Розділ 4

ЗОВНІШНЯ ПОЛІТИКА ТА НАЦІОНАЛЬНА БЕЗПЕКА

http://doi.org/10.26565/1727-6667-2023-1-08
УДК 351/354+341.322

Мирна Надія Володимирівна
кандидат наук державного управління, доцент,
доцент кафедри права, національної безпеки та європейської інтеграції
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0000-0003-3351-5572
e-mail: mail4myrna@gmail.com

Білоконь Михайло Вячеславович
кандидат наук державного управління, доцент,
доцент кафедри права, національної безпеки та європейської інтеграції
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0000-0002-5389-7013
e-mail: m.bilokon@karazin.ua

ЄВРОПЕЙСЬКА ІНТЕГРАЦІЯ ТА ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Анотація. Наукова стаття «Європейська інтеграція та протидія гібридним загрозам: виклики та перспективи» аналізує проблему гібридних загроз для Європи та роль європейської інтеграції у їх протидії. Стаття розглядає особливості гібридних загроз та їхній вплив на європейську інтеграцію. В статті також проаналізовано інструменти протидії гібридним загрозам, які використовуються в ЄС та НАТО.

Стаття відзначає, що гібридні загрози з кожним роком стають складнішими та є дуже небезпечними для нашого регіону, оскільки вони поєднують у собі різні форми агресії, включаючи інформаційну війну, кібератаки, фінансову дестабілізацію та втручання в політичні процеси. У статті підкреслюється, що зростання гібридних загроз потребує розробки нових стратегій та інструментів для протидії їм.

У статті окрему увагу приділено визначенню ролі європейської інтеграції у протидії гібридним загрозам та наголошується на важливості співпраці між державами-членами Єв-

ропейського Союзу та співпраці з НАТО у боротьбі з цими загрозами. Автори статті стверджують, що Європейський Союз на наднаціональному рівні повинен зміцнювати свої інституції та забезпечувати спільну координацію для ефективної протидії гібридним загрозам.

У підсумку, стаття «Європейська інтеграція та протидія гібридним загрозам: виклики та перспективи» робить акцент на важливості розуміння гібридних загроз та їхнього впливу на Європу, а також на необхідності розвитку нових стратегій та інструментів для протидії їм. Дослідження стверджує, що європейська інтеграція може грати важливу роль у боротьбі з гібридними загрозами, забезпечуючи наднаціональну координацію та співпрацю між державами-членами Європейського Союзу.

Стаття містить корисну інформацію для дослідників, експертів з безпеки, політичних діячів та всіх, хто цікавиться проблемою гібридних загроз та розвитком європейської інтеграції. Результати дослідження можуть бути використані для розробки стратегій та інструментів протидії гібридним загрозам в Європі та Євроатлантичному регіоні.

Ключові слова: *європейська інтеграція, ЄС, НАТО, гібридні загрози, національна безпека, стійкість, стримування.*

Як цитувати: Мирна Н. В., Білоконь М. В. Європейська інтеграція та протидія гібридним загрозам: виклики та перспективи. *Теорія та практика державного управління*. 2023. Вип. 1 (76). С. 107–122. http://doi.org/10.26565/1727-6667-2023-1-08

Вступ

Актуальність теми статті обумовлена нестандартністю викликів та загроз сьогодення. У сучасному світі гібридні загрози перетворились на великий виклик для країн Європи, Європейського Союзу та світу в цілому. Гібридна війна охоплює різноманітні форми та види агресії, які використовуються для впливу на внутрішню політику країни, громадську думку та діяльність уряду.

Гібридні загрози – це складне та багатоаспектне явище, яке потребує комплексного та системного підходу до протидії ньому. Гібридні загрози можуть бути спрямовані на різні сфери життя, такі як політика, економіка, культура, інформаційний простір та інші. Оскільки вони мають непередбачуваний характер, протидія ним потребує розробки та впровадження сучасних стратегій та ефективних інструментів як на рівні держави, так і на наднаціональному рівні.

Інструменти протидії гібридним загрозам мають бути комплексними та інтегрованими, забезпечувати широкий спектр заходів для захисту та поєднувати сучасні технології, політику та освіту. Крім того, важливо, щоб такі інструменти постійно оновлювались та підлаштовувалися до ситуації, що постійно змінюється.

Гібридні загрози мають багато форм, включаючи російську пропаганду, кібератаки, фінансову інформаційну війну, підривну діяльність, дезінформацію, терористичні акти та інші. Ці загрози стали особливо актуальними для країн, що намагаються інтегруватися в європейський простір і можуть створювати значні перешкоди на шляху до європейської інтеграції та стабільності.

Європейський Союз повинен розробити ефективну стратегію протидії гібридним загрозам, яка б дозволила йому захистити своїх громадян та запобігти подальшому розширенню цих загроз.

Дослідження проблеми гібридних загроз і з'ясування їх впливу на процес європейської інтеграції допоможе зрозуміти сутність викликів, з якими стикається Європейський Союз в цьому контексті. Дослідження також може допомогти виявити потенційні шляхи протидії гібридним загрозам, які можуть бути найбільш ефективними для захисту європейської інтеграції та стабільності.

Огляд літератури

У ході роботи над науковою статтею були проаналізовані офіційні документи та ресурси ЄС та НАТО [8; 9; 10; 11; 12; 13; 14; 15].

