

Сергій Олександрович ПШЕНИЧНИЙ

Здобувач вищої освіти третього науково-освітнього рівня (доктора філософії) за спеціальністю 052 Політологія, Харківський національний педагогічний університет імені Г.С.Сковороди, вул. Алчевських, 29, м. Харків, 61002, Україна

E-mail: sergiy.pshenychniy@gmail.com, ORCID: <http://orcid.org/0009-0008-8183-8273>

УДК 323.28 +32.019.51

Serhiy PSHENYCHNYI

PhD student in Political Science, G.S.Skovoroda Kharkiv National Pedagogical University, Alchevskikh st., 29, Kharkiv, 61002, Ukraine

**ПРОБЛЕМНЕ ПОЛЕ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ
У ВІТЧИЗНЯНОМУ СОЦІАЛЬНО-ПОЛІТИЧНОМУ ДИСКУРСІ: ДО ВИЗНАЧЕННЯ
СТРАТЕГІЇ ДОСЛІДЖЕННЯ**

Received 11 June 2024; revised 27 June 2024; accepted 28 June 2024

DOI: 10.15421/342432

Анотація

Акцентується увага на визначенні проблемного поля нового виду сучасної терористичної діяльності у інформаційному просторі за умов глобалізації – інформаційного тероризму.

Пропонується систематизувати наробки, які презентовані у вітчизняному соціально-політичному дискурсі та можуть виступати засадами для його подальшого комплексного дослідження у напрямі побудови його відповідної моделі / концепції.

Застосовується дослідницька стратегія відомого американського методолога Л.Козера щодо аналізу елементів соціальної реальності – пошук сукупності взаємопов'язаних між собою показників (змінних), які здатні уточнити зміст, умови виникнення та розвитку цього предмета дослідження.

Обґрунтовується, що при побудові проблемного поля аналізу інформаційного тероризму як елемента соціальної реальності в якості таких показників можуть бути:

по-перше, інтерпретація самого поняття «інформаційний тероризм»;

по-друге, аналіз причин виникнення та умов поширення терористичної діяльності в інформаційному просторі;

по-третє, класифікація основних форм прояву інформаційного тероризму;

по-четверте, аналіз основних технологій та методів здійснення терористичної діяльності інформаційного характеру;

по-п'яте, обґрунтування умов та розробка механізмів, що протидіють широкому поширенню інформаційного тероризму у сучасному світі.

Доводиться, що аналіз сутності інформаційного тероризму з позиції конструювання аналітичної (п'яти ланкової) схеми дослідження проблемного поля цього виду терористичної діяльності дає підставу для узагальнення й тлумачення цієї нової форми тероризму як використання інформації та інформаційної інфраструктури певними (державами, організаціями, структурами), з одного боку, задля насильства над свідомістю людей, маніпулювання їх поведінкою за допомогою певних методів і способів впливу, а з іншого – для впливу на інформаційно-технічну структуру держави, з метою здійснення тиску на прийняття вигідних для них рішень з боку держав, груп людей або окремих осіб шляхом створення умов для хаосу, панічних настроїв тощо

Ключові слова: *аналітична схема, модель, глобалізація, інформаційна війна, безпека.*

**THE PROBLEM FIELD OF INFORMATION TERRORISM
IN THE DOMESTIC SOCIAL AND-POLITICAL DISCOURSE: TO DETERMINE A
RESEARCH STRATEGY**

Abstract

The article concerns the definition of the problem field of a new type of modern terrorist activity in the information space under the conditions of globalization - information terrorism.

The findings systematized, which are presented in the domestic social and political discourse and can serve as the basis for its further comprehensive research in the direction of building its corresponding model / concept. The research strategy of the well-known American methodologist L. Coser used for the analysis of elements of social reality - the search for a set of interrelated indicators (variables) that can clarify the content, conditions for the emergence and development of this research subject.

