ПОЛІТИЧНІ ПРОБЛЕМИ МІЖНАРОДНИХ СИСТЕМ ТА ГЛОБАЛЬНОГО РОЗВИТКУ

УДК 327.88:327.7 (061.1ЄС)
DOI: https://doi.org/10.32782/2312-1815/2024-1-7

Голуб'як Наталія
ORCID: 0000-0001-6021-5482

Голуб'як Ігор
ORCID: 0009-0008-3999-1864

ГІБРИДНІ ЗАГРОЗИ ЯК ВИКЛИКИ БЕЗПЕКОВІЙ ПОЛІТИЦІ ЄС

Стаття присвячена питанням стійкості ЄС до гібридних загроз з інституційної, правової та соціальної точок зору. Автори намагаються окреслити особливості загальноєвропейського підходу до протидії гібридним загрозам і наголошують на потребі в лідерстві ЄС у встановленні стандартів інформаційної безпеки.

Основна мета дослідження полягає у з'ясуванні способів і методів ЄС із запобігання гібридним загрозам із метою забезпечення інформаційної безпеки. Серед поставлених завдань виокремлюються такі: розглянути особливості формування інформаційної безпеки в ЄС; виокремити понятійну специфіку «гібридних загроз» і зосередити увагу на аналізі інституційної спроможності ЄС щодо протидії гібридним викликам.

У першій частині статті розглядається стан формування інформаційної політики Європейського Союзу, а саме загальноєвропейські підходи та спеціалізовані структури захисту.

Друга частина дослідження присвячена визначенню поняття «гібридні загрози» та «протидія гібридним загрозам». Автори вказують на переважання «м'якого підходу» в межах політики ЄС, зосередженого на взаємодії та діалозі. Окремо звернено увагу на становлення інституційно-правової бази протидії гібридним загрозам і напрацюванню міжінституційної взаємодії із НАТО.

За результатами підсумовано актуальні критичні фактори вразливості, що підкреслюють необхідність проактивної політичної участі та виділення ресурсів з боку ЄС із метою реагування та попередження гібридних викликів і загроз.

Ключові слова: *інформаційне суспільство, інформаційна безпека, гібридні загрози, гібридні виклики, протидія гібридним загрозам, Європейський Союз.*

Вступ. На сучасному етапі важливе значення для міжнародної політичної системи мають такі фактори, як зміна геополітичного середовища після закінчення холодної війни; технологічна і правова вразливість, притаманна глобалізації та спільному ринку; постісторичний дух часу Європи, який не сприймає підривну діяльність, не кажучи вже про пряму військову агресію. У 1990-х роках Європа була здебільшого оточена країнами, що реформувалися або молодими демократіями, заклопотаними власними трансформаціями. Тепер же континент сусідить з амбітними потугами, які прагнуть поширювати як жорстку, так і м'яку силу в Європу. Багато з них співпрацюють з антисистемними силами в Європі, які можуть мати різні цілі, у тому числі поширення репресивних інстинктів і популістських ідеологій серед держав ЄС.

Отже, тоді як ворожі державні й недержавні державні суб'єкти вже давно застосовують гібридні методи проти ЄС, тривала гібридна війна Росії в Україні, а також її втручання у президентські вибори в США у 2016 році стали переломним моментом, викривши неготовність

і вразливість західних країн до цих загроз. Останніми роками ми стали свідками численних інших випадків втручання Росії у внутрішні справи країн ЄС, включно із втручанням у референдум щодо Brexit 2016 року, фінансуванням правих партій та ультраправих політичних партій у Франції, Угорщині та Німеччині; проведенням цілеспрямованих замахів на вбивство у Великій Британії та Німеччині тощо.

Технологічні зміни, оцифрування економіки та повсякденного життя в країнах ЄС, формування відкритого і взаємопов'язаного суспільства – усе це надало ворожим іноземним суб'єктам широкий спектр для впливу та втручання. Тож **актуальним** постає питання інформаційної безпеки, яка в Європейському Союзі вибудовується на наддержавному, національному й індивідуальному рівнях. Загалом важливість вивчення цього досвіду вагома для безпечного використання інформації в Україні та відповідності стандартам і вимогам *acquis communautaire*.