Серед наукових досліджень варто виділити «Подолання гібридних загроз: пріоритети для ЄС у 2020 році та надалі» [7], де обговорюються гібридні загрози та кроки, які Європа за допомогою різних національних ініціатив, ініціатив ЄС і НАТО зробила останніми роками для їх вирішення.

Також важливою є стаття «Інституційно-правові засади протидії гібридним загрозам у НАТО та ЄС» [3], де висвітлюються зміни правового забезпечення НАТО у сфері протидії гібридним загрозам яке характеризувалося формальним обмеженням розуміння безпеки та нападу переважно воєнними питаннями, а з 2014 р. змінилося розвитком концепту стійкості та цивільної готовності. В статті «Огляд боротьби НАТО та ЄС з гібридними загрозами» [6] проведено аналіз основних елементів стратегії НАТО та Європейського Союзу по боротьбі з гібридними загрозами Росії проти України з 2014 року.

Мета статті

Основна мета статті полягає в дослідженні сучасних викликів, які ставляться перед Європейським Союзом в контексті протидії гібридним загрозам.

Пошукові завдання які будуть розглянуті в ході досягнення основної мети статті, це: розгляд особливостей гібридних загроз для Європи та європейської інтеграції; аналіз інструментів протидії гібридним загрозам; визначення ролі та перспектив європейської інтеграції у протидії гібридним загрозам.

Стаття спрямована на академічну та експертну спільноти, а також на державних службовців, які займаються питаннями забезпечення національної та міжнародної безпеки, економічного розвитку та підвищення ефективності публічного управління. Результати дослідження можуть бути використані для розробки концептуальних засад протидії гібридним загрозам, розширення рівня співпраці між країнами-членами ЄС.

Методологія дослідження

У статті були використані загальні методи дослідження, такі як аналіз наукової літератури, порівняння та систематизація інформації. Також були використані спеціальні методи, такі як теоретичний аналіз, експертна оцінка та дискусія. Загальні методи дослідження були використанні для збору та аналізу інформації, формулювання питань дослідження та визначення теоретичних підходів. Спеціальні методи дослідження були використанні для глибшого вивчення певних аспектів теми дослідження та отримання даних для аналізу та узагальнення результатів.

Основні результати дослідження

Термін «гібридна загроза» може мати різні визначення, залежно від того, хто його використовує та в якому контексті. Однак, загалом, гібридні загрози відно-

сяться до використання різноманітних засобів та методів для досягнення своїх цілей, що охоплює використання різноманітних технологій, інформаційних впливів, використання різних форм насильства та інших неконвенційних методів [12; 14].

Один з підходів до визначення гібридних загроз полягає в тому, що це є багатовимірна та складна загроза яка поєднує різні форми впливу та використовує вразливості суспільства та інституцій. Крім того, гібридні загрози містять елементи асиметрії та несподіваності. Іншим широко обговорюваним елементом є неоднозначність конфлікту, оскільки гібридна війна навмисно стирає різницю між мирним і воєнним часом. Термін «сіра зона» належить до цієї неоднозначності [7].

Інші визначення гібридних загроз можуть зосереджуватися на певних аспектах загрози, наприклад, на інформаційній складовій. Так, гібридні загрози можуть бути пов'язані зі спробами маніпулювати інформацією для досягнення певних цілей, таких як посилення впливу на суспільство або дестабілізація держави. Інші визначення можуть зосереджуватися на військовій складовій, зазначаючи, що гібридні загрози включають в себе використання різноманітних військових та невійськових засобів для досягнення стратегічних цілей.

У будь-якому разі, визначення гібридних загроз є динамічним та може змінюватися в залежності від нових викликів які постають перед демократичними країнами.

Конвенційна (або звичайна) війна ведеться звичайними озброєннями, та відповідно регулюється міжнародними конвенціями (Гаазькими – про правила ведення війни, та Женевськими – про захист жертв війни). Натомість гібридна війна, усвідомлення глобальності якої стає все очевидніше – не регулюється нічим Тож, сутність та зміст гібридних загроз після початку російського вторгнення в Україну зазнали суттєвих змін. Інше питання яких саме змін – після переходу війни від гібридної форми до конвенційної, гібридна війна не завершилась. Для України вона стала звичайною, але для Заходу вона залишилась гібридною, хоча й більш активною після ескалації. РФ вела та веде гібридну війну не лише проти України (проти якої, зрештою, розпочала конвенційну війну), але й проти Європейського Союзу використовуючи для цього широкий спектр інструментів [2].

Гібридні загрози стали серйозною проблемою для країн Європи та Європейського Союзу, оскільки вони поєднують у собі різноманітні аспекти, такі як військові, політичні, економічні, інформаційні та кібернетичні. Основні гібридні загрози, які відчувають країни Європи, включають наступні:

Російська агресія: РФ здійснює агресивну зовнішню політику щодо країн Європи та Європейського Союзу. Зокрема, вона використовує військову силу в Україні, Грузії та інших країнах, проводить кібератаки та дезінформацію з метою підриву національної безпеки та стабільності в регіоні.

Кіберзагрози: кібератаки стали дедалі більшими загрозами для країн Європи та Європейського Союзу. Атаки на критичну інфраструктуру, таку як електропостачання, транспорт, комунікації, можуть призвести до серйозних наслідків для національної безпеки.

Тероризм: Європа стала мішенню терористичних організацій, таких як ІДІЛ та Аль-Каїда. Атаки на цивільних громадян можуть призвести до паніки, страху та нестабільності в країні.

