МІЖНАРОДНИЙ КІБЕРТЕРОРИЗМ І ОСОБЛИВОСТІ ЙОГО ПРОЯВУ

Олексій Косиєв, Ростислав Гриник

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The current state and development of international cyber especially its manifestation. The key aspects of international cooperation in the fight against cybercrime. The basic problems of international cooperation in this field.

Keywords: cyberspace, cybercrime, cyberterrorism, information security

Визначити поняття «комп'ютерний тероризм» – доволі складне завдання, оскільки нелегко встановити чітку межу для відмінності його від інформаційної війни і інформаційного криміналу. Ще одна складність полягає в тому, що необхідно виділити специфіку саме цієї форми тероризму. Саме поняття «кібертероризм» утворено злиттям двох слів: «кібер» («кіберпростір») і «тероризм». Виходячи з основного поняття тероризму і поєднання його з віртуальним простором, можна зробити висновок, що кібертероризм – це комплексне поняття, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану 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.

Одним із способів кібертероризму є політично мотивована атака на інформацію. Вона полягає в безпосередньому управлінні соціумом за допомогою превентивного залякування. Це проявляється в загрозі насильства, підтримці стану постійного страху з метою досягнення певних політичних чи інших цілей, примусі до певних дій, залученні уваги до особистості кібертерориста або терористичної організації, яку він представляє.

Ряд країн, таких як США, Великобританія, Канада, Австралія та інші використовують глобальну систему радіоелектронної розвідки «Ешелон», яка використовується і для попередження проявів міжнародного тероризму [1]. Але незважаючи на «ешелонування», терористи можуть скоординувати свою діяльність і вдало провести акт тероризму. Цьому може бути кілька пояснень:

- терористи використовували для взаємодії неелектронні засоби телекомунікацій;
- терористи маскували свої повідомлення за допомогою криптографічних або стенографічних методів;
- алгоритм, закладений в систему «Ешелон», неефективний, або ця система попередньо була виведена з ладу.

Терористи підтримують свою діяльність іншими злочинами, вчиненими через Інтернет, наприклад, отримують доступ до баз кредитних карт або здійснюють різні форми прибуткового шахрайства. Інформаційні технології також полегшують безліч дій терористів і міжнародних злочинних груп – від фінансування до створення необхідних документів. За допомогою комп'ютерних технологій організовані злочинні групи здатні створити підроблені документи, що засвідчують особу, документи, що свідчать про ведення будь-якої діяльності, яка є прикриттям для їх операцій. Використання інформаційних технологій злочинцями і терористами відбувалося одночасно із зростанням їх легального використання міжнародною спільнотою. Можливість швидкого впровадження нових технологій в терористичні і злочинні організації обумовлюється і тим, що сучасні злочинні організації існують у вигляді мереж, із осередками діяльності. Вони мають кваліфікованих технічних фахівців в своїх структурах або наймають їх ззовні.

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 [2]. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати мережевий інформаційний обмін, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності.

Проведення кібератак забезпечує високу ступінь анонімності і вимагає більшого часу реагування. Вироблення методів антитерористичної боротьби лежить перш за все в області протидії звичайному тероризму [3]. Здійснення атаки через інформаційні системи взагалі може виявитися не розпізнаною 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. Немає спільної думки з приводу визначення об'єкта актів тероризму. Причому думка коливається від міждержавної спрямованості, коли об'єктом стають не тільки окремі міжнародні організації, а й цілі держави, народи, конкретні особи (політичний або державний діяч) або випадкові люди. Дії кібертерористів можуть бути спрямовані як на цивільні, так і військові об'єкти. 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[1].

Загроза кібертероризму вже не перший рік широко обговорюється в сучасному суспільстві на різних рівнях, породжуючи безліч суперечок, міфів і спекуляцій. Неадекватна оцінка ризиків, пов'язаних із здійсненням цієї загрози, призводить як до недооцінки, так і до переоцінки її серйозності. В результаті поряд з «страхітливими» описами глобальних катастроф, нерідко зустрічається і повне ігнорування цієї проблеми. Поняття кібертероризму часто використовується для політичних спекуляцій. Реальне ж положення справ, залишається не настільки страхітливим, проте, не вселяє і приводів для оптимізму.

Література

1. Goben F. Op. cit. – P. 57-72; Scbwartau W. Information Warfare: Chaos on the Electronic Superhighway. – NY, 1994.
2. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. - СПб.: БХВ - Петербург; Арліт 2002.
3. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : [моногр.] / Голубєв В. О. – Запоріжжя : Гуманіт. ін-т «Запоріз. ін-т держ. і муніцип. упр.», 2003.