Основна **мета дослідження** полягає у з'ясуванні способів і методів ЄС із запобігання гібридним загрозам із метою забезпечення інформаційної безпеки. Серед поставлених **завдань** виокремлюються такі: розглянути особливості формування інформаційної безпеки в ЄС; виокремити понятійну специфіку «гібридних загроз» і зосередити увагу на аналізі інституційної спроможності ЄС щодо протидії гібридним викликам.

У науковій сфері ця проблематика знайшла відображення у працях як вітчизняних, так й іноземних учених, серед них варто відзначити напрацювання О. Твердохліб, С. Троян, Є. Таран, М. Копійки, Є. Тихомирової, Kalniete S. & Pildegovičs T., Gresse G.

Виклад основного матеріалу дослідження. Об'єднана Європа створила абсолютно нову, раніше не існуючу організаційну форму – мережеву державу (*network state*), яка намагається відповідати на сучасні виклики процесів глобалізації та регіоналізації. Формування єдиного інформаційного простору, інформаційна інтеграція європейських держав у межах ЄС здійснюються на основі концепції єдиної загальної інформаційної політики, що втілена в ідеології європейського співробітництва у сфері інформації та комунікацій [1, с. 431]. Виходячи із цього, була сформована так звана європейська специфічність політики [2], закладена в організаційній формі самого ЄС як наднаціонального рівня, побудованого на спільності інтересів держав-членів з урахуванням принципу субсидіарності.

На сучасному етапі європейські фахівці в галузі інформаційних систем, безпеки і стратегічного планування активно обговорюють проблеми, що виникають в умовах можливості застосування інформаційної зброї, тобто засобів спрямованого впливу на інформаційні ресурси ймовірного супротивника у військовий і мирний час. Для цього на практиці реалізуються плани організаційного та технічного забезпечення національної інформаційної безпеки, створюються підрозділи, призначені для відбиття «інформаційної агресії». Уряди беруть на себе роль координаторів міжвідомчих зусиль у цій сфері [3, с. 29].

Вирішуючи проблеми інформаційної спільноти щодо мережевої та інформаційної безпеки, Європейське Співтовариство розробило тристоронній підхід, що передбачає конкретні заходи інформаційної безпеки; захист конфіденційності інформації та даних; боротьбу з кіберзлочинністю й гібридними викликами. Отже, розуміючи важливість єдиної системи інформаційної захисту, Європейський Союз намагається організувати колективний і широкомасштабний підхід до забезпечення інформаційної безпеки як окремих держав – членів ЄС, так й об'єднання загалом [4]. Для цього створені спеціалізовані структури захисту: Європейське агентство з питань мережевої та інформаційної безпеки (ENISA); у структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю; Група співпраці NIS; мережа CSIRTS та інші.

Натомість конкретні цілі та заходи інформаційної безпеки формулюються у програмах і робочих планах інститутів ЄС, які передбачають необхідність пошуку спільних рішень

об'єднання європейських країн щодо інформаційного протиборства та визначають потребу в трансформації програми європейської інформаційної безпеки [5].

Однією з характерних особливостей останніх років є активне використання цілого спектра викликів і загроз міжнародній безпеці й інформаційному суспільству, яке має принципово нову якість і об'єднується поняттям «гібридні загрози». Обговорення навколо проблеми гібридних війн пов'язані з тим, що поряд із використанням звичайного комплексу загроз національній безпеці зростає роль невійськових викликів. Давайте звернемося до поняття «гібридні загрози», за яким закріпилися різні визначення і з яким конкурують інші терміни, такі як «нелінійна війна», «асиметричний конфлікт» і «підривна діяльність». Але, якщо коротко, «гібридні загрози» означають використання спонсорованих державою, але не офіційно афілійованих акторів, які не вдаються до фізичного насильства. Отже, основна мета – примусити об'єкт загрози до втілення стратегічних інтересів агресора.

Гібридні «трюки» використовувалися протягом всієї історії, починаючи з троянського коня, винайденого Одіссеєм, до шкідливого програмного забезпечення Trojan, написаного хакерами. Вважається, що навіть періоди миру є «гібридними», оскільки вони перериваються вбивствами, корупцією, шпигунством, дезінформацією, маніпуляціями й економічним тиском. Основині прояви гібридних загроз втілюються у фейкових новинах, інформаційній війні та маніпуляціях у соціальних мережах, але засоби використання державами нерозкритих і неатрибутованих активів для послаблення своїх супротивників виходять далеко за межі цих елементів [6].

