

УДК 32.019.51

DOI <https://doi.org/10.32782/pdu.2022.4.36>

С.В. Чуб

здобувач кафедри публічного адміністрування
Міжрегіональної Академії управління персоналом,
<https://orcid.org/0009-0001-3703-9414>

МІЖНАРОДНІ НОРМАТИВНО-ПРАВОВІ ЗАСОБИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В УМОВАХ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

В статті автором проаналізовано низку нормативно-правових документів, які регулюють гібридні загрози в межах ЄС та НАТО і не тільки. Зазначено, що під гібридними загрозами варто водночас розуміти різницю між гібридною загрозою та гібридною війною. Хоча характер обох є однаковим, гібридна війна є більш масовим явищем, як у просторовому, так і часовому. Визначено, що гібридні загрози можуть бути «одноразовими заходами», але вони в свою чергу можуть передувати вже більш активним діям. Окрім того, гібридна війна включає також військову агресію, тоді як загрози цілеспрямованої військової атаки не передбачають (але й не виключають терористичні акції, збройні провокації тощо). Метою статті було визначено проаналізувати основні міжнародні нормативно-правові акти з протидії гібридним загрозам з акцентом їх імплементації в українську стратегію боротьби проти російського агресора. Акцент поставлено на документах створених ЄС, ООН та НАТО, як ключовими гравцями на міжнародній арені в питанні протидії гібридним загрозам. Наголошено, що розбудова міжнародної системи протидії гібридним загрозам відбулася вже на фоні військової агресії РФ проти України у 2014 р., таким чином, український досвід, на жаль, став передовим для побудови та законодавчого закріплення протидії відповідним загрозам з боку ймовірних агресорів. Разом з тим, країни ЄС та США більш оперативно оцінили власний потенціал та ступінь відповідних небезпек, нормативно закріпивши механізми протидії гібридним загрозам, саме тому використання подібного досвіду буде ефективним і для українського суспільства.

Ключові слова: гібридна загроза, гібридна війна, міжнародні нормативно-правові акти, імплементація, державне управління, національна безпека, механізми публічного управління.

Постановка проблеми. Гібридні загрози в реаліях сьогодення стали звичною нормою для світу. Поєднання різних типів атак створюють з одного боку ситуацію невизначеності, а з іншого – можуть нанести найбільш критичний вплив. Водночас, гібридні загрози знаходяться на периферії законності, тим самим визнання їх, як цілеспрямована ворожа акція у світлі міжнародного права залишається невизначеним. Водночас, хоча український досвід і підняв питання протидії гібридних загроз на міжнародному рівні, однак, міжнародні нормативно-правові засоби для протидії гібридним загрозам ще не розвинуті належним чином. Незважаючи на це, за останні десять років у нормативно-право-

вій площині міжнародних об'єднань була ухвалена низка нормативно-правових актів, які визначають сутність гібридних загроз та протидії ним у різних площинах. Відповідний досвід буде актуальним Україні в умовах протистояння проти РФ, адже врахування поглядів та практики ЄС, ООН, НАТО в сумі з українським досвідом дозволить більш ефективно протидіяти новим гібридним загрозам з боку агресора.

Мета статті – проаналізувати основні міжнародні нормативно-правові акти з протидії гібридним загрозам з акцентом їх імплементації в українську стратегію боротьби проти російського агресора. Акцент поставлено на документах створених ЄС, ООН та НАТО, як ключовими

гравцями на міжнародній арені в питанні протидії гібридним загрозам.

Аналіз останніх досліджень та публікацій. Тематика гібридних загроз і протидії ним стала досить актуальною у світовій науці після початку війни РФ проти України у 2014 р. Було видано багато статей, як в межах України, так і закордоном, з акцентом на події в Україні. Зокрема варто виділити дослідження С. Санс-Кабаллєро, М. Саарєлян, З. Гбур [856]. Проте, за умов повномасштабного вторгнення та акцентом на ці події ця тема досліджена не була.

Включення до небезпек національного суверенітету поняття «гібридності» відбулося вперше у 2005 р. для висвітлення стратегії Хезболли в Ліванській війні [8], проте світового розголосу та закріплення у свідомості кожного українця відбувся у 2014 р., унаслідок анексії низки українських територій з боку РФ.

