Інформаційна довідка щодо діяльності Європейського Союзу у сфері протидії гібридним загрозам*

Анотація. *В інформаційній довідці аналізуються ключові підходи Європейського Союзу до протидії гібридним загрозам і зміцнення колективної стійкості у сфері безпеки. Проаналізовано нормативно-правові та інституційні механізми Європейського Союзу, включаючи стратегічні документи, інструменти координації й механізми реагування. Сфокусовано увагу на адаптації цих підходів в Україні для формування комплексної системи протидії гібридним загрозам.*

Ключові слова: *гібридні загрози, кібербезпека, критична інфраструктура, дезінформація, стратегічні комунікації, гібридні операції.*

Вступ

Гібридні загрози являють собою комплексну форму зовнішнього впливу, що поєднує військові та невійськові інструменти – від інформаційних операцій і політичного тиску до кібератак та економічного примусу, – з метою підриву держави, проти якої спрямовано відповідні заходи впливу. Особливість таких загроз полягає у прихованому характері дій, використанні внутрішніх вразливостей та створенні стратегічної невизначеності, що ускладнює своєчасне реагування й потребує системної міжвідомчої координації та стійкості національних інституцій.

Попри доволі часте вжиття терміна «гібридні загрози», зокрема у стратегічних безпекових документах, рекомендаціях міжнародних партнерів, аксіоматичне сприйняття його впливу на безпекову політику держави, цей термін невиправдано перебуває за межами української законотворчості і є предметом наукових пошуків[1].

Дослідницькою службою Верховної Ради України спільно з Інститутом Дунайського регіону та Центральної Європи (Австрія), Центром демократичної доброчесності (Австрія) організовано дискусію «Битва за ідентичність: осмислення війни Росії проти України»[2], під час якої за участі європейських партнерів обговорено ключові аспекти російської інформаційно-ідеологічної агресії, зокрема, використання історичних наративів як інструмента пропаганди та дезінформації, системне розповсюдження українофобських меседжів, а також сучасні підходи до розуміння гібридної війни та гібридних загроз.

У цьому контексті протидія загрозам українській ідентичності органічно узгоджується з положеннями стратегічних документів держави, що визначають засади національної безпекової політики. Російська агресія проти України має комплексний характер і виходить за межі традиційної військової площини, поєднуючи інформаційно-пропагандистські, політичні та

---

[1] Кресін О. Протидія гібридним загрозам в українському законодавстві. *Зовнішня торгівля: економіка, фінанси, право*. 2022. № 1. URL: https://www.researchgate.net/publication/361681661_Protidia_gibridnim_zagrozam_v_ukrainskomu_zakonodavstvi

[2] Дослідницька служба Верховної Ради України долучилася до дискусії «Битва за ідентичність: осмислення війни Росії проти України». URL: https://research.rada.gov.ua/print/76754.html

економічні інструменти впливу. Усвідомлення масштабів та механізмів цього багатовимірного тиску стає ключовою передумовою посилення суспільної і державної стійкості перед гібридними загрозами.

У цьому контексті вивчення практики Європейського Союзу (далі – ЄС) щодо законодавчого забезпечення протидії гібридним загрозам не втрачає актуальності, що й зумовило підготовку цієї інформаційної довідки.

Основна частина

Стратегія національної безпеки України «Безпека людини – безпека країни»[3] до складових гібридної війни відносить політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби. Відповідно до Стратегічного оборонного бюлетеня України, затвердженого Указом Президента України № 473/2021[4], однією зі стратегічних цілей розвитку сил оборони є розвиток інтегрованих оперативних (бойових та спеціальних) спроможностей сил оборони, що забезпечують їх стійкість, а також стримування і відсіч збройній агресії проти України, протидію гібридним загрозам.

В євроатлантичному просторі провідну роль у формуванні стійкості до гібридних загроз відіграє НАТО, яке має широкий спектр необхідних інструментів і механізмів. Починаючи з 2016 року, представники Альянсу послідовно наголошують, що гібридні загрози, спрямовані проти одного або кількох союзників, можуть стати підставою для застосування статті 5 Північноатлантичного договору. Попри це, на практиці зазначений механізм поки що не застосовувався[5].

НАТО є ключовим партнером Європейського Союзу у протидії гібридним загрозам, що зумовлено збігом стратегічних цілей та інтересів у цій сфері, зокрема щодо нейтралізації гібридних дій росії. У цьому контексті обидві організації прагнуть уникати дублювання зусиль і реалізовують комплементарний підхід, який ґрунтується на «тандемі» інструментів НАТО та ЄС[6].

