ПОПОВ Владислав Олегович
командир 122 навчальної групи курсу №1 факультету забезпечення державної безпеки Київського інституту Національної гвардії України
Науковий керівник:
ДАШКОВСЬКИЙ Анатолій
викладач кафедри державної безпеки Київського інституту Національної гвардії України

КІБЕРТЕРОРИЗМ ЯК НОВА ФОРМА МІЖНАРОДНОГО ТЕРОРИЗМУ

Беручи за основу поняття тероризму і поєднання його з віртуальним простором, можна вивести таке визначення: кібертероризм – це комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту. Що стосується природи кібертероризму, то він якісно відрізняється від загальноприйнятого поняття тероризму, зберігаючи лише стержень цього явища і ознаки. Однак є приклади кібератак, що знаходяться на межі з реальним тероризмом. По суті, це і є акт кібертероризму, оскільки він реалізований через інформаційну систему і інформаційними засобами. Але цей факт наочно показує потенційні можливості тероризму взагалі, форми його прояви. Головне в тактиці інформаційного тероризму полягає в тому, щоб акт тероризму мав небезпечні наслідки, став широко відомий населенню і отримав великий суспільний резонанс. Як правило, вимоги супроводжуються загрозою повторення акту без вказівки конкретного об'єкта. Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюються угрупованнями або окремими особами. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати кошти мережевого інформаційного обміну, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності. Зростання інформаційних технологій дає терористам можливість отримати істотний прибуток при відносно низькому ризику. Вони можуть фінансувати свою діяльність, без використання силових нападів або грабежів банків, які збільшили б ризик виявлення. Для кібертероризму характерно і те, що всі відомі сьогодні хакерські групи і окремі особи не прагнуть

афішувати свої дані і виступають виключно під псевдонімом. При цьому слід відрізняти хакера-терориста від простого хакера, комп'ютерного хулігана або комп'ютерного злодія, який діє в корисливих або хуліганських цілях [1].

Головне в тактиці кібертероризму полягає в тому, щоб кіберзлочин мав досить небезпечні наслідки, став широко відомий населенню, отримав великий суспільний резонанс і створював атмосферу загрози повторення акту без вказівки конкретного об'єкта. Для організації, які займаються кібератаками необхідна значно більша кваліфікація їх виконавців, так як в деяких випадках кібертерористичні дії можуть виявитися кращими, ніж акти звичайного тероризму. Проведення кібератак забезпечує високу ступінь анонімності і вимагає більшого часу реагування. Вироблення методів антитерористичної боротьби лежить перш за все в області протидії звичайному тероризму. Здійснення атаки через інформаційні системи взагалі може виявитися не розпізнаний як акт тероризму, а буде сприйнято, наприклад, як випадковий збій системи.

Таким чином, загроза кібертероризму в даний час є дуже серйозною проблемою. Актуальність цього питання буде зростати в міру розвитку і поширення інформаційно-телекомунікаційних технологій. На думку американських експертів, найбільш уразливими точками інфраструктури є енергетика, телекомунікації, авіаційні диспетчерські, фінансові електронні та урядові інформаційні системи, а також автоматизовані системи управління військами і зброєю. Так, в атомній енергетиці зміна інформації або блокування інформаційних центрів може спричинити за собою ядерну катастрофу або припинення подачі електроенергії в міста і на військові об'єкти. Ще одна мета кібертерористичних атак – руйнування об'єктів інформаційних систем. Це може привести до знищення інформаційних ресурсів і ліній комунікацій або до фізичного знищення структур, в які включаються інформаційні системи. Вирішення проблеми кібертероризму є важливим при міжнародній інформаційній безпеці. Існують труднощі створення і збереження коаліцій при здійсненні міжнародного співробітництва. Так, з початком серйозного інформаційного акту тероризму міцність коаліцій держав піддається великому випробуванню, оскільки всі союзники поринуть в «інформаційний туман». Можуть виникнути і гострі проблеми з реалізацією спільних планів дій проти транснаціональної кримінальної або терористичної організації. Все це дозволяє сьогодні говорити, що терористична площина переходить з реального простору в простір віртуальний. Інформаційні мережі допомагають терористичним угрупованням в здійсненні задуманих планів, які перетікають в кібертероризм як реальну загрозу діяльності для окремих країн і всього світового співтовариства. Питання забезпечення інформаційної безпеки як однієї з важливих складових національної безпеки держави особливо гостро виникає в контексті появи транснаціональної і транскордонної комп'ютерної злочинності та кібертероризму.

Отже,ефективна боротьба з кібертероризмом можлива тільки на основі превентивних методів. Запобігання йому має полягати у виявленні, усуненні, нейтралізації, локалізації і мінімізації дії тих чинників і причин, які або породжують кібертероризм, або йому сприяють. Жодна держава не є і не буде захищена від такого типу злочинів, тому країни все ретельніше розробляють програми та заходи, спрямовані на запобігання такій терористичній діяльності, а саме створюють різні правозахисні організації, укладають велику кількість міжнародних угод. Однак, для того, щоб мати змогу дати відсіч цій міжнародній загрозі, необхідна спільна та клопітка діяльність та реальні кроки, які б запобігали, а не ліквідовували наслідки «плодів» кібертероризму.

Список використаних джерел:

1. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризмуhttps://sci.ldubgd.edu.ua [1].

2. Тероризм: теоретико-прикладні аспекти: навчальний посібник / за заг. ред. В.К.Грищука. Львів: ЛьвДУВС, 2011. 328 с. https://dspace.pdau.edu.ua/[2].

3. Богданов О.І. Високотехнологічний тероризм нової епохи. Проблеми безпеки особистості, суспільства, держави. 2005. № 4. С. 34-37.