УДК 004.946.5.056

Тарас Васильович Коженівський,
студент 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність як загроза сучасній безпеці

Активний розвиток ІТ (інформаційних технологій), комп'ютеризація та створення світового комп'ютерного простору формують нові терміни і норми – ІС (інформаційне суспільство), кіберпростір, що мають необмежений потенціал і вносять глобальний вклад у економічний та соціальний розвиток.

Проте утворення ІС призводить до формування багатьох кіберзагроз (потенційні явища та чинники, які створюють небезпеку у кіберпросторі), а основним завдання ІС є забезпечення кібербезпеки [4].

На сьогодні загрози, які надходять з кіберпростору, відбуваються дедалі активніше та зазіхають навіть на національну безпеку. Організовані «набіги»на приватні та державні організації подекуди наносять критичну шкоду по економіці не тільки певної організації, а й не дають можливості подальшого розвитку держав. Джерелом усіх загроз є як іноземні військово-роздувальні служби, терористичні групи, так і ОЗУ (організовані злочинні угрупування), хакери, метою яких є протиправний заробіток [2].

До зовнішніх загроз відносяться: шкідливе ПЗ (програмне забезпечення); DDoS-атаки; фішинг-атаки; проникнення у локальну мережу; втрата ґаджету з важливою інформацією. Внутрішньою загрозою може бути вразливе ПЗ та людський фактор, який ніхто не відміняв [5].

Збільшення обсягу клієнтських даних, що весь час знаходиться в обробці та зростаюча вартість, а відповідно і роль інтелектуальної власності приводить до створення нових методів розкрадання приватної інформації. Зловмисників цікавлять дані щодо внутрішньої системи приватної організації чи державної установи: інформація про працівників, бухгалтерія, особиста інтелектуальна власність тощо.

Проблематика кібербезпеки характеризується тим, що ІС рідко або взагалі не використовує антивірусне ПЗ, не вживає заходів для захи-

сту приватної інформації, що включає в себе дані банківських карток, паролів до тих же банківських застосунків. Особливо важливими є персональні коди доступу, оскільки більшість використовують одну і ту ж комбінацію символів і чисел до всього що потребує авторизацію.

Заголовки статей засобів масової інформації (ЗМІ) містять в собі велику кількість повідомлень про електронне шахрайство, витік баз даних, хакерські атаки комерційних та державних структур, крадіжки інтелектуальної власності тощо.

Наприклад у 2014 році Інтерпол та Європол завдяки співпраці з компанією «Лабораторія Касперського» викрили групу Carbanak, яка протягом багатьох років успішно знімала кошти через онлайн-банкінг чи банкомати. Діяльність групи була досить проста, завдяки вірусу, що надсилався через електронну пошту на комп'ютери рядових співробітників, копіювалися дані про структуру та роботу банку. Згодом це допомагало створювати шляхи крадіжки грошей.

Також в практиці WIPO Arbitration and Mediation Center зустрічалися домені справи з організаціями, що просили змінити домен відповідачів у зв'язку з тим, що вони використають його для фішингу користувачів та працівників, наприклад виставлення підроблених рахунків клієнтам.

Щодо українських ЗМІ, то протягом останніх років новини про кібернетичні атаки на енергетичні компанії України, розсилку вірусного ПЗ через електронну пошту з підписом від податкової та майнінг криптовалюти шляхом розміщення шкідливого коду на сайтах державних установ стрімко зростають.

У червні 2017 року відбулась наймасштабніша кібернетична атака, що зупинила роботу декількох тисяч українських компаній та держорганів [1]. Пріоритетною жертвою вірусу «Petya A» виявилася Україна. Лише протягом одного дня комп'ютерний шкідник «Ransom: Win32/Petya» здійснив атаку на державний та приватний сектор економіки країни, до них належать банки, державна залізниця, аеропорти, телекомпанії, гіганти супермаркети, державні фіскальні служби, органи місцевого самоврядування тощо. Вірус-вимагач заморожує дані і вимагав внесення викупу 300 доларів у криптовалюті за відновлення доступу [6].

Вперше проект Закону України про кібернетичну безпеку був зареєстрований депутатами в червні 2015 року. На початку 2016 року у зв'язку з затвердженням президентом «Стратегії кібербезпеки України» нормативний акт втратив актуальність і був відкликаний. Згодом було

зареєстровано вже новий суттєво доопрацьований акт. 5 жовтня 2017 року закон «Про основні засади забезпечення кібербезпеки України» був остаточно прийнятий парламентом. Він спрямований на створення загальної державної політики кібербезпеки, а також розподіл функцій між різними держорганами.

Також цим законом передбачено створення Національної системи кібернетичної безпеки, що об'єднає низку міністерств та відомств, до якої входить державна служба спеціального зв'язку та захисту інформації, Національна поліція, Служба безпеки України (СБУ), Міністерство оборони та Генеральний штаб, Нацбанк, а також розвідувальні органи. Нормативно-правовий акт чітко визначає, яке відомство за що відповідає у сфері кіберзахисту [3].

Отже, забезпечення державної та міжнародної безпеки в інформаційній сфері та світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів для контролю кіберзлочинності. Тому всі без виключення економічні та політичні ресурси з протидії загрозам міжнародної інформаційної кібербезпеки мають розглядатися на найвищому світовому рівні за участю основних кібердержав. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення превентивних дієвих заходів проти кібератак і кіберзлочинів в державному та світовому кіберпросторі.

Список бібліографічних посилань

1. Від кібератаки вірусом Petya.A постраждали до 10 % комп'ютерів в Україні – Шимків // НВ : сайт. 07.07.2017. URL: https://nv.ua/ukr/ukraine/events/vid-kiberataki-virusom-petya-a-postrazhdali-do-10-komp-juteriv-v-ukrajini-shimkiv-1442363.html (дата звернення: 25.10.2019).
2. Войціховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України // Право і безпека у контексті європейської та євроатлантичної інтеграції : зб. ст. та тез наук. доп. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму (м. Харків, 28 верес. 2018 р.) / Нац. юрид. ун-т імені Ярослава Мудрого, НАПН України, Фонд Конрада Аденауера. Харків : Право, 2018. С. 42–48. URL: http://univd.edu.ua/science-issue/issue/3036 (дата звернення: 25.10.2019).
3. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Міжнародні*

відносини. Серія: Політичні науки. 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3389/3066 (дата звернення: 25.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 25.10.2019).
5. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи // Legal Group : сайт. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/ (дата звернення: 25.10.2019).
6. Україна стала першою ціллю принципово нового виду кіберзброї // Укрінформ : сайт. 05.07.2017. URL: https://www.ukrinform.ua/rubric-technology/2259655-ukraina-stala-persou-cillu-principovo-novogo-vidu-kiberzbroi.html (дата звернення: 25.10.2019).

Одержано 01.11.2019