УДК 32.019.51:323.28:323.2(477)

МАЛАХОВ Г.Б., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5333-0666.

ВИКОРИСТАННЯ КІБЕРПРОСТОРУ ЯК ІНСТРУМЕНТУ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

DOI…

Анотація. *У статті проаналізовано основні підходи до визначення інформаційного тероризму, сформульовано його ознаки та принципи. Висвітлені проблеми використання кіберпростору як інструменту інформаційного тероризму, а також тенденції зростання технічного рівня реалізації кіберзагроз. Аналізуються основні акти інформаційного тероризму у кіберпросторі України та діяльність Центру протидії дезінформації РНБО України з ідентифікації цього явища. Проаналізовано новації в підходах країн НАТО у сфері боротьби з інформаційним тероризмом. Запропоновано шляхи удосконалення міжнародної співпраці України з НАТО з питань протидії інформаційному тероризму.*

Ключові слова: *тероризм, інформаційний тероризм, кібертероризм, кіберпростір, кіберпротидія, кіберстримування, НАТО.*

Summary. *The article analyzes the main approaches to the definition of information terrorism, formulates its signs and principles. The problems of using cyberspace as a tool of information terrorism are highlighted, as well as the growing trends of the technical level of cyber threats. The main acts of information terrorism in the cyberspace of Ukraine and the activities of the Center for countering disinformation of the NSDC of Ukraine to identify this phenomenon are analyzed. Innovations in the approaches of NATO countries in the field of combating information terrorism are analyzed. Ways to improve international cooperation with NATO on countering information terrorism are proposed.*

Keywords: *terrorism, information terrorism, cyberterrorism, cyberspace, cyber countermeasures, cyber deterrence, NATO.*

Постановка проблеми. Кіберпростір вже давно визнано одним з можливих театрів воєнних дій. У Стратегії кібербезпеки України наголошується: “російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України”. Пріоритетними цілями кібертероризму залишаються об’єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об’єкти тощо [1].

Рівень загрози інформаційного тероризму в Україні стрімко зростає в умовах неприкритої агресії рф проти України (з лютого 2022 року).

Особливо помітне зростання актів кіберінцидентів на об’єкти критичної інфраструктури України з боку російських хакерів та кіберутворень. CERT-UA урядова команда реагування на комп’ютерні надзвичайні події, яка функціонує при Держспецзв’язку України, за минулий рік зафіксувала 2543 кіберінциденти, що на15,9 %

більше ніж за 2022 рік, коли Україна стикнулася з величезною кількістю атак у зв'язку з повномасштабною російською агресією проти нашої держави [2].

Водночас нинішнє кіберзагострення є наслідком довгострокового тренду використання кіберпростору як нової арени геополітичної боротьби. Крім цього, як відзначають дослідники, чинне кіберзагострення міжнародного безпекового середовища є своєрідним наслідком загальної хаотизації системи міжнародної безпеки. Метод агресії, який масштабно використовує рф, з метою досягнення власних геополітичних інтересів, безпосередньо пов'язаний із використанням наступальних дій в кіберпросторі та спроб впливати завдяки таким діям на політичний порядок денний, на окремі важливі для неї політичні кампанії в інших країнах, або для більшої хаотизації глобальної політичної обстановки [3].

Результати аналізу останніх публікацій. Проблемам протидії інформаційного тероризму присвятили свої роботи Лабенко Л.В. [4], Білан І.А. [5], Банк Р.О. [6], Діордіца І.В. [7], Пилипчук В.Г., Дзьобань О.П. [8], Петришин Г.Р. [9] та ін.

Інформаційний тероризм як форма інформаційної війни в кіберпросторі став предметом поглибленого аналізу у працях Коршунова В.О. [10], Курбана О.В. [11], Леонова Б.Д. [12], Прокоф'єва Д. [13], Почепцова Г.Г. [14], Рижова І.М. [15], Яцик Т.П. [16] та ін.

Водночас, малодослідженими залишаються аспекти використання кіберпростору як інструменту інформаційного тероризму в умовах повномасштабного вторгнення рф на територію України. З'явилися нові інструменти такого тероризму, що зумовлює актуальність цієї тематики.

Метою статті є визначення на базі аналізу кіберпростору України особливостей інформаційного тероризму, ідентифікації його проявів для вироблення ефективних заходів з протидії цьому явищу.

Виклад основного матеріалу. Сьогодні серед вітчизняних вчених відсутні єдині підходи до визначення інформаційного тероризму.

Лабенко Л.В. під інформаційним тероризмом пропонує розуміти небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади і управління, пов'язані із розповсюдженням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникненню кризових ситуацій в державі, нагнітання страху і напруги у суспільстві [4]

На думку Коршунова О.В., інформаційний тероризм являє 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 [10].