It substantiated that when constructing the problem field of the analysis of information terrorism as an element of social reality, such indicators can be: first, the interpretation of the very concept of «information terrorism»; secondly, the analysis of the causes and conditions of the spread of terrorist activity in the information space; thirdly, the classification of the main forms of manifestation of information terrorism; fourth, the analysis of the main technologies and methods of carrying out terrorist activities of an informational nature; fifth, substantiation of conditions and development of mechanisms against the wide spread of information terrorism in the modern world.

The analysis of the essence of information terrorism from the standpoint of constructing an analytical (five-link) scheme for researching the problematic field of this type of terrorist activity provides a basis for generalizing and interpreting this new form of terrorism as the use of information and information infrastructure by certain (states, organizations, structures), on the one hand, for violence against people's consciousness, manipulation of their behavior using certain methods and methods of influence, and on the other hand – to influence the information and technical structure of the state, with the aim of exerting pressure on the adoption of favorable decisions by states, groups of people or individuals by creating conditions for chaos, panic, etc.

Keywords: analytical scheme, model, globalization, information war, security.

Постановка проблеми.

Тероризм у XXI столітті набув нових масштабів, нових видів та форм, став багатоплановим явищем, де політичні перспективи стають ризиковими, невизначеними, драматичними та трагічними як на регіональному, так і на глобальному рівнях.

Еволюція сучасного тероризму призводить до нагальної потреби у фіксації його змін та трактування його нових характеристик, рис та форм. Гібридні війни у сучасному світі продемонстрували розширення меж, можливостей і кордонів терору, де тероризм вже набуває нових форм своєї організації, стратегій та формату здійснення.

На Міжамериканській конференції з прав людини (1970р.), присвяченій питанням розгляду нових загроз свободам та правам громадян світу й розробці відповідних форм їх захисту, було виокремлено три види терористичної діяльності: соціальну, ідеологічну та політичну [Богданов 2005: 35].

Теоретичні напрацювання щодо сучасної класифікації тероризму дозволяють виділити окрім вище зазначених видів терористичної діяльності – технологічний, антидержавний, суїцидальний види тероризму.

Провідні західні дослідники традиційно виокремлюють такі види терористичної діяль-

ності: революційний, субреволюційний і репресивний тероризм (П.Вілкінсон, Р.Шульц); ядерний, технологічний, економічний, екологічний тероризм; психічний і злочинний тероризм (Дж.Белл) та ін. [Шкурат 2020: 39].

Останнім часом вітчизняні та зарубіжні дослідники стали виокремлювати нові види сучасного тероризму – хімічний, біологічний, космічний, високотехнологічний та кібертероризм (електронний, комп'ютерний тероризм).

Разом з цими видами терористичної діяльності все частіше дослідники, що спеціалізуються на вивченні проблемного поля тероризму, пропонують розглядати як один із його провідних окремих самостійних варіантів – інформаційний.

При цьому зазначаючи, що цей вид тероризму за сучасних умов становлення і розвитку інформаційного суспільства постійно супроводжує й інші види здійснення терористичної діяльності.

Саме з цих позицій (як провідний засіб здійснення інформаційної війни) інформаційний тероризм досліджується у працях Б.Хофмана, У.Лакера, Е.Тоффлера, Ж.Бодрійара, П.Вілкінсона, Р.Шафферта, Ф.Перла та ін.

Названі дослідники здійснили значні наукові розвідки цього виду терористичної діяльності у контексті розгляду (як інформаційного

складника) переважно політичного тероризму.

Вітчизняні терорологи мають значні результати, насамперед: у формуванні категоріально-понятійного апарату дослідження цього феномену (В.Антипенко, О.Жайворонко, О.Петрюк, П.Петрюк, О.Українська); у розробці кримінально-правового аспекту та норм відповідальності за сприяння та участь у інформаційному тероризмі (В.Недільниченко, М.Ситенко, Т.Коц); у дослідженні методологічних проблем протидії інформаційному тероризму (В.Ященко, А.Сальникова).

