УДК 343.96+343.326+343.341

Бутузов Віталій Миколайович –
головний науковий співробітник МНДЦ з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук,

Тітуніна Катерина Вікторівна –
старший оперуповноважений Департаменту ДСБЕЗ МВС України, ад'юнкт Донецького юридичного інституту ЛДУВС

Сучасні загрози: комп'ютерний тероризм

Стаття присвячена проблемам боротьби з кібертероризмом та кіберзлочинністю, визначено його природу, особливості та шляхи подолання.

Завдяки широкому впровадженню інформаційно-телекомунікаційних технологій здійснюється регулювання інформаційних потоків у системах управління будь-якого рівня, вирішуються завдання щодо планування, управління, контролю за будь-якими процесами, що, в свою чергу, сприяє оптимальному використанню матеріальних і людських ресурсів. Інформація, що проникає у всі сфери діяльності держави, набула конкретного політичного, матеріального і вартісного вираження.

У свою чергу, з появою та розвитком сучасних інформаційних технологій та глобалізацією інформаційного обміну інформаційна складова в стратегії забезпечення національної безпеки посідає одне з провідних місць через такі причини:

– по-перше, інформаційні відносини та процеси пронизують усі сфери суспільних відносин;

– по-друге, за сучасних умов, при широкому використанні різноманітних інформаційних технологій питання інформаційної безпеки набувають самостійного значення;

– по-третє, система зовнішніх і внутрішніх загроз інформаційної безпеки має комплексний, всеохоплюючий характер для всіх сфер діяльності людини, суспільства та держави.

Розвиток інформаційних та телекомунікаційних технологій призвів до того, що сучасне суспільство все більше залежить від управління різними процесами за допомогою комп'ютерної техніки, електронної обробки, збереження, доступу та передачі інформації. Таким чином, об'єкти енергетичного забезпечення, транспортні системи, фінансові і банківські структури, військові відомства та правоохоронні органи, торгівельні, медичні й наукові установи – усі, хто використовує всесвітню мережу Інтернет, є потенційними жертвами комп'ютерного тероризму.

Поняття "комп'ютерний тероризм", "кібертероризм", "інформаційний тероризм" достатньо давно використовують у засобах масової інформації та наукових публікаціях. При цьому, з огляду на новизну, цей термін досить складний для розуміння і має різноманітне трактування щодо своїх кваліфікуючих ознак.

В українській і зарубіжній науковій літературі, пов'язаній з дослідженням кіберзлочинності, наявні різні підходи до визначення кібертероризму та його кваліфікації.

Прихильники першого підходу відносять кібертероризм до категорії комп'ютерних злочинів. Ними зауважується, що комп'ютерний тероризм слід

розглядати як один із різновидів неправомірного доступу до комп'ютерної інформації, розміщеної в окремій обчислювальній машині чи в мережі ЕОМ, він здійснюється з метою модифікації, знищення зазначеної інформації чи ознайомлення з нею, що забезпечує формування обстановки, за якої функціонування даної ЕОМ чи мережі виходить за межі, передбачені штатними умовами експлуатації, й виникає небезпека загибелі людей, заподіяння майнового збитку або настання будь-яких інших суспільно небезпечних наслідків. При цьому основними цілями здійснення вищезазначених дій вважається тиск на органи влади, дестабілізація суспільно-політичної обстановки за рахунок залякування, ускладнення міжнародних відносин і, як наслідок, вплив на транспортні засоби, лінії зв'язку і банки даних, які ними використовуються, що майже повністю збігається з цілями, які переслідує тероризм [1].

Прихильники другого підходу, вважають, що кібертероризм – це різновид тероризму, в основу якого покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства [2, 3]. Наприклад, Дороті Денинг (експерт американського Центру досліджень тероризму) визначає кібертероризм як елемент класифікації терористичної діяльності в Інтернеті й представляє його як комп'ютерні атаки, сплановані з метою нанесення максимального збитку життєво важливим об'єктам інформаційної інфраструктури [4].

