрадених кредитних карток, щоб охопити ширші аудиторії та надавати спеціалізовані послуги за більш високими цінами.

Зазначимо, що якщо наймаються професійні команди хакерів, то використовується зв’язок, який здійснюється через кілька спеціалізованих сервісів. Тому справжніх виконавців відслідкувати досить важко, і у багатьох випадках хакери можуть просто не виконувати свої завдання.

Методи розрахунків на чорному ринку постійно змінюються. Це пов’язано з тим, що крадіжка криптовалют стає досить поширеним явищем. Відповідно до дослідження аналітичної компанії “Autonomous Research” за минулі роки з моменту появи криптовалют хакери викрали понад 1,2 млрд. доларів в еквіваленті Bitcoin та Ethereum. Постійне зростання кібератак на криптовалюту відзначає і компанія “Bloomberg” [7].

В зв’язку з постійно зростаючим впливом кіберзлочинності на інформаційне суспільство Європейський центр боротьби зі злочинністю Європолу щорічно готує звіт “Оцінка загрози організованої злочинності в Інтернеті” – IOCTA. В звіті IOCTA – 2017 зокрема зазначається, що “Даркнет” ринки є ключовим міжгалузевим інструментом для інших сфер злочинності [8] . Надаючи доступ для платіжних даних для здійснення різноманітних видів шахрайства та підробних документів, торгівлі людьми тощо, цей тіньовий ринок сприяє незаконному обігу наркотиків, зброї та матеріалів сексуальної експлуатації дітей та іншій протиправній діяльності.

Аналітичні матеріали для IOCTA готуються на основі роботи експертів Європолу, правоохоронних органів, партнерів з приватного сектору та наукового середовища. На жаль, в Україні такі дослідження ще не проводилися, хоча актуальність цієї

проблеми вкрай висока, адже українські хакери постійно розшукуються правоохоронними органами різних країн по всьому світу, починаючи від міжнародного злочинного угруповання “CarderPlanet”, яка діяла на початку 2000-х рр. Затримані в різних країнах громадяни України через завдані іноземним компаніям мільйонні збитки отримують великі (30 – 40 років) терміни позбавлення волі.

Серед успішних заходів щодо протидії організованій кіберзлочинності слід зазначити наступні:

У грудні 2015 року німецькі поліцейські з Лейпцига конфіскували велику партію наркотиків, яку продавали через “Даркнет”, загальною вагою більше 210 кілограмів. Експерти оцінили поставку в 4,25 мільйони доларів США.

У жовтні 2016 року пройшла масштабна поліцейська операція під назвою “Гіперіон”. У ній приймали участь правоохоронці з США, Британії, ЄС, Канади, Австралії, Нової Зеландії. В результаті лише у Швеції було ідентифіковано і затримано 3000 покупців наркотиків, 6 продавців були заарештовані та отримали десятирічні терміни в’язниці.

У грудні 2016 року поліція Мальти заарештувала членів організації злочинного угрупування за продаж через Інтернет підроблених купюр Євро. Банкноти по 20, 50 і 100 Євро продавалися за 30 % від їх номінальної вартості, а оплату можна було здійснити в біткоїнах. Було конфісковано 160 000 Євро.

У березні 2017 року ірландським поліцейським вдалося виявити контрабандиста, який торгував зброєю через Інтернет по всьому світу. Продавця було затримано в результаті спільної операції ФБР та ірландської митниці.

Окремо слід відзначити масштабну операцію за участі правоохоронців 30 країн з ліквідації кібермережі “Avalanche” у 2016 році, яка проходила за підтримки Центру боротьби з кіберзлочинністю Європолу (EC3) та Об’єднаної групи боротьби з кіберзлочинністю (J-CAT), а також Євроюсту та Європейської банківської федерації (EBF). Одночасно в багатьох країнах було заарештовано 178 осіб – співучасників організованої злочинної групи, яку організував та очолював громадянин України [9].

В 2018 році в США арештовано трьох українських громадян – Федіра Хладира (33 роки), Дмитра Федорова (44 роки) та Андрія Копака (30 років). Їх підозрюють у зламі тисячі комп’ютерних систем і викраденні мільйонів номерів кредитних карт клієнтів. Після чого хакери продавали інформацію за викуп [10].

