Піскорська Г.А.*

ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА СТРАТЕГІЯ КІБЕРОБОРОНИ США

У статті аналізується загроза використання міжнародними терористичними угрупуваннями сучасних інформаційних технологій. Адміністрація США оцінює кібератаки на свої комп'ютерні мережі як акт війни і займає активну позицію протидії кіберзагрозам.

Ключові слова: кібертероризм, кіберзагроза, кібератака, інформаційна війна, стратегія боротьби з кібертероризмом.

В статье анализируются угроза использования международными террористическими группами современных информационных технологий. Администрация США расценивает кибератаки на свои компьютерные сети как акт войны и занимает активную позицию противодействия киберугрозам.

Ключевые слова: кибертерроризм, киберугроза, кибератака, информационная война, стратегия борьбы с кибертерроризмом.

In article are analyzed use threat by the international terrorist groups of modern information technology. The administration of the USA regards cyberattacks to the computer networks as the certificate of war and occupies an active position of counteraction to cyberthreats.

Key words: cyberterrorism, cyberthreat, cyberattack, information war, strategy of struggle against cyberterrorism.

Сучасні міжнародні конфлікти набувають нових форм, базуються на технічних засобах, які формально не вважаються зброєю. Війни ведуться навіть без використання військової техніки та озброєння, без силового втручання в традиційному розумінні; в ході війни використовуються інформаційні та мережеві технології. Глобалізація сучасної економіки, її насиченість новітніми інформаційно-телекомунікаційними технологіями, інформатизація таких життєво-важливих сфер діяльності суспільства, як зв'язок, енергетика, транспорт, системи зберігання газу та нафти, фінансова та банківська система, оборона та національна безпека, структури забезпечення стабільної роботи міністерств та відомств, перехід на методи електронного врядування створюють умови для розповсюдження кібертероризму [1-5].

Принципово нові загрози міжнародній стабільності виникли з розробкою, використанням і розповсюдженням інформаційної зброї, що уможливлює інформаційні війни. Спецслужби ведуть свої війни безпосередньо в Інтернеті. У жовтні 2010 року в повну силу запрацювало кіберкомандування США (US Cyber Command) зі штатом понад 1 тис. осіб. Спеціальні кіберпідрозділи, що мають на меті ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника із використанням можливостей кіберпростору створено також у Великобританії (Cyber Se-

* кандидат історичних наук, доцент, старший науковий співробітник НДЧ Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

curity Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre),Індії та інших державах. Активну позицію щодо протидії кіберзагрозам посідає провідна міжнародна безпекова організація – НАТО (Cooperative Cyber DefenceCentre of Excellence).

Велику занепокоєність експертів-аналітиків викликає той факт, що терористичні організації більш гнучкі, аніж державні інституції щодо застосування технічних інновацій [6-9]. Відповідно вони мають суттєві переваги у проведенні добре координованих операцій. А високий ступіть організації та реалізації останніх резонансних терористичних актів свідчить, на думку деяких експертів, про те, що за злочинами стояли інтереси різних держав.

Використання злочинними елементами новітніх інформаційно-комунікаційних технологій надзвичайно небезпечно. Вони радикально змінюють методи терористичної діяльності, сприяють екстремістським елементам у формуванні гнучких та ефективних мережевих організаційних структур, що об'єднують окремі групи у транснаціональні терористичні угрупування, які дуже важко виявити до здійснення терористичного акту. За багатьма ознаками мережеві організації подібні до стільникової структури, що складається з декількох груп, які мають різних лідерів або різну спрямованість. Водночас вони здатні об'єднуватися для вирішення спільних завдань. Зазначена структура може існувати тільки в умовах інформаційно розвинутого суспільства. Це динамічна система, що швидко адаптується до мінливих політичних умов.

Для проведення терористичної діяльності мережеві організації потребують надійного зв'язку з їх географічно віддаленими ланками. Зазначимо також, що в мережевих організаціях залежність від зв'язку набагато більша, ніж у ієрархічних. В терористичних мережах, так само, як в арміях технологічно розвинених держав, утворюються ефективні системи управління, зв'язку та контролю. Використання інформаційних технологій надає можливість мережевим терористичним організаціям підвищити ефективність за такими напрямками. По-перше, користування послугами електронної пошти та стільникового зв'язку якісно покращують координацію дій за умов високого ступеню анонімності. По-друге, порівняно невелика вартість цих послуг створює кращі умови для діяльності маргінальних організацій, без сталих джерел фінансування. Отже, відбувається подальша децентралізація терористичних організацій і, відповідно, боротьба проти них ускладнюється.