Цифрова інфраструктура – від військового зв'язку, передавачів 5G і машин для голосування – дає змогу ворожим суб'єктам успішно отримувати доступ до все більшої кількості даних і розвідувальної інформації. Тож виникнення нових гібридних сутичок і постійне притягнення країн до інформаційної боротьби характеризують кібербезпеку як одну з невід'ємних елементів колективної безпеки країн і міжнародного суспільства.

Отже, «гібридні загрози» розглядаються як загальний термін, що охоплює цілу низку дестабілізувальних і синхронізованих цивільних і військових дій. Ці дії можуть передбачати кампанії з дезінформації, кібератаки, підбурювання до політичної або економічної корупції, впровадження агентів впливу, тиск на незалежні ЗМІ та скуповування критично важливої інфраструктури [7].

Крім того, із самого початку слід уточнити, що протидія гібридним загрозам є передусім компетенцією та відповідальністю країн-членів. На відміну від ЄС чи інших міжнародних організацій, національні уряди мають відповідний інструментарій, а саме «розвідувальні та контррозвідувальні органи (як цивільні, так і військові), силові служби (забезпечення громадського порядку та безпеки), засоби зв'язку з громадянами та можливості реагування на кіберінциденти. Водночас, хоча національна безпека належить до сфери життєво важливих інтересів кожної держави-члена, гібридні загрози часто виходять за межі кордонів, що залишає за ЄС важливу роль у підтримці стійкості держав-членів у тих випадках, коли їх реакція на національному рівні є недостатньо адекватною [8].

Старший політичний радник Європейської ради з міжнародних відносин Густав Грессел відзначає, що підвищена вразливість Європи до гібридних атак не є ризиком, притаманним технологічному прогресу і глобалізації: це питання вибору. Європа зупинилася на підході *laissez-faire* до цих питань, тобто залишається такою, що прагне до вирішення проблем через діалог, а не конфронтацію. Варіант рішучої відповіді є дуже незручним для громадськості та політиків у більшості країн ЄС. На думку дослідника, деякі країни – члени ЄС, які визнають гібридні загрози одним із головних пріоритетів, створили спеціальні підрозділи в уряді або міністерствах закордонних справ для координації реагування на гібридні загрози (це Швеція, Фінляндія, Польща, Литва та Іспанія). Цей список свідчить про особливе занепокоєння щодо Росії.

Однак найбільші країни ЄС, Франція та Німеччина, ще не зовсім засвоїли поняття гібридних загроз, але обидві країни шукають шляхи реагування на них, а такі країни, як Австрія, Угорщина та Італія, загалом не надто переймаються гібридними загрозами [6].

Якщо говорити про наднаціональний рівень, то частини апарату ЄС дуже активно працюють над питаннями протидії гібридним загрозам, але все ще бракує цілісного підходу до цих питань. За останні роки з'явилися нові комунікації, закони, стратегії, цільові групи, фінансування та робочі групи країн-членів спрямовані на посилення безпеки та стійкості ЄС.

Інституційний вимір стійкості ЄС до гібридної війни має вирішальне значення для сигналізації про наявність політичної волі сприймати гібридні загрози серйозно. Тому потрібно спочатку розглянути кроки, які інституції ЄС зробили для розбудови своєї спроможності протидіяти гібридним загрозам.

Починаючи з 2014 року, ЄС ухвалив низку законодавчих актів у цій сфері, у тому числі в таких сферах політики, як енергетична безпека, захист критичної інфраструктури, захист даних, перевірка іноземних інвестицій і прозорість політичного фінансування.

Серед ключових ініціатив варто виділити схвалення Європейською Комісією ще у 2016 р. «Спільних принципів протидії гібридним загрозам – відповідь Європейського Союзу» (*Joint Framework on countering hybrid threats a European Union response*). До принципів, що стосуються механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз належать такі: захист об'єктів критичної інфраструктури, оскільки гібридні атаки можуть призвести до серйозних економічних або соціальних порушень; тісна взаємодія з НАТО, яка дасть змогу більш ефективно реагувати на гібридні загрози; служби зовнішніх зв'язків ЄС, спираючись на діяльність оперативних робочих груп, зобов'язані оптимізувати роботу лінгвістів, фахівців із соціальних медіа, які можуть проводити моніторинг інформації не з ЄС; забезпечити цілеспрямовану комунікацію для реагування на дезінформацію [9].