У цілому, треба зауважити на відсутність комплексного підходу щодо аналізу інформаційного тероризму в умовах гібридної війни – терорологи різних наукових шкіл висловлюють розбіжності щодо змісту, ознак, видів, та форм цього варіанту терористичної діяльності

Доцільно стверджувати тільки, що всі представники наукового співтовариства погоджуються з положенням – інформаційний тероризм є результатом терористичної діяльності за умов глобалізації, що певним чином корелює з досягнутим рівнем розвитку інформаційних технологій.

Відтак, **метою статті** є спроба визначити та систематизувати провідні моменти проблемного поля інформаційного тероризму, які презентовані у вітчизняному соціально-політичному дискурсі та можуть виступати засадами для його подальшого комплексного дослідження у напрямі побудови його відповідної моделі / концепції.

Виклад основного матеріалу.

Аналіз відповідних публікацій дозволяє стверджувати, що для досягнення зазначеної мети доцільно буде звернутися до аналітичної схеми аналізу соціальних явищ, запропонованих американським дослідником Л.Козером.

Основна ідея цієї дослідницької стратегії – знайти групу взаємопов'язаних між собою показників (змінних), які здатні уточнити зміст, умови виникнення та розвитку цього шуканого елемента соціальної реальності.

Так, наприклад, природу та генезис конфлікту як елемента соціальної реальності дослідник пропонує аналізувати через п'ять послідовно взаємопов'язаних моментів – по-перше, інтерпретацію самого поняття «со-

ціальний конфлікт»; по-друге, аналіз причин виникнення соціального конфлікту; по-третє, класифікацію основних форм прояву конфлікту; по-четверте, аналіз основних показників розвитку конфлікту: інтенсивність; гострота; тривалість; ступінь нормативного регулювання; по-п'яте, обґрунтування умов, за яких проявляються та домінують негативні чи позитивні функції соціального конфлікту [Coser 1967].

При побудові проблемного поля інформаційного тероризму як елемента соціальної реальності в якості таких показників (що впливає з представлених у сучасному соціально-політичному дискурсі результатів досліджень цього терористичного виду діяльності) можуть бути:

по-перше, інтерпретація самого поняття «інформаційний тероризм»;

по-друге, аналіз причин виникнення та умов поширення терористичної діяльності в інформаційному просторі;

по-третє, класифікація основних форм прояву інформаційного тероризму;

по-четверте, аналіз основних технологій та методів здійснення терористичної діяльності інформаційного характеру;

по-п'яте, обґрунтування умов та розробка механізмів, що протидіють широкому поширенню інформаційного тероризму у сучасному світі.

У контексті розгляду представлених у сучасному соціально-політичному дискурсі результатів досліджень цього терористичного виду діяльності вище зазначені ланки (відповідно) мають такий зміст.

1. У вітчизняному соціально-політичному дискурсі (як і зарубіжному науковому співтоваристві) фіксується відсутність загальноприйнятого визначення поняття інформаційного тероризму.

Найчастіше під цим видом терористичної діяльності пропонується розуміти або «прямий вплив на психіку та свідомість людей з метою формування потрібних думок та суджень, які певним чином спрямовують поведінку людей» [Петрюк П., Петрюк А. 2007: 151-154], або «використання різних форм і методів тимчасового чи безповоротного виведення з ладу

інформаційної структури держави або її елементів, а також цілеспрямоване використання цієї інфраструктури для створення умов, що тягнуть за собою катастрофічні наслідки для різних сторін життєдіяльності суспільства та держави» [Марков, Фролова 2019: 109-115].

