УДК 327.5+327.88-025.26](4-6ЄС)
DOI 10.26693/ahpsxxi2021-2022.03.091

БОРОТЬБА ІЗ ГІБРИДНИМИ ЗАГРОЗАМИ В ЄС (ЗА НОРМАТИВНО-ПРАВОВОЮ БАЗОЮ ЄВРОПЕЙСЬКОГО СОЮЗУ)

Анастасія Хмель,
e-mail: hmelnastia@ukr.net
ORCID: https://orcid.org/0000-0002-4881-7859
Чорноморський національний університет імені Петра Могили,
Україна, 54003, м. Миколаїв, вул. 68 Десантників, 10

Враховуючи актуальність теми протидії гібридним загрозам для України, автор звертає увагу на нормативно-правову базу Європейського Союзу, яка визначає гібридні загрози та передбачає дії та заходи щодо протидії їм. З 2016 року розробляється та поглиблюється нормативно-правова база, яка безпосередньо призначена для боротьби з гібридними загрозами, окремий розділ Стратегії безпеки ЄС 2020 присвячений боротьбі з гібридними загрозами, а також можливість застосування окремих статей Договору про ЄС. Основна відповідальність за боротьбу з гібридними загрозами лежить на державах-членах, але у випадках, коли загрози виходять за межі їхніх кордонів і стосуються організації, відповідальність несуть Комісія, Високий представник та новостворені органи: HFC, East Stratcom, Horizontal Working Group, Center досконалості у боротьбі з гібридними загрозами. Проаналізовані документи демонструють важливість координації всіх інституцій ЄС у боротьбі з гібридними загрозами. Якщо в документі 2016 року йдеться здебільшого про Комісію, Верховного представника, HFC, INTCEN, EEAS, то в наступних документах кількість інституцій, які беруть участь у такій протидії, розширюються завдання для Ради ЄС, Європарламенту та різних ЄС оборонні та розвідувальні органи.

Ключові слова: *ЄС, Європейська Комісія, Верховний представник, гібридні загрози, дезінформація, «Hybrid Fusion Cell».*

Постановка проблеми. Актуальність теми дослідження підвищується для України з кожним роком, адже держава з початку становлення своєї незалежності (1991 р.) постійно потерпає від гібридної загрози з боку Російської Федерації (далі – РФ). Всі дії, якими послуговується РФ щодо України: енергетичний тиск (в першу чергу, газовий шантаж), торгівельні війни, спотворення фактів української історії, дезінформація, з 2014 р. – анексія Криму та війна на Сході України, мають за мету унеможливити її самостійне існування, реалізацію її європейського та євроатлантичного курсу, процвітання та розвитку. Тому, такі дії Російської Федерації щодо нашої держави інтерптеруємо як гібридну загрозу. Схожі дії РФ спостерігаються й щодо Європейського Союзу (далі – ЄС), результатом яких має стати: зниження авторитету до ЄС та його інституцій як в середині організації, так і за її межами, дестабілізація ситуації в середині об'єднання. Відчувши та проаналізувавши перші результати гібридних дій з боку РФ (втручання у виборчий процес, інформаційний вплив, збільшення євроскептичних настроїв), ЄС розробив правову базу для більш зручного та адекватного захисту населення та самих інституцій. Тож ми ставимо

собі за *мету* проаналізувати наявну нормативно-правову базу щодо захисту ЄС від гібридних загроз, визначивши органи та інституції, які відповідають за захист від гібридних загроз та окреслити самі ці функції.

Таких документів розроблено чимало, які містять комплекс заходів для захисту інформаційної, економічної сфер ЄС, його космічного та кібернетичного просторів: «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. Особливої уваги заслуговують перші три документи зі списку та останній, оскільки саме в них визначені центри та інституції ЄС, що беруть участь у боротьбі із гібридними загрозами, їх функції. Щодо документу «EU Playbook» (2016 р.), то він не опублікований ЄС і потребує окремого доступу.

Якщо звернути увагу на *ступінь розробки теми*, то зазначимо, що дана тематика серед українського наукового загалу не є досить популярною. Більшою мірою вітчизняні науковці досліджують гібридні загрози з боку РФ щодо України тільки побіжно, вказуючи на ту ж небезпеку для ЄС. Цьому присвячені не просто окремі статті, а цілі конференції. Зокрема така була ініційована Центром Разумкова в грудні 2016 р. і була присвячена висвітленню думки експертів щодо змісту і значення гібридної війни РФ проти України та ЄС[1]. 8 липня 2021 р. в м. Києві відбулася ще одна важлива конференція, яка стосувалася розгляду сутності гібридної війни з боку РФ як елемента цивілізаційного протистояння, її політико-ідеологічного підґрунтя, інформаційної складової, економічного та військового компонентів, що застосовує РФ[2].

