УДК 32.019.51:323.28:323.2(477)

Г. В. Форос, канд. юрид. наук, доцент

А. В. Форос, викладач

Одеський національний університет імені І. І. Мечникова,
кафедра кримінального права, кримінального процесу і криміналістики,
Французький бульвар, 24/26, м. Одеса, 65058, Україна

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

В статті визначено поняття інформаційний тероризм і вказано на його характерні риси, досліджено основні форми інформаційного тероризму, а також вказано на його загрозу національній безпеці України.

Ключові слова: інформаційний тероризм, кібертероризм, національна безпека.

Одним із основних чинників необхідності удосконалення систем національної, регіональної та міжнародної безпеки є поява кримінальних суб'єктів застосування сили і генезис глобальних терористичних мереж, які становлять загрозу системам забезпечення національної безпеки і вказують на необхідність узгодження та координації зусиль держав щодо розробки та впровадження адекватних механізмів забезпечення глобальної стабільності та безпеки.

Сьогодні, в залежності від політичних цілей терористів, сферою терористичної діяльності стає весь світ, механізмом терористичних дій — насильство відносно цивільних громадян, а його головним об'єктом — суспільство та громадська думка. У сучасних умовах, коли арсенал терористів поповнюється новітніми зразками зброї, сучасними засобами та технологіями отримання, передання, обробки та збереження інформації, а їх організаційні структури ускладнилися і придбали міжнародний характер, гостро встає питання про виявлення і забезпечення надійним захистом потенційних об'єктів терористичних зазіхань, і як наслідок систем національної безпеки держав. Директор ЦРУ, виступаючи на тему проблем світових загроз, заявив, що терористичні угруповання використовують комп'ютерні файли, електронну пошту та шифрування для підтримки своєї протиправної діяльності. Атрибутивною ознакою тероризму на нинішньому етапі його розвитку стало активне використання інформаційних технологій, здатних перетворити цільову аудиторію на об'єкт маніпулювання. Перші випадки комп'ютерного тероризму сталися наприкінці 1990-х років, що пов'язано як з розвитком світових мереж, телекомунікацій, так і з широким розповсюдженням комп'ютерів у всіх сферах життєдіяльності суспільства. Сучасні інформаційно-комунікативні технології забезпечують відносно невеликі терористичні групи могутньою та дієвою зброєю, своєрідним ретранслятором насильства. Таким чином, можна стверджувати, що за сучасних міжнародних реалій значну зовнішню загрозу для України становить розповсюдження інформаційного тероризму.

Розпочинаючи будь-які наукові дослідження, потрібно чітко визначитися з термінологією. Серед наукових та практичних працівників немає єдності у термінологічному позначенні даного виду терористичної діяльності. Такий вид тероризму вони називають по-різному: "інформаційний тероризм", "комп'ютерний тероризм", "кібертероризм", "технологічний тероризм", "віртуальний тероризм" тощо. При цьому зміст зазначених понять визначається по-різному. Складність у

формулюванні цих понять існує, очевидно, як через неможливість виділення єдиного об'єкта злочинного посягання, так і достатньо великої кількості предметів злочинних посягань з погляду їхньої кримінально-правової охорони.

Так, В. О. Коршунов вказує, що інформаційний тероризм — це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [1, 6].

Аналіз положень Закону України "Про боротьбу з тероризмом" свідчить, що інформаційний тероризм є видом технологічного тероризму, і це злочини, що вчиняються з терористичною метою із застосуванням засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля, або створюють умови для аварій і катастроф техногенного характеру [2].

На думку вчених, найбільшу небезпеку представляє кібертероризм, а саме — тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі новітніх інформаційних технологій [3, 13]. Кібератаки здатні завдати інформаційно-телекомунікаційним системам на основних інфраструктурах значної шкоди. Це й атомні електростанції і системи керування польотами, комп'ютерні системи правоохоронних органів, лікувальних закладів тощо. Трагічно закінчилися кібератаки на системи управління польотами в США 11 вересня 2001 року, коли оператори авіарейсів та протиповітряної оборони не змогли своєчасно зреагувати та оголосити тревогу.

