Чередниченко К.Ю.,
студентка 6 курсу, 2 групи, Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого

КРИМІНОЛОГІЧНА ТИПОЛОГІЯ КІБЕРЗЛОЧИНЦІВ

Ключові слова: кіберзлочинність, кіберзлочинець, типологія кіберзлочинців, хакери, кібертерористи.

Анотація. У тезах наведено статистичну інформацію щодо кількість вчинених кіберзлочинів та розмір завданої шкоди за 2019 рік. Проаналізовано різні типології кіберзлочинців.

Аннотация. В тезисах приведена статистическая информация о количестве совершенных киберпреступлений и размере причиненного вреда за 2019 год. Проанализированы различные типологии киберпреступников.

Ключевые слова: киберпреступность, киберпреступник, типология киберпреступников, хакеры, кибертеррористы.

Summary. The abstracts provide statistical information on the number of cybercrimes committed and the amount of harm caused in 2019. Various typologies of cybercriminals are analyzed.

Keywords: cybercrime, cybercriminal, typology of cybercriminals, hackers, cyberterrorists.

Стрімкий розвиток інформаційних технологій, поява нових, потужних комп'ютерів має не лише позитивні наслідки у вигляді різноманітних можливостей у навчанні, роботі, але й створює умови для вчинення кримінальних правопорушень. Кіберзлочинність – негативне явище, яке кожного року набирає оберти та швидко поширюється по всьому світу. Динаміка злочинності протягом останніх років характеризується хвилеподібними коливаннями, які чітко показують виражену тенденцію до зростання злочинності на території нашої держави. Висока складність соціальних систем є безумовною ознакою нелінійності законів залежності станів таких систем від певних зовнішніх та внутрішніх факторів [4]. За часів незалежності України галузь інформаційних технологій розвивалася практично без підтримки з боку держави, роль якої переважно зводилася до збирання статистичних відомостей, що часто не відображали реального стану справ. [7].

Постіндустріальна стадія розвитку людства вимагає переосмислення й уточнення багатьох положень кримінологічної теорії, перегляду традиційних підходів до боротьби зі злочинністю. На сучасному етапі кримінологія проходить етап формування нової парадигми, зміни наукового світогляду, генерування ідей та упровадження інновацій [5, 169]. Міжнародними експертами з кібербезпеки Cybersecurity Ventures було підраховано, що наприкінці 2016 року бізнес ставав жертвою кібер-атак кожні 40 секунд. У 2019 році – кожні 14 секунд, а у 2021 прогнозують, що атаки будуть здійснюватися кожні 11 секунд [1, с. 7].

Статистика вчинених в Україні злочинів показує, що з кожним роком з'являються нові схеми та способи вчинення злочинів у мережі Інтернет. Зокрема, лише за 2019 рік правоохоронними органами було отримано більше 20 000 повідомлень про вчинені крадіжки та шахрайство у кіберпросторі. За загальними підрахунками, збитки українців склали 25,5 млн. грн. При цьому потрібно зважати на те, що деякі кіберзлочини мають досить високу латентність,

зокрема, вимагання, яке характеризуються шантажуванням та погрозами. З цього можна робити висновок, що кількість злочинів та матеріальні втрати є більшими, ніж показує статистика. Мережа Інтернет являє собою просторову структуру, яка включає ієрархію різних учасників: установ реєстрації доменних імен і безлічі посередників, розподілених асиметричним способом (операторів системи і інших). Всі вони забезпечують кінцевим користувачам можливість доступу до мережевих протоколів і веб-серверів. Віртуальний простір став самостійним місцем існування людського інтелекту і, як будь-яка об'єктивна реальність, породив безліч проблем, в тому числі і правових [6, 203].

Найчастіше в Україні застосовують такі схеми, як відсилка фейкових електронних листів, створення несправжніх інтернет-магазинів, імітація виграшу в лотерею, використання банківських карт та платіжних систем, тощо. Для швидшого розслідування та виявлення кіберзлочинців, а також для ефективного попередження злочинності, необхідно проаналізувати особу злочинця та виокремити їхні типи.

Типологія кіберзлочинців дасть можливість хоча б умовно поділити їх на види, виокремити їхні особливості. Така інформація дозволить скласти більш точні профілі осіб, які вчиняють злочини з використанням мережі Інтернет, розробити рекомендації для звичайних громадян, які можуть стати жертвами кіберзлочинців.

Досить цікавою є типологія, розроблена та наведена у дисертаційному дослідженні К. М. Эвдокимовим. Вчений поділяє кіберзлочинців на три типи: соціально дезадаптований (вчиняє кіберзлочини для подолання дезадаптації), емоційно сприйнятливий (вчиняє злочини для задоволення матеріальних потреб) та соціально неадекватний (вчиняє кіберзлочини для задоволення інших особистих потреб) [2]. Дана типологія, на нашу думку, є достатньо широкою.