Дезінформація, яка є серйозною загрозою для національної безпеки країн Європи та Європейського Союзу. РФ та інші країни проводять кампанії дезінформації, які спрямовані на підриву довіри до західних демократій, пропаганди антизахідних настроїв та вплив на громадську думку країн-членів Європейського Союзу.

Крім того, існують такі гібридні загрози, як фінансові маніпуляції, контрабанда, торгівля зброєю та наркотиками, корупція та інші.

Всі ці загрози мають потенційно серйозні наслідки для стабільності та безпеки держави та регіону в цілому, у зв'язку з чим, країни Європи та Європейський Союз ставлять перед собою завдання забезпечення безпеки та формування системи захисту від гібридних загроз. Для цього розробляються та впроваджуються стратегії та програми протидії гібридним загрозам, які передбачають взаємодію державних/публічних органів, громадянського суспільства та приватного сектору.

Важливу роль у протидії гібридним загрозам грає НАТО. До 2014 року, Альянс мав формальне обмеження розуміння безпеки та нападу, що обмежувалося переважно воєнними питаннями, що створювало певні рамки для концептів та орієнтирів НАТО у сфері протидії гібридним загрозам. Проте, з 2014 року, це бачення стало розширюватися, починаючи з розуміння та усвідомлення прихованих операцій та інформаційних засобів протистояння. Найновішою тенденцією є наголос на гібридних загрозах у стратегічних документах НАТО, таких як кібератаки, підривна економічна діяльність та свідоме порушення режиму постачання енергоносіїв. Це свідчить про зміну підходу до безпеки в НАТО та усвідомлення того, що гібридні загрози можуть бути складнішими та більш руйнівними, ніж традиційні військові загрози [3], оскільки вони є менш прямими та очевидними. Гібридні загрози можуть включати в себе широкий (зазвичай прихований) спектр дій, який ускладнює виявлення та протидію. Наприклад, кібератаки можуть завдати значної шкоди системам управління та інфраструктурі, що може мати серйозні наслідки для економіки та громадської безпеки. Також гібридні загрози можуть включати інформаційну війну, яка може бути спрямована на підрив довіри громадян до державних інституцій та підірвати політичну стабільність країни. Крім того, гібридні загрози можуть використовувати різноманітні засоби, включаючи економічний тиск та дипломатичні заходи, що може підривати стійкість та ефективність державних систем.

Гібридні загрози для суспільства та держави мають динамічну та складну природу, що ускладнює їх ідентифікацію та класифікацію. Для боротьби з цими загрозами, Європейський Союз використовує концепцію загальносуспільного менеджменту ризиків, яка охоплює не тільки протидію, але й попередження виникнення гібридних загроз. Ключовим елементом такого підходу є гармонізація суспільних відносин, усунення передумов для розвитку екстремізму і радикалізму, інклюзивний менеджмент ресурсів та інші заходи, що сприятимуть попередженню загроз та збереженню довіри до європейських та національних інституцій. Основний підхід полягає в тому, що ризики мають бути розглянуті як можливість для посилення стійкості суспільств і держав, а не тільки як за-

гроза. Для досягнення цієї мети необхідно розвивати публічно-приватну взаємодію, усвідомлювати безпековий вимір будь-якої сфери політики держав та ЄС, неподільність внутрішнього і зовнішнього вимірів безпеки суспільства [3].

Стратегія захисту країн європейського та євроатлантичного регіону від гібридних загроз включає ключовий аспект – стримування. Головна мета полягає в тому, щоб змінити поведінку противника, використовуючи демонстрацію сили [6].

Концепт «стійкості» в контексті протидії гібридним загрозам означає здатність суспільства витримувати негативний вплив таких загроз та зберігати свою незалежність та суверенітет. Водночас, концепт «стримування» означає дії та заходи, спрямовані на зменшення впливу гібридних загроз на суспільство та державу.

Поєднання цих двох концептів дозволяє досягти більш ефективної та стійкої протидії гібридним загрозам. На перший погляд, може здатися, що надмірний фокус на стримуванні може порушити стійкість суспільства, оскільки заходи з обмеження впливу гібридних загроз можуть призвести до обмеження прав та свобод громадян та порушення демократичних принципів.

Проте, поєднання концепту стримування з концептом стійкості дозволяє знайти баланс між захистом від гібридних загроз та збереженням стійкості суспільства.

По суті, ЄС та НАТО є двома ключовими міжнародними організаціями, які займаються безпековими питаннями в Євроатлантичному регіоні. Обидві організації мають різні повноваження та функції, але вони активно співпрацюють у питаннях безпеки та оборони. Оскільки гібридні загрози є складним явищем, яке вимагає взаємодії між різними секторами та організаціями, передача частини повноважень щодо колективної протидії гібридним загрозам від ЄС до НАТО може бути важливою та конструктивною. Це обумовлено такими аргументами як можливість збільшення ефективності боротьби з гібридними загрозами, забезпечення збалансованості інструментів та ресурсів, злагодженості дій, взаємодії зі іншими країнами та організаціями, та обміну інформацією.