Серед українських дослідників, які найбільш активно останніми роками досліджують питання «гібридної війни» як такої, варто назвати Є. Магду[3] та В. Фесенко[4]. Окрім того, потрібно виокремити Аналітичну доповідь Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році» під редакцією В. Горбуліна, О. Власюка і О. Ляшенко, де наголошується на важливості врахування гібридних загроз під час планування і реалізації внутрішньої і зовнішньої політики України[5].

У свою чергу висвітленням європейської практики боротьби із гібридними загрозами займаються А. Місюра та В. Паливода[6], які у своїх наукових доробках звертають увагу на важливості таких організацій як НАТО та ЄС бути готовими дати

[1] *«Гібридна» війна Росії – виклик і загроза для Європи.* (2016, грудень.). Київ. Retrieved from: https://cutt.ly/QUY2bTV

[2] *Гібридна війна: сутність, виклики та загрози: зб. матер. круглого столу* (2021, 8 липня). Київ: НА СБУ, 189. Retrieved from: https://academy.ssu.gov.ua/uploads/p_57_28744724.pdf

[3] Магда, Є. В. (2015) *Гібридна війна: вижити і перемогти*. Харків: «Віват», 304.

[4] Фесенко, В. (2016, грудень) Спиратися винятково на власні сили і взяти відповідальність за розвиток України на себе *«Гібридна» війна Росії – виклик і загроза для Європи*. Київ, 24-25.

[5] *Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році»* (2017). Київ: НІСД, 928.

[6] Місюра, А., Паливода, В. (2018). *Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки.* Retrieved from: https://cutt.ly/fUY2Ian; Паливода, В. (2020). *Центр протидії тероризму та гібридним загрозам при МВС Чеської Республіки*. Retrieved from: https://cutt.ly/jUY2PEP

вчасну відсіч гібридним загрозам. Окрім того, розглядають досвід Республіки Словаччина та Чехії в цьому напрямку[7]. У 2018 р. вийшов Аналітичний документ в рамках проектів «Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз» (за підтримки ЄС та Міжнародного фонду «Відродження»), «Громадська синергія» (під егідою Української національної платформи Форуму громадянського суспільства Східного партнерства), де один з розділів присвячено підходам ЄС щодо гібридних загроз[8]. Варто зазначити, що українські дослідники, при висвітленні даної проблематики, застосовують термін «гібридна війна» або «гібридна агресія», у той час як європейські науковці – «гібридна загроза».

Серед дослідників ЄС, які активно займаються дослідженням гібридних загроз даного об’єднання, потрібно виокремити праці Ф. Хоффмана «Гібридні загрози: переосмислення еволюційного характеру сучасного конфлікту» (2009 р.), Е. Монагана «Війна» в російській «гібридній війні» та Р. Вілкі «Гібридна війна: щось старе, а не щось нове»[9]. В цих роботах автори надають описові визначення гібридним загрозам, їх основні характеристики, зазначаючи, що гібридні війни – не нове явище для міжнародних відносин.

Литовський політик, колишній посол Литви в РФ та Швеції Ейтвидас Баярунас присвятив кілька статей гібридним загрозам[10], де висвітлюються безпосередньо гібридні загрози та кроки Європи щодо їх подолання протягом останніх років, шляхом застосування різних національних та міжнародних ініціатив. Він зазначає, що подолання гібридних загроз є постійним, нескінченним процесом, який вимагає підвищенню стійкості суспільства та уряду. Автор надає деякі рекомендації для європейських політиків щодо наступних кроків, які ЄС має зробити при подоланні гібридних загроз[11].

Ґрунтовною є й праця Родеріка Паркеса[12], спеціаліста з євроінтеграційної політики, керівника Центру європейських політичних досліджень імені Альфреда фон Оппенгейма, де наявне важливе зауваження щодо розуміння гібридної війни. Автор зазначає, що «гібридна загроза» не нове явище, воно було ще за часів «холодної війни», просто у з часом змінилася назва і визначення. І наголошує на тому, що «гібридна загроза» – це не просто сукупність нетрадиційних загроз. «Недостатньо об’єднати тероризм, громадянську непокору, кібератаки, злочинну діяльність, кампанії дезінформації, втручання у вибори, конфлікти проксі, бійців без знаків розрізнення і назвати це гібридною кампанією»[13]. Паркс наполягає – важливим є те, яким чином такі виклики збігаються і чи дійсно вони використовуються для ескалації

