ДО ПИТАННЯ ПРО КІБЕРЗЛОЧИННІСТЬ В СУЧАСНІЙ УКРАЇНІ

Ольга Борисівна БОДНАР-ПЕТРОВСЬКА,

PhD, науковий працівник, Університет Миколаса Ромеріса (Mykolo Riomerio Universitetas), Вільнюс, Литва (Vilnius, LR)
olha.bodnar@mruni.eu

Розглядаються такі поняття, як кіберзлочин і кіберзлочинність. Особливу увагу приділено трансформації кіберзлочину та кіберзлочинності, кіберпростору з 2014 року та, особливо з 2022 року. Проаналізовано стан протистояння цим явищам в Україні, міжнародній кібербезпеці.

Ключові слова: *кіберзлочин, кіберзлочинність, кіберпіратство, кібернетичне шпигунство, кіберзлочиний ринок росії, кібербезпека*

Проблематика кіберзлочинності, кіберпіратства є надактуальною у наш час, адже з появою віртуального простору для людства відкрились не лише безліч можливостей, які не завжди можна означити як добрі і корисні для самого споживача.

Україна є світовим лідером в царині диджіталізації, ставши першою в світі державою, де цифрові паспорти прирівнюються до паперових і пластикових оригіналів. Проте, всі ці технічні блага і зручності відкривають також нові можливості у вчинені злочинів та правопорушень у кіберпросторі.

Кіберзлочинність як окреме юридичне поняття існує в Україні вже більше 15 років, якщо вести відлік від вступання в силу засадничої Конвенції про кіберзлочинність. Будапештська конвенція Ради Європи про кіберзлочинність у кіберпросторі є основоположною базою для формування вітчизняного законодавчого кістяка в боротьбі з кіберзлочинністю. Як і 18 держав, що її ратифікували і 25 що підписали, Україна також приєдналась до неї 7 вересня 2005 року [1].

Будапештська Конвенція надає умовну кваліфікацію кіберзлочинів, поділяючи їх на такі категорії:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і стстем

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів

3) правопорушення, пов'язані зі змітом інформації, зокрема, дитяча порнографія, расизм та ксенофобія

4) правоорушення, пов'язані з порушенням авторських і суміжних прав

Згодом було ратифіковано додатковий протокол до Конвенції – в ньому виокремлено і доддано такий вид злочину, як криміналізація дій расистського та кснофобського характеру, вчинених через комп'ютерні системи (Додатковий протокол) [2].

Однак навіть з появою передумов для розвитку злочинності в інформаційній сфері, кіберзлочинність довгий час не розглядалась як окреме явище, яке вимагає серйозної юридичної бази. Окремий підрозділ в рамках МВС, на який було покладено боротьбу із кіберзлочинністю, з'явився лише в жовтні 2015 року. Стратегію кібербезпеки було ухвалено роком пізніше, а

спеціальний засадничий закон "Про основні засадизабезпечення кібербезпеки України" ухвалили лише в жовтні 2017 року [4].

Понятя «кіберзлочин» трактується як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачено Законом України Про кримінальну відповідальність та/або яке визнано злочином міжнародними угодами України, а кіберзлочинність визначено як сукупність кіберзлочинів.

Слід зазначити, що в Кримінальному Кодексі ще з 2003 р. існував окремий розділ XVI, який передбачав визначення ряду злочинів саме в сфері комп'ютерів та комп'ютерних мереж, який багато років був мало застосованим на практиці.

Аналізуючи кіберзлочинність в Україні, необхідно розглядати, як мінімум, чотири різних періоди. Така періодизація підтверджується і статистикою кіберзлочинів, яку наводить, наприклад, М. Кравцова [5] та статистична звітність кіберполіції [6].

Для системної боротьби із кіберзлочинами також важливо розуміти, що необхідно обов'язково враховувати саме технологічну складову. Знову ж таки, яскравим прикладом в цьому випадку може слугувати одна із засадничих особливостей цифрової економіки - а саме: потенційна транскордонність будь-яких цифрових послуг. Наприклад, сховище, яке містить цифровий актив, може знаходитись в одній країні, його власник в іншій, а розпорядник (брокер) - в третій. Це відкриває величезні можливості для бізнесу, особливо малого, але також робить можливими численні схеми транскордонного переміщення цінностей, вивезення капіталу і утворення корупційних грошових потоків (це не рахуючи крадіжки ключа, що підтверджує право власності на цифровий актив, і це суттєво ускладнює ефективне розслідування злочину - через конфлікт юрисдикцій і правового статусу активів). Натомість, наприклад, Закон України "Про віртуальні активи" [19] не містить взагалі жодної норми, які б впорядковувала транскордонні операції із цифровими активами. Те саме стосується транскордонних сервісів. Окремі елементи впорядкування транскордонних аспектів, для запобігання кіберзлочинності, почали впроваджуватись в Україні лише в 2022 р. (наприклад, в законопроекті №7357 "Про реєстрацію доменних імен").

Все це свідчить про те, що українське законодавство в галузі кібербезпеки і кіберзлочинності до останнього десятиліття знаходилось на несистемній стадії.

За даними компанції Zecurion Analytics, Росія входить до п'ятірки країн з найрозвиненішими кіберпідрозділами. До прикладу, Росія керує громіздким кіберзлочиним ринком, в якому спостерігається найбільша концентрація глобальних хакерських організацій. Марк Гудмен також зауважує, що в Росії, зокрема, в Санкт-Петерберзі діє злочинний синдикат під назвою Russian Business Network, який надає послуги хостингу для незаконного контенту. На своїх серверах цей синдикат зберігає все, що завгодно, від «дитячої порнографії до обміну сучаснішими експлойтами» [21].

