УДК 338.2:327.5
DOI https://10.33111/iep.2024.41.12

Карпенко Оксана[1]

Європейський досвід протидії гібридним загрозам для економічного відродження України

АНОТАЦІЯ. У статті узагальнено досвід країн ЄС щодо протидії гібридним загрозам, окреслено напрями його можливого і доцільного використання в процесі економічного відродження України, охарактеризовано категоріальний апарат дослідження: визначено такі поняття як: гібридні загрози, актори, дії. Ідентифіковано дієві механізми протидії гібридним загрозам в ЄС, до яких віднесені інституційні ініціативи, санкційна політика, а також конкретні ad hoc заходи щодо інформаційної, енергетичної та кібербезпеки, зокрема діяльність Європейського центру передового досвіду з протидії гібридним загрозам, зменшення ресурсної залежності країн внаслідок диверсифікації постачання, заснування Європейського агентства з кібербезпеки, кампанії протидії дезінформації. Особливу увагу приділено методам та інструментам реалізації створеної в ЄС Концептуальної моделі гібридних загроз (2021 р.), яка має широкий спектр доменів: інфраструктура; кіберсфера; космічна, економічна, військова та оборонна сфери, сфера культури, соціальна сфера, сфера державного управління та юридична; розвідка, дипломатія, політична та інформаційна сфери, внаслідок чого спрямована на підвищення обізнаності, налагодження взаєморозуміння між сторонами, виявлення головних аспектів, що уможливлюють адекватне розуміння ландшафту гібридних загроз. Показано, що гібридні загрози передбачають використання різних підходів до їх уникнення та розвитку стійкості до них, що обумовило появу Моделі комплексної екосистеми стійкості (2023 р.). Розкрито її сутність, конкретизовано сфери застосування, структуру за доменами (сферами діяльності), просторами (громадський, управління та послуг), та рівнями (локальний, національний, міжнародний), що і утворюють екосистему. Виокремлено актуальні вразливості, ворожі актори та ризики національній безпеці та обґрунтовано можливості усунення їх негативного впливу на широкий спектр діяльності в умовах гібридних загроз на основі дослідження європейського досвіду. Досліджено результати реалізації проєкту «Академічна протидія гібридним загрозам» (WARN) в межах Програми ЄС Еразмус+ за напрямом «Розвиток потенціалу вищої освіти» (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP) для забезпечення підвищення національної безпеки та подолання нестачі сервісів безпеки, яка виникла через появу гібридних загроз.

КЛЮЧОВІ СЛОВА: гібридні загрози, європейський досвід, заклади вищої освіти, академічна протидія гібридним загрозам, алгоритм прийняття управлінських рішень, безпека, протидія, економічне відродження України.

[1] **Карпенко Оксана Олександрівна** – доктор економічних наук, професор, перший проректор Міжнародного науково-технічного університету імені академіка Юрія Бугая. Сфера наукових інтересів: тенденції розвитку сучасного менеджменту, реформування державного управління, організаційно-економічні механізми підвищення ефективності функціонування підприємств, теорія та практика трансферу знань на національному та міжнародному рівнях, академічна протидія гібридним загрозам. Електронна адреса: o.karpenko@istu.edu.ua ORCID ID: https://0000-0003-2943-1982

Статтю підготовлено на основі матеріалів проєкту WARN «Академічна протидія гібридним загрозам» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), що співфінансується програмою Erasmus+ Європейського Союзу. Підтримка Європейською Комісією у створення матеріалів, розміщених в Розділі 4, не є схваленням змісту, який відображає погляди лише авторів, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ній.

Вступ

Забезпечення стійкості держави і суспільства до загроз різного роду та вироблення відповідей на численні виклики, спричинені впливом гібридних загроз, лежать в основі глобального безпекового середовища.

Сучасна Україна стикається з численними викликами, зокрема гібридними загрозами, які включають військові, економічні, інформаційні та кібернетичні елементи. Ці загрози мають на меті підрив економічної стабільності, руйнування довіри до державних інституцій та блокування відновлення країни.

У контексті євроінтеграції та тісної співпраці з країнами Європейського Союзу, використання їхнього досвіду протидії гібридним загрозам є важливим для забезпечення економічного відродження України.

