DOI 10.31558/2519-2949.2018.2.22
УДК 323.28:004:316.647.6

Митко А. М., Кольцова І. І.,
Східноєвропейський національний університет імені Лесі Українки

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ІНСТРУМЕНТ ВПЛИВУ НА ІНФОРМАЦІЙНИЙ КОНФОРМІЗМ В ГЛОБАЛЬНОМУ СЕРЕДОВИЩІ

У статті розглянуто форми, у яких проявляється сучасний інформаційний тероризм. В основному це кібертероризм та медіа-тероризм. Доведено, що ці форми виникають, в першу чергу, через необізнаність населення та небажання аналізувати отриману інформацію від мас-медіа, оточення або органів влади; в другу, через бажання керівництва держави чи конкретної особи контролювати соціальну та політичні поведінку громадян. Водночас зазначено, що протистояння з інформаційним тероризмом та конформізмом стикається з проблемами, серед яких: цифрова нерівність у доступі до інформаційно-комунікаційних засобів різних верств населення; недостатнє правове регулювання; інформаційне відставання країн «третього світу» від розвинених країн; контроль інформаційного простору зі сторони державних установ через цензуру, гейткіпінг; захист інформаційного простору від несанкціонованих втручань та хакерських атак тощо. Світове співтовариство та окремо взяті країни успішно здійснюють заходи по убезпеченню свого інформаційного простору від психологічних (за допомогою «м'якої сили) та кібератак; створюються відповідні структури , проводять спеціалізовані навчання з подолання інформаційних прірв та цифрового розриву – явищ, які характеризують асиметричність у доступі до інформаційних джерел у різних суб'єктів. Цифровий розрив є однією з основних проблем розвитку інформаційного простору та інформаційного суспільства. Наголошено, що подолати інформаційне відставання та цифрову нерівність держава може зробивши нові технології доступнішими для менш забезпечених прошарків суспільства, а також організувати навчання комп'ютерної грамотності, особливо молоді та людей похилого віку.

Ключові слова: *інформація, інформаційний тероризм, інформаційний конформізм, інформаційний простір, вплив, протидія, кібертероризм.*

Постановка проблеми. В сучасних умовах дедалі більшого значення набуває роль інформації. У результаті активних процесів глобалізації та розвитку інформаційно-комунікаційних технологій та як наслідок, змін в соціально-інформаційній сфері, змінюються також інструменти реалізації державної політики, як внутрішньої так і зовнішньої, і поряд з економічними і політичними важелями впливу не менш важливими постають інформаційні. Одним із таких важелів є інформаційний тероризм, що породжує інформаційний конформізм – морально-політичний термін, що означає пасивне, пристосовницьке прийняття готових стандартів у поведінці, безапеляційне визнання існуючого стану речей, законів, норм, правил, безумовне схиляння перед авторитетами, ігнорування унікальності поглядів, інтересів, уподобань естетичних та інших смаків окремих людей і т. д. під впливом масиву отриманої інформації. Україна перебуваючи у стані гібридної війни, сповна відчуває вплив інформаційного тероризму та, як наслідок, отримує інформаційний конформізм, тому вважаємо дослідження цієї теми важливим та актуальним сьогодні.

Мета дослідження – проаналізувати прояви, тенденції та особливості інформаційного тероризму та конформізму. Відповідно до поставленої мети ставимо такі завдання: дослідити трактування інформаційного конформізму та тероризму; здійснити аналіз та охарактеризувати особливостей інформаційного тероризму.