У дослідників з проблем тероризму існує й інша точка зору щодо природи кібертероризму. Вони вважають, що кібертероризм проявляється у двох формах: по-перше, комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів-хакерів, серед яких:

– махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання);

– шпигунство (проникнення до конфіденційних каналів зв'язку державних органів для отримання інформації, шпигунство з метою отримання інформації щодо закритих технологій);

– диверсія (завдання шкоди технічному та програмному забезпеченню вірусами, що порушують функціонування державних органів та інших установ);

– незаконне користування комп'ютерними послугами (програмами, покупки за рахунок інших тощо);

по-друге, розголошення таємниці – отримання комерційної та конфіденційної інформації (що нерозривно пов'язане з першим видом), серед чого:

– несанкціоноване отримання інформації для нецільового її використання особами, які не мають на це відповідного доступу;

– незаконний збір та переховування інформації;

– порушення правил користування конфіденційною інформацією [5].

Слід зауважити, що до комп'ютерного тероризму правоохоронці відносять і дії, пов'язані з розміщенням у глобальній мережі Інтернет інформації терористичного та екстремістського змісту через створення відповідних сайтів. Так, на засіданні Ради партнерства Росія – Євросоюз (квітень 2007 року, Москва) Міністр МВС РФ Рашид Нургалієв акцентував увагу на проблемі кібертероризму і зазначив, що у 2007 році співробітники відомства виявили в мережі Інтернет близько 150 сайтів терористичної та екстремістської спрямованості [6].

У першу чергу, таке розходження думок пов'язане з тим, що до структури цього поняття належать дві рівнозначні правові категорії: тероризм і комп'ютерна злочинність (кіберзлочинність).

Зауважимо, що під категорією комп'ютерні злочини слід розуміти сукупність протиправних дій, котрі посягають на відносини у сфері обробки інформації в ЕОМ (комп'ютерах), інформаційних (комп'ютерних) системах, комп'ютерних і

телекомунікаційних мережах; права власності фізичних осіб на інформацію і доступ до неї [7]. Таким чином, до цієї категорії необхідно віднести злочини, у яких комп'ютерні, інформаційні та телекомунікаційні системи і мережі (комп'ютерна інформація) виступають як об'єкт або знаряддя злочинного посягання, а основною метою вчинення злочину у більшості випадків є одержання матеріальної вигоди.

Відповідно до статті 1 Закону України "Про боротьбу з тероризмом" "тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей" [8].

Що ж до чинного законодавства України, то поняття комп'ютерного тероризму не знайшло свого закріплення і роз'яснення в жодному нормативному акті.

Згадування про комп'ютерний тероризм у законодавстві України можна зустріти тільки в статті 7 Закону України "Про основи національної безпеки України", у якій зазначено, що "однією з реальних і потенційних погроз національної безпеки України є комп'ютерна злочинність і комп'ютерний тероризм".

Основні ознаки кібертероризму відбилися у такому понятті, як технологічний тероризм, закріпленому у статті 1 Закону України "Про боротьбу з тероризмом". Зазначена категорія містить злочини, вчинені з терористичною метою, у тому числі із застосуванням засобів електромагнітної дії, комп'ютерних систем і комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, що прямо чи опосередковано створили або загрожують виникненням небезпеки, надзвичайної ситуації внаслідок цих дій і становлять загрозу для персоналу, населення і оточуючого середовища; створюють умови для аварій та катастроф техногенного характеру [8].

Стаття 258 чинного Кримінального кодексу України розуміє під терористичним актом застосування зброї, здійснення вибуху, підпалу або інших дій, що створили небезпеку для життя або здоров'я людини, або заподіяння значної майнової шкоди, або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи здійснення або нездійснення дій органами державної влади чи органами місцевого самоврядування, посадовими особами цих органів, об'єднаннями громадян, юридичними особами, а також залучення уваги громадськості до визначених політичних, релігійних чи інших поглядів винного (терориста) та погроза здійснення зазначених дій з тією ж метою [9].

Цілі здійснення кібертероризму збігаються з цілями і мотивами здійснення усіх відомих видів терористичних дій, а саме: порушення суспільної і державної безпеки; залякування населення; провокація військового конфлікту; ускладнення міжнародних відносин; вплив на прийняття рішень або здійснення (не здійснення) дій органами державної влади або органами місцевого самоврядування, посадовими особами цих органів, об'єднаннями громадян, юридичними особами; залучення уваги громадськості до визначених політичних, релігійних або інших поглядів.