У 2025 році Європейська Комісія представила ProtectEU – комплексну Стратегію Європейського Союзу у сфері внутрішньої безпеки[7], спрямовану на підтримку держав-членів та посилення спроможності ЄС забезпечувати безпеку громадян. Документ визначає стратегічне бачення та план дій на

---

[3] Стратегія національної безпеки України «Безпека людини – безпека країни». URL: https://zakon.rada.gov.ua/rada/show/392/2020#Text

[4] Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 17 вересня 2021 року № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121

[5] The EU's Approach Towards Countering Hybrid Threats: Conceptualisation and Capacity Building. URL: https://finabel.org/wp-content/uploads/2024/10/IF-PDFs-7-1.pdf#:~:text=In%20the%20Euro%2DAtlantic%20space%2C%20NATO%20plays%20the,defence);%20however%2C%20this%20has%20not%20happened%20yet

[6] Там само.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025DC0148&utm_source

майбутнє, включно з формуванням більш дієвої нормативно-правової бази, розширенням механізмів обміну інформацією та зміцненням міжінституційної та міждержавної співпраці. Окремий акцент зроблено на підвищенні стійкості до гібридних загроз шляхом захисту критичної інфраструктури, посилення кібербезпеки та протидії загрозам в онлайн-середовищі[8].

У Спільному повідомленні Європейського Парламенту та Ради «Спільна рамкова програма щодо протидії гібридним загрозам – відповідь Європейського Союзу» 2016 року[9] вказано, що хоча визначення поняття гібридної загрози варіюються і повинні залишатися гнучкими з огляду на їх мінливу природу, сама концепція таких загроз поєднує примусові та підривні дії, традиційні, а також і нетрадиційні методи (дипломатичні, військові, економічні, технологічні), які можуть застосовуватися державними або недержавними суб'єктами у скоординований спосіб для досягнення визначених цілей, залишаючись при цьому нижче порогу формального оголошення війни. Зазвичай гібридні загрози зосереджуються на використанні вразливостей об'єкта впливу і на створенні ситуації невизначеності, яка ускладнює ухвалення рішень. Масштабні дезінформаційні кампанії, включаючи використання соціальних мереж для контролю політичного дискурсу, радикалізації, вербування та спрямування проксі-акторів, можуть виступати інструментами реалізації гібридних загроз.

У законодавстві Європейського Союзу відсутнє нормативно закріплене визначення поняття проксі-актора. На основі узагальнення стратегічних, політичних та аналітичних документів ЄС, в яких використовується цей термін, слід зазначити, що проксі-актори – це недержавні суб'єкти, які діють у координації з державою-спонсором, під її контролем або за її підтримки з метою просування її політичних, економічних, воєнних або інформаційних інтересів. Їхня діяльність організована таким чином, щоб забезпечити можливість заперечення причетності та приховати безпосередню участь держави-спонсора у гібридних впливах чи втручанні.

Згідно з аналітичними матеріалами Європейського центру з протидії гібридним загрозам поняття «недержавний суб'єкт» є загальним та визначається як «суб'єкт, що бере участь у міжнародних відносинах і володіє достатніми можливостями для втручання, здійснення впливу або спричинення змін без будь-якої формальної належності до державних інституцій». Недержавні суб'єкти охоплюють широкий спектр учасників – від фізичних осіб до приватних корпорацій, гуманітарних і релігійних організацій, збройних формувань і владних режимів, які здійснюють контроль над певною територією та населенням[10].

---

[8] European Commission rolls out ProtectEU strategy to boost internal security, resilience against hybrid threats. URL: https://industrialcyber.co/regulation-standards-and-compliance/european-commission-rolls-out-protecteu-strategy-to-boost-internal-security-resilience-against-hybrid-threats/

[9] Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

[10] Countering state-sponsored proxies: Designing a robust policy. URL: https://www.hybridcoe.fi/wp-content/uploads/2025/02/web_Hybrid_CoE_Paper-23_rgb.pdf

Директива Європейського Парламенту та Ради (ЄС) 2022/2557 від 14 грудня 2022 року про стійкість критично важливих об'єктів та скасування Директиви Ради 2008/114/ЄС (далі – Директива 2022/2557)[11] інтегрує поняття «гібридної загрози» як частину «динамічного ландшафту загроз», поряд із терористичними загрозами і зростаючими взаємозалежностями між інфраструктурами й секторами. Наприклад, гібридна атака, що поєднує кібервтручання в енергомережу з фізичним пошкодженням інфраструктури, може паралізувати надання основних послуг, викликаючи економічні, соціальні чи безпекові наслідки на транскордонному рівні. Директива 2022/2557 наголошує на необхідності врахування гібридного характеру загроз для критично важливих об'єктів при впровадженні своїх стратегій посилення стійкості.