Яцик Т.П. вважає, що зміст інформаційного тероризму складає множина інформаційних війн та інформаційних спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [16].

З точки зору Герасименка К.С., суть інформаційного тероризму полягає у дестабілізації суспільства, створенні в ньому атмосфери громадянської непокори і недовіри суспільства до дій та намірів влади шляхом організації спеціальних медіакампаній [17].

Фахівці Центру протидії дезінформації РНБО України наполягають на тому, що інформаційний тероризм – це прямий свідомий вплив на психіку та свідомість з метою формування необхідних думок і суджень, що певним чином задають напрям поведінки людей [18].

Аналізуючи вказані концепції визначення інформаційного тероризму, потрібно зазначити, що вони містять у собі раціональне зерно, доповнюючи одна одну.

Чинне законодавство України, на жаль, не містить визначення інформаційного тероризму. Натомість Закон України "Про боротьбу з тероризмом" передбачає поняття "технологічного тероризму", під яким розуміються кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, 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; створюють умови для аварій і катастроф техногенного характеру (ст. 1) [19].

Ст. 10 Закону України "Про основні засади забезпечення кібербезпеки України" визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням [20].

Відсутність у законодавстві України визначення інформаційного тероризму та його ознак негативно позначається на боротьбі з цим явищем.

Ще до початку повномасштабного вторгнення рф на територію України Стратегія кібербезпеки України фіксувала посилення тенденції:

зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі;

здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу;

постійного вдосконалення та розробку нових інструментів і механізми кібератак;

використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси.

використання кіберпростору терористичними організаціями в глобальному масштабі [2].

Зазначені тенденції свідчать про зростання технічного рівня реалізації кіберзагроз.

Для формування потенціалу кіберстримування Україна визначала на рівні Стратегії необхідність досягнення таких стратегічних цілей:

- ціль С. 1. Дієва кібероборона;
- ціль С. 2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму [2].

Для досягнення першої з названих цілей Україна має забезпечити розвиток (у тому числі кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, забезпечити ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності [2].

Реалізація цілі С. 2. "Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму" вимагає від України забезпечення безперервного здійснення контррозвідувальних заходів з виявлення, попередження та припинення актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян [2].

Між тим з початку (з 24.02.2022 р.) повномасштабного вторгнення РФ на територію України Центр протидії дезінформації РНБО України та інші державні органи фіксують появу нових інструментів реалізації кіберзагроз та проявів інформаційного тероризму, які стали досить різноманітними й такими, що спрямовані на сильний психологічний вплив на аудиторію.

Серед таких методів (інструментів) називаються: дезінформація, пропаганда, маніпулювання, інсайди, матеріали, створені злочинним шляхом (шантаж, погроза життю і здоров'ю, вбивство, підкуп) [18; 21, с. 8-9].

Серед усіх різновидів інсайдів на увагу заслуговують, в першу чергу, інсайд-залякування та агресивні інсайди. Інсайд-залякування – це контент, який викликає лякаючи настрої в аудиторії, серед якої поширюється. Найчастіше вони запускається в момент соціального напруження суспільства (терористичні акти, війна, стихійні лиха). Їхні сюжети варіюється від песимістичних до панічних, а особливого поширення такі сюжети набувають під час складних політичних і соціальних реформ, зміні влади чи соціально-політичної системи загалом [18].

Інсайди-провокації – контент, спрямований на стимулювання жорсткої реакції та провокування людей до агресивної поведінки. Такі інсайди виникають у гострих протиріччях, пов'язаних із соціальними, міжгруповими, міжетнічними, міжнаціональними конфліктами [18]. Серед поширюваних країною агресором проти України прикладів найбільш часто згадується "в Україні панує нацизм", "влада в Україні – наркомани та нелюди" тощо.

Окрім цього, виділяють інші інструменти інформаційного тероризму:

відеоконтент, який може бути представлений не лише на телебаченні, а й на платформах "Ютуб", "Інстаграм", "Фейсбук", "Тік Ток";

дезінформаційні кампанії, інформаційно-психологічні спецоперації (так звані "інсайти");

сучасні онлайн-платформи, які відкрили доступ до нових способів поширення дезінформаційних меседжів – фейкові акаунти/сторінки, боти, таргетована реклама тощо;

шкідливе програмне забезпечення, яке дозволяє створювати й поширювати діпфейки;

створені злочинним шляхом матеріали [21, с. 33].

Важливими є принципи інформаційного тероризму, серед яких фахівці Центру протидії дезінформації при РНБО України виділяють:

1. Використання шокуючих матеріалів – постановочні зображення жорстокості або здійснення реальних актів насильства для отримання такого матеріалу;

2. Залякування аудиторії, часто вигаданою, "неминучою загрозою", нагнітання панічних настроїв;

3. Перевантаження інформаційного поля великою кількістю контенту, що знижує можливості людського мозку критично оцінювати інформацію;

4. Охоплення всіх платформ та медіа, включаючи залучення осіб, які посідають найвищі посади та щаблі у політичній, військовій, церковній та інших ієрархіях;

5. Координованість органами державної влади або централізоване поширення [18].