[7] Паливода, В. (2020). *Підходи Словаччини до боротьби з гібридними загрозами: аналітика від експерта НІСД*. Retrieved from: https://niss.gov.ua/en/node/3492

[8] *Гібридні загрози Україні і суспільна безпека. досвід ЄС і Східного Партнерства. Аналітичний документ* \ За загальною редакцією В. Мартинюка. (2018). Київ. Retrieved from https://cutt.ly/gUY2GYR

[9] Fiott, D, Parkes, R. (2019). Protecting Europe: The EU’s response to hybrid threats. *European Union Institute for Security Studies (EUISS)*. Retrieved from: http://www.jstor.com/stable/resrep21143.4

[10] Bajarūnas, E. (2020, March 22). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*. Retrieved from: https://doi.org/10.1177/1781685820912041; Bajarūnas, E., Keršanskas, V. (2019). Hybrid threats: Analysis of their content, challenges posed and measures to overcome. *Lithuanian Annual Strategic Review*, 16(1), 123–170. Retrieved from: https://cutt.ly/IUY2Zn3

[11] Bajarūnas, E. (2020, March 22). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*. Retrieved from https://doi.org/10.1177/1781685820912041

[12] Fiott, D, Parkes, R. (2019). Protecting Europe: The EU’s response to hybrid threats. *European Union Institute for Security Studies (EUISS)*. Retrieved from: http://www.jstor.com/stable/resrep21143.4

[13] Ibiden.

нестабільності. Він зауважує, що боротьбою із гібридними загрозами мають опікуватися всі дотичні до безпеки та спільної зовнішньої політики ЄС інституції.

Італійський науковець Луіджи Лонардо підкреслює, що багато правових профілів гібридних загроз розглядалися в літературі, але всеосяжного підходу до регуляторної реакції ЄС досі бракує, тому його дослідження було спрямоване навколо п'яти гібридних загроз: дезінформація, ворожі іноземні субсидії та інвестиції, кібератаки, тиск на кордони і законність, правова база ЄС для можливості їх подолання[14]. Окрім того, дослідник у своїй праці розглянув документи ЄС щодо можливості відповідати на данні загрози.

Викладення основного матеріалу. Перш за все звернемо увагу на документ: *Спільне повідомлення до Європейського парламенту та Ради «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» (*2016 р.), де зазначається, що у червні 2015 р. Європейська Рада звернула увагу на необхідності мобілізації інструментів ЄС для протистояння гібридним загрозам[15], визначення яких має залишатися гнучким, щоб реагувати на їх еволюційну природу. У свою чергу концепція боротьби із гібридними загрозами повинна охопити поєднання примусової і підривної діяльності, звичайні та нетрадиційні методи (дипломатичні, військові, економічні, технологічні), які можна використовувати у скоординований спосіб державними або недержавними суб'єктами для досягнення конкретних цілей, не оголошуючи при цьому війни»[16].

В цьому документі, як і у всіх наступних, визначено, що оскільки протидія гібридним загрозам пов'язана з національною безпекою та обороною, підтриманням законності і правопорядку, то головна відповідальність лежить на державах-членах, крім тих випадків, коли вони стикаються зі спільними загрозами, які також можуть бути спрямовані на транскордонні мережі або інфраструктури. Такі загрози можна більш ефективно подолати за допомогою скоординованої реакції на рівні ЄС, використовуючи політику та інструменти ЄС, щоб активізувати європейську солідарність, взаємодопомогу та повний потенціал Лісабонського договору[17]. Зовнішні дії ЄС, запропоновані в рамках цієї структури, керуються принципами, викладеними у статті 21 Договору про Європейський Союз (далі – ДЕС), які включають демократію, верховенство права, універсальність і неподільність прав людини, повагу до принципів Статуту Організації Об'єднаних Націй та міжнародне право.

Крім іншого, «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» 2016 року наголошує на тому, що дії ЄС базуються на існуючих стратегіях та галузевій політиці, які сприяють досягненню безпеки, передбачена співпраця з НАТО у протидії гібридним загрозам. Запропонована відповідь гібридним загрозам зосереджена на таких елементах як: підвищення обізнаності, підвищення стійкості, запобігання, реагування на кризу та відновлення[18].

---

[14] Lonardo, L. (2021) EU Law Against Hybrid Threats: A First Assessment. *European Papers*, 6 (2), 1075-1096. Retrieved from: https://cutt.ly/WUY2V2h

[15] Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final. Document 52016JC0018. Retrieved from: https://cutt.ly/0UY9H0d

[16] Ibiden.