Аналіз наукових праць, спеціальної літератури та повідомлень засобів масової інформації свідчить про той факт, що вирізняють абсолютно новий вид тероризму — віртуальний. Це тероризм, при якому у терористів є можливість доступу до інформаційно-комп'ютерних технологій, за допомогою яких вони створюють видимість терористичної кампанії або окремого терористичного акту, якого насправді немає, чим можливе досягнення потрібного терористам психологічного впливу на широку аудиторію. Особливістю сучасного тероризму є активне використання інформаційно-психологічного впливу як важливого елемента маніпуляції свідомістю людей. Не таємниця, що сьогодні засоби комунікацій, що оперують, трансформують та дозують інформацію, стають головним інструментом впливу в сучасному суспільстві. Для підвищення ефективності здійснення стратегій використовуються найсучасніші інформаційні технології, які допомагають перетворити публіку в об'єкт маніпулювання. Тому роль засобів масової інформації полягає в дії на користь суспільству, а не терористів. Висвітлення подій у засобах масової інформації не повинно працювати для досягнення терористичних цілей, а сприяти вихованню у свідомості людей неприйняття методів насильства й шантажу, підтримці дій влади, а також навчанню прийомам особистої і колективної безпеки в ситуаціях, пов'язаних з терористичними погрозами.

Так, в науковій літературі, серед основних зовнішніх загроз, що можуть виступати джерелами вчинення терористичних актів, виділяють: прагнення деяких держав до встановлення свого воєнно-політичного впливу в окремих регіонах світу; можливість підриву стратегічної стабільності внаслідок порушення режиму не- розповсюдження ядерної зброї, міжнародних домовленостей в галузі обмежень і скорочення озброєнь, якісного та кількісного нарощування останніх іншими державами; збереження чи створення у суміжних з Україною регіонах значних угруповань збройних сил держав (коаліцій держав), що перевищують їх оборонну потребу; наявність у деяких держав великих арсеналів ядерної та інших видів зброї

масового знищення; сепаратистські тенденції у крайніх формах вияву, що дестабілізує внутріполітичну ситуацію в багатонаціональних державах, якою є Україна; збереження загрози міжнародного шантажу, в тому числі з використанням ядерної та інших видів зброї масового знищення; виникнення збройних конфліктів у сусідніх державах, в які можуть втягнути Україну. Але на рівні з зазначеними виділяють також інформаційну експансію з боку інших держав і можливість витоку інформації, яка становить державну та іншу передбачувану законом таємницю, а також конфіденційної інформації, що є власністю держави.

Проведене дослідження основних компонентів змісту поняття даного явища відіграє важливу роль для загального однакового розуміння суті явища. Однак має місце ще одна досить суттєва розбіжність, вона полягає в тому, як визначити даний вид тероризму: комп'ютерний чи інформаційний, а, може, кібертероризм? Узагальнюючи різні точки зору, можна зробити висновок про те, що в даний час існують два основні напрямки наукової думки щодо досліджуваної проблеми.

Одна частина дослідників схильна к визначенню терористичних проявів, у яких комп'ютер є або об'єктом, або знаряддям посягань, як кібертероризм.

Дослідники ж другої групи терористичні прояви з використанням новітніх досягнень науки і техніки в галузі інформаційних технологій відносять до інформаційного тероризму.

При цьому необхідно враховувати ще одну особливість — інформаційно-телекомунікаційні системи та мережі в цих злочинах можуть виступати одночасно і як предмет, і як знаряддя вчинення злочину. Ми пропонуємо розглядати "інформаційний тероризм" як базове поняття, виходячи з того, що сформована система правовідносин в галузі інформаційної діяльності і захисту інформаційно-телекомунікаційних систем та мереж, а також враховуючи, що саме інформаційна безпека розглядається як елемент або підсистема національної безпеки.

