УДК 004.49

Андріученко М.С.
Центральноукраїнський національний технічний університет

Дослідження проблеми комп'ютерної злочинності та комп'ютерного тероризму

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 .

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. 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 .

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 .

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 .

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 . 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" .

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 .

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.

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 // <Ошибка! Недопустимый объект гиперссылки.>.*
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.*