Одним з найбільш відомих прикладів інформаційного тероризму є масштабна атака вірусу NotPetya у квітні 2017 року, в результаті якої було заблоковано роботу значної кількості веб-сайтів та автоматизованих систем в Україні (міністерств, банків, ЗМІ, об'єктів критичної інфраструктури). Ще одним з прикладів інфотероризму є активне використання російськими ЗМІ демонстрації "злочинів" українських військових перед

початком повномасштабного вторгнення російської федерації в Україну. У соціальних мережах та ЗМІ ширилися неправдива інформація про те, що українці продовжують спроби проведення терористичних актів проти життєво важливих об'єктів інфраструктури та проти цивільного населення [22].

18 березня 2022 року експерти Центру протидії дезінформації при РНБО України на своєму сайті почали знайомити громадськість з проявами інформаційного тероризму.

Дослідники відзначають, що сьогодні кібертерористичні угруповання діють насамперед із метою поширення хаосу, зруйнування критичної інфраструктури, завдання фізичної та матеріальної шкоди тощо [23, с. 11-12]. З цією метою вони використовують такі основні методи:

– APT-атаки (різновид складних кібератак із метою отримання несанкціонованого доступу до інформаційних систем і встановлення прихованого доступу до них з метою використання або контролю) на об'єкти критичної інфраструктури, державні установи;

– використання шкідливого програмного забезпечення, ціллю якого стають системи керування електромереж, транспортних систем,

– DoS/DDoS-атаки – це атаки, які мають на меті зробити електронні інформаційні ресурси недосяжними для легітимних користувачів. Така кібератака спрямована на порушення доступності електронних інформаційних ресурсів;

– отримання несанкціонованого доступу до державних, банківських чи інших установ із метою викрадення інформації з обмеженим доступом;

– використання програм-вимагачів (ransomware), що зашифровують інформацію критично важливих систем і, фактично, блокують діяльність організацій, установ чи окремих осіб [23, с. 11-12].

Сучасні витончені інструменти інформаційного тероризму, масштабність кібератак ускладнюють роботу правоохоронних органів України з виявлення таких проявів та їх протидії. Водночас, Україна не лишається наодинці з проблемою кібервикликів, до подолання яких активно залучаються країни НАТО.

Поява сучасних кіберзагроз зумовлює потребу міжнародної співпраці України з країнами НАТО, де рф розглядається не лише як порушник міжнародної безпеки, а й безпосередній агресор у кіберпросторі [3].

НАТО як структура міжнародної безпеки хоч і не досить швидко, однак реагує на зміни у військово-політичній обстановці у світі, пов'язані із посиленням мілітаризації кіберпростору [3]. На даний час НАТО і країни-члени здійснили значні стратегічні, оперативні і технічні кроки задля протидії зловмисній кібердіяльності.

Діяльність НАТО в питанні кіберзагроз та кіберконфліктів декларує принципи взаємної відповідальності у діяльності усіх членів Альянсу щодо захисту кіберпростору та реакції на можливі публічні загрози [24, с. 64]. Так, відповідно до статті 3 Вашингтонського договору "члени Альянсу будуть підтримувати і розвивати свої індивідуальні і колективні можливості протистояти збройному нападу". Особлива увага приділяється забезпеченню кібероборони усіх країн НАТО.

Політика НАТО щодо впливу на кіберконфлікт, як нову форму політичного протистояння виражається у системній боротьбі членів Альянсу з кібератаками та фейками [24, с. 65].

Разом з тим, продовжується співпраця НАТО з Україною щодо приведення національного законодавства останньої у відповідність до стандартів Альянсу з метою зниження ризиків кіберзагроз.

10 липня 2024 року союзники з НАТО домовились створити новий центр для кращого захисту від кіберзагроз. Інтегрований центр кібероборони НАТО (NICC) має

посилити захист мереж НАТО і членів Альянсу і використання кіберпростору як сферу операцій. Кадровий потенціал Центру складають цивільні і військові співробітники НАТО, країн Альянсу, а також експерти з цієї галузі. Центр застосовуватиме передові технології для покращання обізнаності громадськості з обстановкою в кіберпросторі і посилення колективної стійкості і оборони [25].

Висновки.

Інформаційний тероризм залишається однією із серйозних загроз безпеці та життєво важливим інтересам особи, суспільства і держави. Його інструменти стають більш витонченими і ефективними в кіберпросторі України. Серед основних методів (інструментів) інформаційного тероризму виділяється: дезінформація, пропаганда, маніпулювання, інсайди, матеріали, створені злочинним шляхом, використання кібератак як інструменту спеціальних інформаційних операцій, впливу на виборчі процеси.