Одна із найкращих типологій була розроблена спеціалістами IT-компанії Malwarebytes. Вони поділяють кіберзлочинців на чотири типи:

Традиційні злочинці, які використовують свої хакерські вміння та навички для отримання матеріальної вигоди.

Зловмисники, діяльність яких спонсують держави для кібершпіонажу за іншими країнами. Яскравим прикладом є північнокорейські формування.

Ідеологічні хакери, які викрадають інформацію, яка збирається та оберігається державами та різноманітними структурами. Наприклад, міжнародна некомерційна організація Wikileaks, яка публікує секретну інформацію, отриману із анонімних джерел.

Хакери, які працюють по найму. Такі зловмисники пропонують свої послуги по поширенню спаму, хакерству, розповсюдженню вірусів, DDoS-атакам. Статистика показує, що такі послуги користуються популярністю.

Дана типологія є вже більш вузькою, а тому правильне її використання дасть можливість визначити тип злочинця, скласти його профіль та спрямувати розслідування у потрібне русло. При цьому, за допомогою наведеної типології можна визначити й жертв кіберзлочину.

Існують також інші типології. Зокрема, М. Ю. Батурин серед комп'ютерних злочинців виділяє зломщиків, крекерів та шпигунів, А. Н. Копирюлін та М. Ю. Дворецький поділяють злочинців на наступні групи: порушники правил користування ЕОМ, «білі комірці» (респектабельні злочинці), комп'ютерні шпигуни і хакери.

Однак, на нашу думку, більш точною є інша типологія кіберзлочинців. Логічним є здійснювати поділ на п'ять груп [3, с. 113-114]:

Пірати – зловмисники, які займаються поширенням ігор, фільмів, музичних композицій, програм у мережі Інтернет.

Вандали (хулігани) – зловмисники, які знищують програмне забезпечення, створюють та поширюють вірусні програми.

Допитливі кібезлочинці – зловмисники, які зламують паролі заради розваги.

Шпигуни – найбільш небезпечні зловмисники, які полюють за конфіденційною інформацією. Потім отримані дані поширюють мережею або шантажують тих, у кого така інформація була викрадена.

Хакери – зловмисники, які займаються отриманням незаконного доступу до охоронних систем (фрікери), спеціалізуються на шпигунстві або диверсіях проти держав, організацій (терористи),

або ті, хто займаються обходом систем захисту для надання доступу до програмного забезпечення певному колу осіб (крекери).

Із розвитком новітніх технологій в інтернеті поширюється різного роду діяльність, особливого розвитку зазнала кіберзлочинність, яка активно процвітає. За сферою злочинних проявів особливе місце посідають злочини у сферах захисту інформації, використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку [9, с. 17].

Безумовно, існує ще безліч типологій, однак, остання, на нашу думку, є найбільш точною. Даний поділ кіберзлочинців на типи дасть можливість зрозуміти небезпечність кожного типу, виявити потенційних жертв, розробити систему захисту проти кожного типу та створити рекомендації для населення, компаній, які допоможуть захиститися від кібератак.

ЛІТЕРАТУРА:

1. Steve Morgan. A 2019 Official Cybercrime Report from Cybersecurity Ventures. 2019. p. 12. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

2. Євдокимов К. Н. Кримінально-правові і кримінологічні аспекти протидії неправомірному доступу до комп'ютерної інформації: за матеріалами Східно-сибірського регіону: дис. ... канд. юрид. наук: 12.00.08 / Костянтин Миколайович Євдокимов. Іркутськ, 2006. 203 с.

3. Кримінологія: підручник / [Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.]; за заг. ред. Б. М. Головкіна. Харків: Право, 2020 – 384 с. 462.

4. Robotization of manufacturing process: economic and social problems and legal ways of their solution / O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi // Financial and credit activity: problems of theory and practice. – 2019. – Vol. 3, is. 30. – P. 454–462.

5. Головкін Б.М. Теперішнє і майбутнє кримінології //Проблеми законності. Харків : Нац. юрид. ун-т імені Ярослава Мудрого. 2020. № 149. С. 168- 184

6. Таволжанський О. В. .Сучасні реалії кіберпростору України / О. В. Таволжанський // Забезпечення правопорядку в умовах коронакризи : матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. – Харків, 2020. – С 203–208.

7. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація . Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. 2017. № 4. - С. 158-164.

8. Головкін Б. М. Види злочинності // Журнал Східноєвропейського права. 2015. № 18. С. 14-21. URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

Науковий керівник: к.ю.н.,доц О.В. Таволжанський

.