УДК 343.9:343.71

Гавриш Степан Богданович –
перший заступник Секретаря Ради національної безпеки і оборони України, доктор юридичних наук, професор, академік Академії правових наук України, заслужений юрист України

Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії

У статті розглянуто сучасний стан протидії комп'ютерному тероризму як в Україні, так і у світі, тенденції розвитку цієї злочинної діяльності, перспективи вироблення ефективних заходів протидії.

Ключові слова: кіберпростір, тероризм, комп'ютерний тероризм, заходи протидії комп'ютерному тероризму.

Особливості розвитку процесів глобалізації в сучасних умовах обумовлені переходом від суспільства індустріального до інформаційного. Впровадження новітніх технологій в усі сфери життєдіяльності суспільства формує інші потенціали для країн із транзитивною економікою. Це стосується і політики, і самої держави, а також суспільства та свідомості його громадян. Практично кожна галузь у господарстві країни, включаючи енергетику, транспорт, зв'язок, банківський сектор тощо, використовує комп'ютерні мережі і, відповідно, залежить від їх працездатності. Порушивши роботу цих мереж, можна паралізувати інфраструктуру країни. Таким чином, швидкий прогрес у розвитку інформаційних технологій призводить до виникнення нових істотних проблем у сфері міжнародної безпеки й стабільності й може мати несподівані наслідки у вигляді зростаючої уразливості систем.

На думку низки міжнародних експертів, проблеми безпеки займають серед проблем подальшого розвитку кіберпростору одне із центральних місць, а питання про контроль інформаційного простору стає дедалі актуальнішим і повинно розглядатися й вирішуватися негайно [1; 2].

У цьому контексті, однією з нових і небезпечних загроз людству стає використання терористичними організаціями новітніх інформаційних технологій. Відповідно до досліджень ряду вітчизняних вчених і даних закордонних дослідницьких центрів, тероризм став міжнародною індустрією, здатною розпоряджатися величезними інформаційними, фінансовими, технологічними й іншими можливостями [3; 4]. Тому, дослідження феномену комп'ютерного тероризму (кібертероризму) у контексті інформаційної політики стає важливим аспектом національної та міжнародної безпеки.

Власне природа комп'ютерних злочинів та комп'ютерного тероризму є всесвітньою проблемою, оскільки не має значення, де саме вчинено подібний злочин. Відтак розглянемо, що таке комп'ютерний тероризм більш детально.

Взагалі зазначимо, що під *"комп'ютерним тероризмом" слід розуміти свідоме, цілеспрямоване застосування комп'ютерної інформації, комп'ютерів, комп'ютерних систем та мереж для захоплення комп'ютерних систем управління потенційно небезпечними об'єктами з метою*:

а) виведення цих об’єктів з ладу або їх руйнування, що прямо чи опосередковано створює або загрожує виникненням загрози надзвичайної ситуації внаслідок цих дій та становить небезпеку для персоналу, населення та довкілля;

б) створення умов для аварій і катастроф техногенного характеру;

в) залякування населення та органів влади погрозами вчинення вищезазначених протиправних дій;

г) вчинення провокацій воєнного конфлікту та міжнародного ускладнення;

д) здійснення впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об’єднаннями громадян, юридичними особами; забезпечення організаційного чи іншого сприяння створенню або діяльності терористичної групи чи терористичної організації.

Таким чином “комп’ютерний тероризм” проявляється у двох аспектах – *технологічному та інформаційному*. *Технологічний аспект* комп’ютерного тероризму пов’язаний з технологічною формою прояву різних видів тероризму – використанням комп’ютерних технологій для вчинення терористичних дій. *Інформаційний аспект* пов’язаний із здійсненням за допомогою комп’ютерної інформації впливу на психіку та свідомість людей з метою формування потрібних думок та суджень, що певним чином направляють поведінку людей у потрібному для терористів напрямі. При цьому комп’ютери, комп’ютерні системи та мережі виконують роль засобу доставки такої інформації до споживачів – користувачів глобальних мереж.

Щодо *технологічного аспекту* комп’ютерного тероризму, то у переважній більшості ранніх робіт, присвячених комп’ютерному тероризму, перебільшуються можливості кібертерористів. Так, експертом з питань тероризму, директором Міжнародного центру дослідження тероризму при Потомакському інституті політичних досліджень у Вашингтоні професором Йона Александером (Yonah Alexsander), було висловлено наступне застереження: “Варто очікувати ескалації терору в усьому світі… Буде практикуватися також кібертероризм – злочинці спробують одним натисканням клавіші порушити, наприклад, енергопостачання цілого району або роботу аеропорту” [5; 6; 7].