На думку вітчизняних дослідників проблем тероризму, інформаційний тероризм проявляється у двох формах:

1) комп'ютерні економічні злочини за допомогою спеціалістів-хакерів:

- махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання);
- шпигунство (проникнення на конфіденційні канали зв'язку державних органів для здобуття інформації, шпигунство для здобуття закритих технологій);
- диверсія (завдання шкоди технічному та програмному забезпеченню вірусами, що порушує функціонування державних органів та інших установ);
- незаконне користування комп'ютерними послугами;

2) розголошення таємниці — отримання комерційної та конфіденційної інформації (нерозривно пов'язані з першим видом):

- несанкціоноване здобування інформації для нецільового її використання особами, які не мають відповідного доступу;
- незаконний збір та переховування інформації;
- порушення правил користування конфіденційною інформацією.

Інформаційний тероризм, під яким розуміється використання сучасних інформаційних технологій і, в першу чергу мережі Інтернет, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур, стає реальною загрозою для національної безпеки нашої держави.

Однією з основних загроз для національної безпеки України є використання сучасних інформаційних технологій в злочинній діяльності організованих злочинних угруповань з терористичною спрямованістю. Директор ЦРУ, виступаючи на тему проблем світових загроз, заявив, що терористичні угруповання використовують комп'ютерні файли, електронну пошту та шифрування для підтримки своєї протиправної діяльності. Саме ці угруповання застосовують високі технології у своїй протиправній діяльності в якості: джерела отримання інформації,

засобу її збереження, засобу передачі інформації, знаряддя та об'єкта злочинного посягання.

На наш погляд, це пов'язано з такими чинниками: по-перше, діяльність стійких злочинних організованих структур є часткою великомасштабного легального і нелегального бізнесу; по-друге, із організацій, які використовують комп'ютерні системи, значно простіше і зручніше "витягувати" гроші при допомозі комп'ютерних технологій; по-третє, як вказує Біленчук П. Д. [4, 127], оскільки сили безпеки і поліції використовують комп'ютерні технології для боротьби зі злочинністю, то, відповідно, щоб попередити їхнє стеження й розгадати плани правоохоронців, лідери злочинних угруповань широко використовують як могутню зброю протидії комп'ютерні технології.

На замовлення організованих злочинних угруповань терористичної спрямованості, нерідко не знаючи про це, хакери розробляють і вишукують різні методи несанкціонованого проникнення до комп'ютерних мереж, постійно працюють над тим, як за допомогою комп'ютерних програмних засобів обійти системи програмно-математичного захисту. Сьогодні останні у більшості випадків стають все досконалішими, ціни на них постійно зростають, але діє вічний принцип техніки: що зроблено руками однієї особи, з часом, однак, буде подолано іншими. Категорію "хакери" О. М. Бандурка розглядає як досить небезпечну, вказуючи на те, що вони зламують мережі просто заради власних бажань або заради завоювання авторитету в хакерських колах. Але нерідко вони зламують системи і з метою фінансової наживи та інших злодіянь [5]. В науковій літературі існує точка зору, що дану категорію слід розглядати як складову кількох груп, у зв'язку з чим пропонується така класифікація комп'ютерних правопорушників: "аматори", "зрадники", "мафіозі", "політики", "альтруїсти", "шпигуни", "пірати", "хулігани".

На нашу думку, особливу загрозу для національної безпеки України становлять "хакери-політики". Вони організують комп'ютерні атаки на сайти і сервери організацій, що мають відмінні від них політичні чи громадські переконання. Жертвами політичних атак здебільшого стають урядові сайти. Як правило, метою політичних хакерських нападів є руйнування інформаційних систем урядових установ, а в деяких випадках політична пропаганда. Найбільш розповсюдженим видом атаки даного підвиду на системи є зміна інформаційного наповнення сайту, інколи — блокування роботи ресурсу, на який спрямовано атаку. До особливо небезпечних для інформаційної безпеки України категорій комп'ютерних правопорушників слід віднести таку, як "хакери-шпигуни" — це люди, які отримують секретну інформацію шляхом вторгнення до чужих комп'ютерів. Вони працюють переважно на замовлення. При допомозі цього різновиду хакерів здійснюються організовані розвідувальні акції в різних сферах економіки та оборони.