Метою статті є дослідження європейського досвіду протидії гібридним загрозам. Для досягнення поставленої мети в роботі використано комплексний підхід, що базується на загальнонаукових, загальноекономічних та прикладних аспектах впливу гібридних загроз на національну безпеку.

Гібридні загрози, актори, дії

У сучасному світі гібридні загрози стали серйозним викликом для багатьох країн, включаючи Україну. Поняття «гібридні загрози» відноситься до дій, які здійснюються державними чи недержавними акторами, мета яких полягає в тому, щоб підірвати або завдати шкоди цільовій групі шляхом здійснення впливу на її прийняття рішень на місцевому, регіональному, державному чи інституційному рівні. Такі дії координуються і синхронізуються та навмисно націлені на вразливі місця демократичних держав та інститутів. Дії можуть мати місце, наприклад, у політичній, економічній, військовій, громадянській або інформаційній сферах. Вони проводяться з використанням широкого кола засобів і розраховані на те, щоб залишатися нижче порога виявлення і атрибуції[2].

Гібридні загрози спрямовані на дестабілізацію демократичних держав через економічний тиск (санкції, маніпуляції з енергоресурсами, підрив ланцюгів постачання), кіберзагрози (атаки на критичну інфраструктуру, фінансову систему, державні реєстри), інформаційні кампанії (дезінформація, спрямована на створення паніки та недовіри до держави), політичні впливи (підтримка корупційних практик, втручання у внутрішню політику).

Гібридні гравці намагаються не переконати, не битись, а вплинути на алгоритм прийняття управлінських рішень[3].

---

[2] Hybrid threats as a concept. Hybrid CoE. ULR: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

[3] Methodology of training in the context of hybrid threats: a manual / E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC “TECHNOLOGY CENTER GROUP”, 2023. 84 p. https://sciencebookgroup.org/catalog/book/338

Гібридні дії характеризуються неоднозначністю, що створюється шляхом поєднання традиційних і нетрадиційних засобів – дезінформації і втручання в політичні дебати або вибори, порушення критичної інфраструктури, кібернетичні напади, різні форми злочинної діяльності і, нарешті, асиметричне використання військових засобів і ведення війни.

Механізми протидії гібридним загрозам у ЄС

Зазначене вище актуалізує необхідність посилення протидії гібридним загрозам, у зв'язку з чим поряд з прийняттям важливих програмних документів в Європейському Союзі створено і нині функціонує ряд організацій, метою діяльності яких є проведення досліджень з питань генезису та трансформування гібридних загроз, напрацювання методів, засобів та механізмів для протидії цим загрозам, організація спільного навчання та консультацій для країн-учасниць тощо (табл. 1).

Таблиця 1

ДІЄВІ МЕХАНІЗМИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В КРАЇНАХ ЄС

Механізми	**Характеристика**
Інституційні ініціативи	Сформовано нормативно-правову базу щодо захисту ЄС від гібридних загроз «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» (2016 р.), «Підвищення стійкості та посилення можливостей для подолання гібридних загроз» (2018 р.), «Звіт про впровадження Спільної програми протидії гібридним загрозам 2016 р. та Спільного повідомлення 2018 р. щодо підвищення стійкості та зміцнення можливостей для подолання гібридних загроз» (2020 р.), «Картографування заходів, пов'язаних із підвищенням стійкості та протидією гібридним загрозам» (2020 р.), «Операційний протокол ЄС для протидії гібридним загрозам (EU Playbook)» (2016 р.), Стратегія безпеки ЄС 2020, щодо якої Європейська Рада прийняла не законодавчу Резолюцію. У ЄС діє Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE), який об'єднує зусилля держав-членів у боротьбі з гібридними атаками. Його завдання включають аналітику, навчання і обмін досвідом.
Енергетична безпека	Зменшення залежності від російських енергоресурсів через диверсифікацію постачальників. Наприклад, Польща й Литва створили LNG-термінали, що дозволило їм знизити залежність від російського газу. Створення Енергетичного союзу ЄС, який забезпечує інтеграцію енергетичних систем країн-членів.