Але це не підкріплюється жодними фактами. Брюс Шнайер, засновник компанії Counterpane Internet Security і відомий фахівець з криптографії, взагалі вважає, що загроза кібертероризму, про яку говорять багато урядових органів і спецслужби, сьогодні переоцінюється [8].

Більш прискіпливе вивчення взаємозв’язку комп’ютерних мереж і найважливіших інфраструктур, їх уразливості до атак і значення нападів для національної безпеки, дає підстави вважати, що наявні дані про уразливість не досить вірні. Тому, для дослідження вразливості найважливіших інфраструктур до проявів комп’ютерного тероризму необхідна набагато більш детальна оцінка кожної з них, а саме: оцінка надмірності інфраструктури, норм збоїв, ступеню людської участі в процесах управління та контролі, втручання людини в критичних ситуаціях.

Проведення такої оцінки дає підстави стверджувати, що *інфраструктури в індустріальних країнах стійкі до проявів комп’ютерного тероризму*. Це твердження базується на детальному аналізі окремих сценаріїв нападу на найважливіші інфраструктури та допомагає більш точно визначити роль терористичних кібератак у стратегічному контексті або в контексті національної безпеки.

Взагалі переоцінка загрози комп’ютерного тероризму в технологічному аспекті базується на аналізі кібератак на фоні звичайних аварій, що відбуваються, зокрема: відключення електроенергії, затримка польотів, аварії на комунікаціях і їх наслідки, що є індикатором для визначення можливих наслідків комп’ютерного тероризму, а

так само – визначення ступеню залежності ключових інфраструктур від комп'ютерних мереж.

Аналіз останніх наукових робіт та публікацій у ЗМІ щодо діяльності терористичних організацій в інформаційному просторі показав, що найбільший інтерес для терористів становлять: енергетична сфера; військова та ядерна структура держави; сфера транспортних перевезень (особливо повітряний транспорт) та фінансова сфера держави. При цьому, проаналізувавши кожну з цих структур, можна стверджувати, що вони не такі вразливі до кіберзагроз, як це висвітлюється у ЗМІ.

Дослідження, проведені Інформаційною групою Комісії з консультацій в області безпеки національних телекомунікацій США щодо уразливості систем електропостачання кібератакам, показали, що "фізичне руйнування все ще являє найбільшу загрозу, з якою може зіштовхнутися енергетична інфраструктура. Поряд із цим вже з'явилася проблема електронного вторгнення, але вона все ще становить відносно незначну небезпеку" [9].

Що стосується іншої загрози, яка досить часто згадується ЗМІ у контексті комп'ютерного тероризму, – погроза *військовим структурам держави*. Проте, незважаючи на регулярні повідомлення ЗМІ про десятки тисяч щорічних нападів на мережі різних військових об'єктів, у жодній країні не спостерігалося деградації військових можливостей.

Ще одна тема, що постійно обговорюється, – втручання в національні *системи транспортних перевезень* з метою виведення їх з ладу. Але, говорячи про систему управління транспортним рухом, експерти з кібербезпеки відзначають її виокремленість із системи, пов'язаної з мережею Інтернет, тому захопити літак або потяг "дистанційно" в принципі не можливо [10].

На думку експертів, з усіх перелічених сфер життєдіяльності людини найбільш відкритою для глобального інформаційного простору є саме *фінансова сфера*, яка є привабливою для потенційних кіберзагроз – втручання у роботу банків, фондових бірж, зрив міжнародних фінансових угод. Це пов'язано з тим, що сьогодні вся фінансова система зорієнтована на спрощення системи доступу клієнтів до банківських, торгівельних і біржових послуг із використанням нових інформаційних технологій (в тому числі і здійснення багатьох операцій у мережі Інтернет) [11]. Але в цьому контексті доцільно навести дані з публікацій китайських військових журналів, де деякі автори висловлювали думку щодо можливості за допомогою кібератак вивести з ладу американські фінансові ринки. Але Китай настільки ж залежить від цих фінансових ринків, наскільки і США, і від збою може постраждати навіть більше [12].