1. Як зазначалося вище, гібридна війна вимагає взаємодії різних секторів та організацій. ЄС та НАТО мають різні функції та повноваження, і передача частини повноважень щодо колективної протидії гібридним загрозам від ЄС до НАТО може допомогти забезпечити більш ефективну координацію зусиль у боротьбі з цими загрозами через можливість мультиплікації їх спроможностей.
2. ЄС та НАТО мають різні інструменти та ресурси для боротьби з гібридними загрозами. ЄС має інструменти економічного тиску та санкцій, які можуть бути корисними для боротьби з недержавними акторами, які використовують фінансові ресурси для здійснення гібридних дій. НАТО має військові та розвідувальні інструменти та може бути корисним для боротьби з державними акторами, які використовують військову агресію або кібератаки. Передача частини повноважень щодо колективної протидії гібридним загрозам від ЄС до НАТО може допомогти забезпечити збалансованість використання різних інструментів та ресурсів у боротьбі з цими загрозами.

3. ЄС та НАТО є двома різними організаціями зі своїми власними процедурами та процесами прийняття рішень. Передача частини повноважень щодо колективної протидії гібридним загрозам – може допомогти забезпечити злагодженість дій та координацію між цими двома організаціями.

4. Гібридні загрози можуть мати транснаціональний характер та вимагати взаємодії зі сторонніми країнами та організаціями. ЄС та НАТО мають свої відносини зі сторонніми країнами та організаціями, і передача частини повноважень щодо колективної протидії гібридним загрозам від ЄС до НАТО може забезпечити більш ефективну координацію зі сторонніми країнами та організаціями, які також займаються боротьбою з гібридними загрозами.

5. ЄС та НАТО зібрали значну кількість інформації про гібридні загрози та їх джерела. Передача частини повноважень щодо колективної протидії гібридним загрозам від ЄС до НАТО може допомогти забезпечити більш ефективний обмін цією інформацією та використання її для попередження та протидії гібридним загрозам.

Необхідно зазначити, що передача частини повноважень від ЄС до НАТО не повинна призвести до зменшення ролі та впливу ЄС в боротьбі з гібридними загрозами, а має стати частиною більш широкої стратегії співпраці та координації між ЄС та НАТО. Тож для того, щоб передача повноважень була ефективною та мала б позитивний вплив на боротьбу з гібридними загрозами, необхідна чітка взаємодію між ЄС та НАТО, та координація дій між країнами-членами обох організацій.

Гібридні загрози можуть мати значний вплив на європейську інтеграцію, яка вже й так є складним і тривалим процесом. На цей час ЄС класифікують сфери протидії таким загрозам: інформаційна сфера, енергетика, транспорт та інфраструктура, космос, військова сфера, охорона здоров'я і продовольча безпека, кіберпростір, фінансова сфера, промисловість, громадський або суспільний вимір [4].

Основні впливи гібридних загроз на євроінтеграцію можна охарактеризувати наступним чином:

Створення політичної нестабільності: Гібридні загрози можуть призвести до збільшення політичної нестабільності в країнах-кандидатах на членство в ЄС. Це може стати перешкодою для проведення реформ і впровадження вимог щодо євроінтеграції, а також може призвести до скасування референдумів про вступ до ЄС.

Зниження довіри громадськості до євроінтеграції: Гібридні загрози можуть викликати збільшення недовіри громадськості до процесу євроінтеграції, зокрема через широкомасштабні кампанії дезінформації та маніпуляції.

Загрози безпеці та обороні: Гібридні загрози можуть створювати загрози для безпеки та оборони країн-кандидатів на приєднання до ЄС. Наприклад, військова агресія, кібератаки, диверсії та інші форми гібридної війни можуть стати серйозною загрозою для країн-кандидатів та призвести до скасування планів про вступ до ЄС.

Економічна нестабільність: Гібридні загрози можуть викликати економічну нестабільність у країнах-кандидатах на приєднання до ЄС. Наприклад, бойкот

товарів, зниження інвестицій, зниження туристичного потоку та інші форми економічного тиску.

Отже, гібридні загрози можуть впливати на процес європейської інтеграції на різних рівнях. Вони можуть порушувати демократичні процеси, підривати довіру до європейських інституцій, викликати безпекові проблеми та економічні негаразди.

Існує багато інструментів, які можуть бути використані для протидії гібридним загрозам на рівні окремих країн та міжнародному рівні. Наприклад, одним з найважливіших інструментів є розвиток інформаційної безпеки та кібербезпеки, що охоплює заходи, спрямовані на захист від кібератак, фейкових новин та маніпулювання громадською думкою. Ефективна протидія гібридним загрозам потребує застосування нових технологій, які можуть допомогти виявляти та боротися з ними, таких як інтелектуальний аналіз даних та блокчейн.

Ще одним дієвим інструментом є розробка та впровадження системи раннього попередження гібридних загроз, що дозволить вчасно виявляти та запобігати можливим ризикам та небезпекам.

Важливим елементом протидії гібридним загрозам є збільшення рівня свідомості населення щодо цих явищ та їх наслідків, шляхом підвищення освіти та обізнаності про гібридні загрози, а також забезпечення швидкої та ефективної комунікації між різними державними та недержавними структурами для вчасної реакції на загрозу.

Як інструмент протидії гібридним загрозам можна розглядати вживання економічних заходів, таких як санкції, що можуть зменшити фінансування та ресурси, необхідні для гібридних загроз.

Важливого значення за сучасних умов набуває міжнародне співробітництво, співпраця з іншими країнами для розробки та впровадження спільних заходів протидії гібридним загрозам.