Гібридні операції – це системні дії, спрямовані на здобуття функціонального (політичного, економічного, енергетичного тощо) та/або рефлексивного (дезінформація, пропаганда) контролю над державою чи певною територією шляхом здійснення немілітарних, а також парамілітарних операцій. Останні передбачають використання терористів, найманців і злочинних угруповань для здійснення викрадень і вбивств із метою залякування населення, застосування саботажу й кібератак проти критичної інфраструктури, а також залучення радикалізованих місцевих груп до підривної діяльності проти цільової держави. Економічна складова є одним із основних інструментів гібридних операцій, спрямованих на досягнення контролю над державою без прямого застосування військової сили. Економічні механізми використовуються для поступового захоплення стратегічно важливих секторів економіки, насамперед об'єктів критичної інфраструктури, що забезпечують функціональне управління державними процесами. Такі об'єкти надалі можуть слугувати платформами для реалізації інших гібридних заходів, зокрема парамілітарних. Одним із найбільш поширених інструментів є укладення торговельних та інвестиційних угод, за допомогою яких гібридний оператор формує залежність ключових економічних або політичних суб'єктів у державі, яка стає об'єктом такої загрози. Така залежність створює можливість впливу на ухвалення ними рішень та використовується як важіль стратегічного тиску. Через злиття і поглинання встановлюється контроль над об'єктами критичної інфраструктури, а також засобами масової інформації. Крім того, корупція сприяє формуванню внутрішніх мереж лояльності, так званих «п'ятих колон», усередині цільової держави[12].

Дезінформація активізує локальну радикалізацію та підривну діяльність. Поширення певних наративів, часто у формі конспірологічних теорій або викривлених інтерпретацій подій, спрямоване на підтримку місцевих

---

[11] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[12] Best Practices in the whole-of-society approach in countering hybrid threats. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU%282021%29653632_EN.pdf?utm_source=chatgpt.com

екстремістських груп і створює ґрунт для формування підривного середовища всередині цільової держави. Розпалювання та підтримка протестних рухів через дезінформаційні кампанії, які згодом можуть бути інфільтровані провокаторами для провокування актів насильства, становить невід'ємну складову парамілітарного арсеналу гібридних операцій[13].

Кібератаки є невід'ємною складовою гібридних загроз не лише через їх технічну ефективність, але й через поєднання гнучкості, масштабованості та здатності до глибокої синергії з іншими засобами впливу. Використання цього інструмента дозволяє досягати стратегічних цілей, уникаючи відкритого конфлікту та зберігаючи при цьому прихованість, економічну вигоду й політичну гнучкість.

Директива Європейського Парламенту та Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (далі – Директива NIS 2)[14] встановлює інструменти, що мають на меті досягнення високого спільного рівня кібербезпеки в Європейському Союзі, зміцнення стійкості держав-членів до кіберінцидентів та забезпечення стабільного функціонування внутрішнього ринку ЄС. Ключовий внесок цієї Директиви полягає у встановленні уніфікованої політики кіберстійкості, управління ризиками та інформаційного обміну між державами-членами, що дозволяє нейтралізувати багатовекторні впливи, характерні для гібридних загроз.

Одним із базових інструментів є обов'язок держав-членів забезпечити стратегічне планування та координаційний механізм кіберзахисту на національному рівні шляхом ухвалення національних стратегій, визначення компетентних органів і створення органів управління кіберкризами. Україна взяла на себе зобов'язання гармонізувати національне законодавство з положеннями Директиви NIS2 у межах Плану Ukraine Facility, який передбачає фінансову підтримку ЄС для відновлення та реалізації ключових реформ[15].

У червні 2022 року Рада ЄС ухвалила висновки щодо Рамкових засад для скоординованої відповіді Європейського Союзу на гібридні загрози[16], якими передбачено створення Інструментарію протидії гібридним загрозам (Hybrid Toolbox), який може включати превентивні, кооперативні, стабілізаційні,

---

[13] Там само.

[14] Директива Європейського Парламенту та Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text

[15] Директива ЄС NIS2: що це таке, для яких потреб розроблена та для чого Україна її імплементує. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye

[16] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/?utm_source=chatgpt.com

обмежувальні та відновлювальні заходи, а також передбачає посилення солідарності та взаємної допомоги (Рис. 1)[17].