Таким чином, слід зробити висновок, що в контексті макроекономіки збої в системах електропостачання, збої у функціонуванні транспортного руху та інші "сценарії" кібертерору – стандартні події, які не стосуються національної безпеки. Для національної економіки, де десятки або навіть сотні систем забезпечують найважливіші інфраструктури, збій у системах унаслідок кібератаки може залишитись непоміченим у повсякденному житті або бути віднесеним до стандартних затримок та виходу з ладу обладнання (крім випадків, коли атака буде поєднана з фізичним нападом – застосуванням вогнепальної зброї, вибухами, захопленням стратегічно значущих об'єктів). Кібератаки не можуть мати такого драматичного та політичного ефекту, до якого прагнуть терористи. З метою залякування та досягнення своїх стратегічних цілей, або будь-якого значимого ефекту кібертерористи повинні атакувати безліч цілей одночасно й продовжувати атаки протягом досить тривалого періоду. Щодо більшості найважливіших інфраструктур, такий сценарій чисельних нападів неможливий для хакерів, терористичних груп або держав. Так, згідно доповіді CNet. com report, аналітики інформаційної безпеки дійшли висновку, що для досягнення успіху подібної атаки

терористам “буде потрібна організація, яка має значні ресурси (приблизно 200 млн дол. США), досить потужну розвідку і п’ять років для підготовки” [13].

На думку окремих фахівців, сьогодні не існує переконливих доказів того, що будь-яка терористична організація готова використовувати комп’ютери для серйозної руйнівної діяльності. Військові аналітики-експерти корпорації RAND Сет Джонс (Seth G. Jones) та Мартін Лібіцкі (Martin C. Libicki) вважають, що “немає жодних доказів того, що люди, відомі нам як терористи, збираються займатися кібертероризмом і планують використовувати Інтернет не тільки для комунікації й координації атак традиційного типу, але й для кібератак” [14]. У доповіді Головного контрольного управління Сенатському комітету з державних справ США щодо погроз критично важливим елементам інфраструктури зазначалося, що: “Досьогодні жодна із традиційних терористичних груп, таких, як “Аль-Каїда”, не використовувала Інтернет для атак на інфраструктури держав” [15]. Навіть Річард Кларк (Richard A. Clarke), колишній координатор Білого дому з питань тероризму, охоче визнає, що “до цього часу взагалі не бачив відомих терористичних груп, що здійснюють кібератаки проти держав” [16].

Зокрема, професор права Університету штату Огайо Петер Свайр (Peter Swire) зазначив, що “сьогодні розповсюдження думки про невідворотність загрози комп’ютерного тероризму є, перш за все, корисним великим IT-компаніям, яким через перенасичення ринку технологіями необхідно знайти нові джерела доходу. Одним із таких джерел є державне фінансування проектів, пов’язаних з новими витратами на IT-безпеку” [17]. З огляду на це, проблема кібербезпеки в контексті тероризму вбачається сумнівною.

Такої ж думки дотримується професор Джорджтаунського університету Дороті Деннінг (Dorothy E. Denning), одна із самих авторитетних експертів в області комп’ютерної злочинності та кібербезпеки, яка зазначає, що кібертероризм не можна порівнювати з хімічною, біологічною або ядерною зброєю, його навіть не можна вважати такою ж серйозною загрозою, як заміновані автомобілі або терористи-самогубці [18].

Між тим чимало фахівці схиляються до думки, що атаки на комп’ютерні мережі ззовні обмежувалися модифікаціями офіційних сайтів і не могли мати непередбачуваних наслідків. “Зламати сайт не важко, важко зробити так, щоб це призвело до дійсно серйозних наслідків, – вважає Мартін Лібіцкі, – завдати серйозної шкоди, навіть терористу, який знається на комп’ютерних технологіях, набагато складніше, ніж вважається” [14].

Крім того, аналізуючи загрозу комп’ютерного тероризму, привертає увагу той факт, що більшість інцидентів комп’ютерного проникнення на потенційно небезпечні об’єкти, які пов’язані з тероризмом у кіберпросторі, насправді не мають політичного забарвлення, це лише прояви активності звичайних комп’ютерних злочинців, метою яких є отримання матеріальної вигоди, задоволення дослідницького інтересу або помста. Так, інциденти, які відбулися за останні роки, свідчать, що сьогодні їх переважну більшість вчиняють нудьгуючі підлітки або інсайдери.

З огляду на вищевикладене, необхідно зазначити, що при значній уразливості комп’ютерних мереж, яка існує сьогодні, найважливіші інфраструктури держави є достатньо захищеними.