Наразі досі немає чіткого розуміння поняття «гібридна загроза» та їх складової. Так, відповідно до позиції М. Саарєлян, гібридна загроза – це методи та інструменти, що використовуються окремими державними або недержавними суб'єктами для покращення власних інтересів, стратегій та цілей [5]. З. Гбур у свою чергу наголошує, що гібридна загроза – це будь-який противник, який одночасно та адаптовано використовує співвідношення звичайного озброєння, нерегулярну тактику, тероризм та злочинну поведінку в зоні бойових дій для досягнення своїх політичних цілей [8].

Щотижневий правовий часопис «Юридичний вісник України» розуміє гібридну загрозу, як будь-який противник, який одночасно та адаптовано використовує співвідношення звичайного озброєння, нерегулярну тактику, тероризм та злочинну поведінку в зоні бойових дій для досягнення своїх політичних цілей [9].

Згідно зі Стратегічною концепцією НАТО 2010 р., гібридні загрози – це «загрози, створені супротивниками, здатні одночасно використовувати звичайні та нетрадиційні засоби адаптивного переслідування своїх цілей [2].

Відповідно до офіційної позиції ЄС, гібридні загрози – це такі загрози, що впливають на вразливі місця та використовують

їх, щоб завдати шкоди нижче порогу відкритої агресії. Вони являють собою суміш примусової та підривної діяльності, звичайних і нетрадиційних методів, які використовуються скоординовано в багатьох сферах. Авторитарні режими дедалі частіше намагаються підірвати спільні демократичні цінності і поляризувати суспільства для власних цілей, використовуючи різні типи гібридної діяльності, такі як маніпулювання інформацією, кібератаки, закон, економічний примус або інструменталізація мігрантів [3]. Прикладами є перешкоджання демократичним процесам прийняття рішень шляхом масових кампаній дезінформації, використання соціальних медіа для контролю над політичним нарративом або для радикалізації, вербування та спрямування проксі-акторів.

Виходячи з вищезначеного, гібридна загроза – це складна стратегія або тактика, яка використовує комбінацію різних методів та засобів, щоб досягти політичних, військових, економічних або інших стратегічних цілей. Гібридні загрози можуть включати в себе різні елементи, такі як інформаційна війна, кібератаки, економічний тиск, підтримку нелегальних груп, дезінформацію та інші дії, що не обов'язково включають в себе військову агресію. Метою гібридних загроз може бути дестабілізація ситуації в інших країнах, вплив на їх політичний процес або отримання переваги в геополітичних конфліктах без прямого застосування військової сили. Такі загрози стають все більш актуальними у сучасному світі міжнародних відносин і вимагають комплексного підходу для їх виявлення та протидії.

Говорячи про гібридні загрози варто водночас розуміти різницю між гібридною загрозою та гібридною війною. Хоча характер обох є однаковим, гібридна війна є більш масовим явищем, як у просторовому, так і часовому. Так, гібридні загрози можуть бути «одноразовими заходами», але вони в свою чергу можуть передувати вже більш активним діям. Окрім того, гібридна війна включає також військову агресію, тоді як загрози цілеспрямованої військової атаки не передбачають (але й не виключають терористичні акції, збройні провокації тощо).

Варто також наголосити, що розбудова міжнародної системи протидії гібридним загрозам відбулася вже на фоні військової агресії РФ проти України у 2014 р., таким чином, український досвід, нажаль, став передовим для побудови та законодавчого закріплення протидії відповідним загрозам з боку ймовірних агресорів. Разом з тим, країни ЄС та США більш оперативно оцінили власний потенціал та ступінь відповідних небезпек, нормативно закріпивши механізми протидії гібридним загрозам, саме тому використання подібного досвіду буде ефективним і для українського суспільства.

Гібридні загрози породили серйозну проблему законності щодо законів війни, права на самооборону, легітимності превентивних заходів і використання контрзаходів у відповідь на цю непрозору наступальну тактику. Додатковий ризик гібридних загроз полягає в тому, що вони можуть змінити існуюче звичаєве міжнародне право в цих сферах шляхом перетлумачення правових норм в оманливий спосіб.