Аналіз останніх досліджень і публікацій з проблеми. В епоху інформатизації традиційні конфлікти перемістилися із матеріального простору в принципово новий – інформаційний, де маніпулятивні технології набувають дедалі ширшого використання. Завдяки їм ведуться інформаційні війни, знищуються опоненти, здійснюється вплив на маси і багато інших дій. Тому, останнім часом великої популярності набув інформаційний тероризм, як метод «м'якої сили». Осмислення цього феномену є передумовою формування більш чітких уявлень щодо сутності сучасного міжнародного тероризму, запобігання деструктивного впливу на державні інститути і

основи національної безпеки загалом. Коли фіксується наявність конфлікту між думкою індивіда і думкою групи та подолання цього конфлікту на користь групи з'являється явище конформності – схильність індивіда піддаватися думці групової більшості, реальному чи уявному тискові групи [1] «Конформна поведінка», вказуючи на психологічну характеристику позиції індивіда відносно позиції групи, приймає або не приймає визнані групою певні стандарти думки, норми, властивості, цінності [2]. Пристосування до думки інших та вплив інформаційного поля на прийняття рішення громадянином в державі залежить від ступеня його конформізму.

У загальному трактуванні конформізм найчастіше вивчається психологами та означає відсутність власної позиції домінантності, безпринципна і некритична покора певній моделі, що володіє найбільшою силою тиску (думка більшості, визнаний авторитет, традиція). Р. Мертон виділив конформізм як один із основних видів девіантної поведінки. У. Еко розглядав конформізм як прояв «нездатності середньої людини звільнитися від формальних систем, що нав'язані їй ззовні, а не набуті завдяки власному дослідженню реальності, результат пасивного засвоєння тих норм розуміння і судження, які ототожнюються з «хорошою формою» як в моралі, так і в політиці, як в дієтиці, так і в моді – на рівні естетичних смаків і педагогічних принципів» [3]. У психологічних дослідженнях, за допомогою експериментів С. Аша і С. Мілрама, Р. Кратчфілда, М. Шеріфа вивчалося, в якій мірі людина може бути конформною. Також, зазначали, що основною причиною конформної поведінки є інформаційний та нормативний впливи (Е. Аронсон, Х. Джерард, М. Дойч, Ф. Зімбардо, С. Московічі, та ін).

У соціально-політичному трактуванні груповий тиск отримав назву феномен інформаційного конформізму та досліджується як підпорядкування людини соціальній групі у результаті пристосування до інформаційного простору, пасивне прийняття існуючого порядку речей, пануючої думки та ін. [4]. За таким тлумаченням, конформізм охоплює різні явища і проявляються у відсутності у людини власних поглядів, слабкості в характері, у згоді індивіда у поглядах, нормах, цінностях людей, які її оточують. Також проявляється у результаті тиску групових норм сприйняття інформації на індивіда, який у наслідок цього тиску починає діяти, думати, відчувати так само, як й інші члени групи, сприймати відомості «під кутом зору» оточення [5]. І тому поняття «конформізм» набуває негативного відтінку. Дана тема є мало дослідженою в політичній сфері, більше досліджень маємо в психологічній та соціальній галузях, але заперечувати вражаючий вплив інформації на сучасний політичний процес, прийняття рішень в політичній системі, ми не можемо.

Виклад основного матеріалу дослідження. Причинами сучасного конформізму можемо визначити такі: нормативний та інформаційний впливи. Людина може підкорятися групі, щоб бути прийнятим нею і не бути зневаженою або одержати важливу інформацію. Ці причини називаються відповідно нормативним впливом та інформаційним впливом.

Нормативний вплив – це соціальний вплив, який породжує конформізм, що ґрунтується на бажанні задовільнити очікування інших, аби досягти їхнього визнання. Нормативний вплив є «відповідальним» за те, що людина вважає за краще «йти в ногу з натовпом», щоб не бути знехтуваним нею. Часто висока ціна, яку доводиться платити за відступництво, примушує людей підтримувати те, у що вони не вірять, або, принаймні, приховувати свою незгоду. Інформаційний вплив породжує конформізм схвалення, заґрунтований на небажанні чи неспроможності мати власну точку зору. Коли реальність неоднозначна, то посилюється дія інформаційного впливу. Оточуючі люди стають цінним джерелом інформації. Коли особа почувається некомпетентною посилюється інформаційний вплив різних джерел [6]. Тому особа стає найбільш вразливою та піддається впливам інформаційних потоків.