Щодо *інформаційного аспекту* комп’ютерного тероризму, то в даному випадку заперечувати його руйнівний характер було б невірно. В контексті інформаційної безпеки все більшу небезпеку становить всесвітня глобальна мережа Інтернет, що через свою відкритість і анонімність стає головним “інформаційним полем”, яке використовують терористичні організації у своїх цілях:

– збір коштів для підтримки терористичної діяльності (у тому числі шляхом шахрайства, вимагання та шантажу);

– поширення агітаційно-пропагандистської інформації про діяльність терористичних організацій, їх цілі та завдання, наміри, форми протесту, звернення до масової аудиторії з повідомленнями про визнання своєї відповідальності за вчинені теракти тощо;

– здійснення організаційної діяльності, наприклад, розміщення у відкритому доступі й розсилання відкритих та зашифрованих інструкцій (наприклад, інструкцій з самостійного виготовлення вибухових пристроїв), повідомлень про час зустрічей зацікавлених осіб тощо;

– анонімне залучення до терористичної діяльності співучасників, наприклад, хакерів і представників бізнесу, які надають різні інформаційні послуги на комерційній основі;

– планування та координація дій, яка надає можливість децентралізувати управління терористичними організаціями та розширити потенціал малих терористичних груп;

– здійснення інформаційно-психологічного впливу на населення з метою шантажу, створення паніки та поширення дезінформації тощо.

Крім того, на даному етапі терористи зосереджують свої зусилля на зборі інформації та формуванні баз даних. У цьому контексті терористи переслідують дві основні мети. Одна – формування компромату (на підставі отриманих персональних даних про приватне життя керівників країн, банків і корпорацій), завдяки якому можна спробувати вплинути на керівників різних рівнів і отримати доступ до необхідних інформаційних ресурсів країни або корпорації. Інша – створення баз розвідувальних даних, які використовуються при підготовці атак. Наприклад, японське терористичне угруповання “Аум Сінрікьо”, яке здійснило газову атаку в токійському метро в 1995 році, перед цим створило комп’ютерну систему, що була здатна перехоплювати повідомлення поліцейських радіостанцій і відслідковувати маршрути руху поліцейських автомобілів [19].

Разом з тим, на думку Даніела Ларкіна (Daniela Larkina), керівника Центру реєстрації Інтернет-злочинів ФБР, оцінка потенційної небезпеки й збитку, що може бути завданий терористами, які заволоділи персональними даними, – є завищеною у багато разів. Ця інформація не завжди використовується, а тому інтерес навколо цієї проблеми є надмірним. Найчастіше фіксуються не факти розкрадань інформації, а спроби її використання у комерційних цілях [20].

На думку сучасних фахівців з комп’ютерного тероризму, сьогодні основною метою терористів, перш за все, є здійснення масового деструкційного впливу на психіку та свідомість людей у потрібному для них напрямі, з використанням інформаційних систем і систем зв’язку. Можна припустити, що головним напрямом кібертерористів у майбутньому буде створення систем дистанційного маніпулювання свідомістю як конкретної людини, так і суспільства в цілому [21]. Тому таке використання терористичними організаціями інформаційних технологій і глобальної мережі Інтернет у недалекому майбутньому може стати однією з нових і небезпечних загроз людству.

Щодо проявів “комп’ютерного тероризму” на території України, слід зазначити, що одержуючи безсумнівні переваги від використання новітніх інформаційних систем, побудованих на основі глобальних комп’ютерних мереж, Україна також поступово входить у певну залежність від їх ефективного функціонування. У звітах правоохоронних органів та роботах дослідників відмічається, що світові тенденції розвитку комп’ютерних технологій дозволяють прогнозувати, що його загроза з кожним роком у світі, в тому числі і для України, буде зростати. Але на думку багатьох фахівців, *такий феномен, як тероризм та*

його нові високотехнологічні форми для нашої держави сьогодні є ще не досить актуальними [22], як, наприклад, у тих державах, які міжнародні терористичні організації вже визначили як своїх основних ворогів. Це, насамперед, США та Великобританія. Терористи також історично активні там, де є військовий, національний, етнічний або територіальний конфлікт – у Росії, Іспанії, Малайзії, Іраку, Туреччині та інших країнах [4].