Закінчення табл. 1

Механізми	**Характеристика**
Кібербезпека	Введення Директиви NIS 2 щодо безпеки мереж і інформаційних систем, яка посилює вимоги до захисту критичної інфраструктури. Заснування Європейського агентства з кібербезпеки (ENISA) для координації зусиль у боротьбі з кіберзагрозами.
Інформаційна безпека	Кампанії протидії дезінформації, наприклад, ініціатива East StratCom Task Force, спрямована на викриття російської пропаганди. Зміцнення незалежних ЗМІ та медіаграмотності серед населення.
Санкційна політика	ЄС активно застосовує економічні санкції проти агресорів, включаючи замороження активів і обмеження торгівлі.

Джерело: складено з використанням[4]

Функціонування зазначених вище організацій та реалізація прийнятих документів дозволить сприяти запобіганню та виявленню гібридних загроз, зокрема посилити боротьбу з тероризмом та організованою злочинністю, підвищити стійкість критичної інфраструктури до кібератак, сприяти науковим дослідженням та інноваціям, розвитку системи освіти тощо.

Концептуальна модель гібридних загроз

Однією з відповідей ЄС на численні виклики, які зумовлені впливом гібридних загроз, є розробка «Концептуальної моделі гібридних загроз» («Hybrid Threats conceptual model»)[5] спільними зусиллями Об'єднаного дослідницького центру Європейської комісії (JRC)[6] та Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE)[7].

Об'єднаний дослідницький центр Європейської комісії (Joint Research Centre – JRC) надає незалежні, науково обґрунтовані знання, підтримуючи політику ЄС з метою позитивного впливу на суспільство.

Діяльність Європейського центру передового досвіду з протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE) спрямована на: проведення досліджень, аналіз

[4] Khmel A. Combating Hybrid Threats in the EU (based on the regulatory framework of the European Union). Acta de Historia & Politica: Saeculum XXI. 2021/2022. VOL. III. P. 91-101.

[5] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[6] Joint Research Centre. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies-old/joint-research-centre en

[7] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: https://www.hybridcoe.fi/about-us/

гібридних загроз та методів боротьби з ними; організацію спільного навчання для країн-учасниць; проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, залучення до діалогу урядових та неурядових експертів.

Основні завдання «Концептуальної моделі гібридних загроз»[8]: підвищити обізнаність, налагодити розуміння із зацікавленими сторонами, ідентифікувати ключові проблеми та прогалини в майбутніх дослідженнях.

У «Концептуальній моделі гібридних загроз»[9] виділено чотири основні стовпи, шо необхідно вивчити, щоб мати можливість повністю зрозуміти ландшафт гібридних загроз:

- ворожі актори (та їхні стратегічні цілі);
- інструменти, які використовує ворожій актор;
- цільові домени (сфери);
- фази (включаючи види діяльності, що спостерігаються в кожній фазі).

Так, ворожий актор (державний чи недержавний), який має цілі, але обмежені можливості для їх досягнення, може застосувати різноманітні інструменти до ряду доменів для виконання певного типу діяльності на різних фазах, щоб досягти ряд цілей і підірвати здатність приймати рішення у державі, яка є мішенню гібридних загроз (цільовій державі).

Ворожі актори, які вдаються до гібридної діяльності, пов'язаної з загрозами, намагатимуться вплинути на алгоритм прийняття рішень об'єктом. Прийняття рішень може бути невеликим (бізнес-угоди), локальними (люди під час виборів) та рішення, які приймають фахівці, які формують політику та законодавство. Якщо операція буде успішною, тоді вона міститиме лише деякі аспекти, які робитимуть загрозу гібридною за своєю природою. Це означає, що дія може завдати шкоди сама по собі, і її потрібно виявляти та протидіяти на ранній стадії. З цієї причини важливо вивчити акторів, які стоять за гібридною загрозою.

У «Концептуальній моделі гібридних загроз»[10] виділено такі домени: інфраструктура; кіберсфера; космічна сфера; економічна сфера; військова та оборонна сфери; сфера культури; соціальна/суспільна сфера; сфера державного управління; юридична (правова) сфера; розвідка; дипломатія; політична сфера; інформаційна сфера. Домени не слід досліджувати окремо, оскільки вплив на один домен може викликати каскадний ефект в інших. Це особливо важливо, коли розглядається вплив гібридної загрози на домен. У кожному домені може бути безліч інструментів,

[8] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[9] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[10] Ibid.