Комп'ютерний тероризм (кібертероризм) передбачає інформаційні атаки на обчислювальні центри, центри управління воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж. Він може здійснюватись з метою саботажу (урядових установ), заподіяння економічного збитку (великим виробничим корпораціям), дезорганізації праці з потенційною можливістю смертей. Інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші

складові інформаційної інфраструктури, що здійснюється терористичними угрупованнями або окремими особами, є основною формою кібертероризму. Така атака дозволяє проникати у систему, перехоплювати управління або пригнічувати засоби інформаційного обміну в мережі, чинити інші деструктивні впливи.

Засоби здійснення можуть бути гранично різноманітними і містити усі види сучасної інформаційної зброї. При цьому за своєю результативністю інформаційна зброя порівнюється зі зброєю масового ураження [10]. Так за даними Міжнародного Інституту Антитерористичної Політики (International Policy Institute for Counter-Terrorism) терористи вже використовують такі види "кіберзброї", як комп'ютерні віруси, "хробаки", "троянські коні", "логічні бомби" та інші засоби хакерського софту. Однак, на сьогодні найбільш популярним і помітним видом кібертероризму є зламування сайтів і розміщення на них гасел і закликів. Прикладом таких дій є випадок, що стався на початку війни в Іраці, коли група пакистанських хакерів "Al Qaeda Alliance Online" розмістила певні повідомлення на одному із сайтів Пентагону і на сайті National Oceanic and Atmospheric Association (Національної адміністрації з дослідження океанів і атмосфери).

У травні поточного року на сайт Президента РФ було здійснено хакерську атаку з серверів країн Балтії. У свою чергу, естонські урядові сайти атакувалися хакерами з Росії, внаслідок чого представники НАТО направили до Естонії спеціалістів по боротьбі з хакерами для розслідування зазначених атак на сервери.

Поряд із такими засобами ураження інформаційних комп'ютерних систем, як комп'ютерні віруси, програмні закладні пристрої слід зазначити засоби пригнічення інформаційного обміну в телекомунікаційних мережах, його фальсифікації, передачі каналами державного і недержавного управління інформацією та засоби, що дозволяють впроваджувати програмні закладки у державні та корпоративні інформаційні системи й управляти ними на відстані. До таких засобів належить, наприклад, нейтралізатор тестових програм, що забезпечує неможливість виявлення природних і штучних недоліків програмних засобів спеціальними тестовими програмами [11].

Крім того, слід наголосити, що тактика і прийоми, що використовуються при вчиненні даного злочину, відрізняються від тактики і прийомів вчинення класичних комп'ютерних злочинів тим, що комп'ютерний терористичний акт повинен мати небезпечні наслідки та стати широко відомим населенню й одержати великий суспільний резонанс. Від комп'ютерних злочинів кібертероризм відрізняється, насамперед, своїми цілями, що властиві тероризму в цілому, дії завжди мають публічний характер і спрямовані на вплив відносно окремих осіб, суспільства чи влади, а від традиційного тероризму (політики залякуванням, подавлення супротивників здійсненням актів насильства) відрізняється засобами здійснення, а також своєю анонімністю та знеособленістю.

Збитки від терористичної операції суттєво збільшуються при підключенні засобів масової інформації (варіант, що вже практикується в глобальному інформаційному суспільстві). Роль ЗМІ у такому випадку може виконувати телебачення та Інтернет. У результаті рівень впливу терористичної операції суттєво зростає. Таким чином, у терористів з'являється потенційна можливість впливати на зміст інформації про теракт, використовуючи контрольовані джерела інформації, підключені до ЗМІ. Їх роль можуть виконувати розроблені в мережі Інтернет сайти (з метою легалізації інформації офіційні ЗМІ посилаються на такі сайти). Завдяки цьому негативні наслідки від терористичної операції у відношенні системи, на яку здійснюється атака, значно зростають.