Занепокоєння викликає також те, що терористи здатні без особливих проблем використати інфраструктуру держав, які підтримують тероризм. Адже сьогодні немає точних відомостей про рівень розвитку інформаційних інфраструктур серед арабських держав. Проте відомо, що більшість країн Близького Сходу серйозно розглядають можливість асиметричного впливу на інформаційну сферу потенційного супротивника. При цьому ЄС, США, Ізраїль та міжнародні організації неспроможні зупинити або, принаймні контролювати циркуляцію інформації та інформаційних технологій на Близькому Сході. Сучасні засоби зв'язку та Інтернет використовуються терористичними організаціями для пропаганди своєї діяльності та збільшення кількості своїх членів. Зараз в Інтернеті знаходяться сайти практично усіх великих ісламських організацій, серед них також організації радикального спрямування («Ісламський джихад Палестини», «Хезболах» та інші). Більшість таких сайтів утворюють підмережу в Інтернеті, головна мета якої – інформаційно-пропагандистський вплив та організаційна діяльність. Так, за словами представників ізраїльських спецслужб, терористи передають через електронну пошту у зашифрованому вигляді інструкції, карти, схеми, паролі та інше. Фахівці не

виключають можливості утворення міжнародної ісламістської організації нового типу, основа якої не чіткі організаційні зв'язки, а єдине інформаційне середовище [3]. За оцінками експертів нараховується близько 4 тисяч таких веб-сайтів. Терористи публікують свої матеріали 40 мовами. Зокрема, Баскська терористична організація ЕТА пропонує інформацію іспанською, англійською. французькою, італійською мовами; шрі-ланкійське угрупування «Тигри визволення Тамиллама» – англійською, японською, італійською.

Новітні інформаційно-комунікаційні технології уможливлюють перехід терористичних організацій від окремих акцій до систематичного впливу на інформаційні інфраструктури. У державах з високим рівнем розвитку новітніх інформаційних та комунікаційних технологій набір цілей для атак на стратегічному рівні дуже великий: телекомунікації і телефонія, космічні супутники, автоматизовані засоби ведення фінансової, банківської і комерційної діяльності; енергосистеми; культурні системи і весь набір устаткування і програм, на підставі яких ворог одержує знання. Стратегічні інформаційні системи у високотехнологічних державах часто дублюються на оперативному рівні. Усі вони вразливі для атаки. Чим сучасніше суспільство, тим більше воно покладається на інформацію та засоби її доставки. Сюди відноситься і Інтернет – але це лише вершина цієї інформаційної конструкції. Будь-яка розвинена країна має телефонну банківську та безліч інших мереж що керуються комп'ютерами, отже мають властиві для них слабкі місця. Інформаційні ресурси збройних сил США, що налічують до 2 000.000 комп'ютерів, 100.000 локальних мереж і приблизно 10.000 інформаційних систем, щомісяця стають об'єктом до 750 хакерських атак, певна частина яких досягає своєї мети, тобто – порушує зв'язок, навігацію, системи космічної розвідки, наведення зброї, тилового забезпечення. Війна проти Югославії стала першою в історії інтерактивною війною – всі, хто мав доступ до Інтернет, в будь-який момент часу мали можливість спостерігати за розвитком збройного конфлікту. Вперше в історії збройних конфліктів хакери використали мережу проти ведення військових дій як Югославії, так і НАТО, шляхом порушення роботи урядових комп'ютерів та встановлення контролю над сайтами.

Інтенсивність кібератак в сучасному світі невпинно зростає. У 2002 р. радник президента США по технологіям Ричард Кларк оголосив список країн – потенційних носіїв кібертероризму. До нього потрапили Ірак, Ірак, Південна Корея, Китай та Росія. За переконаннями Кларка в цих країнах є спеціалісти, здатні порушити безпеку США через Інтернет [7]. Проте, за даними фірми Riptech, кібератаки з небезпечних для США країн становлять 1%, а найбільша кількість атак - 40% зафіксована за самими США. Далі за кількістю нападів йдуть Німеччина та Південна Корея. Зазначимо, що нині США мають 42% світових комп'ютерних ресурсів та 60% ресурсів Інтернету, Китай – 1%, Росія – 1%, а Україна – менше 1%.

