ОКРЕМІ ПИТАННЯ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРАТАК ЯК НЕГАТИВНОГО ФАКТОРУ ВПЛИВУ НА ЖИТТЄВО ВАЖЛИВІ ІНТЕРЕСИ ЛЮДИНИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ

Марія Артемівна ЗАВОРІНА,

студентка факультету «Комп'ютерних наук»
кафедри «Штучного інтелекту»
групи ІТШІ-20-2 Харківського національного
університету радіоелектроніки

Науковий керівник: *Юхно О. О., докт. юрид. наук,*
професор, професор кафедри криміналістики,
судової експертології та домедичної підготовки
Харківського національного університету
внутрішніх справ

На сьогодні, коли світ зазнав максимального впливу технічного прогресу, це призвело до появлення нових видів кримінальних правопорушень, зокрема кіберзлочинів. Згідно п. 9 ст. 1 Закону України від 05.10.2017 року «Про основні засади забезпечення кібербезпеки України» кіберзлочинність – це сукупність кіберзлочинів. 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 яке визнано злочином міжнародними договорами України, які ратифіковано Верховною Радою України (п. 8 ст. 1 Закону) [1].

Протягом останніх років, у багатьох країнах світу значно зросла кількість і злочинна активність кібератак на різні сфери діяльності людини. Так, лише у 2020 році було зафіксовано 1120 витоків і кібератак. Про більшість таких фактів повідомляли провідні світові ЗМІ. В цілому 20 120 074 547 записів хакерами були зламані. Отже, кіберзлочини є вкрай негативним фактором впливу на життєво важливі інтереси людини, суспільства та держави, а протидія їм – важливий напрямок діяльності держави.

Слід тому актуальним питанням забезпечення кібербезпеки є детальний аналіз таких видів кіберзлочинів, як кібератаки, зокрема їх види, особливості правової кваліфікації, форми їх вчинення, а також превентивні заходи у цьому напрямі.

Встановлено, що хакери застосовуючи програми-вимагачі (ransomware), які є шкідливим програмним забезпеченням, призводять до блокування доступу користувачів до їх програмного забезпечення, на підставі чого і користуючись цим, правопорушники вимагають заплатити викуп. Зазвичай ransomware поширюється за допомогою спаму або соціальної інженерії комп'ютерних мереж, що слід враховувати у своїй діяльності кіберполіцейським, слідчим, дізнавачам, прокурорам, суддям.

Як встановлено в ході дослідження шкідливі програми при їх застосуванні злочинцями, зупиняють роботу пристроїв або значно уповільнюють їх. Зокрема, при цьому кіберзлочинцями використовуються програми-

шпигуни, віруси, черв'яки, програми-вимагачі або програми-трояни. Шкідливе програмне забезпечення впроваджують злочинцями за допомогою введення у відповідні пристрої через вкладення електронної пошти з шкідливим кодом або через програми обміну файлами, які поширюють небезпечні матеріали, замасковані під музику або зображення, що здійснюється для конспірації.

Витік даних відбувається, коли конфіденційна інформація користувача стає вразливою. Наприклад, у 2020 році багато комерційних компаній повідомили про витік даних, і така ж тенденція зберігається у 2021 році. Так, торік хакер розкрив 2,5 мільйона облікових даних компанії Drizly, що займається доставкою алкоголю. Ще один випадок, коли Prestige Software - система бронювання, що підтримує Expedia, Booking.com та Hotels.com, розкрила витік номерів кредитних карт більш ніж 10 млн. клієнтів, починаючи з 2013 року. Більшість випадків витоку даних мають фінансове підґрунтя (86%), проте такі ж дії можуть здійснюватись з метою економічного шпигунства між конкурентами або в окремих випадках може спрацьовувати й людський фактор.

DDoS-атаки відбуваються й у випадках коли зловмисники направляють великий обсяг трафіку до системи або сервера, змушуючи його зупинити або призупинити роботу комп'ютерної системи або мережі. Враховуючи велику конкуренцію, у 2020 році компанія Google повідомила, що вона піддалася DDoS-атаці потужністю 2,5 Тбіт/с, що стало найбільшою атакою хакерів на сьогоднішній день, що торкнулася і стало негативним впливом для 180 тис. веб-серверів. Для превентивного захисту від атак типу «відмова в обслуговуванні» користовувачам (потерпілим) важливо переконатися, що вони використовують «хмарні веб-сервери», здатні поглинати переповнення обсягу трафіку, регулярно проводити тести безпеки, оновлення програмного продукту і пропускну здатність, а також працювати з постачальниками інтернет-послуг із забезпеченням безпечних аутсорсингових рішень з метою пом'якшення таких атак. Як встановлено працівниками кіберполіції та спеціалістами, яких вони задіюють у превентивних заходах та тих, що використовуються для викриття і запобігання дослідженим видам кримінальних правопорушень, атаки посередника відбуваються, коли зловмисник перехоплює і змінює електронні повідомлення. Прикладом може служити підроблена точка доступу Wi-Fi, яка виглядає і працює як справжня, але при цьому перехоплює інформацію потерпілої сторони. У зв'язку зі зростаючою тенденцією віддаленої роботи і цифрових комунікацій для комерційних компаній стає все більш важливим використовувати наскрізне шифрування засобів обміну повідомленнями та відеоконференцій. У відповідь на критику на початку пандемії компанія Zoom впровадила наскрізне шифрування для захисту підприємств під час відеодзвінків. Таким чином, злочини в сфері використання інформаційних технологій, які є одним з видів злочинів в сфері інформаційної безпеки, являють собою передбачені законодавством про кримінальну відповідальність, суспільно небезпечні, винні, вчинені суб'єктом злочину діяння, які заподіюють шкоду забезпеченим засобами обчислювальної техніки відносинам у сфері реалізації інформаційної потреби. Аналіз чинного КК України дозволяє зробити висновок, що до таких кримінальних правопорушень слід відносити посягання, передбачені ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК України.

Слід враховувати, що об'єктивну сторону злочину, відповідальність за який регламентується ст. 361 КК України становлять 1) витік; 2) втрата; 3) підробка; 4) блокування інформації; 5) спотворення процесу обробки інформації або 6) порушення встановленого порядку її маршрутизації.

Отже, на сучасному етапі кібератаку можна кваліфікувати не лише як злочин проти інформаційних ресурсів, але і як сучасну форму здійснення акту агресії. Адже здійснюючи подібний вид атаки, злочинцями може бути викрадена інформація, яка становить державну таємницю, порушення системи життєзабезпечення держави та ін.

Безумовно, превентивним питанням кібернетичної безпеки слід приділяти більше уваги, використовуючи захищені з'єднання та ліцензоване програмне забезпечення, що дозволить захистити бізнес та уникнути багатьох негативних наслідків для прав та свобод людини, інтересів суспільства та держави. Втім, підняті питання підлягають окремому дослідженню.

Список використаних джерел:

1. «Про основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/ laws/show/2163-19 (дата звернення: 02.10.2021).

2. Найпопулярніші види кібератак у 2021 році URL: https://spilno.org/news/ naipopulyarnishi-vydy-kiberatak-u-2021-rotsi

3. Дубов Д.В. Проблемні питання комунікування кібератак в Україні: можливі шляхи вирішення URL: http://old2.niss.gov.ua/content/articles/files/CyberCommunication-e06b5.pdf