[17] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. OJ C 306. 17.12.2007. Retrieved from: https://cutt.ly/7UPnXI2

[18] Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final. Document 52016JC0018. Retrieved from: https://cutt.ly/oUY9Hod

Першим кроком документ передбачає, що Високий представник ЄС із зовнішніх справ (далі – Високий представник) і Європейська Комісія (далі – Комісія) працюватимуть разом з державами-членами, щоб підвищити обізнаність щодо ситуації шляхом моніторингу та оцінки ризиків, які можуть бути спрямовані на вразливі місця ЄС. Комісія розробляє методики оцінки ризиків безпеки для інформування осіб, що приймають рішення, та сприяє формуванню політики, яка ґрунтується на ризиках в різних сферах від авіаційної безпеки до фінансування тероризму і відмивання грошей.

Загалом у Стратегії визначена 21 дія у боротьбі ЄС із гібридними загрозами. Більшість обов’язків у цій ситуації покладені на Комісію, Верховного представника, Центр для аналізу гібридних загроз «Hybrid Fusion Cell» ЄС (далі – HFC), який був створений в рамках Центру розвідки та ситуації ЄС (далі – EU INTCEN) і Європейської служби зовнішніх дій (далі – EEAS).

HFC має отримувати, аналізувати та обмінюватися секретною інформацією, інформацію з відкритим вихідним кодом, що стосується індикаторів та попереджень щодо гібридних загроз від різних зацікавлених сторін у EEAS (включаючи представництва ЄС), Комісії (з агенціями ЄС) та держав-членів. У свою чергу Європейська Комісія повинна підтримувати зв'язок з існуючими органами на національному та європейському рівнях. Даним документом державам-членам ЄС було запропоновано створити національні контактні пункти щодо оцінки гібридних загроз для забезпечення співпраці та безпечного зв'язку з HFC ЄС[19].

Якщо проаналізувати 21 захід, що запропонований документом, у боротьбі із гібридними загрозами та систематизувати функції, що покладені на Комісію, Верховного представника, HFC та держав-членів, отримаємо наступну схему.

Високий представник разом з державами-членами досліджуватиме шляхи оновлення та координації потенціалу для забезпечення активних стратегічних комунікацій та оптимізації використання засобів моніторингу ЗМІ та спеціалістів із лінгвістики. За необхідності вони повинні запропонувати проекти щодо адаптації обороноздатності та розвитку, протидії гібридним загрозам в державах-членах, а також здійснювати розвідувальну діяльність, долучивши до цього Європейське оборонне агентство[20].

Державам-членам було запропоновано розглянути можливість створення Центру передового досвіду для «протидії гібридним загрозам». Власне, такі Центри були створені майже у всіх державах-членах, як зазначено у «Звіті про реалізацію Спільної платформи протидії гібридним загрозам 2016 року та Спільного повідомлення 2018 року щодо підвищення стійкості та зміцнення можливостей для подолання гібридних загроз» 2020 року[21-22].

Виконавчий орган ЄС *Комісія* має співпрацюючи із державами-членами та зацікавленими сторонами; визначати загальні інструменти, включаючи індикатори, з метою покращення захисту та стійкості критичної інфраструктури до гібридних загроз у відповідних секторах; підтримувати зусилля з диверсифікації джерел енергії та просування стандартів безпеки, стійкості ядерних інфраструктур; відстежувати загрози, що виникають у транспортному секторі; за необхідності оновлювати законодавство.

[19] Ibid.
[20] Ibid.
[21] Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Joint Staff working document. SWD (2020)153. 24/07/2020. Retrieved from: https://cutt.ly/0UUC527
[22] Паливода, В. (2020). Retrieved from: https://cutt.ly/jUY2PEP

Комісія та Високий представник (у межах своїх повноважень) у координації з державами-членами вивчатимуть як реагувати на гібридні загрози, зокрема ті, що стосуються транспортної критичної інфраструктури; стійкість космічної інфраструктури до гібридних загроз, зокрема, шляхом можливого розширення сфери космічного спостереження та відстеження на гібридні загрози. Комісія у співпраці з державами-членами має покращити обізнаність та стійкість до гібридних загроз у рамках існуючих механізмів готовності та координації, зокрема Комітету з безпеки здоров'я, створивши Групи реагування на інциденти з комп'ютерної безпеки (Computer Security Incidents Response Teams, далі – CSIRT) та CERT (Computer Emergency Response Team, далі – CERT), а також структуру для стратегічного співробітництва[23].