Кібертероризм – є частиною такого явища, як інформаційний тероризм. У середині 1980-х рр. Беррі Коллін, співробітник американського Інституту безпеки і розвідки, ввів термін «кібертероризм» для визначення терористичних дій у віртуальному просторі. Автор терміну зазначив, що про реальний кібертероризм можна говорити не раніше, як у першому десятилітті XXI ст. Проте вже у 1990 р. було зафіксовано перші серйозні кібератаки. А згодом Пентагон наказав Агентству супутникових телекомунікацій розробити стратегію ведення кібервійни (OPLAN 3600), яка передбачає «безпрецедентне об'єднання комерційних і державних структур країни». До її розробки залучається і ФБР, оскільки ситуація вимагає рішучого об'єднання усіх зусиль для протидії можливим атакам через Інтернет. Уряди інших країн теж розпочали розробку своїх стратегій ведення інформаційної війни.

Термін «кібертероризм» означає дії з дезорганізації інформаційних систем (несанкціоноване втручання в комп'ютерні мережі, перепрограмування, порушення роботи серверів та інше), що становлять небезпеку для життя людей, призводять до значних майнових збитків, або інших суспільно небезпечних наслідків, якщо їх здійснено з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішення органами влади, а також загроза здійснення зазначених дій. Головне в тактиці інформаційного тероризму полягає в тому, що терористичний акт мав небезпечні наслідки, був широко відомий населенню і викликав потужний резонанс у суспільстві. Вимоги терористів супроводжуються погрозами повторення акту без зазначення конкретного об'єкту. Таким чином, характерною особливістю кібертероризму є те, що на відміну від кіберзлочинності, умови терориста широко висвітлюються в інформаційній мережі.

Діяльність кібертерористів виявляється в загрозі насильства, підтримці стану залякування з метою досягнення політичних та інших цілей, примусі до певних дій, притягненні уваги до особи терориста та терористичної організації, яку він репрезентує. Кібертероризм ще не призводив до людських втрат, але спричиняв суттєві фінансові збитки та впливав на психологічний клімат у суспільстві. Таким чином, кібертероризм є одним з сучасних викликів високотехнологічним державам світу. Фахівці вирізняють наступні засоби тероризму у кіберпросторі для досягнення терористичних цілей:

- нанесення збитків окремим фізичним елементами кіберпростору, зокрема, знищення мереж електроживлення, використання спеціальних програм, що стимулюють руйнування апаратних засобів, а також біологічних та хімічних засобів для порушення елементарної бази;
- знищення або крадіжка інформаційного, програмного та технічного ресурсів кіберпростору, що мають значення для суспільства в цілому, шляхом порушення систем захисту, встановлення вірусів, програмних закладок та інше;
- вплив на програмне забезпечення та інформацію з метою їх викривлення та модифікації в інформаційних системах та системах управління;
- розкриття та загроза оприлюднення або оприлюднення закритої інформації про функціонування інформаційної інфраструктури держави, принципів роботи системи шифрування, успішного досвіду проведення актів інформаційного тероризму;
- погрози здійснення терористичного акта у кіберпросторі, що викликають серйозні економічні наслідки;порушення ліній зв'язку, неправильне адресування, штучне перевантаження вузлів комутації та інше;
- вплив на операторів, розробників, експлуатаційників інформаційних та телекомунікаційних систем шляхом насильства або загрози насильства, шантаж, підкуп, введення наркотичних засобів, використання гіпнозу, засобів створення ілюзій, мультимедійних засобів та інше;
- проведення інформаційно-психологічних операцій [8].

Основною формою кібертероризму серед вищезазначених є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури. Здійснення кібератак призводить до втручання в систему, перехоплення управління, або блокування засобів обміну в мережі та інше.