Отже, існує дві основні причини конформізму: люди хочуть подобатися оточенню і отримати схвалення, а також тому, що вони прагнуть чинити вірно. Джерелом нормативного впливу є турбота про імідж. Інформаційний вплив виникає як наслідок думок, суджень інших людей про реальний світ. Бажання людини мати знання, що відображають реальність, обумовлює інформаційний вплив на цю людину. У повсякденному житті нормативний та інформаційний вплив нерідко виявляються разом.

В експериментах, метою яких є дослідити, коли люди стають конформістами, нормативний та інформаційний впливи розмежовані. Конформність вище тоді, коли досліджувані відповідають у присутності групи; у цьому, звичайно, виявляється нормативний вплив. Доведено що численнішою є група, тим більше відповідь дана наодинці відрізняється від публічної.

Існує такі види інформаційного тероризму: медіа-тероризм, кібертероризм. Під впливом медіа-тероризму індивід не здатен самостійно орієнтуватися в необмеженому інформаційному просторі, тому що мас-медіа представлені сьогодні у вигляді інструментів для конструювання недостовірної реальності. Завданням цієї реальності є не відображати істину та приховувати її здійснюючи там самим «м'яку силу», яка прагне підкорити людину невластивим їй судженням. Таким чином, сьогодні не можна говорити про перехід кількості інформації в її якість. Особливо це стосується ЗМІ та ЗМК, так як вони виступають майданчиком для політичних ігор, які на меті викривити реальний стан речей.

Наступним видом інформаційного тероризму є кібертероризм, під яким розуміють сукупність дій, що включають інформаційну атаку на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупуваннями або окремими особами. Кібертероризм спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та здійснення інших деструктивних дій. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж (терористичні акції можуть здійснюватися з будь-якої точки світу) та в проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність через декілька підставних комп'ютерів, що ускладнює його ідентифікацію та визначення місцезнаходження [7]. Зброя кібертерористів постійно вдосконалюється залежно від засобів захисту, застосовуваних користувачами комп'ютерних мереж. Таким чином, на сьогодні кібертероризм є одним з найнебезпечніших видів злочинності. Кібератаки можуть спричинити величезну шкоду на локальному, державному та навіть міжнародному рівні. Адже, зовнішні кібератаки можуть переслідувати і більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібертероризму можуть бути грошова і секретна інформація, апаратура контролю над космічними приладами, ядерними електростанціями, воєнними комплексами головні комп'ютерні вузли тощо.

Слід зауважити, що у зв'язку з глобалізацією інформаційного тероризму та його інтернаціональним характером постала об'єктивна необхідність правовому регулюванні цього явища на міжнародному рівні і тому заходи боротьби з інформаційним тероризмом повинні ґрунтуватися на єдиних законах, вироблених міжнародним співтовариством. Немає необхідності говорити, що політика «подвійних стандартів», коли оцінка тих чи інших дій інформаційного характеру часто залежить від політичних симпатій, релігійних переконань чи національної приналежності, не сприяє знищенню однією з глобальних проблем людства. Тому інформаційному тероризму необхідно протиставити об'єднану силу всього світового співтовариства, оскільки це явище загрожує безпеці всіх держав світу [8].

Згідно з Конвенцію Ради Європи із кіберзлочинів (2001), засобами кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги ІКТ та дані трафіку[9]. На сьогодні існують дві великі організації, які готові взяти на себе провідну роль у боротьбі з інформаційним тероризмом на міжнародному рівні. Це Підрозділ по боротьбі з тероризмом ОБСЄ – організації, що діє під егідою ООН, а також Інтерпол та Центр по боротьбі з кіберзлочинністю у Європейському Союзі. Країни-члени ЄС і європейські інституції підтримувати спільна заходи та розслідування для створення оперативних і аналітичних можливостей її розслідування і для співпраці з міжнародними партнерами [10].