Окремої уваги заслуговують політико-правові інструменти, нормативні акти, які приймаються як на державному, так і на наднаціональному рівні і створюють правові підстави для протидії гібридним загрозам. Ці документи запроваджують необхідні інституційно-правові механізми для гарантування безпеки в ЄС, оскільки вони визначають політику та стратегію ЄС щодо протидії гібридним загрозам, включаючи заходи з кібербезпеки та комунікаційну стратегію.

В ЄС протидія гібридним загрозам регулюється низкою нормативно-правових актів, які спрямовані на створення дієвого механізму протидії будь-якій діяльності, що здійснюється державними або приватними особами з метою спричинення шкоди або завдавання збитків інтересам, цінностям та правам держави-члена або спільним інтересам ЄС. Механізм протидії гібридним загрозам має забезпечити:

- запровадження системи взаємодії та обміну інформацією між національними, регіональними та іншими компетентними органами, а також між державами-членами ЄС та Комісією;
- забезпечення безпеки критично важливої інфраструктури та послуг, а також запобігання або мінімізація наслідків збоїв;

- розробку та здійснення різноманітних заходів для попередження та протидії дезінформації та інших форм впливу на громадську думку та рішення державних органів;
- встановлення вимог до захисту державної та конфіденційної інформації, а також внутрішніх мереж та інформаційних систем;
- розробку та здійснення заходів з протидії фінансуванню тероризму та організованої злочинності, а також з протидії легалізації доходів, отриманих злочинним шляхом;
- підготовку та проведення досліджень, спрямованих на аналіз гібридних загроз та розробку заходів щодо їх протидії;
- забезпечення належного навчання та підвищення кваліфікації фахівців, що працюють у галузі протидії гібридним загрозам;
- здійснення заходів з міжнародного співробітництва та партнерства, зокрема з державами-членами ЄС, НАТО та іншими міжнародними організаціями.

У квітня 2016 Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response) [12]. У Спільних принципах наголошується на необхідності забезпечення взаємодії між державами-членами ЄС в галузі безпеки та протидії гібридним загрозам, запропоновано створити необхідні механізми для обміну інформацією, аналізу потенційних загроз та запровадження спільних заходів щодо протидії цим загрозам.

Кожна з країн ЄС має свої специфічні фактори вразливості, проте багато держав-членів ЄС стикаються зі спільними загрозами, які можуть впливати на транскордонні мережі або інфраструктуру. Протидія гібридним загрозам є складовою національної безпеки, оборони та забезпечення правопорядку, і основна відповідальність за це лежить переважно на державах-членах, але протистояти цим загрозам більш ефективно можливо за умов успішної координації дій на рівні ЄС з використанням відповідних наднаціональних інструментів ЄС, які підтримують європейську солідарність, взаємодопомогу та відповідають принципам Лісабонського договору.

Спільні політики та інструменти ЄС відіграють ключову роль у підвищенні свідомості та поліпшенні стійкості держав-членів щодо реагування на спільні загрози. Спільна комунікація має на меті сприяти цілісному підходу, який дозволить ЄС, спільно з державами-членами, ефективно протидіяти загрозам гібридного характеру, шляхом створення синергії між всіма відповідними інструментами та підтримки тісної співпраці між усіма зацікавленими сторонами. Це включає обмін інформацією, аналіз потенційних загроз, розробку та впровадження заходів щодо протидії цим загрозам. Спільні підходи представлені і реалізуються в стратегіях та секторальних політиках, які сприяють досягненню більшої безпеки, таких як Європейська програма з безпеки [13], Стратегія кібербезпеки ЄС [11], Стратегія енергетичної безпеки [8], Морська стратегія Європейського Союзу щодо безпеки [10]. Ці інструменти мають значний вплив і можуть сприяти протидії гібридним загрозам.

У Спільних принципах зазначається, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО, оскільки співпраця ЄС та НАТО дозволить обом організаціям більш ефективно реагувати на гібридні загрози як на політичному, так і на оперативному рівні. У документі запропоновано кілька напрямів для поглиблення співпраці та координації між ЄС і НАТО, включаючи стратегічну комунікацію, кібербезпеку та запобігання та реагування на кризи. Окремо наголошується на посиленні неформального діалогу між ЄС і НАТО щодо гібридних загроз з метою синхронізації діяльності цих двох організацій у цій сфері.

Європейська комісія і Європейська служба зовнішніх справ (EEAS) створили міжвідомчу групу з протидії гібридним загрозам, яка проводить регулярні засідання на різних рівнях. Ця група покликана забезпечувати спільну обізнаність з подіями і процесами за допомогою європейських інституцій, що стосуються протидії гібридним загрозам і є першим перспективним кроком до комплексної моделі викликів у галузі безпеки.

Важливу комунікативну роль у спільній роботі ЄС та НАТО з протидії гібридним загрозам відіграє Центр передового досвіду з протидії гібридним загрозам в Гельсінкі (Hybrid CoE) [15]. Рішення щодо створення Центру було ухвалене в квітні 2017 представниками країн НАТО та ЄС, але оперативної спроможності він набув у вересні 2017 року. Засновниками центру стали 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Великобританія, Іспанія, Польща, Естонія, Латвія і Литва. Початковий річний бюджет Центру становить близько 1,5 млн Євро. Метою Центру є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах» [1].

Центр передового досвіду з гібридних загроз забезпечує координацію дій між державами-членами ЄС в разі виникнення кризових ситуацій, що становлять загрозу для безпеки ЄС. Метою діяльності центру є підтримка ЄС і його держав-членів у забезпеченні безпеки та стабільності в Європі, сприяння взаємодії та координації відповідних заходів у сфері протидії гібридним загрозам, зокрема в контексті кризових ситуацій, кризового управління, запобігання, виявлення та реагування на гібридні загрози.