Б.Леонов та С.Ляхова при узагальненні результатів досліджень, присвячених вивченню різних аспектів інформаційного тероризму в контексті міждисциплінарного підходу, прийшли до висновку, що інформаційний тероризм є базовий концепт теорії інформаційної безпеки, що розглядається як:

– суспільне небезпечне явище, що існує та спостерігається у форматі терористичної діяльності;

– певний вид деструктивного інформаційно-психологічного впливу на особистість, соціальні групи, суспільство;

– деструктивні дії інформаційного характеру, спрямовані на соціальні групи та структури, державні органи влади і управління, пов'язані із поширенням інформації, що містить погрози життю та правам громадян, а також факти й дані, які є викривленням об'єктивної ситуації;

– деструктивний вплив на свідомість та психічний стан людини із застосуванням провідних методів насильницької пропаганди;

– новий вид терористичної діяльності, спрямований на незворотне чи тимчасове порушення функціонування інформаційної інфраструктури держави або її елементів із активним застосуванням різних форм і методів інформаційно-технологічної боротьби;

– сукупність інформаційних спецоперацій, що організовані та підтримуються представниками національних (транснаціональних) кримінальних структур та певних спецслужб окремих іноземних держав;

– поєднання фізичного насильства зі злочинним застосуванням інформаційних систем, цілеспрямоване зловживання цифровими інформаційними структурами та мережами (їх окремими компонентами) з метою сприяння та підтримки здійснення як окремих терористичних акцій, так й масштабних терористичних операцій;

– ідеологічно обґрунтована інформацій-

но-технологічна практику впливу, що спрямований на дезорієнтацію та залякування населення [Леонов, Ляхова 2021: 172].

Таку ситуацію з відсутністю загальноприйнятого визначення інформаційного тероризму у науковому співтоваристві найчастіше пояснюють відсутністю єдиного загальнови-знаного визначення терористичної діяльності загалом.

Термін «тероризм» у соціально-політичному дискурсі постійно набуває нових визначень, ознак, детермінанти тероризму постійно змінюють свої причини, фактори та умови.

Часто термін «тероризм» вживається для характеристики негативних дій, що спричиняють загрозу для життя людей. Останнім часом тероризм стає потужним методом політичного впливу, що використовується для досягнення своїх цілей. Поняття тероризму має дихотомічний характер, з одного боку терористична діяльність є порушенням закону або кримінальним злочином, а з іншого – може являти собою боротьбу за високі ідеали, за національне визволення. Поняття «тероризм» може бути характеристикою дій уряду або діяльності політично вмотивованих груп недержавного рівня.

О.Жайворонок, аналізуючи відсутність загальноприйнятого визначення інформаційного тероризму у політичній науці, поси-лається на висновки В.Антипенко та вважає, що через наявність багатьох доктринальних понять тероризму та відсутністю загальнови-знаного конвенційного визначення тероризму, необхідно звертатись до першоджерел та умов його виникнення як соціально-політичного феномену, аналізувати його в контексті інтерпретації не як низки поодиноких дій, а як певного системного процесу, що існує та поширюється в географічному й соціальному просторах та часі і взаємопов'язаний із геополітичними, гео економічними та соціально-економічними чинниками, які детермінують його генезу та динаміку [Жайворонок 2019: 220].

2. Слід наголосити, що причини виникнення інформаційного тероризму у сучасному світі ще не стали самостійним предметом вивчення вітчизняних дослідників.

Але, виходячи з його визначення як нового різновиду терористичної діяльності в інформаційному просторі, можна обґрунтовано припустити, що вони тотожні до причин виникнення та розвитку тероризму в цілому.

Серед останніх у сучасному соціально-політичному дискурсі розглядаються, насамперед, загострення протиріч у політичній, економічній, соціальній, ідеологічній та правовій сферах життєдіяльності сучасного суспільства та прагнення окремих як індивідуальних, так і групових суб'єктів політичного процесу досягти певних політичних цілей за умов активного використання терористичних стратегій та методів.

При цьому наголошується, що саме розвитку та становленню інформаційного тероризму сприяє безліч факторів, але головними є процес глобалізації та пов'язаний із ним процес формування глобальної мережі технічних та цифрових сегментів, процедур та технологій.

