УДК 351.745.7

Анатолій Васильович Мовчан,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ

Окремі аспекти протидії кіберзлочинності підрозділами кіберполіції Національної поліції України

Термін «кіберзлочинність» (cybercrime) часто вживається поряд з терміном комп'ютерна злочинність» (computer crime), причому нерідко ці поняття використовуються як синоніми. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – це 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 [1].

Згідно з даними офіційної статистики в Україні за 9 місяців 2019 р. зареєстровано 1796 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж або мереж електрозв'язку, у тому числі:

- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку (ст. 361 КК України) – 1014;

- несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України) – 576;

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України) – 165;

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах

(комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України) – 33 [2].

Одним із суб'єктів протидії кіберзлочинності в Україні є підрозділи кіберполіції. Зокрема, основним завданням Департаменту кіберполіції Національної поліції України є участь у формуванні та забезпеченні реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Наприклад, у вересні 2019 р. поліцейські Департаменту кіберполіції викрили хакера, який за час своєї злочинної діяльності отримав несанкціонований доступ до тисяч серверів постраждалих з більш ніж 100 країн світу. Отримані інструменти він використовував як для продажу даних, так і для отримання доступу до банківських аккаунтів і платіжних систем. Для залучення клієнтів 29-річний житель Харкова розміщував на спеціалізованих сайтах і форумах оголошення про продаж доступів до віддалених серверів. Для оплати таких послуг використовувалися електронні платіжні системи [3].

Також кіберполіцейські викрили злочинну групу з п'яти осіб, які протягом останніх двох років створювали і продавали в мережі шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу систем постачання та обліку спожитої електроенергії. Надалі ці апаратні комплекси налаштовувалися і використовувалися для блокування роботи процесора електролічильника, у результаті чого енергопостачальні підприємства несли мільйонні збитки. Для збуту цих пристроїв організатор злочинної групи створив окремий інтернет-сайт. Залежно від виду електролічильника вартість кожного такого технічного засобу коливалася від 3 до 15 тисяч гривень. Таким чином зловмисники заробили понад мільйон гривень [4].

11 вересня 2019 р. в ході проведення в Києві форуму «Cellebrite User Forum Kyiv 2019» фахівці компанії Cellebrite і Лабораторії комп'ютерної криміналістики ЕПОС розповіли учасникам конференції про свої напрацювання протягом останнього року і поділилися кращими практиками останніх досягнень цифрової криміналістики. У сучасних умовах боротися з комп'ютерною злочинністю державі самостійно важко, адже технології розвиваються щохвилини, а злочинці постійно вдосконалюють свої схеми, щоб максимально приховати сліди. Нині

злочинці вже перестають користуватися аналоговими каналами зв'язку і класичними місцями для зберігання інформації. Все частіше вони використовують хмарні сервіси зберігання інформації і абузостійкі хостинги, які не контролюються з боку держави.

Тому для кіберполіції важливо використовувати сучасні високотехнологічні інструменти для отримання доказової бази. Завдяки співпраці з приватними організаціями кіберполіцейським вдається отримувати дані, які в подальшому використовуються в якості цифрових доказів. Крім того, за допомогою якісної аналітики Національна поліція отримує не тільки докази протиправної діяльності, а й виявляє нові злочини [5].

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування // Генеральна прокуратура України : офіц. сайт. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113897&libid=100820&c=edit&_c=fo (дата звернення: 21.10.2019).
3. Кіберполіція викрила злочинну групу у створенні приладів для блокування роботи лічильників // Кіберполіція України : офіц. сайт. 04.10.2019. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnu-grupu-u-stvorenni-pryladiv-dlya-blokuvannya-roboty-lichylnykiv-1345/ (дата звернення: 21.10.2019).
4. Кіберполіція викрила хакера у зламі більше двох тисяч комп'ютерів українців // Кіберполіція України : офіц. сайт. 04.10.2019. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-bilshe-dvox-tysyach-kompyuteriv-ukrayinczіv-4967/ (дата звернення: 21.10.2019).
5. Сергій Демедюк: Для протидії сучасній злочинності правоохоронці потребують якісних інструментів реверсної інженерії // Кіберполіція України : офіц. сайт. 11.09.2019. URL: https://www.cyberpolice.gov.ua/news/sergij-demedyuk-dlya-protydiyi-suchasnij-zlochynnosti-pravooxoronczi-potrebuyut-yakisnyx-instrumentiv-reversnoyi-inzheneriyi-1575/ (дата звернення: 21.10.2019).

Одержано 22.10.2019