У березні 2014 року під час підступної анексії Криму військами росії Україну було втягнуто в затяжний етап гібридної війни, який не лише триває до сьогодні, але й набирає все більших обертів. Методи ведення цієї війни різні, але мета завжди однакова – це дестабілізація і погіршення політичного, вій-

ськового, економічного становища в Україні та повернення її на геополітичну орбіту Кремля.

Агресія РФ у кіберпросторі почалась задовго до 2014 року, однак перед початком військової агресії проти України було розгорнуто кілька успішних кампаній кібернетичного шпигунства. Дані, отримані під час цих кампаній, забезпечили Росії стратегічну перевагу та можливість передбачати деякі кроки українського керівництва як у цивільній, так і у військовій сферах.

На жаль, з початком великої війни в Україні і зростанням волонтерсткого руху поле діяльності для кіберзлочинців ще більше розширилось. Окрім крадіжки матеріальної власності, значно зросла інформаційна атака. З'являються фейкові інформаційні сайти, повідомлення фейкового характеру. Виникає сталий вид бізнесу із застосуванням ботчатів, ботів – загальноприйняте означення неідентифікованих або складноідентифікованих з їх власниками сторінок, сайтів в соціальних мережах, задача яких публікувати недостовірну інформацію, відслідковуваня та реагування відповідним чином на публікації в соцмережах та ЗМІ. Оскільки даний нарямок злочину набуває все більше обертів та самовдосконалюється, дедалі важче їх виявляти і виокремлювати з загального інформаційного потоку - протистояти цим викликам можна лише зростаючою освіченістю споживачів, професійним моніторингом відповідних служб. Кіберзлочинність є міжнародною бідою, кримінальним явищем транскордонного харктеру, яке входить в трійку найсуворіших, боротись та протистояти якому неможливо, не об'єднавши зусилля світової спільноти.

З метою попередження або своєчасного усунення наслідків кіберзлочину, вдосконалення освіченостті серед споживачів комп'ютерних мереж, інтернету, в першу чергу слід чітко дотримуватись виконання поставлених безпекових цілей, передбачати своєчасність реагування на випередження, вдосконалювати законодавчу базу, проводити постійний мережевий моніторинг, забезпечувати тісне та своєчасне співробітництво на міжнародому рівні, вдосклоналювати технічну, інформаційну, правову бази. Кібербезпека сьогоді є однією з найбільш затребуваних навчичок як на світовому ринку, так і в Україні. Цей попит буде тільки зміцнюватися.

Список використаних джерел:

1. Кіберзлочинність та відмивання коштів. Дані Департаменту фінансових росзілдувань Державної служби фінаснсового моніторингу України. К., 2013

2. Про ратифікацію додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расиського та ксенофобського характеру, вчинених через комп'ютерні системи - Закон України від 21 липня 2006 року №23-V. Відомості Верховної Ради України. 2006. №39. С.1384. ст.328

4. Закон України від 05.10.2017 №2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403

5. Кравцова М. "Сучасний стан і напрями протидії кіберзлочинності в Україні" - Вісник кримінологічної асоціації України, №2, 2018 р.

6. Звітність Кіберполіції України - 2018, 2019, 2020, 2021 рр.

7. Воронцов А. В. Кіберзлочинність: її детермінація та запобігання - Лекція для Одеського Державного Університету Внутрішніх Справ, Одеса, 2016

8. Динаміка використання Інтернету в Україні: лютий-березень 2016 - КМІС, 2016

9. Фесик А.В. Роль органів державної влади у протидії кіберзлочинності. Вісник Кримінологічної асоціації України.2013. № 4

10. Маркарян М.В. До питання про реформування законодавства України у сфері кіберзлочинності - Конференція Актуальні проблеми державно-правового розвитку України в контексті євроінтеграційних процесів. Запорізький національно технічний університет, 23-24.06.2016

11. "За останні п’ять років кількість кіберзлочинів в Україні зросла вдвічі" - OpenDataBot, 21 жовтня 2019 р.

12. Закон України №5491-VI від 20.11.2012 (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)

13. Закон України від 20.11.2012 № 5492-VI/ - Відомості Верховної Ради (ВВР), 2013, № 51, ст.716.

14. " У львів'янки вкрали цифрову особу та набрали на її ім'я кредитів" - Фокус, 11 січня 2022 р.

15. Солонина Є. Злив персональних даних українців: що сталося і як захиститися - Радіо Свобода, 14 травня 2020 р.

16. А. Оленін "Великий злив" - Lb.ua, 23 січня 2022 р.

17. Stern J. Spiritual Property, “Intellectual” Property, and a Solution to the Mystery of IP Rights In Jewish Law [PDF]//University of St. Thomas Law Journa, 10 (2013), 603

17. Erlank W. Introduction To Virtual Property: Lex Virtualis Ipsa Loquitur, 2542

18. Закон №2074-IX від 17.02.2022 - Офіційний вісник України від 22.04.2022 — 2022 р., № 31, стор. 15, стаття 1629, код акта 110860/2022

19. Hampson N. Hacctivism, Anonymous & A new breed op protest in a Networked World [PDF]//Boston College International&Comparative Law Review, 35 (2011), 516

20. Гудмен М. Злочини майбутнього, www.fabulabook.com, (2016), 40

21. https://cybersecurityventures.com/jobs/