Правоохоронці, постійно підвищуючи рівень своєї майстерності, вишукують все нові методи протидії кіберзлочинності.

Наприклад, в Канаді правоохоронці використовують спеціалізовану пошукову систему, яка аналізує інформацію з “Даркнету”. Завдяки використанню цієї системи у серпні 2016 року відбулося затримання жінки, яка придбала через Інтернет смертельний радіоактивний елемент Полоній-210.

У березні 2017 року поліція Данії повідомила, що розробила власну аналітичну систему під назвою EC3, яка порівнює активність у “Даркнеті” з криптовалютною активністю користувача. Результатом використання такої системи став арешт 150 користувачів, які придбали заборонені товари.

Поліцейський департамент в американському місті Бостон розробляє програму, яка аналізує дані з “Даркнет” та соціальних мереж. Даний інструмент допоможе протидії тероризму, торгівлі людьми та захистить дітей від педофілів у мережі. Програмне забезпечення допоможе визначити геолокацію можливих правопорушень у реальному часі.

Крім того, правоохоронні органи для протидії кіберзлочинності, згідно огляду Дослідницького інституту “RAND Europe” [11], використовують наступні методи:

1. Традиційні методи розслідування.

Як тільки слідчі виявляють активність, пов’язану з наркотиками в реальному світі, вони аналізують відповідний кіберпростір. Спостереження дозволяють визначити ті точки, де зустрічаються реальний і віртуальний світ. Наприклад, арешт члена організації злочинного угрупування Ульбрихта в 2013 році відбувся, коли він скористався загальнодоступною мережею Wi-Fi, що співпало з появою адміністратора Silk Road у віртуальному просторі.

2. Отримання даних з відкритих веб-сайтів.

Торговці наркотиками використовують свої глибоко законспіровані сайти тільки як магазини, займаючись пошуком клієнтів у загальнодоступних мережах. Це робить дилерів протиправної продукції більш уразливими. Тому власники загальнодоступних сайтів повинні передавати у поліцію будь-яку інформацію щодо протиправної діяльності на їх ресурсах.

3. Перехоплення поштових відправлень.

Правоохоронні організації працюють із компаніями доставки та поштовими відділеннями, щоб досліджувати підозрілі пакети. Поліцейські можуть також взяти номер підозрілого відправлення, щоб стежити за одержувачем.

4. Великі дані і самонавчання машин.

Використовуючи великі обсяги даних, поліцейські визначають зв’язки, які неможливо встановити іншими способами. Вони враховують IP-адреси та розміщують онлайн-інформацію, роблячи висновки і поступово налаштовують до аналізу штучний інтелект.

5. Відстеження грошових потоків.

Хоча криптовалюта біткоїн має високу ступінь анонімності, слабким місцем її є купівля або продаж цифрової валюти. Поліція може вимагати дані від криптобіржі, хто і коли здійснив транзакції з криптовалютою. Правоохоронні органи також співпрацюють з цією метою з банками.

6. Робота під прикриттям.

Поліцейські агенти в різних країнах входять до довіри до адміністраторів заборонених сайтів, а також зображують продавців або роздрібних та оптових покупців.

7. Злом.

Модифіковане на замовлення поліцейських або ФБР програмне забезпечення широко використовується для визначення користувачів Deep Web. Наприклад, саме таким чином було розкрито великий нелегальний форум кіберзлочинців. Спеціалісти ФБР внесли в нього програму, яка пересилала IP-адреси користувачів до відповідного підрозділу служби.

В Україні після потужних кібератак, які були спрямовані на об’єкти критичної інфраструктури, було прийнято низку заходів щодо посилення кібербезпеки та протидії кіберзлочинності. Зокрема це прийняття Стратегії кібербезпеки України, створення Департаменту кіберполіції, посилення спроможності нових структур завдяки західним партнерам, навчання кіберполіцейських та слідчих виявленню та розслідуванню кіберзлочинів [12].

Проте, кількість кіберзлочинів продовжує щорічно зростати. Але найбільше занепокоєння викликають використання “Даркнету” для поширення наркотиків, у тому числі серед юнаків та дітей. І хоча точну кількість таких правопорушень через високий рівень латентності визначити складно, масштаби проблеми впажають суспільство [13].