які може використовувати ворожий актор для ураження певних доменів задля досягнення своїх цілей.

Гібридні загрози є всеохоплюючою концепцією, яка включає широкий спектр видів діяльності в ландшафті гібридних загроз: втручання, вплив, кампанії та війна.

Різні типи діяльності гібридних загроз у «Концептуальній моделі гібридних загроз»[11] поміщено на часову шкалу, що вказує на те, що існує потенціал ескалації гібридних загроз, який охоплює як короткострокові, так і довгострокові можливості. Хронологія має три різні фази, а саме: підготовка, дестабілізація та примус. Всі фази мають сильну психологічну складову. Спектр дій, зокрема, втручання, вплив, кампанії та війна на різних етапах збігаються.

Гібридна війна передбачає синхронізоване використання багатьох інструментів впливу, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів.

Модель комплексної екосистеми стійкості

Наразі спостерігається стрімкий розвиток подій і зростання витонченості гібридних загроз. Тому стійкість до гібридних загроз необхідно розробляти і впроваджувати на всіх рівнях, а також розглядати показники стійкості не лише з точки зору різних сфер, але й як комплексний екосистемний підхід. Іншими словами, розвиток стійкості до гібридних загроз вимагає виходу за межі стійкості в окремих сферах, розбудовуючи її системно, враховуючи залежності та взаємозалежності між різними частинами суспільства – «Модель комплексної екосистеми стійкості («The comprehensive resilience ecosystem (CORE) model»)[12], яка має полегшити процес прийняття обґрунтованих управлінських рішень на різних рівнях управління.

«Модель комплексної екосистеми стійкості – це системне представлення демократичного суспільства в цілому. Вона використовується для аналізу і, зрештою, протидії гібридним загрозам, які прагнуть підірвати і завдати шкоди цілісності та функціонуванню демократій, змінити процеси прийняття рішень і створити каскадні ефекти[13].

---

[11] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[12] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

[13] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

Новизна цієї моделі полягає в тому, що вона дозволяє політикам оцінити, як супротивники використовують гібридні загрози, щоб змінити можливості демократичного прийняття рішень. Вона показує, як гібридні загрози крок за кроком кидають виклик демократичним системам, створюючи різні види стресу. Це також дозволяє відстежувати залежності та можливі каскадні ефекти. Це важливо для виявлення гібридних загроз. Передбачення відіграє вирішальну роль у цьому процесі.

В основі екосистеми лежать сім засад демократичних систем: відчуття справедливості та рівного ставлення, громадянські права і свободи, політична відповідальність та підзвітність, верховенство права, стабільність, надійність/доступність, здатність до передбачення. Ці сім засад є основою стійкого, демократичного суспільства і є важливими для розбудови стійкості до гібридних загроз. Саме вони є кінцевими цілями атак ворожих акторів для задоволення при цьому їхніх власних стратегічних інтересів.

Домени (сфери) з «Концептуальної моделі гібридних загроз»[14] також є невід'ємною частиною екосистеми: інфраструктурна, кібернетична, космічна, економічна, військова/оборонна, культурна, соціальна/суспільна сфери, сфера державного управління, правова, розвідувальна, дипломатична, політична, інформаційна сфери. Якщо в доменах добре розвинена стійкість, вони можуть діяти як щити проти зловмисних дій. З іншого боку, відсутність стійкості в доменах може відкрити точки входу для ворожих акторів.

Екосистема складається з трьох просторів – Громадянського простору, Простору управління та Простору послуг, які представляють три сектори суспільства.

Три рівні екосистеми представляють різні «шари», які існують в організації суспільства – локальний, національний, міжнародний.

Оскільки елементи взаємопов'язані, заходи з розбудови стійкості з для одного елемента впливатимуть на інші елементи, позитивно чи негативно. Ворожі актори, що стоять за гібридними загрозами, прагнуть використати різні елементи та їхній взаємозв'язок для максимізації свого впливу. Тому політикам необхідно розуміти взаємозалежність між різними елементами, щоб розбудовувати стійкість до гібридних загроз і своєчасно виявляти зловмисну діяльність на ранніх стадіях.