Аналізувавши зростаючи обсяги проведення акцій з інформаційного тероризму та їхній вплив на суспільство через інформаційний конформізм, можемо зазначити, що перед кожною державою, зокрема й Україною, постає об'єктивна необхідність здійснення ефективних заходів з метою протидії інформаційному тероризму та конформізму.

Для успішного протистояння загрозам слід виокремити ряд основних напрямів такої боротьби [11]:

– уніфікація та гармонізація національного законодавства та міжнародних актів;

– проведення наукових розробок в області створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

– створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом;

– удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

– удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.

Варто взяти до уваги, що інформаційно-комунікаційні можливості, які отримує політична система в результаті використання ІКТ, спонукають її до бажання контролювати інформаційний простір, Інтернет-трафік громадян, корегувати інфопростір за допомогою гейткіпінгу та спіндокторингу. У світі склалася досить велика практика застосування заходів із контролю за інформаційними потоками в медіа-середовищі й у мережі Інтернет зокрема. Застосування маніпулятивних технологій спонукає до вирішення такої важливої проблеми, як необхідність інформаційної безпеки та захисту інформаційного простору від втручання іноземних держав в інфопростір і спотворення інформації [12].

Необхідною є розробка загальнодержавної системи інформаційної протидії тероризму шляхом чіткого визначення функцій та повноважень державних органів, громадських організацій, засобів масової інформації в комплексі заходів щодо інформаційної блокади будь-яких дій терористів. Не менш важливим видається формування за допомогою мас-медіа комплексу науково-просвітницьких програм, покликаних сприяти ідеології ненасильства, толерантної поведінки, формуванню "антитерористичної свідомості" в суспільстві, повазі культурного розмаїття. Міжкультурний діалог, що має реалізовуватися за допомогою мас-медіа, може допомогти уникнути виникнення різних видів екстремізму, насильства, ксенофобії, релігійної нетерпимості в державі [13].

Подолання «цифрових розривів», які утворюються через те, що певні частини населення мають значно ширші можливості отримати вигоду з економіки, ніж інші верстви населення, також є одним з першочергових завдань у питання протистояння інформаційному конформізму. Цифровий розрив вимірюють відповідно до умовної шкали, що складається з п'яти характеристик: фізичний доступ (наявність реальної можливості використовувати інфраструктуру, програмне забезпечення та обладнання); фінансовий доступ (наявність економічних можливостей для регулярної оплати інформаційних послуг); когнітивний доступ (здатність здійснити пошук, отримати необхідну інформацію, обробити її та застосувати); доступ до значущості інформації (можливість знайти та використати корисні дані, якщо володієш необхідними мовами); політичний доступ (можливість населення впливати на політичний процес і розподіл суспільних благ).

Набуваючи особливої ваги, інформація й знання стають найважливішим ресурсом і капіталом розвитку країни, визначають прогрес у високотехнологічних сегментах різних сфер життєдіяльності суспільств, а доступ до них – один із основних чинників політичного та соціально-економічного розвитку. Уряди країн проводить цілеспрямовану політику з підвищення комп'ютерної грамотності, створення центрів навчання й поліпшення умов для зростання кваліфікації персоналу в галузі ІТ. Можливість використання інформаційних мереж і систем створює для всіх громадян принципову можливість безпосередньої участі в політичному волевиявленні та забезпеченні прав і свобод. Це велика перевага інформаційного століття. Залучення інститутів громадянського суспільства, окремих людей, населення, професійних груп і самоорганізованих мережевих спільнот, що реалізують свої функції завдяки розвитку інтерактивної взаємодії через різні соціальні, урядові й бізнес-мережі в процес прийняття найважливіших політичних і соціально-економічних рішень, управління суспільно-політичними процесами зумовлюють істотні зміни в демократичному

процесі, який із традиційного трансформується в інформаційну демократію.