Також важливу роль у становленні інформаційного тероризму, на думку Ю.Марченка, грає поширення демократичних принципів свобод (свободи пересування, свободи слова та інформації та ін.) та симбіоз глобалізації та локалізації, що сприяє використанню глобальних мереж у досягненні локальних цілей [Марченко 2003: 64].

Цей новий вид тероризму реалізується в інформаційному просторі, що є сукупністю інформації, відповідної інфраструктури, акторів, які функціонують щодо її збору, обробки, розповсюдження, застосування й використання, а також суспільних відносин, що формуються та існують за таких умов.

Інформаційний простір має суттєві особливості, які кардинально відрізняють його від інших сфер життєдіяльності суспільства: невичерпність та заповнюваність інформаційних ресурсів; можливість їх миттєвого тиражування; переміщення великих обсягів цих ресурсів з мінімальними витратами, з високою швидкістю та на великі відстані; компактність джерел та носіїв будь якої за обсягом інформації та ін. [Украинская 2008].

3. Дослідники проблемного поля інформаційного тероризму пропонують виділяти в

ньому два види:

– «психологічний» / «інформаційно-психологічний» (пропаганда тероризму, створення атмосфери страху та паніки в суспільстві тощо);

– «технічний» / інформаційно-технологічний (контролювання чи блокування різних каналів передачі масової інформації, порушення стабільного функціонування об'єктів та провідних елементів інфраструктури та ін.).

Крім того, як свідчить ціла низка публікацій, їх автори пропонують розглядати, як інформаційну терористичну діяльність, такі види тероризму – «кібертероризм», «комп'ютерний тероризм», «електронний тероризм», «тероризм у прямому ефірі» тощо.

4. У сучасній соціально-політичній літературі, присвяченій вивченню терористичної діяльності в інформаційній сфері як технології та методи негативного впливу на її окремі елементи та структуру в цілому розглядаються:

– заміщення даних та викривлення інформаційного змісту сайтів;

– пошкодження, руйнування або зниження рівня ефективності функціонування структурних елементів інформаційно-телекомунікаційних систем (завдяки застосуванню спеціальних технологічно-програмних процедур та методів на засадах програмного коду);

– різні форми так званої «віртуальної блокади» (блокування каналів поширення інформації на різних (або всіх) рівнях їх функціонування);

– так звані «семантичні атаки» (злам та фальсифікація сайтів) [Петришин 2021: 49].

Інформаційний тероризм в умовах інформаційної війни (яка відбувається, зокрема, зараз на теренах України) змінює свої контексти та підходи. Крім того, глобалізаційні зміни сприяють поширенню застосування саме нових інформаційно-комунікаційних технологій.

Інформаційний тероризм за таких умов характеризується:

– дезінформаційними кампаніями на різних рівнях поширення інформації;

– розповсюдженням фейків та діпфейків

по всіх сегментах інформаційного простору;

- розробкою та впровадженням в інформаційні системи відповідних вірусів;
- активним та масштабним застосуванням маніпулятивних психологічних технологій;
- посиленням за допомогою медіа комунікацій психологічного впливу та тиску на свідомість і поведінку особистості;
- трансляцією із активним застосуванням продуктів масової культури (фільмів, серіалів, музики, літератури, живопису тощо) відповідних наративів опонентів (супротивників);
- використанням інформаційно-технологічного інструментарію сучасного варіанту пропаганди [Харамурза 2023: 35].

Окрім використання офіційних засобів масової інформації, інформаційний тероризм продовжує активно застосовувати цілеспрямоване поширення певного типу чуток, які багаторазово посилюють атмосферу напруженості у суспільстві. Виділяють два види найбільш значущих варіантів чуток: так звані «чутки-лякало» та «агресивні чутки» [Петрюк П., Петрюк А. 2007: 151-154].