Втручання в мережі, обладнані комплексами захисту, надзвичайно складне завдання, яке не під силу здійснити самим терористам, що не мають необхідних знань та кваліфікації. Проте, маючи відповідні фінансові кошти, вони в змозі найняти для цього хакерів. Хакерством називають експлуатацію комп'ютерів витонченими засобами за допомогою спеціального програмного забезпечення. Небезпека кібертероризму в тому,

що він не має національних меж і терористичні акти можуть відбуватися з будь-якої частини світу. Терориста дуже важко виявити, тому що він діє через один або декілька підставних комп'ютерів.

Цілі, що переслідують для своїх атак терористи, відповідають в цілому складовим національної інфраструктури: обладнання, в тому числі комп'ютери, периферійне, комунікаційне, теле-, відео-, та аудіо обладнання; програмне забезпечення; мережеві стандарти та коди передачі даних; інформація як така, що може бути представлена у вигляді баз даних, аудіо-, відеозаписів, архівів та інше; люди, які діють в інформаційній сфері. Групи цілей (мішені) кібертерористів - це міжнародні організації (цілі кібератак учасників антиглобалістського, антивійськового рухів та учасників різних військових конфліктів), вищі органи виконавчої та законодавчої влади, установи економічного блоку та університети окремих держав (цілі суб'єктів політичного, соціального та інших форм протесту), громадські організації (цілі носіїв релігійної, національної та інших форм ворожості) та банківські і фінансові структури (цілі суб'єктів кримінальної діяльності).

Незважаючи на те, що здійснення таких атак вимагає високої кваліфікації від їх виконавців, інколи кібертерористичні дії можуть виявитися зручнішими для її замовників, ніж акти звичайного тероризму. Адже проведення кібератак забезпечить високу ступить анонімності і вимагає більше часу на реагування. Подекуди атаки через інформаційні системи залишаються непізнаними як терористичний акт – їх сприймають як випадковий збій у системі.

Інформаційні атаки високого рівня, що кваліфікують, як акти кібертероризму можна розподілити на дві категорії. Це виведення з ладу інформаційних систем та руйнівні атаки. Кожна категорія виокремлюється, але чітких меж між ними немає. Одна особа, або терористична група може здійснювати одночасно весь спектр дій. Діяльність кібертерористів аналізуються виходячи з міркувань її небезпеки для суспільства. Найбільшу загрозу становлять дії, спрямовані проти об'єктів критичної інфраструктури – командних пунктів ядерних сил, систем управління АЕС, промислових підприємств, транспорту. Порушення, чи блокування їх роботи може установити миттєву загрозу для життя багатьох людей.

В контексті даної статті переважно розглядаються політично мотивовані атаки на інформацію, що обробляється комп'ютером, комп'ютерні системи та мережі, що становить небезпеку для життя та здоров'я людей, здійснені з метою порушення стабільності у суспільстві, залякування населення, провокації військового конфлікту. Наведені приклади діяльності терористів в інформаційному просторі показують широкий діапазон використання електронних засобів впливу, різні цілі, гравців та географічні діапазони [9, 10].

1. Виведення з ладу інформаційних систем.

Хакерські атаки цього типу є найбільш поширеними; вони спрямовані на тимчасове виведення з ладу окремих Інтернет-служб, переадресацію інформації. Вони зазвичай проводяться «тимчасовими терористами» – приватними особами, що не пов'язані напряму з терористичними організаціями, але поділяють опозиційні ідеї.

Існує багато способів, за допомогою яких певна особа може порушити, або припинити роботу Інтернет-серверів (в основному це DOS-документи). Белградські хакери в період війни в Косово організовували атаки проти серверів НАТО. Вони бомбардували сервери командами, які перевіряли, чи працює сервер і чи пов'язаний він з Інтернетом. Очікуваним ефектом таких атак було перевантаження лінії сервера – мішені. Косовські хакери, як засіб віртуального протесту, використовували бомбардування

електронної пошти. Вони надсилали політикам тисячі листів одночасно за допомогою автоматизованих інструментів, що часто призводило до блокування електронної скриньки і вона припиняла роботу. Американські засоби масової інформації писали, що Косовський конфлікт перетворив кіберпростір в нематеріальну військову зону, де військові зіткнення відбуваються через електронні зображення, групові поштові відправлення та хакерські атаки.

На думку Дороті Денінг, автора дослідження «Активність, хактивізм та кібертероризм: Інтернет як засіб впливу на зовнішню політику», Інтернет вплинув на політичний діалог, тому що активно експлуатувався активістам, які мали на меті тиснути на осіб, відповідальних за прийняття політичних рішень [12].

