УДК 614.8

РОДИК Р. В., здобувач вищої освіти
ДРОЖЧАНА О. У., старший викладач
Полтавська державна аграрна академія

КІБЕРТЕРОРИЗМ ЯК НОВА ФОРМА ТЕРОРИЗМУ

Науково-технічний прогрес, створивши нові інформаційні технології, в короткі терміни революційно трансформував процеси створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Сьогодні його результати нерідко використовують і злочинці. Проникнення в інформаційну сферу та її використання кримінальними, в тому числі й терористичними елементами породило явища, які називаються кіберзлочинністю і кібертероризмом.

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.

Засоби і методи кібератак вже давно освоєні як міжнародними екстремістськими організаціями, так і національними сепаратистськими рухами. Перші приклади «комп’ютерного тероризму» з’явилися наприкінці 1990-х рр., що пов’язано як з розвитком комп’ютерних мереж, так із зростаючою роллю комп’ютерів у всіх сферах життя [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.

Так, керівники ряду радикальних мусульманських організацій Близького Сходу надають дедалі більшого значення використанню у своїй діяльності саме сучасних інформаційних технологій, розглядаючи їх як ефективний різновид зброї в боротьбі з режимами Ізраїлю, Саудівської Аравії і підтримуючих їх західними країнами. Це, по-перше, досить недорогий засіб здійснення терористичного акту(тому до кібертероризму вдаються в основному країни з нерозвиненою економікою), а по-друге – складнощі з виявленням кіберзлочинця. На думку аналітиків, більшість транснаціональних терористичних організацій дотримуються раціонального підходу, домагаючись насамперед політичних цілей і використовуючи тактику терору в надії на суспільне визнання законності своєї боротьби.

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 [2].

На думку американських експертів, найбільшу 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.

За статичними показника ми визначено, що 40% респондентів в Україні вважають, що кіберзлочинність це зовнішня загроза, 24% – внутрішня загроза, 36% – вважають, що загроза може виходити як ззовні,так і зсередини організації.

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. Тероризм: теоретико-прикладні аспекти: навчальний посібник / за заг. ред. В.К.Грищука. Львів: ЛьвДУВС, 2011. 328 с.

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