«Чутки-лякало» – це чутки, що містять і викликають виражені негативні настрої та емоційні стани, які віддзеркалюють певні актуальні, але разом з тим небажані очікування в аудиторії, в якій вони з'являються і розповсюджуються. Традиційно чутки такого виду з'являються або відверто «запускаються» силами, що розв'язують інформаційний терор, у масову свідомість у періоди соціальної кризи, соціально-політичної напруги (терористичні акти, стихійні лиха, війна, організація та здійснення військового перевороту, у ситуаціях складних соціальних та політичних реформ, зміни влади, режиму чи соціально-політичної системи в цілому і т. ін.) [Петрюк П., Петрюк А. 2007: 151-154].

«Агресивні чутки» – чутки, які не просто викликають негативні настрої та стани, що відбивають небажані очікування аудиторії, а що саме направлені на стимулювання агресивного емоційного стану та поведінкової «відповіді», жорсткого агресивного впливу. Чутки такого виду з'являються за умов розвитку гострих протиріч, пов'язаних із існуванням певних міжгрупових, міжетнічних, міжнаціо-

нальних проблем (релігійних, територіальних та ін.) [Петрюк П., Петрюк А. 2007: 151-154].

При цьому слід зауважити, що технології та методи негативного впливу на окремі елементи інфраструктури та на неї в цілому раціонально розглядати в контексті аналізу принципів функціонування інформаційного тероризму, які виокремлюються вітчизняними дослідниками:

- принципу пріоритетності (домінування у засобах масової інформації повідомлень та матеріалів, які для життєдіяльності суспільства є визначальними, найбільш значущими (загроза миру та безпеці громадян, тероризм, екологічні та інші катастрофи тощо));

- принцип неординарності фактів (домінування при наданні інформації по всіх каналах фактів про екстремальні події (війни, катастрофи, надзвичайно жорстокі злочини тощо) над фактами, що висвітлюють явища буденного, повсякденного життя суспільства);

- принцип новизни фактів (акцент на поширенні фактів, що ще не отримали широкої популярності в інформаційному просторі (найновітніші дані про результати виборчих кампаній, про темпи розвитку економіки, про досягнення в науці та техніці тощо));

- принцип успіху (домінування повідомлень про успіхи політичних лідерів, партій чи цілих держав);

- принцип високого суспільного статусу (прагнення подавати повідомлення та матеріали від імені осіб, які займають найвищі місця у політичній, військовій, церковній чи інших ієрархіях суспільства, та через найвідоміші та найвпливовіші джерела інформації).

При цьому часто для позначення процесу негативної дії на сучасний інформаційний простір у контексті здійснення політичної боротьби окремими дослідниками активно використовується поняття «інформаційна зброя».

Інформаційна зброя визначається цілою низкою вітчизняних дослідників (зокрема, В.Головченко, В.Гондюл, О.Зернецька та ін.) «як комплекс заходів, методів та технологій, спрямованих на встановлення контролю над інформаційними структурами потенційного супротивника, втручання у роботу його систем управління з метою знищення або моди-

фікації даних, дезінформації, поширення інформації спеціального призначення, а також, як сукупність засобів впливу на свідомість та психологічний стан політичних та військових структур, спецслужб та населення» [Головченко, Гондюл, Зернецька 2006: 14].

О.Українська стверджує, що «у змістовному плані інформаційна зброя – це спеціально підібрана інформація, під впливом якої відбуваються зміни інформаційно-комунікативних процесів у різних інформаційних системах (фізичних, біологічних, соціальних та ін.) відповідно до задуму суб'єктів його застосування, якими можуть виступати: держава; її спеціальні служби; міжнародні або національні терористичні центри та організації; політичні течії та партії екстремістського штибу; групи громадян і навіть окремі особи, які прагнуть досягти своїх цілей із застосуванням методів терору» [Українская 2008].

Крім того, дослідником уточняється, що «з точки зору мети використання та об'єкта впливу, інформаційну зброю можна розглядати як:

а) набір технічних засобів, які використовуються впливу на інформаційно-технічну інфраструктуру;

б) сукупність засобів на психіку і свідомість людей» [Українская 2008].

5. Під час розробки цієї ланки в аналітичній схемі дослідження проблемного поля інформаційного тероризму необхідно враховувати два моменти.