Несанкціонований доступ та його найнебезпечнішу похідну – кібертероризм можна розглядати як один із аспектів інформаційного протиборства інтересів конкуруючих компаній, політичних сил, держав і т. ін., що, в свою чергу, слід

розуміти як дії, спрямовані на досягнення інформаційної переваги в інформаційному протиборстві шляхом впливу на інформацію та інформаційні системи супротивника з одночасним забезпеченням безпеки власних інформаційних систем та інформації [12]. Інформаційне протиборство може охоплювати всі види інформації та інформаційні системи; поширюватись на весь інформаційний простір чи територію супротивника (конкурента); створювати кризові ситуації в різноманітних сферах життєдіяльності людини; здійснюватись як фахівцями громадських структур, так і спецпідрозділів силових структур.

Інформаційну боротьбу можна визначити як боротьбу сторін за завоювання переваги щодо кількості, якості та швидкості здобування інформації, її своєчасного аналізу й використання [13]. Напади на комп'ютерні мережі за допомогою несанкціонованого доступу здійснюються з метою порушення роботи відповідних установ. Так, Відділ захисту Пентагона свідчить, що кожного тижня інформаційні вузли Міністерства піддаються більш ніж 60 нападам. Більшість із них здійснюють хуліганські хакери, але під час бомбардування Югославії у 1999 році групи хакерів з Росії, Сербії та інших країн цілеспрямовано атакували належні американським державним структурам сервери, що завдало значної економічної, військової та політичної шкоди країнам НАТО. До сьогодні кібертероризм не завдав будь-якої суттєвої шкоди урядовим чи комерційним мережам й поки не становить великої загрози (крім таких країн, як США, Швеція, Шрі-Ланка та деяких інших). Разом із тим багато спеціалістів наголошують на недостатньому рівні захисту життєво важливих інформаційних вузлів.

Водночас, розглядаючи структуру та сутність кібертероризму як інформаційного протиборства, вважаємо за доцільне віднести до його основних напрямів такі положення:

– здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів подолання систем захисту інформаційних і телекомунікаційних систем супротивника), що призводить до витоку, втрати, підробки, блокування інформації або до порушення встановленого порядку її маршрутизації;

– створення та використання шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– здобуття необхідної інформації шляхом несанкціонованого втручання до інформаційних потоків, що передаються каналами зв'язку, чи баз даних, що перебувають в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку;

пригнічення елементів інформаційної інфраструктури державного або приватного сектору економіки.

Програмні та технічні засоби, створені для подолання систем захисту інформаційних і телекомунікаційних систем супротивника й призводять до витоку, втрати, підробки, блокування інформації або до порушення встановленого порядку її маршрутизації, є інформаційною зброєю в арсеналі злочинців. Такі засоби (інформаційна зброя) можуть бути застосовані для деструктивних впливів на державні організації при виконанні ними своїх управлінських функцій, кредитно-фінансові установи, транспортні та промислові підприємства, інформаційно-телекомунікаційні організації та ін.

Програмні та технічні засоби, створені для подолання систем захисту інформаційних і телекомунікаційних систем, можуть використовуватись з метою:

– дезорганізації діяльності структур з управління транспортних, інформаційних потоків, засобів комунікації тощо;

– блокування нормальної діяльності окремих компаній (фінансово-промислових груп, транснаціональних корпорацій, холдингів), а також стратегічних галузей промисловості шляхом порушення технологічних зв'язків, системи документообігу, фінансових розрахунків тощо;

– створення техногенних катастроф у результаті порушення технологічних процесів на об'єктах, діяльність яких пов'язана з виготовленням, використанням, переробкою небезпечних речовин та енергії, їх високою концентрацією.

Зазначені засоби мають такі основні властивості:

– латентність, тобто можливість досягти поставленої мети з вирогідністю бути невстановленим, та здійснення негативних дій (або) без наявних ознак;

– масштабність, трансграничність – можливість завдати шкоди, долаючи національні кордони;

– універсальність – можливість багатоваріантного використання в залежності від мети виготовлення.

