УДК 004.056: 341(045)

Гриник Р.О., Пилипенко В.М.
Львівський державний університет безпеки життєдіяльності

Кібертероризм як нова форма міжнародного тероризму

Технічний прогрес розвивається настільки стрімко, що деякі його наслідки усвідомлюються суспільством занадто пізно, коли для виправлення ситуації потрібні значні зусилля. Кількість користувачів мережі Інтернет постійно зростає. У США їх вже 240 мільйонів, в Європі – 476, в Латинській Америці – 236, в Африці – 140, а в Азії – 1 мільярд. В Україні, за різними оцінками, кількість користувачів Інтернет становить від 12 до 16 мільйонів чоловік [1]. Впровадження сучасних інформаційних технологій, призвело, на жаль, до появи нових видів злочинів, таких як комп'ютерна злочинність і комп'ютерний тероризм – незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, викрадення, привласнення, вимагання комп'ютерної інформації, а також кібертероризм, який характеризуються високим рівнем латентності і низьким рівнем розкриття злочинів.

Твердження «кібертероризм» утворено злиттям двох понять: «кібер» («кіберпростір») і «тероризм». ». У літературі все частіше зустрічаються терміни «віртуальний простір», «віртуальний світ». 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[2].

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[3].

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.

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 країни), 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. 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[4]. 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.

Список використаних джерел

1. *Website monitoring for everyone. – [Електронний ресурс]. – Режим доступу: https://www.pingdom.com/*
2. *Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. – СПб.: БХВ – Петербург; Арліт 2002. – 496 с.*
3. *Ендрю Конрі-Мюррей. Політика безпеки в часи терору. – [Електронний ресурс]. – Режим доступу: http://www.osp.ru/lan/2002/02/083.htm.*
4. *Юрій Травников. Злочини в Паутині: Кордони без замків. − [Електронний ресурс]. – Режим доступу: http://www.pl-computers.ru/article.cfm?Id=742&Page=3.*