Крижна Валентина Володимирівна,
старший науковий співробітник наукової лабораторії з проблем кримінальної поліції Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ІСТОРИКО-ПРАВОВИЙ АСПЕКТ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

Розвиток інформаційних технологій та процес глобалізації зумовили появу нових загроз як міжнародній, так і національний безпеці, зокрема кібертероризму. Твердження «кібертероризм» утворено злиттям двох понять: «кібер» («кіберпростір») і «тероризм». У літературі все частіше зустрічаються терміни «віртуальний простір», «віртуальний світ». Беручи за основу поняття тероризму і поєднання його з віртуальним простором, можна вивести таке визначення: кібертероризм – це комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і 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.

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. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або здійснювати інші деструктивні дії [1].

Історія сучасного кібертероризму має давню історію і сягає своїм початком у далеке минуле. Кібертероризм є похідним від більш ширшого загального поняття «тероризму» і полягає у глобальній загрозі інформаційній безпеці суспільства. Термін «кібертероризм» був запропонований у 1980-х р. старшим науковим співробітником амери-канського Інституту безпеки і розвідки (анг. – Institute for Security and Intelligence) Баррі Колліном, який використав його в контексті тенденції до переходу тероризму від фізичного до віртуального, породжуючого перетин та злиття цих світів [2].

Визначення ж інформаційного або кібертероризму можна знайти як в міжнародно-правових документах та проектах конвенцій, так і в дослідженнях фахівців з цієї проблематики. Однією з характерних рис визначень інформаційного тероризму є те, що в переважній більшості в них згадується тільки один аспект

інформаційної безпеки, пов'язаний із засобами оброблення інформації, що звужує поняття інформаційного тероризму, тим самим обмежуючи сферу правового регулювання, що не сприяє ефективній співпраці держав у справі боротьби з інформаційним тероризмом [3].

Під кібертероризмом розуміють навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [4]. Таким чимом, можна визначити кібертероризм як похідний тероризму, об'єктом посягання якого є інформаційна безпека. Він є найбільш небезпечним, оскільки межі його визначені віртуальним середовищем, і знайти порушника дуже важко.

Розгляд «кібертероризму» в історичних рамках охоплює чималий період і пов'язаний головним чином із еволюцією комп'ютерної обчислювальної техніки. Перший період – 1960–1970 рр. – поява перших транзисторних обчислювальних систем, як наслідок поява дрібних кіберзлочинів. Другий період – 1980–1990 рр. – випуск першої операційної системи, перший арешт «віртуальних злочинців», зареєстроване перше «сімейство комп'ютерних вірусів». Третій етап – поява і активне запровадження «кібератак», втручання у роботу державний органів, в т. ч. військових, утворення хакерських груп та проведення шпіонських кібероперацій. Отже, із еволюцією людського суспільства розросталася і система кібезлочинності, кіберзлочинів.

У Ковенції Ради Європи про кіберзлочинність від 23.11.2001 р. немає чіткої дефініції «кібертероризму», проте з її положень випливає, що кібертероризм є навмисне застосування незаконно встановленого повноваження, насильства, руйнування або проникнення в кіберсистеми, у разі якщо подібні дії можуть спричинити смерть або заподіяти шкоду особі або особам, істотної шкоди майну, цивільний безлад або значну економічну шкоду. Ця Конвенція є свого роду реакцією США на терористичні акти 11 вересня 2001 р.

У Конвенції Ради Європи згадується 4 типи комп'ютерних злочинів: незаконний доступ; незаконне перехоплення; втручання в дані; втручання в систему. Згідно з цим документом, засобами кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги інформаційно-комп'ютерних технологій та дані трафіку [5].

Боротьба із кібертероризмом має включати усі дієві шляхи та методи захисту і попередження вчинення таких злочинів. На наш погляд, до таких основних шляхів належать: належне законодавче врегулювання поняття «кіберзлочинності», «кіберзлочину», його

видів, основних характеристик, відповідальності за його вчинення, порядку притягнення особи до відповідальності; створення відповідних державних органів, із безумовним залученням спеціалістів у сфері комп'ютерних технологій, для захисту та боротьби з кібертероризмом; розроблення стійкого системного захисту інформації, інформаційних технологій, захисту ЕОМ; належне фінансування такого роду діяльності із привенції та захисту інформаційної безпеки; міжнародне співробітництво як у теоретичних розробках, так і у практичній діяльності.

З огляду на сучасні реалії життя, загроза кібертероризму є дуже серйозною проблемою. Актуальність цього питання буде зростати в міру розвитку і поширення інформаційно-телекомунікаційних технологій. Все це дозволяє сьогодні говорити, що терористична площина переходить з реального простору в простір віртуальний. Інформаційні мережі допомагають терористичним угрупованням в здійсненні задуманих планів, які перетікають в кібертероризм як реальну загрозу діяльності для окремих країн і всього світового співтовариства. Питання забезпечення інформаційної безпеки як однієї з важливих складових національної безпеки держави особливо гостро виникає в контексті появи транснаціональної і транскордонної комп'ютерної злочинності та кібертероризму.

Список використаних джерел

1. Ендрю Конрі-Мюррей. Політика безпеки в часи терору. – [Електронний ресурс]. – Режим доступу: http://www.osp.ru/lan/2002/02/083.htm.

2. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк //Ukrainian Scientific Journal of Information Security, 2013. – Vol. 19/ – Issue-2.

3. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс] / О. В. Кубишкін. – Режим доступу: http://pravolib.pp.ua/informatsionnyiyterrorizm-15103.html.

4. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/638-15/page2.

5. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575/page.