Разом з тим, окремі українські експерти з проблем тероризму вважають, що *передумови для проявів тероризму в Україні є* [23]. Можна виділити як внутрішні протиріччя, так і зовнішні фактори. До *внутрішніх* можна віднести економічні та соціальні проблеми, що виникли сьогодні у державі, такі, наприклад, як різке розмежування населення за рівнем доходів, напруженість у політичному житті, криміналізація всіх сфер життя суспільства тощо. До *зовнішніх* – те, що процеси глобалізації та подальша ескалація тероризму у світі, навряд чи залишать Україну осторонь, бо сьогодні наша держава залишається одним з найбільших європейських коридорів; Україна є активним учасником міжнародної безпеки, наші контингенти беруть участь у миротворчих операціях у різних країнах світу, що неминуче притягує до нас увагу світового тероризму тощо. Ще одним фактором, який викликає занепокоєння у контексті безпеки держави, є підготовка до проведення в Україні чемпіонату Європи з футболу у 2012 році, що само по собі є чинником, принадним для терористів. Міжнародний тероризм незмінно діє там, де є масові скупчення людей та можливість привернути увагу світової спільноти.

Підсумовуючи викладене, можна *прогнозувати розвиток комп'ютерного тероризму* у подальшому та надати деякі пропозиції щодо ефективної протидії цьому явищу.

Так, аналіз характеристик і проявів комп'ютерного тероризму дозволяє дійти висновку, що терористична активність різного роду екстремістських організацій найближчим часом збережеться, як мінімум, на попередньому рівні. При цьому масштаби й географія терористичних акцій з метою посилення деструктивного впливу на стан політичної, економічної та екологічної безпеки держав світового співтовариства, можливо будуть розширюватися.

Тероризм розробляє безліч нових стратегій для досягнення своїх цілей. Серед них є й такі, що орієнтовані не стільки на проведення традиційних командних операцій із знищення конкретних цілей, скільки на дезінтеграцію тих або інших систем за допомогою "інформаційних операцій", а також координованих атак. При цьому деякі фахівці вважають, що саме "інформаційний потенціал" (комунікаційні канали і контент-повідомлення) може стати ключовою метою терористів. Зокрема, окремі фахівці з кібербезпеки прогнозують, що "нові терористи" направлять свої зусилля на освоєння інформаційної зброї, руйнівна сила якої може бути у багато разів більшою від біологічної та хімічної [24; 25]. Наведене дозволяє дійти висновку, що тероризм еволюціонує в напрямі, який називають "інформаційною (мережною) війною".

Саме тому протидія проявам комп'ютерного тероризму вимагає комплексного підходу, що поєднує силові, політико-дипломатичні, економічні й гуманітарні форми та методи дій, а також ефективного поєднання антитерористичних заходів, що вживаються як на національному, так і на міжнародному рівнях.

У протистоянні з новою терористичною загрозою можна виділити ряд основних напрямів боротьби:

– уніфікація та гармонізація національного законодавства та міжнародних актів, сутність яких повинна бути спрямована на попередження та запобігання комп'ютерного тероризму;

– розробка єдиного понятійного апарату;

– удосконалення критеріальної основи безпеки інформаційних систем;

– проведення наукових розробок в області створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

– створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом із ефективною системою координації їх взаємодії;

– удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

– удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.

Настільки масштабне завдання вимагає багато часу та істотних фінансових витрат. Однак сучасна реальність така, що існування тієї або іншої країни багато в чому визначається її здатністю вчасно формувати ефективну відповідь на виклики зовнішнього світу. Тому питання щодо створення ефективної національної системи протидії комп'ютерному тероризму – це питання про виживання індустріальної держави в сучасних умовах.

Список використаних джерел

1. *Dertouzous Michel L.* What will be: How the New World of Information will Change our Lives. – Piaktus, 1997. – 384 p.

2. *Webster Frank.* Theories of the Information Society. – London: Routledge, 2006. – 320 p.

3. *Власихин В.А.* "Патриотический акт": юридический аналіз. [Электронный ресурс]. – Режим доступа: <http://www. agentura. ru/dossier/usa/ zakon-antiterror/>.

4. *Терроризм* как угроза национальной безопасности. – 2004. [Электронный ресурс]. – Режим доступа: <http://www. regions. ru>.

5. *CRS* report 32114. Computer attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. October 17, 2003. – pp. 4–5.

6. *Тимати Л.* Томас. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху// Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. – М., 2002. – С. 164–175.

7. *Yonah* Alexsander. Combating Terrorism: Strategies of Ten Countries // University of Michigan Press (August 7, 2002). – 448 p.