Про категорію "хакери-мафіозі" йшлося вище: це члени організованих злочинних формувань, метою яких є одержання фінансової вигоди, їхня мішень — це банки, фінансові й торгові компанії. Іноді до послуг "мафіозі" вдаються терористи. Протидія даній категорії осіб значно ускладнюється з причини здійснення терористами заходів конспірації щодо злочинної діяльності, головною метою яких є протидія оперативним підрозділам.

Протидія даному виду злочинної діяльності відстає від потреб правоохоронної практики. Ряд уже прийнятих законів частково регламентує деякі аспекти боротьби, але цього явно недостатньо. Визнаючи загрозу безпеці та добробуту народу, які несе в собі злочинність в інформаційній сфері, Президент України на Самміті Тисячоліття у Нью-Йорку виступив з ініціативою про розробку Міжнародної конвенції по боротьбі з комп'ютерним тероризмом. Процес протидії інформаційній агресії в ряді країн почався із формування спеціальних підрозділів, до завдань яких входить не тільки захист від хакерських атак, але й кібернетичний наступ на власників кіберзброї. На думку американського генерала Едварда Андерсена, готов

ність до бойових дій у кіберпросторі з точки зору національної безпеки так само важлива, як ядерні ракети та контроль над космосом [6, 8]. А якщо враховувати, що з'явились праці, в яких доведено, що інформаційний тероризм є підґрунтям ще для однієї нової форми тероризму — космічного, який тісно пов'язаний з новітніми комп'ютерними технологіями, то проблема протидії набуває нових форм та аспектів.

Таким чином, інформаційний тероризм — це новий вид терористичної діяльності, спрямований на використання сучасних інформаційних технологій з метою порушення або знищення значних державних інфраструктур. Особливістю сучасного тероризму є активне використання інформаційно-психологічного впливу як важливого елемента маніпуляції свідомістю людей. Серед основних зовнішніх загроз для національної безпеки України слід виділити інформаційну експансію з боку інших держав і можливість витоку інформації, яка становить державну та іншу передбачувану законом таємницю, а також конфіденційної інформації, що є власністю держави. Протидія даному виду злочинної діяльності відстає від потреб правоохоронної практики, а саме знаходиться на стадії становлення і потребує обґрунтованого наукового забезпечення в особливості на рівні організаційно-правового аспекту.

Література

1. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.02 "Політична інститути та процеси"/Коршунов В. О. — Дніпропетровськ, 2008. — 18 с.

2. Закон України "Про боротьбу з тероризмом" від 20 березня 2003р. // Відомості Верховної Ради України. — 2003. — № 25. — Ст. 180.

3. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб. /Б. М. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов; За заг. ред. проф. Я. Ю. Кондратьева. — К. : Вид. ПАЛИВОДА А. В., 2004. — 144 с.

4. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність: Навчальний посібник — К.: Атіка, 2002. — 240 с.

5. Бандурка О. М. Інтерпол: Міжнародна організація кримінальної поліції: науково-практичний посібник. — Х. : Основа, 2003. — 324 с.

6. WHITE PAPER. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998, c. 127.

А. В. Форос, канд. юрид. наук, доцент

А. В. Форос, преподаватель

Одесский национальный университет имени И. И. Мечникова,
кафедра уголовного права, уголовного процесса и криминалистики,
Французский бульвар, 24/26, г. Одесса, 65058, Украина

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ

РЕЗЮМЕ

Информационный терроризм — новый вид террористической деятельности, направленный на использование современных информационных технологий с целью нарушения или уничтожения важных государственных инфраструктур. Информационный терроризм следует рассматривать как одну из основных угроз национальной безопасности Украины. Проблематика противодействия информационному терроризму находится на стадии становления и требует обоснованного научного обеспечения и особенно на уровне организационно- правового аспекта.

Ключевые слова: информационный терроризм, кибертерроризм, национальная безопасность.