До завдань Центру належить: аналіз та виявлення гібридних загроз; надання порад державам-членам та іншим органам ЄС з питань протидії гібридним загрозам; проведення навчань та тренувань з протидії гібридним загрозам. Центр забезпечує належний рівень координації та співпраці між національними органами та установами ЄС, що працюють в галузі протидії гібридним загрозам та розвиває взаємодію з іншими установами ЄС та міжнародними організаціями, зокрема з ООН, НАТО та ОБСЄ, з метою підвищення ефективності спільної діяльності у протидії гібридним загрозам.

Центр має мережу національних контактних пунктів у державах-членах. Центр також має свій власний штат і адміністративну структуру. Завдання національних контактних пунктів включає надання центру необхідної інформації та координацію дій у країні. Фінансування діяльності Європейського центру з протидії гібридним загрозам здійснюється з бюджету ЄС.

Окремої уваги заслуговує Стратегія безпеки ЄС 2020 року [9], в якій на відміну від двох попередніх стратегій «Безпечна Європа в кращому світі» (2003 р.) і «Сильніша Європа. Глобальна стратегія зовнішньої політики та політики безпеки Європейського Союзу» (2016 р.), гібридним загрозам приділено більше уваги. Так, з 4-х розділів Стратегії саме частина 2-го – «Боротьба з загрозами, що розвиваються» була присвячена гібридним загрозам. Якщо документ 2018 р. був своєрідною відповіддю на події в Солсбері, то Стратегія 2020 р. – відповіддю на поширення дезінформації під час пандемії COVID-19, коли кілька державних і недержавних акторів намагалися інструменталізувати пандемію, зокрема, маніпулюючи інформаційним середовищем та кидаючи виклик основним інфраструктурам [5].

Стратегія безпеки ЄС 2020 робить наголос на тому, що наявні сучасні загрози можуть розвиватися в нових обставинах. Організовані злочинні групи використовують дефіцит товарів, що створює можливість для створення нових нелегальних ринків. Нелегальна торгівля наркотиками залишається найбільшим злочинним ринком в ЄС. Торгівля людьми не зникає, оцінки свідчать про щорічний глобальний прибуток від всіх форм експлуатації дорівнює 30 мільярдів євро. Міжнародна торгівля підробленими лікарськими засобами сягнула 38,9 мільярда євро. Разом з тим низькі рівні конфіскації дозволяють злочинцям продовжувати розширювати свою злочинну діяльність та проникати в законну економіку. Злочинці та терористи все легше отримують доступ до вогнепальної зброї через Інтернет та нові технології. Використання штучного інтелекту, нових технологій і робототехніки містять ризик, що злочинці скористаються перевагами інновацій для зловживання.

Усі ці загрози мають прямий або опосередкований вплив на різні сегменти суспільного життя. Вони всі представляють серйозну загрозу для осіб та підприємств і вимагають всебічної та послідовної реакції на рівні ЄС та країн-членів ЄС. Коли вразливості в області безпеки можуть виникати навіть з невеликих побутових пристроїв, таких як підключені до Інтернету холодильники або кавоварки, світ вже не можемо покладатися лише на традиційних державних акторів, щоб забезпечити безпеку людини та держави в цілому. Економічні оператори повинні взяти більшу відповідальність за кібербезпеку продуктів та послуг, які вони продають на ринку, а громадяни повинні мати хоча б базове розуміння кібербезпеки, щоб захистити себе [9].

Особлива увага у Стратегії безпеки приділяється процесу прийняття рішень, який має враховувати потенційні небезпечні впливи та гібридні загрози як внутрішнього, так і зовнішнього характеру.

Стратегія безпеки сприяє створенню ефективної системи комунікації з громадськістю та партнерами щодо гібридних загроз, шляхом проведення інформаційних кампаній, консультацій та нарад з зацікавленими сторонами. Ці заходи мають забезпечити підвищення рівня свідомості громадськості щодо гібридних загроз та сприяння формуванню культури кібербезпеки в європейському суспільстві. Стратегія робить наголос на розвитку новітніх технологій та інструментів для протидії гібридним загрозам, таких як штучний інтелект, кіберзахист та інші.

Отже, Стратегія безпеки ЄС спрямована на зміцнення резистентності суспільства до гібридних загроз, забезпечення прозорості та ефективної комунікації з громадськістю і партнерами.

Стратегія акцентує увагу на розвитку міжнародного співробітництва та координації зусиль з протидії гібридним загрозам на наднаціональному рівні. У першу чергу мова йде про співробітництво з Організацією Північноатлантичного договору (НАТО) та Організацією з безпеки та співробітництва в Європі (ОБСЄ).

Отже, гібридні загрози становлять значну небезпеку для сталого розвитку Європейського Союзу (ЄС) та країн-членів. З метою ефективної протидії цим загрозам, ЄС впроваджує комплексний підхід, який включає аналіз, попередження, реагування та відновлення. Аналіз гібридних загроз відбувається на національному та європейському рівнях шляхом збору та обміну інформацією. Попередження гібридних загроз вимагає підвищення кіберстійкості та здатності виявляти та реагувати на кібератаки, а також розширення співробітництва країн щодо зменшення ризиків безпеки в інших сферах. Реагування на гібридні загрози вимагає швидкої та координованої реакції. У цьому контексті, ЄС використовує наявні механізми реагування та координує свої зусилля з національними механізмами цивільного захисту країн-членів. Відновлення після гібридних загроз передбачає надання допомоги постраждалим країнам у відновленні та забезпеченні їхнього сталого розвитку шляхом залучення наявних фінансових та регуляторних інструментів.