Висновки. Проблема протидії актам інформаційного тероризму – це комплексна проблема. Інформаційний тероризм активно розвивається та поширюється, становлячи загрозу практично всій світовій спільноті. Внаслідок стрімкого розвитку ІКТ він набуває нових форм, внаслідок чого дослідження цього явища є недостатнім і таким чином, властивості сучасного інформаційного тероризму являються предметом пильної наукової уваги дослідників цього психологічного, соціологічного та політичного явища. Інформаційний тероризм як сучасне явище становить серйозну загрозу безпеці та життєво важливим інтересам як особистості, так суспільства і держави, отримую нові форми завдяки незнання та небажання аналізувати інформацію, тобто конформізм у вигляді пристосування до чужої зручної думки.

Бібліографічний список:

1. Парыгин Б. Д. Социальная психология / Б. Д. Парыгин. – СПб, 1999. – 592 с.
2. Зимбардо Ф. Социальное влияние / Ф. Зимбардо, М. Ляйппе. – Питер, 2000. – 448 с.
3. Эко У. Открытое произведение. – Санкт-Петербург: Академический проект, 2004. – с.169-170.
4. Платонов Ю. П. Психология коллективной деятельности. Теоретико-методологический аспект / Ю. П. Платонов. – Л.: Изд-во ЛГУ, 1990. – 184 с.
5. Кон И.С. В поисках себя. Личность и ее самосознание / И.С. Кон. – М.: «Политиздат», 1984. – 151 с.
6. Куса І. Інформаційний аспект тероризму та переговорний процес із терористами [Електронний ресурс] / І. Куса. – Режим доступу: http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniy-protses-iz-teroristami/.
7. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): друга міжнар. наук.-практ. конф. (25-28 травня 2009 р.). – К.: НАУ, 2009. – С. 230-232.
8. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс]. – Режим доступу: www.nbuv.gov.ua/Portal/soc_gum/bozk/2007/17text/g17_30.htm.
9. Конвенція про кіберзлочинність : за станом на 7 вересня 2009 р [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575
10. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс]. – Режим доступу: www.nbuv.gov.ua/Portal/soc_gum/bozk/2007/17text/g17_30.htm.
11. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 20.
12. Митко А. М. Інформаційна демократія: реалії та виклики часу : [монографія]. – Луцьк : Вежа-Друк, 2014. – 400 с.
13. Свентицька О.В. Інформаційний тероризм як феномен сучасної міжнародної політики: автореф. дис… канд. політ. наук: 23.00.03 / Свентицька О.В. – К., 2007. – 19 с.

Mytko A. M., Koltsova I. I. Information terrorism as instrument of influence on the information conversion in the global environment

The article examines the forms in which modern information terrorism manifests itself, and is basically cyberterrorism and media-terrorism. It is proved that these forms arise, first of all, due to lack of knowledge of the population and the reluctance to analyze the information received from the media, the environment or authorities; in the second, because of the desire of the leadership of the state or a specific person to control the social and political behavior of citizens. At the same time, it is noted that the confrontation with information terrorism and conformism faces problems, including: digital inequality in access to information and communication facilities of different sections of the population; insufficient legal regulation; information gap of the Third World countries from developed countries; control of information space on the part of state institutions through censorship, gatekeeping; protection of information space from unauthorized interference and hacker attacks, etc. The world community and individual countries are successfully taking steps to protect their information space from psychological (through soft power) and cyber-attacks; appropriate structures are being created, specialized training is provided to overcome informational abysses and digital divide – phenomena that characterize asymmetry in access to information sources in different subjects. The digital divide is one of the main problems of the development of information space and information society. It is stressed that the state can overcome the information gap and digital inequality, making new technologies more accessible to less well-off sections of society, and organize computer literacy training, especially for young people and the elderly.

Key words: *information, information terrorism, informational conformism, information space, influence, counteraction, cyberterrorism.*