По-перше, те, що інформаційний тероризм є одним із різновидів терористичної діяльності, і, відповідно, для розробки напрямів та механізмів комплексної протидії йому необхідно планувати ефективний вплив на всі причини, що його породжують.

По-друге, те, що інформаційний тероризм є терористичною діяльністю, яка здійснюється виключно в інформаційному просторі, що має свою специфіку системного відтворення та функціонування як на глобальному, так і на локальному рівнях, і, відповідно, комплексний механізм протидії розповсюдженню цього виду діяльності повинен включати системний блок захисту та підтримання безпечної роботи всіх інформаційно-комунікативних

мереж.

Вітчизняні дослідники усвідомлюють небезпечні наслідки інформаційного тероризму як нового виду терористичної діяльності, що здатна вивести з ладу інформаційну інфраструктуру держави та її елементи й призвести до тяжких наслідків для державних установ та суспільства в цілому.

Разом з цим, вони реально розуміють, що розробка ефективної державної програми протидії сучасному інформаційному тероризму на всіх рівнях його існування є важким і не миттєвим процесом, який вимагає, перш за все, продовження комплексного дослідження проблемного поля цього виду терористичної діяльності з усіх аспектів її існування.

Висновки.

Аналіз сутності інформаційного тероризму з позиції конструювання аналітичної (п'яти ланкової) схеми дослідження проблемного поля цього виду терористичної діяльності дає нам підстави для узагальнення особливостей виникнення та розвитку цієї нової форми терористичної діяльності й інтерпретації її як процесу використання інформації та відповідної інфраструктури, з одного боку, задля здійснення насильства над свідомістю громадян сучасного суспільства, маніпулювання їх моделями поведінки із застосуванням провідних методів і способів впливу та тиску, а з іншого – для впливу на інформаційно-технічну структуру інфраструктуру держави, що є реальним підґрунтям для певних політичних акторів чинити тиск щодо прийняття вигідних для них рішень з боку держав, груп людей або окремих осіб через організацію, створення та підтримку ситуації невизначеності, соціально-психологічної напруги, панічних настроїв, культурного шоку тощо [Петришин 2021: 45].

Зрозуміло, що все це потребує подальшої активної розробки проблематики інформаційної безпеки особистості, держави та суспільства в цілому. Останнє, в свою чергу, безпосередньо пов'язане з подальшими дослідженнями проблемного поля нового виду терористичної діяльності у контексті подовження світових процесів тотальної глобалізації та інформатизації.

Бібліографічні посилання

- Coser, L. (1967). *Continuities in the Study of Social Conflict*. New York: Free Press.
- Богданов, О. (2005). Високотехнологічний тероризм нової епохи. *Проблеми безпеки особистості, суспільства, держави*, 4, 34-37.
- Головченко, В.І., Гондюл, В.П., Зернецька, О.В. (2006). *Міжнародна інформаційна безпека: сучасні виклики та загрози*. К.: Центр вільної преси.
- Жайворонок, О. (2019). Причини і джерела ескалації інформаційного тероризму в Україні та світі. *Підприємництво, господарство і право*, 10, 218-223.
- Леонов, Б.Д., Ляхова, С.Я. (2021). Інформаційний тероризм як загроза національної безпеці України. *Юридичний вісник*, 2(59), 170-176.
- Марков, В.В., Фролова, Т.А. (2019). Маніпуляція інформацією як метод інформаційного тероризму та інформаційної війни. *Протидія кіберзагрозам та торгівлі людьми*. Харків: ХНУВС, 109-115.
- Марченко, Ю. (2003). На тлі ціннісної кризи. Тероризм: анатомія витоків. *Політика і час*, 12, 61-66.
- Петришин, Г.Р. (2021). Інформаційний тероризм: джерела формування та активізації в Україні. *Габітус*, 21, 44-50.
- Петрюк, П.Т., Петрюк, А.П. (2007). К уточнению основных понятий и видов терроризма. *Ліки України*, 112, 151-154.
- Украинская, О.А. (2008). Феномен информационного терроризма в современном обществе. *Вісник ХНУ ім. В.Н.Каразіна. Теорія культури і філософія науки*, 36(829), 86-92.
- Харамурза, Д. (2023). Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіа простору. *Інтегровані комунікації*, 2(16), 29-37.
- Шкурат, І.В. (2020). Теоретико-методичне обґрунтування поняття «міжнародний тероризм» як складника глобалізаційних процесів. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*, 6, 38-42.