2. Руйнівні атаки.

Насамперед, це інформаційні (хакерські) операції проти об'єктів, які здатні знищити інформаційний ресурс, лінії комунікації, або викликати фізичне знищення структур, що включають інформаційні системи. Якщо системи діють у критичних інфраструктурах, то при найгіршому розвитку подій мережеві інформаційні атаки можуть мати масштабні наслідки з людськими жертвами, як і традиційні терористичні акти.

Саме такі кібератаки були організовані в трагічний день 11 вересня 2001 р., що уможливило на деякий час «засліпити» операторів авіарейсів, баз ВПС тощо. Вони не оголосили своєчасної тривоги лише тому, що «картинка» на екранах їх комп'ютерів відповідала «нормі», хоча й не мала нічого спільного з тим, що відбувалося насправді. Близькою за формою до військової була атака на цілу низку серверів державних установ США, яку здійснили китайські хакери в період війни в Югославії.

Хакерський рух в Китаї організовано на державному рівні. Зокрема, Китай дозволив своїм кібертерористам об'єднатися в Honker Union of China (honker — гібрид англійського «hacker» і китайського «hong» — червоний). За даними ФБР, КНР на сьогоднішній день має армію у 180 000 хакерів, які щоденно атакують кібермережі США і лише 2009 року здійснили 90 000 атак протии комп'ютерів Міністерства оборони США. З 180 тис. хакерів 30 тис. Є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору (працівники приватних компаній, що залучаються до виконання військових чи роззвідувальних завдань в кіберпросторі), місією яких є отримання доступу до військових і комерційних секретів США та внесення розладу в діяльність рядових і фінансових служб [11].

Незважаючи на заяви офіційних осіб США про перебільшення загрози кібератак, американці розуміють, що вона реально існує. Ще 7 січня 2000 р. президент США підписав «Національний план захисту інформаційних систем», відповідно до якого було визначено 10 програм:

- визначення критично важливих ресурсів інфраструктури, їх взаємозв'язків та загроз щодо них;
- виявлення нападів та несанкціонованих вторгнень;
- розвідувальне забезпечення та розробка правових актів , спрямованих на захист критичних інформаційних систем;
- своєчасний обмін інформацією про напади;
- створення засобів реагування та поновлення;
- активізація науково-дослідної роботи в цій галузі;
- підготовка кадрів фахівців в сфері інформаційної безпеки;
- внесення необхідних змін та доповнень до національного законодавства;
- забезпечення захисту громадянських свобод.

В результаті було створено широку систему управління критичними об'єктами інфраструктури США. 16 жовтня 2001 р. розпочала діяльність Рада з захисту критичної інфраструктури США, а 14 лютого 2003 р. підписано розроблену за розпорядженням президента Буша Національну стратегію з підтримки безпеки кіберпростору. Вона базується на усвідомленні того, що з поширенням інформаційних технологій критичні інфраструктури залежать від ефективної роботи мережі, порушення якої може мати непередбачені наслідки.

Боротьба з кібертероризмом є одним з пріоритетних завдань США за Адміністрації Б. Обами. За заявами офіційних осіб, США вже сьогодні готові вести інформаційну війну, якщо на країну буде здійснений інформаційний напад. 30 січня 2010 р., під час Всесвітнього економічного форуму в Давосі, сенатор США від республіканської партії С. Колінз зазначила, що США всерйоз розглядають питання щодо ставлення до кібератак як до оголошення війни, а 12 травня 2010 року помічник заступника міністра оборони США з політичних питань Дж. Мілер заявив, що США готові завдати воєнного удару у відповідь на кібератаки на свої комп'ютерні мережі. Така позиція США щодо трактування кібератак та потенційних кібервоєн має своє продовження в позиції НАТО: група експертів під керівництвом М. Олбрайт у червні 2010 року запропонувала трактувати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору і вважаються атаками на всіх членів Альянсу.