Висновки з даного дослідження і перспективи подальших досліджень

Можна зробити висновок, що процес євроінтеграції є важливим елементом протидії гібридним загрозам для європейських країн та регіону в цілому. Європейський Союз надає значну підтримку у боротьбі з гібридними загрозами, зокрема, шляхом співпраці та координації з країнами-членами. Одним з важливих елементів євроінтеграції є зближення законодавства та стандартів безпеки між країнами. Це дозволяє зменшити ризики та підвищити рівень захисту від гібридних загроз. Важливою складовою євроінтеграції є співпраця у сфері кібербезпеки. Розробка та впровадження спільних стратегій та інструментів дозволяє підвищити ефективність боротьби з гібридними загрозами на рівні регіону. Окрім цього, євроінтеграція може допомогти країнам розробити та впровадити нові стратегії та інструменти протидії гібридним загрозам, зокрема, шляхом надання фінансової та технічної підтримки. Це дозволить ефективніше боротися з цими явищами та забезпечити безпеку країн та регіону в цілому.

Підхід ЄС до визначення та характеристики гібридних загроз та шляхів протидії ним викладений у «Спільних принципах протидії гібридним загрозам – відповідь Європейського Союзу» (2016), «Підвищення стійкості та посилення можливостей для подолання гібридних загроз» (2018), Стратегії безпеки ЄС (2020). Інтегрована система протидії гібридним загрозам охоплює повний спектр заходів як на рівні країн-членів, так і на наднаціональному рівні ЄС – починаючи від раннього виявлення, аналізу, підвищення обізнаності, стійкості, запобігання до реагування в кризових ситуаціях та управління наслідками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Безверха А.О., Дубов Д.В., Каздобіна Ю.К., Шулімов С.Ф. Аналітичний звіт «Впливи у цифровому просторі: як Європа шукає свій шлях протидії та що може запозичити Україна?». URL: https://ufss.com.ua/wp-content/uploads/2021/06/UFSS_countering_influence.pdf.

2. Білоконь М.В. Конвенційна фаза гібридної війни чи гібридна – конвенційної? Публічне управління XXI століття: в умовах гібридних загроз: зб. наук. матер. XXII Міжнар. наук. конгресу. Х. : НІІ "Інститут державного управління" Харківського національного університету імені В.Н. Каразіна, 2022. С. 63–66.

3. Кресін О.В. Інституційно-правові засади протидії гібридним загрозам у НАТО та ЄС. Правова держава. Випуск 33. Київ: Ін-т держави і права імені В. М. Корецького НАН України, 2022. URL: http://pravova-derzhava.org.ua/files/pravova-derzhava.-volume-33-_2022_.pdf#page=516.

4. Мирна Н.В., Соколова В. Європейський досвід визначення і протидії гібридним загрозам. Публічне управління XXI століття: в умовах гібридних загроз: тези XXII Міжнар. наук. конгресу. Х. : НІІ "Інститут державного управління" Харківського національного університету імені В.Н.Каразіна, 2022. С. 71.

5. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta de Historia & Politica: Saeculum XXI*. №3. 2021-2022. URL: https://ahpsxxi.org/index.php/journal/article/download/52/38.

6. Ahmadly J. Overview of NATO and EU's struggle against hybrid threats. Політологія, № 2(54), 2022. URL: http://visnyk-psp.kpi.ua/article/view/264384.

7. Bajarūnas E. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, Volume 19, Issue 1. 2020. URL: https://journals.sagepub.com/doi/10.1177/1781685820912041.

8. Communication from The Commission to The European Parliament and The Council European: Energy Security Strategy / EU. 2014. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014DC0330.

9. Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic And Social Committee and The Committee of The Regions: on the EU Security Union Strategy / EU. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

10. Joint communication on the update of the EU Maritime Security Strategy and its Action Plan: An enhanced EU Maritime Security Strategy for evolving maritime threats / EU. 2023. URL: https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime_en.

11. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / EU. 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

12. Joint Framework on countering hybrid threats a European Union response: Joint communication to the European Parliament and the Council. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

13. The European Agenda on Security / European Commission. Strasbourg, 28.4.2015. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015DC0185.

14. Warsaw Summit Communiqué / NATO. 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

15. What is Hybrid CoE? / The European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi/who-what-and-how.

Стаття надійшла до редакції 04.05.2023
Стаття рекомендована до друку 05.06.2023

Nadiya Myrna, PhD in Public Administration, Associate Professor of Law,
National Security and European Integration Chair,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: https://orcid.org/0000-0003-3351-5572 e-mail: mail4myrna@gmail.com

Mykhailo Bilokon, PhD in Public Administration, Associate Professor of Law,
National Security and European Integration Chair,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: https://orcid.org/0000-0002-5389-7013 e-mail: m.bilokon@karazin.ua

EUROPEAN INTEGRATION AND COUNTERING HYBRID THREATS: CHALLENGES AND PROSPECTS

Abstract. The relevance of the article's topic is determined by the non-standard nature of the challenges and threats of today. In the modern world, hybrid threats have become a major challenge for European countries, the European Union, and the world as a whole. Hybrid warfare encompasses various forms and types of aggression that are used to influence a country's domestic politics, public opinion, and government activities.