У тому ж році прийнято Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (*EU strategic communication to counteract propaganda against it by third parties*), яка виділяє перелік ключових проблем, а саме: стратегічні комунікації та інформаційна війна є не лише зовнішнім аспектом ЄС, але й внутрішнім; дезінформація та пропаганда трактуються як складові частини гібридної війни; «позитивні меседжі ЄС повинні бути наступальними (*offensive*), а не захисними (*defensive*)»; окремі аспекти інформаційного впливу Росії стосуються, зокрема, роботи окремих фундацій та органів (наприклад, «Росспівпраця»), телеканалів (RT), мультимедійних сервісів («Супутник»); проблему інформаційної війни з ІДІЛ та протидії дезінформації й радикалізації; потреба в моніторингу джерел фінансування антиєвропейської пропаганди; «розпалювання ненависті, насильства або війни не може ховатися за ширмою свободи висловлення думок» [9].

У червні 2018 року Комісія опублікувала Спільне повідомлення про підвищення стійкості та посилення спроможності протистояти гібридним загрозам. У подальшому новий стратегічний порядок денний ЄС на 2019–2024 роки чітко підкреслює стійкість до гібридних загроз і дезінформації як один із ключових напрямів майбутньої роботи. Нарешті, у грудні 2019 року Європейська Рада оприлюднила Висновки щодо протидії гібридним загрозам, які стали історичними завдяки тому, що в них є посилання на «можливість для держав-членів посилатися на положення про солідарність» (стаття 222 ДФЄС) (стаття 222 Договору про заснування Європейського Союзу) для вирішення серйозної кризи, спричиненої гібридною діяльністю [8].

Крім створення інституційних рамок і політико-правової основи для гібридної стійкості ЄС, кілька інституційних ініціатив принесли відчутні результати. У масштабах ЄС працюють два найбільш відомі центри протидії дезінформації – Оперативна робоча група зі стратегічних комунікацій ЄС (East StratCom Task Force) та Європейський центр передового досвіду для протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats) [10].

Важливим компонентом щодо стримування та протидії гібридним загрозам стало функціонування трьох сил StratCom під егідою Європейської служби зовнішньої діяльності (EEAS) – одна з них зосереджена на регіоні Східного партнерства, друга – на Західних Балканах, третя – на Південному сусідстві. Робота спецпідрозділів EEAS з викриття дезінформації, спрямованої проти ЄС у цих регіонах, є критично важливою, оскільки, надаючи допомогу країнам-кандидатам на вступ у розбудові стійкості, ЄС не лише зміцнює демократичні інститути, але й безпосередньо просуває власні безпекові інтереси [8].

Окремо слід відзначити міжінституційну співпрацю в розбудові стійкості до гібридних загроз, зокрема, на прикладі взаємодії між ЄС і НАТО, які є природними партнерами і діють на основі схожих стратегічних перспектив, оцінки ризиків та інтересів у протидії гібридним загрозам, особливо з боку Росії. Так, у липні 2016 року президент Європейської Ради, президент Європейської комісії і генеральний секретар НАТО підписали спільну декларацію, у якій окреслили сім сфер співпраці, у тому числі зусилля з протидії гібридним загрозам.

Помітним зрушенням стало створення Європейського центру передового досвіду для протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats). Засновниками Центру стали 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Велика Британія, Іспанія, Польща, Естонія, Латвія і Литва. Ця структура під гібридними загрозами має на увазі, зокрема, поширення неправдивої інформації, атаки проти інформаційних систем, а також інші види атак за допомогою сучасних технологій. Загалом це ворожі дії, спрямовані на дестабілізацію держави без формального оголошення війни. Такі дії є скоординованими, синхронізованими та свідомо спрямованими на вразливість демократичних держав й інституцій. Нині Центр має три активні спільноти – гібридний вплив (на чолі з Великою Британією), уразливості та стійкості (на чолі з Фінляндією), стратегії та оборони (на чолі з Німеччиною) [9].

Крім інституційної адаптації до зростаючого потенціалу гібридних загроз, ЄС намагається використовувати регуляторні інструменти для обмеження поширення дезінформації, яка підриває стійкість суспільства, сприяючи поляризації та радикалізації, а також підриває довіру до державних інституцій. Розвиток онлайн-платформ ускладнив контроль потоків неправдивої інформації, тому в цифровому просторі досить актуальним питанням на сьогодні також є проблема наростаючої дезінформації, головним джерелом «виробництва» від інституційних джерел якої є Інтернет.