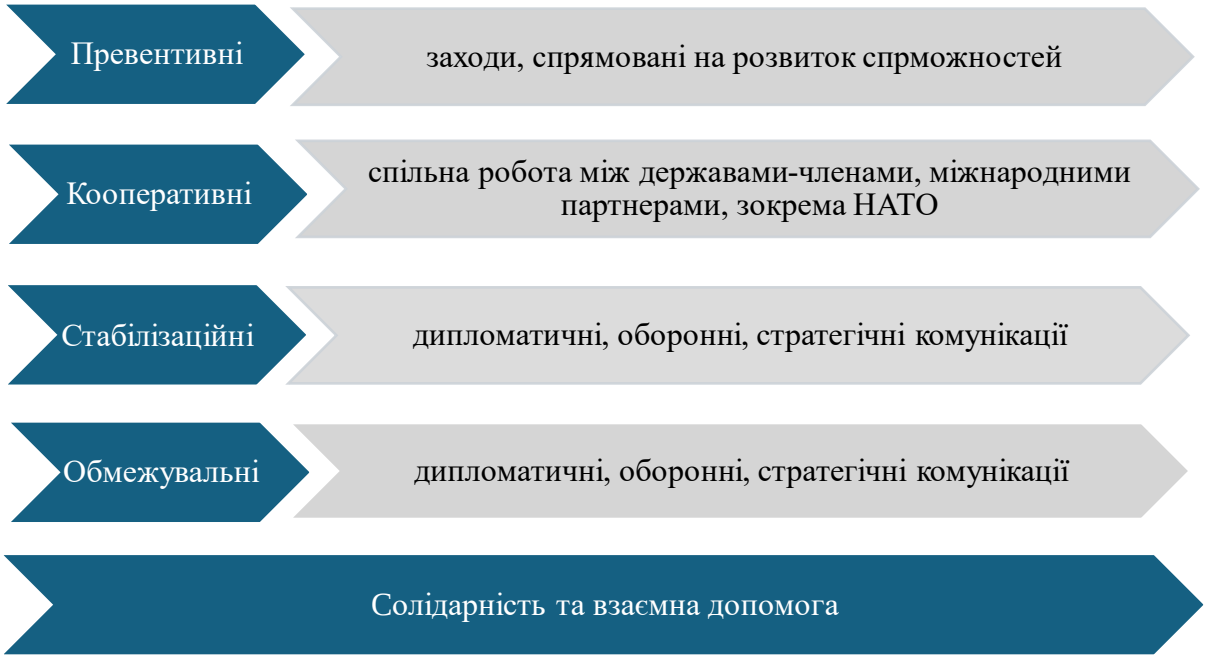

Рис. 1.

Підготовка комплексних оцінок гібридних загроз у державах-членах ЄС здійснюється Єдиною системою аналітичної розвідки (далі – SIAC), складовими якої є Центр розвідки та ситуаційного аналізу ЄС (EU INTCEN) і Розвідувальний директорат Військового штабу ЄС (EUMS INT). SIAC є механізмом, створеним для координації та інтеграції цивільної і військової розвідки з метою забезпечення ефективного реагування на безпекові загрози й виклики. Ця система забезпечує: раннє виявлення і оцінку загроз; підтримку стратегічних рішень інституцій ЄС; підвищення ситуаційної обізнаності держав-членів[18]; інтеграцію розвідувальної інформації з різних джерел (національні служби, відкриті джерела, супутникові дані)[19].

У 2024 році Європейський Союз ухвалив рішення про створення Груп швидкого реагування ЄС на гібридні загрози з метою надання короткострокової та спеціалізованої підтримки державам-членам і країнам-партнерам у реагуванні на відповідні загрози[20]. Ці групи передбачають поєднання профільних національних експертів та спеціалістів з ЄС, які

[17] Realising the EU Hybrid Toolbox: opportunities and pitfalls. URL: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf
[18] Handbook on CSDP. The Common Security and Defence Policy of the European Union. Fourth edition. URL: https://www.egmontinstitute.be/app/uploads/2021/06/CSDP-HANDBOO-4th-edition.pdf
[19] Impetus. Magazine of the EU Military Staff. 2019. Issue № 28. URL: https://www.eeas.europa.eu/sites/default/files/documents/eums_impetus_28_final_web.pdf
[20] Strengthening Europe's actions against hybrid threats: Setting up a proteus programme. URL: https://docs.ie.edu/GPC/3_AAFF_short%20CGP_Strengthening%20Europe%27s.pdf

діятимуть за принципом індивідуального реагування на конкретні ситуації та надаватимуть підтримку національним органам державної влади[21].

Висновки

Україні доцільно адаптувати європейський підхід до протидії гібридним загрозам, поєднавши безпекові, інформаційні та правові механізми в єдиній державній політиці. Важливим є нормативне закріплення поняття гібридної загрози, а також понятійного апарату у сфері протидії таким загрозам (гібридні операції, проксі-актор тощо) з метою підвищення правової визначеності та запровадження комплексної системи реагування.

Досвід ЄС демонструє ефективність міжвідомчої взаємодії, стратегічних комунікацій та розвитку спроможностей раннього попередження (запобігання), що має стати орієнтиром для України. Формування цілісної моделі протидії гібридним загрозам сприятиме зміцненню національної стійкості та посиленню інтеграції України до європейського безпекового простору. Тому питання протидії гібридним загрозам потребує розв'язання у законодавчому полі.

Дослідницька служба
Верховної Ради України

[21] Realising the EU Hybrid Toolbox: opportunities and pitfalls. 2022. URL: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf?utm_source