Hybrid threats are complex and multifaceted phenomena that require a comprehensive and systemic approach to counter them. They can target different spheres of life, such as politics, economy, culture, the information space, and others. Since they have an unpredictable nature, countering them requires the development and implementation of modern strategies and effective tools at both the national and supranational levels.

The European Union must develop an effective strategy to counter hybrid threats that would allow it to protect its citizens and prevent the further expansion of these threats.

Therefore, the process of Eurointegration is an important element in countering hybrid threats for countries and the region as a whole. The European Union provides significant support in combating hybrid threats, including through cooperation and coordination with member countries. One important element of Eurointegration is the alignment of legislation and security standards among countries. This helps reduce risks and enhance protection against hybrid threats. Collaboration in the field of cybersecurity is also a crucial component of Eurointegration. The development and implementation of joint strategies and tools enhance the effectiveness of countering hybrid threats at the regional level. Furthermore, Eurointegration can assist countries in developing and implementing new strategies and tools to counter hybrid threats, including through financial and technical support. This will enable more effective combat against these phenomena and ensure the security of countries and the region as a whole.

The EU's approach to defining and addressing hybrid threats is outlined in the «Joint Framework on Countering Hybrid Threats - European Union Response» (2016), «Increasing Resilience and Strengthening the Capacity to Address Hybrid Threats» (2018), and the EU Security Strategy (2020). The integrated system for countering hybrid threats encompasses a wide range of measures at both the member state and supranational EU levels, including early detection, analysis, raising awareness, building resilience, prevention, crisis response, and consequence management.

Keywords: *European Integration; EU; NATO; Hybrid Threats; National Security, Sustainability, Deterrence.*

In cites: Myrna N. V., Bilokon M. V. (2023). European Integration and Countering Hybrid Threats: Challenges and Prospects. *Theory and Practice of Public Administration*, 1 (76), pp. 107–122. http://doi.org/10.26565/1727-6667-2023-1-08 [in Ukrainian].

REFERENCES:

1. Bezverkha, A.O., Dubov, D.V., Kazdobina, YU.K., & Shulimov, S.F. (2021). *Analytical report "Influences in the digital space: how Europe is looking for its way of counteraction and what can Ukraine borrow?"*. Retrieved from: https://ufss.com.ua/wp-content/uploads/2021/06/UFSS_countering_influence.pdf [in Ukrainian].

2. Bilokon', M.V. (2022). Conventional phase of hybrid war or hybrid-conventional? *Public administration of the 21st century: in the conditions of hybrid threats: coll. of science the mother XXII International of science congress*. Kh.: Institute of Public Administration of the V.N. Karazin Kharkiv National University. 63–66 [in Ukrainian].

3. Kresin, O.V. (2022). Institutional and legal principles of countering hybrid threats in NATO and the EU. *Constitutional State*. Issue 33. Kyiv: V. M. Koretskyi Institute of State and Law of the National Academy of Sciences of Ukraine. Retrieved from: http://pravova-derzhava.org.ua/files/pravova-derzhava.-volume-33-_2022_.pdf#page=516 [in Ukrainian].

4. Myrna, N.V., & Sokolova V. (2022). European experience in identifying and countering hybrid threats. *Public administration of the 21st century: in the conditions of hybrid threats: coll. of science the mother XXII International of science congress*. Kh.: Institute of Public Administration of the V.N. Karazin Kharkiv National University. 71 [in Ukrainian].

5. Khmel, A. (2022). Combating hybrid threats in the EU (by the European Union regulation and legal framework*). Acta De Historia & Politica: Saeculum* XXI, (03), 91-101. Retrieved from: https://doi.org/10.26693/ahpsxxi2021-2022.03.091 [in Ukrainian].

6. Ahmadly, J. (2022). Overview of NATO and EU's struggle against hybrid threats. *Politology*, № 2(54). Retrieved from: http://visnyk-psp.kpi.ua/article/view/264384.

7. Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, Volume 19, Issue 1. Retrieved from: https://journals.sagepub.com/doi/10.1177/1781685820912041.

8. Communication from The Commission to The European Parliament and The Council European: Energy Security Strategy. (2014) / EU. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52014DC0330.

9. Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic And Social Committee and The Committee of The Regions: on the EU Security Union Strategy. (2020) / EU. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

10. Joint communication on the update of the EU Maritime Security Strategy and its Action Plan: An enhanced EU Maritime Security Strategy for evolving maritime threats. (2023) / EU. Retrieved from: https://oceans-and-fisheries.ec.europa.eu/publications/joint-communication-update-eu-maritime-security-strategy-and-its-action-plan-enhanced-eu-maritime_en.

11. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013) / EU. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001.

12. Joint Framework on countering hybrid threats a European Union response: Joint communication to the European Parliament and the Council. (2016). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

13. The European Agenda on Security. (2015, April 28) / European Commission. Strasbourg. Retrieved from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015DC0185.
14. Warsaw Summit Communiqué. (2016) / NATO. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
15. What is Hybrid CoE? / The European Centre of Excellence for Countering Hybrid Threats. Retrieved from: https://www.hybridcoe.fi/who-what-and-how.

The article was received by the editors 04.05.2023
The article is recommended for printing 05.06.2023