Такий екосистемний підхід допомагає виявити ранні сигнали, підтримувати їхній аналіз та визначати потенційні траєкторії реагування. «Модель комплексної екосистеми стійкості»[15] можна використовувати як «дошку для гри в дартс» для відображення того, як актори використовують

[14] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

[15] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

конкретні інструменти для атак на різні сфери і створюють каскадні ефекти в різних просторах і на різних рівнях. Це допомагає проаналізувати і зрозуміти вплив, розвиток/етапи, а також те, наскільки інтенсивно, на які сфери і рівні впливають гібридні загрози і наскільки вони залежать один від одного. По суті, це допомагає особам, які приймають рішення вибрати, які ресурси, інструменти і заходи мобілізувати на рівні ЄС, держав-членів і на оперативному рівні.

Стійкість є ключем до протидії гібридним загрозам і має розроблятися системно. Розбудова стійкості в окремих сферах окремо не є оптимальним, оскільки гібридні загрози мають на меті створювати каскадні ефекти та використовувати взаємозв'язки. Необхідний системний підхід, з урахуванням існуючих залежностей та взаємозалежностей в суспільстві.

Проєкт «Академічна протидія гібридним загрозам»

Однією з відповідей на виклики, зумовлені впливом гібридних загроз, була реалізація проєкту «Академічна протидія гібридним загрозам» (WARN) в межах Програми ЄС Еразмус+ за напрямом «Розвиток потенціалу вищої освіти» (Erasmus+ Capacity Building Project 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)[16], який завершено 14 листопада 2024 року. Місія проєкту – підвищення національної безпеки та подолання нестачі сервісів безпеки, яка виникла через появу гібридних загроз. Цільові групи: студенти, університети, викладачі, компанії та організації, суспільство загалом.

Над реалізацією проєкту працювали сім українських ЗВО, а саме: Харківський національний університет радіоелектроніки, Український католицький університет, Державний університет інфраструктури та технологій, Національний університет «Острозька Академія, Національна академія керівних кадрів культури і мистецтв, Харківський національний університет ім. В.Н. Каразіна, Горлівський інститут іноземних мов Донбаського державного педагогічного університету. Від європейських партнерів до складу консорціуму входили: Університет Ювяскюля (Фінляндія) – координатор проєкту, Вища інженерна школа Франції; Університет Коїмбри (Португалія); Університет Тарту (Естонія).

За результатами реалізації проєкту[17]:

— Створено та обладнано 7 центрів передового досвіду (на базі оновлених лабораторій).

— Адаптовано 11 існуючих магістерських програм ЗВО консорціуму проєкту та створено і акредитовано 1 нову програму.

[16] WARN Project Website. URL: http://warn-erasmus.eu

[17] Golovianko Mariia. Application of European Resilience Experience Against Hybrid Threats in the Erasmus+ Project WARN. URL: https://warn-erasmus.eu/wp-content/uploads/2024/11/warn_application_eu-resilience_experience_against_hybrid_threats.pdf

— Підготовлено 24 силабуси розроблених нових дисциплін.

— Створено і оприлюднено робочі програми 18 курсів з протидії гібридним загрозам для циклу освіти впродовж життя у 11 проєктних доменах.

— Розроблено 7 навчальних курсів для підвищення кваліфікації викладачів ЗВО усіх галузей на основі нової методики викладання протидії гібридним загрозам.

— Оформлені і оприлюднені на сайтах ЗВО навчально-методичні матеріали для 12 нових дисциплін та для 39 оновлених дисциплін з протидії гібридним загрозам.

— Розроблено і оприлюднено на сайтах університетів 51 новий комплект навчальних матеріалів для практичних занять.

— Розроблено один електронний посібник за новою методикою гібридного навчання «Нова методика навчання протидії гібридним загрозам» (єдиний для всіх партнерів)[18].

— Створено і оприлюднено «Глосарій з гібридних загроз»[19].

— 2432 студентів зараховано і підготовлено на магістерських проєктних програмах з протидії гібридним загрозам.

