УДК 343.85(477)

Петро Анатолійович ЧИННИК,
студент 3 курсу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

СВІТОВИЙ ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Світ швидко рухається в напрямку комп'ютеризації та цифровізації. Ми отримали з одного боку, пришвидшення передачі інформації, прискорилась її обробка та впровадження. З іншого боку, серйозне занепокоєння викликає поширення фактів протизаконного збору та використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку. На сьогодні інформація може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. У зв'язку з цим інформаційна безпека є однією з важливих складових національної безпеки держави.

У США з кіберзлочинністю основному бореться Федеральне бюро розслідувань (ФБР) (Federal Bureau of Investigation (FBI)). У нього такі пріоритети:

- комп'ютерні та мережеві вторгнення;
- вимагання через кіберпростір (закодували ваші дані без вашого відома і просять гроші за їхнє декодування, наприклад, вірус WannaCry);
- краджіка особистих даних;
- інтернет-хижаки (сексуальна експлуатація дітей в кіберпросторі) [1].

Також у складі ФБР є спецпідрозділи по запобіганню так званого «нульового дня». «Нульовий день» – це коли знаходиться вразливість і всі її починають використовувати без відома власника ПЗ (програмного забезпечення). ФБР може швидко реагувати на це в будь-якій точці світу і розгорнути свою команду по боротьбі з кіберзлочинністю протягом 48 годин.

У світі важливий внесок у налагодження міжнародної співпраці щодо боротьби з високотехнологічною злочинністю здійснює Міжнародна організація кримінальної поліції (Інтерпол) (International Criminal Police Organization (*ICPO,* Interpol)) [2].

Інтерпол розслідує велику кількість кіберзлочиннів, а саме:

— інтернет-афери, шахрайства;
— кібер-атаки;
— боротьба з кіберзлочинністю в ASEAN (Асоціація Держав Південно-Східної Азії) [2].

Також Інтерпол допомагає правоохоронним структурам інших держав з цифровою криміналістикою. У складі Інтерполу є Центр кіберсинтезу. Центр кіберсинтезу об'єднує кіберекспертів із правоохоронних органів та промисловості, щоб зібрати та проаналізувати всю наявну інформацію про злочинну діяльність в кіберпросторі та надати країнам цілісну, діючу розвідку.

В Європейському Союзі боротьбою з кіберзлочиністю займається Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre – EC3) [3]. Він був створений у 2013 р. Європолом. EC3 щороку видає Оцінку загрози організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment – IOCTA), що визначає пріоритети діяльності Оперативного плану дій EMPACT у сфері кіберзлочину. EC3 також організовує діяльність Об'єднаної робочої групи з боротьби проти кіберзлочинності (Joint Cybercrime Action Task force – J-CAT) [4].

Таким чином, за останні 20 років міжнародне співтовариство отримало важливий досвід у боротьбі з кіберзлочинністю та створило за цей час досить ефективні структури по протидії кіберзлочинності. Вони, звісно, завжди трохи «відставатимуть» від кіберзлочинців, тому що міжнародні структури по боротьбі з кіберзлочинністю займають роль того, хто захищається, але вони навчилися швидко реагувати на загрози і швидко давати рішучу відповідь. Ці структури весь час вдосконалюються, знаходять у себе вразливі місця та усувають їх, готують нових фахівців по боротьбі з кіберзлочинністю. Тому Україні потрібно активно співпрацювати з міжнародними структурами по боротьбі з кіберзлочинністю для вдосконалення своїх правоохоронних органів у цій сфері і вдосконалення кіберзахисту держави.

Список бібліографічних посилань

1. Cybercrime // Interpol. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 30.04.2020).
2. What We Investigate. Cyber Crime // Federal Bureau of Investigation. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 30.04.2020).
3. European Cybercrime Centre EC3 // European Union Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення: 30.04.2020).
4. Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право : сайт. 15.12.2019. URL: https://www.ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/?month=7&year=2022 (дата звернення: 30.04.2020)

Одержано 01.05.2020