Підсумовуючи, зауважимо, що, по-перше, завдяки досягненням науки та техніки створюється та модернізується інформаційна зброя, яка може використовуватися терористами для реалізації своєї мети. Через ЗМІ (в тому числі цифрове телебачення) та глобальну інформаційну мережу Інтернет у терористів з'являється можливість широкого оповіщення суспільства про свої наміри. Тобто, тероризм набуває нових рис і виходить на новий техногенний та організаційний рівень; по-друге, враховуючи тенденцію розвитку інформаційно-телекомунікаційних технологій та можливостей вільного доступу до них широкого кола осіб, небезпека проявів кібертероризму збільшується. У свою чергу, роль інформаційної безпеки, що зумовлена посиленням загрози використання інформаційної зброї в глобальному інформаційному обігу, постійно зростає; по-третє: комп'ютерний тероризм спроможний не тільки локалізувати чи нейтралізувати діяльність об'єктів чи груп об'єктів, побудованих на основі функціонування інформаційно-телекомунікаційних технологій, але й створити системну кризу в тих суспільствах, де широко розвинута інфраструктура інформаційного обігу.

Для України раніше ця проблема не поставала так гостро, але з приєднанням до глобального інформаційного простору потенційна загроза, яку становлять диверсії на об'єктах підвищеної небезпеки, пошкодження яких може призвести до катастрофічних наслідків існує. І поки кібертероризм з розряду "потенційної" загрози не перейшов до розряду "реальної" загрози, слід застосовувати превентивні заходи для недопущення його становлення. Адже більшість високорозвинених країн вже зазнали значної шкоди від кібертероризму. Зазначене зумовлює необхідність невідкладного вирішення проблеми, а основою забезпечення боротьби з кібертерозмом є створення ефективної системи заходів із запобігання, виявлення та припинення такого виду діяльності.

Список використаних джерел

1. *Малышенко Д.Г.* Противодействие компьютерному терроризму – важнейшая задача современного общества и государства. – ВНИИ МВД России, "Вестник РАЕН". – № 4 – Т. 3. – 2004.

2. *Голубєв В.О.* Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. – Запоріжжя: ГУ "ЗІДМУ", 2003. – 250 с.

3. *Старостина Е.* Терроризм и кибертерроризм – новая угроза международной безопасности // <http://www.crime-research.ru/articles/starostina>.

4. *Dorothy E. Denning*. The Terrorism Research Center // <http://www.washprofile.org/en/node/686>.

5. *Тероризм*: сучасний стан та міжнародний досвід боротьби / В.П. Журавльов, Б.В. Романюк, В.В. Коваленко. – Національна академія внутрішніх справ України, 2003. – 403 с.

6. *Кибертерроризм* по-русски. Інформ. бюлетень: Міжвідомч. НДЦ з проблем організованої злочинності при РНБО України – 2007. – № 5. – С.144–145.

7. *Голубєв В.О., Тітуніна К.В.* Визначення поняття та змісту категорії комп'ютерних злочинів // <http://www.crime-research.ru>.

8. *Закон* України "Про боротьбу з тероризмом" // Відомості Верховної Ради, 2003. – № 25. – ст.180.

9. *Науково-практичний* коментар до Кримінального кодексу України: За станом законодавства і Постанов Пленуму Верховного суду України на 1 грудня 2001 р. / За ред. С.С. Яценка. – К., 2002. – 936 с.

10. *Новейший* словарь иностранных слов и выражений. – Мн. Харвест, М.: ООО "Издательство АСТ", 2001. – 976 с.

11. *Мунтіян В.І.* Основи теорії інформаціогенної моделі економіки. – К.: Видавництво "КВІЦ". – 368 с.: 10.

12. *Циганков В.Д., Лопатин В.М.* Психотропное оружие и безопасность России. Серия "Информатизация России на пороге XXI века". – М.: СИНТЕГ, 1999. – С. 113.

13. *Попов М.О., Лук'янець А.Г.* До забезпечення воєнної безпеки в умовах загрози інформаційної війни // Наука і оборона. – 1999. – № 2. – 37–43.

The article is devoted to the problems of fight against cyberterrorism and cybercrime. The author determines its nature, character and the overcoming ways.