Під зростаючим тиском щодо протидії цій загрозі ЄС уперше випустив Кодекс практики для боротьби з дезінформацією у вересні 2018 року, який був визнаний першою світовою рамкою для саморегулювання, спрямованого на боротьбу з дезінформацією. Кодекс практики підписали соціальні мережі та партнери з рекламної індустрії. У грудні 2018 року цей крок було доповнено Планом дій ЄС щодо дезінформації, який був задуманий як проактивний захід для «захисту демократичних систем Союзу та боротьби з дезінформацією, у тому числі в контексті майбутніх європейських виборів» [9].

Висновки. У світі є необхідність загального розуміння визначення гібридної загрози, що потребує періодичної співпраці, ефективної політики в межах ЄС, так і налагодженої співпраці між ЄС і НАТО. Тож усім державам слід визначити їхні вразливі сторони, щоб усвідомити, які гібридні загрози апріорі могли бути використані їхніми противниками. Обмін наявним досвідом кожної з країн потрібно сформувати так, щоб співпраця принесла якомога більше продуктивних рішень із питань гібридних загроз і кібербезпеки.

Загалом політика ЄС у сфері кібербезпеки, незважаючи на явний прогрес, досягнутий останніми роками, усе ще не є повністю узгодженою, і їй бракує прозорості. Це проявляється як на регулятивному, так і на інституціональному рівні. У традиційному вимірі (так звана жорстка сила) бачення повної стратегічної автономії, пов'язаної з наявністю власних можливостей кіберзахисту, залишається нереалізованою. Держави-члени визнають необхідність зміцнення

своїх ресурсів, але не хочуть ділитися своїми можливостями. ЄС спрямований більшою мірою на так звану м'яку безпеку: посилення зовнішнього виміру політики, підвищення стійкості мереж і систем ІКТ до кіберзагроз, розробку можливостей та інструментів для реагування на кібератаки, ефективну співпрацю в боротьбі з кіберзлочинністю, просування стандартів і цінностей у кіберпросторі.

Отже, стійкість до гібридних загроз неможливо досягти без загальноєвропейського набору норм, які б забезпечували стандарти підзвітності та прозорості. Роль ЄС полягає у зміцненні стійкості до гібридної війни, має охоплювати все суспільство, а також сприяти міжнародному та міжвідомчому співробітництву і встановленню спільних стандартів для зменшення вразливостей.

Література:

1. Угрин Л. Інформаційна політика. Політологія: навч. енцикл. слов.-довід. для студентів ВНЗ I–IV рівнів акредитації / за наук. ред. д-ра політ. наук Н. М. Хоми [В. М. Денисенко, О. М. Сорба, Л. Я. Угрин та ін.]. Львів : Новий Світ-2000, 2014. С. 270.

2. Твердохліб О. С. Європейський підхід до розроблення інформаційної політики держави актуальні проблеми. *Економіка*. 2016. № 3 (177). С. 429-435. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ape_2016_3_51.pdf.

3. Троян С. Інформаційно-безпекова політика Європейського Союзу. Зовнішні справи : суспільно-політичний журнал. 2019. № 2/3. С. 28–32.

4. Таран Є. Політика забезпечення інформаційної безпеки у США та ЄС: досвід для України. Вісник Львівського університету. *Серія: Філософсько-політологічні студії. 2019*. Вип. 25. С. 170–175. URL: http://fps-visnyk.lnu.lviv.ua/archive/25_2019/25.pdf.

5. Копійка М. В. Стратегічні ризики інформаційної безпеки європейських країн. *Міжнародні та політичні дослідження*. 2019. Вип. 32. С. 85–102. URL: https://doi.org/10.18524/2304-1439.2019.32.173847.

6. Gresse G. Protecting Europe against hybrid threats. 2019. URL: https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf.

7. Hybrid COE. Countering disinformation: News media and legal resilience. Hybrid CoE Papers. 2019. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

8. Kalniete S., & Pildegovičs T. Strengthening the EU's resilience to hybrid threats. European View. 2021. 20 (1). P. 23–33.

9. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. *Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром*. URL: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf.

10. Тихомирова Є. ЄС: проекти з протидії сфабрикованим новинам. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2019. № 1 (5). URL: https://relint.vnu.edu.ua/index.php/relint/article/view/90.

