УДК 339
Козицька Г.В.[1],Монастирьова А.Д.[2]
[1] канд. екон. наук, доц. НУ «Запорізька Політехніка»
[2] студ. гр. ГФ-113сп НУ «Запорізька політехніка»

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

У сучасному світі стрімкий розвиток інформаційних технологій відкриває безліч нових можливостей для розвитку суспільства та економіки. Однак, разом з цим виникають і нові загрози, серед яких кібертероризм займає одне з провідних місць.

Існує декілька підходів до розуміння сутності кібертероризму. Зокрема кібертироризм розглядається як використання комп'ютерних мереж і технологій для здійснення терористичних актів з метою досягнення політичних, ідеологічних або релігійних цілей. За цим підходом, кібертероризм включає такі дії, як атаки на критичну інфраструктуру, фінансові системи, державні установи та інші об'єкти, важливі для функціонування суспільства. Цей погляд підкреслює політичну та соціальну мотивацію кібертерористів.

За іншим підходом акцентується увага на технічних аспектах кібертероризму, визначаючи його як деструктивні дії в кіберпросторі, що включають зломи, викрадення даних, поширення шкідливого програмного забезпечення та інші форми кібератак. Цей підхід фокусується на технологічних засобах, що використовуються терористами, та на їхніх технічних можливостях.

Деякі дослідники розглядають кібертероризм у контексті інформаційної війни, де основною метою є підрив інформаційних систем та дезінформація. У цьому випадку, кібертероризм стає частиною ширшої стратегії інформаційного впливу та пропаганди, спрямованої на маніпулювання суспільною думкою та підрив довіри до державних інституцій. Незалежно від підходу, кібертероризм є серйозною загрозою для суспільства, що може мати руйнівні наслідки.

Основними факторами, що створюють загрози реалізації кіберзлочинів в Україні є:

- мілітаризація кіберпростору та зростання технологічних можливостей кіберзброї, які дають змогу здійснювати приховані кібератаки та кібероперації противника, дистанційне керування системами управління, пошкодження та руйнування критичної інформаційної інфраструктури;

- активне використання кіберінструментів у міжнародній конкуренції за світове лідерство, конкурентний характер розвитку кібербезпеки та впровадження кіберзагроз у процесі швидких прогресивних змін в інформаційно-комунікаційних технологіях, хмарних обчисленнях, мережах 5G, великих даних, Інтернеті речей, штучний інтелект, тощо;

- низька якість аудиту кібербезеки. Дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати з інформаційної безпеки та IT-аудиту наразі не визнаються, що негативно впливає на якість аудиту.

- низький рівень залучення професійної спільноти, відсутність трансформаційного підходу. Національна система кібербезпеки обмежується перева-

жно участю в ній силових органів (Нацполіція, СБУ, Держспецзв'язок тощо). Приватний бізнес та кіберспільнота до вирішення важливих питань майже не залучаються. Відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації, яка керує впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження. До того ж, через специфіку багатьох галузей (охорона здоров'я, енергетика, телекомунікації тощо) існує гостра потреба в окремих галузевих стандартах з кіберзахисту;

- інша і не менш важлива проблема – неготовність реагувати на кіберінциденти. Більшість компаній все ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті. Відсутнє й централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні. А якщо спуститися на щабель нижче – від державних структур та приватних компаній до пересічних громадян – то ситуація ще гірша. Рівень обізнаності українців з питань кібербезпеки залишає бажати кращого. Державна програма для заповнення цієї прогалини в Україні наразі, на жаль, відсутня.

Надзвичайно актуальною загрозою сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов’язана з розвідувальними службами іноземних держав, розвідувальною діяльністю з розкрадання інформації (кібершпигунство) та підривними діями з метою зриву штатної роботи критично важливих об’єктів, зокрема таких як. інформаційна інфраструктура, насамперед державні системи; електроенергетика, транспорт, атомна та хімічна промисловість, банківська справа.

Цифрова трансформація, яка є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Впровадження нових технологій, цифрових сервісів і механізмів взаємодії громадян і держави, в тому числі у виборчому процесі, створює велику кількість прихованих взаємозв’язків на рівні технологій і процесів. Без системного підходу до кібербезпеки та оцінки ризиків існує ймовірність втрати довіри суспільства до процесів цифрової трансформації.

В Україні за останні роки значно зросла загроза кібертероризму. Перш за все, це пов’язано з кіберможливостями держави-агресора, яка веде кібервійну проти України із застосуванням кіберзброї. Існує використання кіберпростору для фінансування терористичних груп. Водночас недостатньою є співпраця України з міжнародними партнерами щодо розробки взаємовигідних механізмів протидії кібертероризму.

Україна має необхідний потенціал для розбудови можливостей кібербезпеки, щоб адекватно протистояти викликам і загрозам сьогодення.