Висновки.

Необхідно зазначити, що більш ефективній боротьбі з кіберзлочинністю в Україні, особливо з організованими її формами, сприяло би посилення кримінальної відповідальності за вчинення зазначених злочинів. Через те, що покарання передбачене нормами чинного Кримінального кодексу, значно м’якше ніж покарання за аналогічні злочини в різних країнах, що призводить до формування в Україні протиправних угруппувань.

Доцільним було б прийняття змін до Кримінального процесуального кодексу України щодо внесення поняття “електронні (цифрові) докази та особливості роботи з ними” до рекомендацій експертів ЄС. Відповідні напрацювання у цьому напрямку проведені у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю [14].

Необхідною умовою протидії кіберзлочинності залишається співпраця з зарубіжними партнерами та активізація роботи з такими організаціями як Європол та Євроюст.

В зв’язку з необхідністю оперативного обміну комп’ютерними даними з відповідними правоохоронними структурами різних країн необхідно вдосконалити механізми співпраці з провайдерами та процедурами офіційної передачі таких даних.

Потрібно також постійно підвищувати професійну підготовку українських правоохоронців як завдяки зарубіжним партнерам, так і на основі розробки спеціалізованих курсів для вищих учбових закладів та курсів перепідготовки [15].

Отже, анонімною діяльність користувачів “Даркнет” залишається тільки до того часу, поки правоохоронні органи не починають вживати ефективні контрзаходи.

Використана література

1. Cybercrime Damages $6 Trillion By 2021. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (дата звернення 07.09.2018).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-VIII. – (База даних “Законодавство України” / ВР України). – Режим доступу : http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 07.09.2018).

3. Directive 2013/40/EU Of The European Parliament And Of The Council, of 12 August 2013. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32013L0040 (дата звернення 07.09.2018).

4. Конвенція про кіберзлочинність. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 07.09.2018).

5. Gutsalyuk M.V. Fighting Cybercrimes. URL: http://www.crime-research.org/library/Gutsaluk.html (дата звернення 07.09.2018).

6. Here’s how easy it is to buy anything – legal or illegal – on the ’dark web’. URL: https://www.businessinsider.com/find-anything-on-dark-web-tor-internet-2016-11 (дата звернення 07.09.2018).

Hacking communities in the Deep Web. URL: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref

7. Cryptocurrency Attacks Are Rising. URL: https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw (дата звернення 07.09.2018).

8. Internet Organised Crime Threat Assessment (IOCTA) 2017. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (дата звернення 07.09.2018).

9. В Україні затримали організатора хакерської мережі Avalanche. – Режим доступу : https://www.dw.com/uk/в-україні-затримали-організатора-хакерської-мережі-avalanche/a-42738720 (дата звернення 07.09.2018).

10. У США арештували українських хакерів. – Режим доступу : https://www.pravda.com.ua/news/2018/ 08/1/7188031 (дата звернення 07.09.2018).

11. The Hackers’ Bazaar : Markets for Cybercrime Tools and Stolen Data. URL: https://www.rand.org/events/2016/05/24.html (дата звернення 07.09.2018).

12. DR Mykhaylo Gutsalyuk. Ukraine’s Cybersecurity strategy and ways to implement it // European Cybersecurity journal. – Volume 2 (2016). – P. 65-69. – (The Kosciuszko Institute. Poland). URL: https://twitter.com/i/moments/781827366100140032 (дата звернення 07.09.2018).

13. Масштабы ужасают: в “Даркнете” работает крупная наркобиржа Украины. – Режим доступу : https://newsonline24.com.ua/masshtaby-uzhasayut-v-darknete-rabotaet-krupnaya-narkobirzha-ukrainy (дата звернення 07.09.2018).

14. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М.В. Гребенюк, В.Д. Гавловський, М.В. Гуцалюк, В.Г. Хахановський та ін.] ; за заг. ред. М.В. Гребенюка. – К. : МНДЦ при РНБО України, 2017. – 76 с.

15. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів : навч. посіб. / Н.М. Ахтирська . – К. : ВПЦ “Київський університет”, 2018. – 229 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~