Сучасні кібертерористи діють в глобальному масштабі насамперед із метою руйнування об'єктів критичної інфраструктури, поширення хаосу, дезінформації, маніпуляції, залякування населення, деструктивного інформаційно-психологічного впливу на особистість, суспільство і державу. Ефективна протидія інформаційному тероризму вимагає від України здійснення заходів з виявлення, запобігання та припинення актів інформаційно-психологічного та технічного тероризму, усунення умов, що їм сприяють, створення спеціальних підрозділів з повноваженнями ведення протиборства в кіберпросторі України. Все більш ефективною визнається політика НАТО щодо впливу на кіберконфлікт як нову форму політичного протистояння [3]. Тому міжнародна співпраця України з НАТО по лінії забезпечення кібербезпеки є надзвичайно актуальною в сучасних умовах збройної агресії РФ проти нашої країни. Найбільш важливим в даному контексті є приведення діяльності суб'єктів забезпечення кібербезпеки з кіберстримування та кібероборони у відповідність до стандартів НАТО.

При формуванні Плану реалізації Стратегії кібербезпеки України на 2025 рік слід врахувати необхідність розвитку потенціалу кібероборони в частині протидії інформаційному тероризму (в т.ч. – проведення діяльності суб'єктів кібербезпеки України з кіберстримування у відповідність до стандартів НАТО).

Використана література

1. Стратегія кібербезпеки безпеки України: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

2. Державна служба спеціального зв'язку та захисту інформації України. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. – (Новини. 08.02.2024). URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

3. Щодо актуалізації використання кіберпростору як інструменту геополітичного суперництва: аналітична записка Національного інституту стратегічних досліджень. – (28.09.16 р.). URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/schodo-aktualizacii-vikoristannya-kiberprostoru-yak

4. Лабенко Л.В. Інформаційний тероризм: поняття та ознаки. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3439/%D0%9B%D0%B0%D0%B1%D0%B5%D0%BD%D0%BA%D0%BE.pdf?sequence=1&isAllowed=y (дата звернення: 04.02.2021).

5. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* № 1(16)/2016. С. 110-116.

6. Білан І.А. Кібертероризм: інформаційно-правовий аспект. *Інформація і право.* № 4(47)/2023. С. 64-71. URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoy-federatsii/viewer

7. Діордіца І.В. Поняття та зміст кібертероризму. URL: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu

8. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.

9. Петришин Г.Р. Інформаційний тероризм: джерела формування та активізації в Україні. *Габітус*: науковий журнал. 2021. Вип. 21. С. 44-50.

10. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. …канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

11. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навч. посіб. Київ: ВІКНУ, 2016. 286 с.

12. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. № 2(37)/ 2021. С. 72-79.

13. Почепцов Г.Г. Інформаційні війни. Серія: Освітня бібліотека. Видавництво: Рефл-бук, 2001. 576 с.

14. Прокоф'єв Д. Інформаційна війна та інформаційна злочинність. URL: http://www.crime-research.ru/library/Prokop.htm (дата звернення: 08.08.2024).

15. Рижов І.М., Строгий В.І. Концептуальні засади соціально-інформаційних технологій упередження кризових явищ соцілального характеру (на прикладі моніторингу тероризму). *Науковий вісник Львівського державного університету внутрішніх справ*. *Серія юридична*. 2014. № 3. С. 219-228.

16. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право).* 2014. № 2(65). С. 55-60.

17. Герасименко К.С. Сучасні ознаки загроз "інформаційного тероризму". *Форум права*. 2009. № 3. С. 162-166.

18. Інформаційний тероризм. *Центр протидії дезінформації при РНБО України.* URL: https://web.archive.org/web/20220412094834/https://cpd.gov.ua/announcement (дата звернення: 08.08.2024).

19. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15#

20. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

21. Харамурза Д. Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. *Інтегровані комунікації.* 2023. № 2 (16). С. 29-37. URL: https://intcom.kubg.edu.ua/index.php/journal/article/view/272/220 (дата звернення: 08.08.2024).

22. Інформаційний тероризм. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80% (дата звернення: 08.08.2024).

23. Андрусишин Ю.І., Бараннік В.В. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави. *Інформаційна безпека людини, суспільства, держави.* 2021. № 1-3 (31-33). С. 6-12.

24. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами: політико-правовий аспект. *Регіональні студії*. 2022. № 30. С. 62-65.

25. Союзники домовились про новий Інтегрований центр кібероборони НАТО. URL: https://www.nato.int/cps/uk/natohq/news_227647.htm?selectedLocale=uk (дата звернення: 08.08.2024).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~