References:

1. Uhryn, L. (2014). Informatsiina polityka. Politolohiia: navch. entsykl. slov.-dovid. dlia studentiv [Information policy. Political science: a textbook.] VNZ I–IV rivniv akredytatsii/za nauk. red. d-ra polit. nauk N. M. Khomy; [V. M. Denysenko, O. M. Sorba, L. Ya. Uhryn ta in.]. Lviv: Novyi Svit-2000. P. 270 [in Ukrainian].

2. Tverdokhlib, O. S. (2016). Yevropeiskyi pidkhid do rozroblennia informatsiinoi polityky derzhavy aktualni problemy [European approach to state information policy-making] *Ekonomika.* № 3 (177). P. 429–435. Retrieved from: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ape_2016_3_51.pdf [in Ukrainian].

3. Troian, S. (2019). Informatsiino-bezpekova polityka Yevropeiskoho Soiuzu [European Union policy in the field of information security]. *Zovnishni spravy : suspilno-politychnyi zhurnal*. № 2/3. P. 28–32 [in Ukrainian].

4. Taran, Ye. (2019). Polityka zabezpechennia informatsiinoi bezpeky u SShA ta YeS: dosvid dlia Ukrainy [Policy of providing information security in the US And EU: experience for Ukraine]. *Visnyk Lvivskoho universytetu. Seriia: Filosofsko-politolohichni studii.* №. 25. P. 170–175. Retrieved from: http://fps-visnyk.lnu.lviv.ua/archive/25_2019/25.pdf [in Ukrainian].

5. Kopiika, M. V. (2019). Stratehichni ryzyky informatsiinoi bezpeky yevropeiskykh krain [Strategic risks of information security of the european countries]. *Mizhnarodni ta politychni doslidzhennia*. № 32. P. 85–102. Retrieved from: https://doi.org/10.18524/2304-1439.2019.32.173847 [in Ukrainian].

6. Gresse, G. (2019) Protecting Europe against hybrid threats. Retrieved from: https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf.

7. Hybrid COE (2019). Countering disinformation: News media and legal resilience. Hybrid CoE Papers. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

8. Kalniete S., & Pildegovičs T. (2021) Strengthening the EUs resilience to hybrid threats. European View. 20 (1). P. 23–33.

9. Parshikova, A. (n.d.). Mizhnarodnyi dosvid protydii hibrydnym zahrozam: zakonodavche rehuliuvannia ta orhanizatsii z pytan stratehichnykh komunikatsii [International experience in countering hybrid threats: legislative regulation and strategic communications organisations]. *Informatsiina dovidka, pidhotovlena Yevropeiskym informatsiino-doslidnytskym tsentrom*. Retrieved from: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf [in Ukrainian].

10. Tykhomyrova, Ye. (2019). YeS: proekty z protydii sfabrykovanym novynam [EU: prospects for combated news]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*. № 1 (5). Retrieved from: https://relint.vnu.edu.ua/index.php/relint/article/view/90 [in Ukrainian].

Nataliia Holubiak, Ihor Holubiak. Hybrid threats as a challenge for EU security policy

This article focuses on the EU's resilience to hybrid threats from an institutional, legal and societal perspective. The authors try to outline the characteristics of a pan-European approach to countering hybrid threats and emphasise the need for EU leadership in setting information security standards.

The main objective of the study is to identify ways and means for the EU to prevent hybrid threats in order to ensure information security. Among the tasks set are: to consider the peculiarities of information security formation in the EU; to highlight the conceptual specificity of "hybrid threats"; and to focus on the analysis of the EU's institutional capacity to face hybrid challenges.

The first part of the article examines the state of formation of the European Union's information policy, namely common European approaches and specialised protection structures.

The second part of the study is devoted to the definition of "hybrid threats" and "countering hybrid threats". The authors point to the prevalence of a "soft approach" within EU policy, focusing on interaction and dialogue. Particular attention is paid to the establishment of an institutional and legal framework for countering hybrid threats and the development of inter-institutional cooperation with NATO.

As a result, authors summarise the current critical vulnerabilities that underline the need for proactive political engagement and resource allocation by the EU to respond to and prevent hybrid challenges and threats.

Key words: *information society, information security, hybrid threats, hybrid challenges, countering hybrid threats, European Union.*