References

- Bohdanov, O. (2005). Vysokotekhnolohichnyi teroryzm novoi epokhy [High-tech Terrorism of the New Era]. *Problemy bezpeky osobystosti, suspilstva, derzhavy*, 4, 34-37. (in Ukrainian)
- Coser, L. (1967). *Continuities in the Study of Social Conflict*. New York: Free Press.
- Holovchenko, V.I., Hondiul, V.P., Zernetska, O.V. (2006). *Mizhnarodna informatsiina bezpeka: suchasni vyklyky ta zahrozy* [International Information Security: Modern Challenges and Threats]. K. (in Ukrainian)
- Kharamurza, D. (2023). Informatsiinyi teroryzm yak instrument hibrydnoi viiny ta faktor ruinatsii media prostoru [Information Terrorism as a Tool of Hybrid War and a Factor in the Destruction of the Media Space]. *Intehrovani komunikatsii*, 2(16), 29-37.
- Leonov, B.D., Liakhova, S.Ya. (2021). Informatsiinyi teroryzm yak zahroza natsionalnoi bezpetsi Ukrainy [Information Terrorism as a Threat to the National Security of Ukraine]. *Yurydychnyi visnyk*, 2(59), 170-176. (in Ukrainian)
- Marchenko, Yu. (2003). Na tli tsinnisnoi kryzy. Teroryzm: anatomiiia vytokiv [Against the Background of the Value Crisis. Terrorism: Anatomy of Origins]. *Polityka i chas*, 12, 61-66. (in Ukrainian)
- Markov, V.V., Frolova, T.A. (2019). *Manipuljacija informaciej kak metod informacionnogo terrorizma i informacionnoj vojny* [Information Manipulation as a Method of Information Terrorism and Information Warfare], in: *Protydiia kiberzahrozam ta torhivli liudmy*. Kharkiv: KhNUVS, 109-115. (in Russian)
- Petrjuk, P.T., Petrjuk A.P. (2007). K utochneniju osnovnyh ponjatij i vidov terrorizma [To Clarify the Basic Concepts and Types of Terrorism]. *Liky Ukrainy*, 112, 151-154. (in Russian)
- Petryshyn, H.R. (2021). Informatsiinyi teroryzm: dzherela formuvannia ta aktyvizatsii v Ukraini [Information Terrorism: Sources of Formation and Activation in Ukraine]. *Habitus*, 21, 44-50. (in Ukrainian)
- Shkurat, I.V. (2020). Teoretyko-metodychne obhruntuvannia poniattia «mizhnarodnyi teroryzm» yak skladnyka hlobalizatsiinykh protsesiv [Theoretical and Methodological Justification of the Concept of «International Terrorism» as a Component of Globalization Processes]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Serii: Derzhavne upravlinnia*, 6, 38-42.
- Ukrainskaja, O.A. (2008). Fenomen informacionnogo terrorizma v sovremennom obshhestve [The Phenomenon of Information Terrorism in Modern Society]. *Visnyk KhNU im. V. N. Karazina*, 36(829), 86-92.
- Zhaivoronok, O. (2019). Prychyny i dzherela eskalatsii informatsiinoho teroryzmu v Ukraini ta sviti [Causes and Sources of Escalation of Information Terrorism in Ukraine and the World]. *Pidpriemnytstvo, hospodarstvo i pravo*, 10, 218-223 (in Ukrainian)