Т. В. Іванова
студ. ІІІ курсу
спеціальність «Право»
Науковий керівник: д.ю.н., проф. О. А. Чуваков

ОСНОВНІ ТЕНДЕНЦІЇ РОЗВИТКУ І ЗАХОДИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В УКРАЇНІ

На сьогоднішній день, в результаті активних процесів глобалізації та розвитку інформаційно-комунікаційних технологій, внаслідок чого відбулися зміни в соціально-інформаційній сфері, дедалі більшого значення набуває роль інформації. Звертаючи увагу на положення Доктрини інформаційної безпеки України, інформаційна безпека визначена невід'ємною складовою національної безпеки і, у той же час, важливою її самостійною сферою, а згідно ст. 17 Конституції України вона детермінується як одна із головних функцій держави. Завдяки маніпулятивним технологіям ведуться інформаційні війни, знищуються опоненти, здійснюється вплив на маси і багато інших дій, у зв'язку із цим великої популярності останнім часом набув інформаційний тероризм.

Відповідно до ст. 1 Закону України «Про боротьбу з тероризмом», законодавець визначає тероризм як суспільно небезпечну діяльність, що полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [1, ст. 1].

У широкому розумінні тероризм можна розглядати як використання насильства з метою залякування, у якому суб'єктом можуть виступати окремі особи або неурядові організації. Об'єктом насильства можна визначити владу в особі окремих державних службовців або суспільство в особі окремих громадян, а також інфраструктури та системи життєзабезпечення. Одним із видів тероризму є кібертероризм, відповідно до якого відбувається співвідношення із розвитком віртуального світу, симулякризацією інформаційних потоків.

Розглядаючи поняття кібертероризму можна дійти висновку, що відсутнє загальноприйняте визначення. Кібертероризм можна розглянути як навмисну мотивовану атаку на інформацію яка обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту. Основними ознаками кібертероризму є : використання комп'ютера або іншого пристрою, що має доступ до мережі як інструмента злочину; існування Інтернету як міжнародного інформаційного простору, в

якому перебуває об'єкт злочину; зловмисна атака з боку кримінальних індивідів чи їх угрупувань на такі специфічні об'єкти як інформація, програми, комп'ютери, локальні та глобальні мережі.

У Конвенції Ради Європи про кіберзлочинність від 23.11.2001 р. немає чіткого визначення кібертероризму, проте з її положень випливає, що кібертероризмом є навмисне застосування незаконно встановленого повноваження, насильства, руйнування або проникнення в кіберсистеми, у разі якщо подібні дії можуть спричинити смерть або заподіяти шкоду особі або особам, істотної шкоди майну, цивільний безлад або значну економічну шкоду [3]. У Конвенції визначено 4 типи комп'ютерних злочинів, а саме: незаконний доступ; незаконне перехоплення; втручання в дані; втручання в систему, а основними засобами кібертероризму: комп'ютерна система, комп'ютерні дані, послуги ІКТ та дані трафіку. На сьогоднішній день Кримінальний кодекс України не виокремлює поняття кібертероризму як злочину, лише окремим Розділом XVI визначено злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж чи мереж електрозв'язку та передбачена кримінальна відповідальність за статтями 361-1, 361-2 та 363-1.

У п. 13 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», зазначається, що кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням [2, ст. 1].

Кібертероризм може розглядатися як один із найбезпечніших видів злочинів і як загроза кібернетичній безпеці України, адже кібератаки можуть завдати значної шкоди на локальному, державному та навіть міжнародному рівні.

На даний момент в Україні законодавчо не регулюється такий вид злочинів як кібертороризм. Проте варто звернути увагу на те, що провадиться законодавча робота у сфері створення нормативної бази, яка б захищала суспільство та державу в цілому від проявів агресії в кіберпросторі. Зокрема було запропоновано підготувати Проект Закону про внесення змін до Кримінального кодексу України № 2439а від 24.07.2015 щодо встановлення відповідальності за кібертероризм. Пропонується доповнення Кримінального кодексу України ст. 258-6, відповідно до якої кібертероризмом є умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту [4].

Окрім відсутності певної законодавчої бази, треба зазначити, що Україна потребує створення адекватної системи безпеки, де загрози національній безпеці все частіше набувають рис, відмінних від традиційних.

Іншою важливою проблемою залишається взаємодія між державними та недержавними структурами. Приватний сектор, незважаючи на те, що переважна більшість об'єктів інформаційної інфраструктури належать саме йому, не сприймається державою як рівноправний партнер, а тим більше – помічник у посиленні обороноздатності країни в кіберпросторі.

Проаналізувавши найвідоміші випадки кібератак за останні 25 років можна зробити висновок, що у багатьох випадках об'єктами кібертероризму є системи функціонування та управління приватних та державних компаній у нафто-, газопереробних та металургійній сферах. Так, можна привести приклад доволі потужного акту нападу на одну із інфраструктур України. 25 грудня 2015 р. відомою міжнародною компанією ESET було виявлено аварію на «Прикарпаттяобленерго», яка стала результатом зовнішньої хакерської атаки. За допомогою вірусу-троян Black Energy було запущено спеціальну програму KillDisk і як наслідок відбувся збій комп'ютерних програм.

Також, варто згадати, що найбільш масова атака відбулась 27 червня 2017 р., в результаті якої близько 30 банків, система інфраструктури (80% підприємств, підпорядкованих Міністерству інфраструктури), Кабмін, мобільні оператори, ЗМІ, підприємства енергетичної сфери були уражені, що призвело до тимчасового припинення їх роботи. Близько 12-ї години дня вірус невідомого походження атакував комп'ютерні системи сотень державних установ, підприємств та організацій. Цей вірус отримав назву «вірус Petya».

На сьогоднішній день, найбільшу проблему складає відсутність законодавства, в якому було б чітко визначено це поняття, передбачено відповідальність за протиправні діяння. Пріоритетним напрямом у боротьбі з кібербтероризмом є організація зусиль та взаємовідносин правоохоронних органів із спецслужбами, судовими органами, спрямовані на протидію і розслідування таких видів злочинів як кібертероризм, а також потреба у вдосконаленні законодавчої бази України.

Список використаної літератури

1. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-IV (зі змін.та доп.). URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 20.03.2019).

2. Про основні засади забезпечення кібербезпеки України : Закон України VIII від 05.10.2017 р. № 2469-VIII (зі змін. та доп. від 21.06.2018). URL: https://zakon.rada.gov.ua/laws/show/ru/2163-19/sp:max100 (дата звернення: 20.03.2019).

3. Конвенція про кіберзлочинність : Закон України від 07.09.2005 р. № 994_575 (зі змін.та доп.). URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.03.2019).

4. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм від 24.07.2015 р. № 2439а. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1VR68A.html (дата звернення: 20.03.2019).