Крім іншого, передбачені функції Комісії у галузі кібербезпеки: у координації з державами-членами вона повинна забезпечити, щоб галузеві ініціативи щодо кіберзагроз (авіація, енергетика, морське транспортування) відповідали міжгалузевим можливостям у рамках Директиви щодо мережевої та інформаційної безпеки (далі – NIS). Комісія має розробити та видати рекомендації власникам інтелектуальних мереж для покращення кібербезпеки їхніх установок.

У контексті ініціативи з розробки ринку електроенергії Комісія розгляне пропозицію «планів готовності до ризиків» і процедурних правил для обміну інформацією та забезпечення солідарності між державами-членами під час кризи, включаючи правила щодо запобігання та пом'якшення кібератак. Окрім того, Комісія у співпраці з ENISA, державами-членами, відповідними міжнародними, європейськими, національними органами влади і фінансовими установами сприятиме розвитку платформ та мереж обміну інформацією про загрози, а також усуне фактори, які перешкоджають обміну такою інформацією. Комісія разом з Європейським агентством з авіаційної безпеки (далі – EASA) мають розробити Дорожню карту з кібербезпеки для авіації у співпраці[24].

Високий представник у координації з Комісією продовжить неформальний діалог та посилить співпрацю та координацію з НАТО щодо ситуаційної обізнаності, стратегічних комунікацій, кібербезпеки та «попередження криз та реагування» для протидії гібридним загрозам, дотримуючись принципів інклюзивності та автономності процесу прийняття рішень кожною організацією. Документ визначає, що співпраця може включати військову підготовку, наставницькі та консультативні місії для покращення безпеки та обороноздатності держави, що перебуває під загрозою, планування дій у надзвичайних ситуаціях для виявлення сигналів гібридних загроз та посилення можливостей раннього попередження, підтримка управління прикордонним контролем у разі надзвичайних ситуацій, підтримка в спеціалізованих областях, таких як зниження ризику CSDP та евакуація некомбатантів.

Тож в Спільному повідомленні до Європейського парламенту та Ради *«Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу»* 2016 р. були намічені дії для підвищення стійкості в таких сферах як кібербезпека, критична інфраструктура, захист фінансової системи від незаконного використання та зусилля з протидії насильницькому екстремізму та радикалізації. Для реалізації яких заплановано виконання державами-членами узгоджених стратегій ЄС, імплементацію існуючого законодавства.

Атака нервово-паралітичною речовиною в Солсбері (Велика Британія) 1 березня 2017 р. ще більше підкреслила небезпеку гібридних загроз для ЄС, тому документ

[23] Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final. Document 52016JC0018. Retrieved from: https://cutt.ly/oUY9Hod

[24] Ibid.

«Підвищення стійкості та посилення можливостей для подолання гібридних загроз» 2018 року був більшою мірою спрямований на протидію гібридним загрозам, пов’язаним із небезпекою хімічної або бактеріологічної зброї[25]. В повідомленні наголошувалося, що ЄС досяг відчутних результатів в таких сферах, як стратегічні комунікації, ситуаційна обізнаність, посилення готовності та стійкості, спроможності реагувати на кризи.

Оперативна група East Stratcom (про яку лише раз згадано в документі 2016 р.), очолила роботу з прогнозування, відстеження та боротьби з дезінформацією, що надходить з іноземних джерел. Її експертний аналіз та публічна продукція значно підвищили обізнаність щодо впливу російської дезінформації (упродовж 2016-18 рр. було виявлено понад 4000 таких випадків). Завдяки такому результату було створено дві оперативні групи з різним географічним фокусом – оперативна група для Західних Балкан і спеціальна оперативна група на південь для арабомовного світу.

Створений у квітні 2017 р. для заохочення стратегічного діалогу та проведення досліджень та аналізу гібридних загроз, Центр передового досвіду (HFC) розширив своє членство до 16 країн, заручившись при цьому підтримкою ЄС. У своїй роботі робить акцент на боротьбі з дезінформацією, шляхом підвищення прозорості, надійності та підзвітності онлайн-платформ; забезпечення стійкості виборчих процесів; сприяння медіаграмотності; підтримки якісної журналістики; допомоги стратегічним комунікаціям[26].