— 1504 викладачів ЗВО поза консорціумом пройшли тренінг для викладачів за новою викладацькою методикою для навчання протидії гібридним загрозам, про що отримали Сертифікати, які підтверджують набуті навички.

— 4594 слухача з професійних секторів пройшли курси підвищення кваліфікації за проєктними програмами освіти впродовж життя з метою оволодіння навичками протидії гібридним загрозам у власній галузі.

— 17 нових партнерів приєдналося до WARN середовища.

— Проєкт заснував окрему конференцію, присвячену дослідженням щодо протидії гібридним загрозам в різних галузях «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці».

Заклади вищої освіти України шляхом впровадження відповідних навчальних дисциплін та організації курсів підвищення кваліфікації можуть створити ефективні засоби щодо роз'яснення сутності, інформування про гібридні загрози, можливості та способи їх попередження, а також мінімізації негативних наслідків впливу гібридних загроз.

Висновки

Протидія гібридним загрозам стає пріоритетом, оскільки вони розмивають чітку межу між війною та миром, поєднуючи військові можливості з

[18] Methodology of training in the context of hybrid threats: a manual / E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC "TECHNOLOGY CENTER GROUP", 2023. 84 p. https://sciencebookgroup.org/catalog/book/338

[19] Glossary of hybrid threats / Erasmus+ project WARN "Academic Response to Hybrid Threats". 2024. 203 c. https://openarchive.nure.ua/handle/document/29379

політичними, дипломатичними, економічними, кібербезпековими та дезінформаційними заходами.

Для прийняття обґрунтованих управлінських рішень на різних рівнях в умовах гібридних загроз слід впроваджувати підхід, що базується на стійкості. Особливістю прийняття таких рішень є те, що їх потрібно приймати в умовах турбулентності навколишнього середовища: невизначеності, неоднозначності, обмеження часу.

Враховуючи європейський досвід, Україна має інтегруватися в європейські ініціативи кібер- та енергетичної безпеки, використовувати технічну та фінансову підтримку ЄС для модернізації інфраструктури, удосконалити власну стратегію протидії гібридним загрозам на основі європейських практик, зосередитися на боротьбі з дезінформацією через підвищення рівня медіаграмотності населення.

Європейський досвід протидії гібридним загрозам є важливим ресурсом для економічного відродження України. Комплексний підхід, інтеграція у відповідні європейські ініціативи та адаптація найкращих практик дозволять не лише захистити українську економіку, а й закласти фундамент для її розвитку в умовах сучасних безпекових викликів.

Список літератури

1. Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rбcz, A., Schmid, J. and Schroefl, J., The landscape of Hybrid Threats: A Conceptual Model (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

2. Glossary of hybrid threats / Erasmus+ project WARN "Academic Response to Hybrid Threats". 2024. 203 c. https://openarchive.nure.ua/handle/document/29379

3. Golovianko Mariia. Application of European Resilience Experience Against Hybrid Threats in the Erasmus+ Project WARN. URL: https://warn-erasmus.eu/wp-content/uploads/2024/11/warn_application_eu-resilience_experience_against_hybrid_threats.pdf

4. Hybrid threats as a concept. Hybrid CoE. ULR: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

5. Joint Research Centre. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies-old/joint-research-centre_en

6. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/113791, JRC129019. URL: https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf

7. Khmel A. Combating Hybrid Threats in the EU (based on the regulatory framework of the European Union). *Acta de Historia & Politica: Saeculum XXI*. 2021/2022. VOL. III. P. 91-101.

8. Methodology of training in the context of hybrid threats: a manual / E. Balashov, M. Bilokon, T. Borozentseva, M. Holovyanko, S. Hryshko, T. Zhovtenko et al. Kharkiv: LLC "TECHNOLOGY CENTER GROUP", 2023. 84 p. https://sciencebookgroup.org/catalog/book/338 (in Ukrainian)

9. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: https://www.hybridcoe.fi/about-us/

10. WARN Project Website. URL: http://warn-erasmus.eu

Стаття надійшла до редакції 20 жовтня 2024 р.
Прийнято до публікації: 18 листопада 2024 р.
Опубліковано: 31 грудня 2024 р.