8. *Брюс* Шнайер. Угроза кибертерроризма переоценена, 24 ноября 2005 года. [Электронный ресурс]. – Режим доступа: <http://www. ibusiness. ru/news/ 240221/page2. html>.

9. *Strategic* Goal One: Keep America Safe by Enforcing Federal Criminal Laws (Fiscal Year 2000 Performance Report and Fiscal Year 2002 Performance Plan). – P. 25. [Електронний ресурс]. – Режим доступу: <http://www. usdoj. gov/ag/ annualreports/pr2000/NewSG1. pdf>.

10. *Лукацкий А.* "Безопасность сетей: Кибертерроризм: За и Против" [Электронный ресурс] // КомпьютерПресс. – 2001. – № 11. – Режим доступа к журналу: <http://www. compress. ru/article. aspx? id=12296&iid=465>.

11. *Гриняев С.Н.* Информационный терроризм: предпосылки и возможные последствия. [Электронный ресурс]. – Евразийский вестник. – № 19, Режим доступа к журналу: <www. e-journal. ru/besop-st3-19. html>.

12. *James A.* Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, Washington, D. C., December, 2002. [Електронний ресурс]. – Режим доступу: <www. csis. org/media/csis/pubs/021101_risks_of_cyberterror. pdf>.

13. *Joshua* Green. The Myth of Cyberterrorism: There are many ways terrorists can kill you computers aren't one of them. – Washington Monthly, November, 2002. [Електронний ресурс]. – Режим доступу: <http://www. washingtonmonthly. com features/2001/0211. green. html>.

14. *Seth* G. Jones, Martin C. Libicki. How Terrorist Groups End Implications for Countering al Qa'ida, 2008. [Електронний ресурс]. – Режим доступу: <http://www. rand. org/pubs/research_briefs/RB9351>.

15. *Government* Accountability Office U. S. [Електронний ресурс]. – Режим доступу: < http://www. gao. gov>.

16. *Richard* A. Clarke. Against All Enemies: Inside America's War on Terror // Free Press; 1St Edition edition (March 22, 2004). – 304 p.

17. *The Security* Traders. By Brendan I. Koerner | Sun September 1, 2002 12:00 AM PST. [Електронний ресурс]. – Режим доступу: <http://www. motherjones. com/print/15774>.

18. *Denning D.E.* Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. [Електронний ресурс]. – Режим доступу: <http://www. nautilus. org/archives/info-policy/workshop/papers/denning. html>.

19. *Verton D.* Black Ice: The Invisible Threat of Cyberterrorism. – N. Y, 2004. – 304 p.

20. *Роговский Е.А.* Россия в борьбе с международным терроризмом. Грани повышения позитивного образа страны. [Электронный ресурс] // Россия и Америка в XXI веке. – 2007. – № 3. – Режим доступа к журналу: <http://www. rusus. ru/? act=read&id=66>.

21. *Клепов А*. Кибертерроризм и свобода личности. [Электронный ресурс]. – Режим доступа: <http://www. proza. ru/2009/04/10/500>.

22. *Вареник Н.В.* Украина: ниша для кибертерроризма или зона благоденствия? [Электронный ресурс]. – Режим доступа: <http://www. litsovet. ru/ index. php/material. download? material_id=171579&rand=0.9993588433135301>.

23. *Актуальне* інтерв'ю. Василь Крутов: "За міжнародну безпеку у відповіді всі країни". [Електронний ресурс]. – Режим доступу: <http://www. antiterunity. org/ru/massmedia/krutov080627. php>.

24. *Walter* Laqueur, "Postmodern Terrorism" Foreign Affairs, Vol. 75, № 5, September / October 1996. – pp. 24–36.

25. *John* Arquilla, David Ronfeldt, and Michele Zanini. "Networks, Netwar, and Information-age Terrorism" in Michael Jenkins eds. "Countering the New Terrorizm". RAND Air Force federally funded research and development center (FFRDC) 1998. – pp. 39–82.

В статье рассмотрено современное состояние противодействия компьютерному терроризму как в Украине, так и в мире, тенденции развития этой преступной деятельности, перспективы разработки эффективных мер противодействия.

The current state of counteraction to computer terrorism both in Ukraine and in the world, the progress trends of this criminal activity, prospects of the development of the effective measures of counteraction are considered in the article.

Стаття надійшла до редакції журналу 27 травня 2009 року.