«Огляд кібербезпеки» (Cyber SecurityReview) – комплексний документ, що визначає пріоритети нової команди президентва Барака Обами у сфері кібербезпеки; створено посаду Керівника кібербезпеки Ради національної та внутрішньої безпеки; створено Кіберкомандування США (U.S. Cyber Command) під головуванням генерала К. Александера, що одночасно очолюватиме і згаданий підрозділ, і Агентство з національної безпеки. Приблизна чисельність структури – 30 000 військових; оприлюднено нову «Стратегію національної безпеки» (2010), в якій вперше в загальній структурі загроз США окреме місце відведено кіберзагрозам; оприлюднено «Міжнародну стратегію для кіберпростору» («International Strategy for Cyberspace») як цілісне бачення урядом США найближчого майбутнього у розвитку кіберпростору; оголошено про додаткові заходи з посилення внутрішньої кібербезпеки. З 1 жовтня 2009 року в США оголошено про додатковий набір 1000 співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (Department of Homeland Security), які займатимуться виключно безпекою високотехнологічних систем США. Однак навіть ця кількість співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки.

16 травня 2011 року Адміністрація Б. Обами оприлюднила Міжнародну стратегія для кіберпростору (International Strategy for Cyberspace) [13], в якій безпосередньо йдеться про те, що США залишають за собою право на самозахист відповідно до положень установчих документів ООН та у відповідь на загрозу інформаційній інфраструктурі США готові застосовувати «дипломатичні, інформаційні, військові та економічні» засоби для реагування на інциденти. Керівництво США запропонувало цей документ як глобальну ініціативу і фактично закликає приєднуватися до такого бачення майбутнього кіберпростору всім партнерам США.

Таким чином, американські стратеги в умовах відсутності всезагального міжнародного підходу до проблеми забезпечення міжнародної інформаційної безпеки і існуючих загроз інформаційного протистояння готують грунт для нанесення контрудару у відповідь на інформаційну агресію. Відповідно до стратегії США залишають за собою

право адекватно реагувати на кібератаки. На думку експертів-аналітиків, існує небезпека, що прагнення розширеного тлумачення поняття тероризму створює загрозу використання тези боротьби з тероризмом, кібертероризмом, зокрема, для збільшення власної військової та інформаційної присутності у світі.

Викликає занепокоєність те, що в зазначеній стратегії питання міжнародної співпраці не деталізуються та не конкретизуються. У відповідному розділі зазначається, що США планують працювати в рамках міжнародних організацій, щоб просувати, так звану, культуру безпеки, сприяти розслідуванню кіберзлочинів та притягненню до відповідальності винних у їх скоєні, брати участь у створенні міжнародної мережі для нагляду та оприлюднення відомостей про загрози кібератак або про факти їх здійснення. Щодо розробки будь-якого міжнародного документу в цій сфері, навіть на перспективу, не йдеться.

Список використаних джерел

1. Волковский Н.Л. История информационніх войн: В 2 ч. – СПб, 2003.
2. Расторгуев С.П. Информационная война. – М., 1998. – 415 с.
3. Расторгуев С.П. Философия информационной войны. – М.: Московский психолого-социальний институт, 2003. – 496 с.
4. Панарин И.Н. Технология информационной войны. – М.: «КСП+», 2003. – 320 с.
5. Технологический прогрес и современные международные отношения: Учебник.- М.: Просвещение, 2004. – 448 с.
6. Libicky M/C/ What is Information Warfare? – Wash.:NDU, 1995.
7. Wilkinson P. The Laws of War and Terrorism // The Morality of Terrorism / Ed. by D. Rappoport, Y. Alexander. – N.-Y.: Columbia University Press, 1989.
8. What is Cyber-terrorism? [Електронний ресурс]. – Режим доступу: http://www.crime-research.org/library/Cyberterrorism.
9. CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Dorothy E. Denning Georgetown University May 23,2000. [Електронний ресурс]. – Режим доступу: http://www.cs.georgetown.edu/~denning.
10. Див.: Activism, Hacktivism, and Cyberterrorism:The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning Georgetown University New-York, 2001.
11. China's Secret Cyberterrorism [Електронний ресурс]. – Режим доступу: http://www.thedailybeast.com/blogs-andstories/2010-01-13/chinas-secret-cyber-terrorism/full.
12. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України: аналітична доповідь. – К.: НІСД, 2011 [Електронний ресурс]. – Режим доступу: www.niss.gov.ua/articles/510/.
13. International Strategy for Cyberspace [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.