Щодо хімічних, біологічних, радіологічних та ядерних ризиків, план дій Комісії від жовтня 2017 р. запропонував практичні дії та заходи, спрямовані на кращий захист громадян та інфраструктури від цих загроз: зменшення доступності хімічних, біологічних, радіологічних та ядерних матеріалів; забезпечення більш надійної готовності та реагування на інциденти хімічної, біологічної, радіологічної та ядерної безпеки; налагодження міцніших внутрішніх і зовнішніх зв'язків у сфері хімічної, біологічної, радіологічної та ядерної безпеки з ключовими регіональними та міжнародними партнерами ЄС; поглиблення знань про хімічні, біологічні, радіологічні та ядерні ризики. Співробітництво проти гібридних загроз визначено як ключову сферу співпраці ЄС-НАТО (відповідно до Варшавської спільної декларації 2016 р.)[27].

Як і в попередньому документі передбачено функції для Високого представника і Комісії, які перш за все мали завершити роботу над індикаторами вразливості, щоб дозволити державам-членам краще оцінити потенціал гібридних загроз у різних секторах.

В документі зазначалося що до кінця 2018 р. *Комісія* повинна була розробити перелік небезпечних хімічних речовин; налагодити діалог з приватними виробниками щодо поставок прекурсорів для ліквідації хімічних речовин; прискорити перегляд сценаріїв загроз та аналіз існуючих методів виявлення таких загроз з метою розробки оперативних вказівок по виявленню хімічних загроз для держав-членів. Комісія мала провести заходи на високому рівні з державами-членами та іншими зацікавленими сторонами щодо вироблення рекомендацій по реакції на загрози кібернетики та дезінформації.

---

[25] Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats. European Commission. Brussels, 13.6.2018. JOIN (2018) 16 final. Document 52018JC0016. Retrieved from: https://cutt.ly/qUUqv4y

[26] Ibid.

[27] Joint Communication to the European Parliament, the European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats. European Commission. Brussels, 13.6.2018. JOIN (2018) 16 final. Document 52018JC0016. Retrieved from: https://cutt.ly/qUUqv4y

Держави-члени зі свого боку мали провести інвентаризацію запасів основних медичних контрзаходів, лабораторного, лікувального та іншого потенціалу і продовжити роботу з визначення кібератак і практичного використання інструментарію кібердипломатії для посилення політичної реакції на кібератаки[28].

EEAS і Комісія повинні сприяти співпраці усіх представників у сфері стратегічних комунікацій, для боротьби з дезінформацією, що надходить з ЄС та з-за його меж; запровадити практичні заходи для підтримки та розвитку здатності ЄС взаємодіяти з державами-членами для протидії ворожій розвідувальній діяльності, спрямованій на їх установи.

Європейський парламент і Рада мали прискорити роботу для завершення переговорів щодо пропозицій по кібербезпеці шляхом узгодження законодавства щодо збору електронних доказів та для завершення переговорів щодо пропозиції перевірки інвестицій[29].

Документ 2018 р. закріпив більш поглиблені функції HFC, East Stratcom, подальші дії Європейського Парламенту, Ради ЄС та EEAS у протидії гібридним загрозам.

Також варто зупинитися на *Стратегії безпеки ЄС 2020 року*[30], 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.

В Стратегії 2020 визначено, що такі дії послабили соціальну згуртованість і підірвали довіру до інституцій ЄС та урядів держав-членів. Комісія та Високий представник виклали в цій Стратегії підхід ЄС до гібридних загроз, який об'єднує зовнішній та внутрішній вимір у безперебійний потік. Підхід охопив весь спектр дій - від раннього виявлення, аналізу, поінформованості, підвищення стійкості та запобігання до кризового реагування та управління наслідками. Передбачено і подальше посилення розвідувальної співпраці з компетентними службами держав-членів через EU INTCEN; оптимізацію інформаційних потоків з різних джерел країн-членів та агенцій ЄС (ENISA, Європол, Frontex, Комісія, HFC); забезпечення безперебійної співпраці ЄС з НАТО[31]. Таким чином, Стратегія 2020 р. лише зафіксувала ті положення, які були розроблені у документах 2016 та 2018 р.

Згідно із Стратегією 2020 *HFC* і надалі виконує центральну координуючу роль у попередженні гібридних загроз; проводить аналіз гібридних та кіберзагроз з усіх джерел на основі розвідки у тісній співпраці з Управлінням розвідки Військового штабу ЄС (EUMSINT; надає письмові оцінки та організовує брифінги; продовжує організовувати два рази на рік зустрічі своєї мережі національних контактних пунктів для протидії гібридним загрозам; підтримує тісну співпрацю з Відділом аналізу

[28] Ibid.
[29] Ibid.
[30] 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 COM/2020/605 final. Document 52020DC0605. Retrieved from: https://cutt.ly/7UUC4ao
[31] Ibid.

гібридних загроз НАТО та Центром передового досвіду з протидії гібридним загрозам[32].

Функції *Комісії* включають зміцнення співпраці з державами-членами, зокрема з Бельгією, у сфері контррозвідки та кібернетики; розповсюдження повідомлень про загрози між інституціями, органами та агентствами ЄС (упродовж червня 2019-квітня 2020 р. було 110 записок із загрозами)[33] щодо хакерства виборів, зловмисних дій у соціальних медіа, можливостей ведення кібервійни, спонсорованої державними суб’єктами, кібершпигунства, дезінформації тощо.

Європейський центр передового досвіду з протидії гібридним загрозам, який розташований у Гельсінкі і налічує 27 членів, продовжує надавати активну підтримку в ключових сферах за допомогою спеціальних освітніх заходів, таких як: семінари і конференції, співпрацюючи при цьому з усіма державами-членами ЄС, EEAS, Комісією, Генеральним секретаріатом Ради, Європейським оборонним агентством, Європейським коледжем безпеки та оборони та Європейським парламентом[34].

Тож, звіт демонструє поступ у плані координації на рівні ЄС та підтримки зусиль держав-членів щодо протидії гібридним загрозам та розширення співпраці між різними агенціями та інституціями ЄС й державами-членами ЄС, підтверджує особливість та багатогранність співробітництва з НАТО та з однодумцями в багатонаціональних форматах, таких як G7.

Результати дослідження. 1) Основними документами ЄС, в яких розглянуто визначення гібридних загроз, зазначено сфери, де вони можуть бути реалізовані та визначено заходи боротьби із ними є: «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» (2016), «Підвищення стійкості та посилення можливостей для подолання гібридних загроз» (2018), «Звіт про впровадження Спільної програми протидії гібридним загрозам 2016 року та Спільного повідомлення 2018 року щодо підвищення стійкості та зміцнення можливостей для подолання гібридних загроз» (2020), Стратегія безпеки ЄС 2020. 2) Протягом створення нормативної бази ЄС у боротьбі із гібридними загрозами значно розвинулося загальне розуміння термінології, визначено сфери можливих гібридних загроз: кібербезпека, критична інфраструктура, захист фінансової системи від незаконного використання та зусилля з протидії насильницькому екстремізму та радикалізації, сфера охорони здоров'я, космічний та морський простори. 3) Основна відповідальність у боротьбі із гібридними загрозами була покладена на держави-члени, але в тих випадках, коли загрози виходять за їх кордони та стосуються організації – відповідальність покладена на Комісію, Верховного представника і новостворені органи: HFC, East Stratcom, Горизонтальна робоча група, Центр передового досвіду для протидії гібридним загрозам. 4) Всі зазначені документи були відповідями ЄС, зокрема Комісії на зовнішні загрози: хімічні, біологічні, радіологічні та ядерні, кібербезпеку (Документ 2018 р.), дезінформацію під час пандемії COVID-19 (Стратегія 2020 р.). 5) У всіх проаналізованих документах була підтверджена важливість, особливість та багатогранність співробітництва з НАТО і розширення взаємодії з однодумцями в багатонаціональних форматах, таких як G7.

[32] Ibid.
[33] Ibid.
[34] Ibid.

References

Analitychna dopovid' do Shchorichnoho Poslannya Prezydenta Ukrayiny do Verkhovnoyi Rady Ukrayiny «Pro vnutrishnye ta zovnishnye stanovyshche Ukrayiny v 2017 rotsi» [Analytical report to the Annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine "On the Internal and External Situation of Ukraine in 2017"]. (2017). Kyiv: NISD. Retrieved from: https://cutt.ly/GUY2Tof [in Ukrainian].

Bajarūnas, E. Keršanskas, V. (2019). Hybrid threats: Analysis of their content, challenges posed and measures to overcome. *Lithuanian Annual Strategic Review,* 16 (1), 123–170. Retrieved from: https://cutt.ly/IUY2Zn3 [in English].

Bajarūnas, E. (2020, March 22). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*. DOI: https://doi.org/10.1177/1781685820912041 [in English].

Fesenko, V. (2016, Hruden′). Spyrat′sya vynyatkovo na vlasni syly i vzyaty vidpovidal′nist′ za rozvytok Ukrayiny na sebe [Rely solely on their own strength and take responsibility for the development of Ukraine]. *«Hibrydna» viyna Rosiyi – vyklyk i zahroza dlya Yevropy*. Kyiv, 24-25. [in Ukrainian].

Fiott, D. Parkes, R. (2019). Protecting Europe: The EU's response to hybrid threats. *European Union Institute for Security Studies (EUISS)*. Retrieved from: http://www.jstor.com/stable/resrep21143.4 [in English].

Hibrydna viyna: sutnist', vyklyky ta zahrozy: zbirnyk materialiv kruhloho stolu [Hybrid War: Essence, Challenges and Threats: Proceedings of the Round Table] (2021, 8 Lypnya). Kyiv: NA SBU. Retrieved from: https://academy.ssu.gov.ua/uploads/p_57_28744724.pdf [in Ukrainian].

Hibrydni zahrozy Ukrayiny i suspil'na bezpeka. Dosvid YES i Skhidnoho Partnerstva. Analitychnyy dokument [Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership. Analytical document] (2018). Za zahal′noyu redaktsiyeyu V.V. Martynyuka. Kyiv. Retrieved from: https://cutt.ly/gUY2GYR [in Ukrainian].

«Hibrydna» viyna Rosiyi – vyklyk i zahroza dlya Yevropy [Russia's "hybrid" war is a challenge and a threat to Europe]. (2016, Hruden′). Kyiv. Retrieved from: https://cutt.ly/QUY2bTV [in Ukrainian].

Lonardo, L. (2021). EU Law Against Hybrid Threats: A First Assessment. *European Papers*, 6 (2), 1075-1096. Retrieved from: https://cutt.ly/WUY2V2h [in English].

Mahda, E.V. (2015). *Hibrydna viyna: vyzhyty i peremohty* [Hybrid war: survive and win]. Kharkiv: «Vivat». [in Ukrainian].

Misyura, A., Palyvoda, V. (2018). *Kontseptual'ni pidkhody NATO ta ES do zabezpechennya stiykosti derzhavy i suspil'stva u sferi natsional'noyi bezpeky* [NATO and EU Conceptual Approaches to Ensuring the Sustainability of the State and Society in the Sphere of National Security]. Retrieved from: https://cutt.ly/fUY2Ian [in Ukrainian].

Palyvoda, V. (2020). *Pidkhody Slovachchyny do borot'by z hibrydnymy zahrozamy: analityka vid eksperta NISD* [Slovakia's approaches to combating hybrid threats: analyst from NISS expert]. Retrieved from: https://niss.gov.ua/en/node/3492 [in Ukrainian].

Palyvoda, V. (2020). *Tsentr protydiyi teroryzmu ta hibrydnym zahrozam pry MVS Ches'koyi Respubliky* [Center for Countering Terrorism and Hybrid Threats at the Ministry of Internal Affairs of the Czech Republic]. Retrieved from: https://cutt.ly/jUY2PEP [in Ukrainian].

Anastasiia Khmel,
Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
ORCID: https://orcid.org/0000-0002-4881-7859

Combating hybrid threats in the EU
(by the European Union regulation and legal framework)

Given the relevance of the topic of combating hybrid threats to Ukraine, the author draws attention to the regulatory framework of the European Union, which identifies hybrid threats and provides actions and measures to combat them. During 2016-2020, the main EU documents were adopted, which consider the definition of hybrid threats, identify areas where they can be implemented and identify measures to combat them: «Joint structure to combat hybrid threats – the response of the European Union» (2016), «Improving resilience and Strengthening Capabilities to Overcome Hybrid Threats» (2018), «Report on the Implementation of the Joint Program on Countering Hybrid Threats 2016 and the Joint Communication 2018 on Enhancing Sustainability and Strengthening Capabilities to Overcome Hybrid Threats "(2020), EU Security Strategy 2020. Hybrid threats include cybersecurity, critical infrastructure, protection of the financial system from illicit use and efforts to combat violent extremism and radicalization, health care, outer space and maritime space. The primary responsibility for combating hybrid threats lies with Member States, but in cases where threats go beyond their borders and affect the organization, the Commission, the High Representative and the newly established bodies are responsible: HFC, East Stratcom, Horizontal Working Group, Center for Excellence in combating hybrid threats. The analyzed documents demonstrate the importance of coordination of all EU institutions in the fight against hybrid threats. If the 2016 document is mostly about the Commission, the High Representative, HFC, INTCEN, EEAS, then the number of institutions involved in such countermeasures will expand the tasks for the Council of the EU, the European Parliament and various EU defense and intelligence agencies.

Key words: *EU, European Commission, High Representative, hybrid threats, disinformation, Hybrid Fusion Cell.*