Гібридні операції постійно та таємно підривають здатність держав функціонувати. Якщо держава використовує гібридні можливості, вона діятиме всупереч своїм зобов'язанням згідно з міжнародним правом, непрозоро та всупереч принципу добросовісності. Гібридні загрози також суперечать принципу невтручання у внутрішні справи. Таким чином, хоч їм і не вистачає відкритої війни, гібридні загрози явно уникають ідеї мирного вирішення суперечок [6].

Відповідно до пункту 2 статей 8–11 Європейської конвенції з прав людини (ЄКПЛ), відповіді на гібридні загрози мають бути встановлені законом, переслідувати законну мету та бути необхідними для демократичного суспільства. Зауважимо, що у випадку широкомасштабних гібридних чи невійськових дій європейські держави завжди можуть застосувати на свою користь статтю 17 ЄКПЛ. Ця стаття забороняє зловживання правами і тісно пов'язана з принципом добросовісності в міжнародних відносинах.

Подібним чином, у разі надзвичайного стану в державі, стаття 15 тієї ж конвенції дозволяє державам-учасницям призупинити виконання своїх зобов'язань згідно з ЄКПЛ, за винятком застосування права на

життя, заборони тортур, рабства, смертної кари та подвійного покарання. небезпека, а також принцип *nulla poena sine lege* («немає покарання без закону»).

Власне НАТО були першими, хто законодавчо надав характеристику гібридним загрозам, проте, найбільш цілісна нормативно-правова система протидії гібридним загрозам наразі функціонує у ЄС, як міжнародній організації та власне країнах-членах, які входять до її складу. З 2016 р. Європейська Комісія разом із Верховним представником ЄС із закордонних справ і політики безпеки запровадила широкий спектр заходів для протидії гібридним загрозам у значній кількості сфер політики за допомогою Спільної рамкової програми 2016 р. щодо протидії гібридним загрозам – «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» [3].

Взагалі, у Стратегії визначено 21 заходи для боротьби Європейського Союзу із гібридними загрозам. Більшість відповідальностей у цьому контексті покладено на Комісію, Верховного представника, а також на Центр для аналізу гібридних загроз «Hybrid Fusion Cell» ЄС (далі – HFC). Цей центр був створений в рамках Центру розвідки та ситуації ЄС (далі – EU INTCEN) та Європейської служби зовнішніх дій.

HFC повинен отримувати, аналізувати і обмінюватися конфіденційною інформацією, а також інформацією з відкритим доступом, яка стосується показників і попереджень щодо гібридних загроз від різних зацікавлених сторін у EEAS, включаючи представництва ЄС, Комісії та агентства ЄС, а також від держав-членів. Зі свого боку, Європейська Комісія повинна забезпечувати зв'язок з існуючими національними та європейськими органами. Цим документом пропонується державам-членам ЄС створити національні контактні пункти для оцінки гібридних загроз з метою співпраці та безпечного зв'язку з HFC ЄС [3; 10, с. 94–95].

Документом було визначено, що для ефективною протидії гібридним загрозам необхідно звернути увагу на потенційну вразливість ключових інфраструктур, ланцюгів постачання та суспільства. Такими галузями були визнані: енергетика (диверсифікації джерел енергії та

просування стандартів безпеки та безпеки для підвищення стійкості ядерної інфраструктури); безпека транспорту та мережі постачання (комплексно вирішувати проблеми безпеки на морі, включаючи протидію гібридним загрозам, шляхом міжгалузевої співпраці між цивільними та військовими особами для захисту критично важливої морської інфраструктури, глобального ланцюга поставок, морської торгівлі та морських природних та енергетичних ресурсів); космос (налагодження безперервного супутникового зв'язку).

Реалії першого року війни продемонстрували відсутність законодавчої підготовки при виникненні подібних кризових ситуацій. Тому акцент на вже наявних прописаних нормах міжнародного права та їх часткова імплементація в українську нормативно-правову сферу має забезпечити Україну від гібридних загроз або принаймні бути готовою реагувати на них та наслідки, які завдають подібні загрози.

Повертаючись до вищезначеного документу, було регламентовано безпеку у сфері кіберпростору, економіки, будівництва тощо. Окремим питанням визначена стратегія взаємодії з НАТО. Було визначено низку сфер для більш тісної співпраці та координації між ЄС і НАТО, включаючи ситуаційну обізнаність, стратегічну комунікаційну кібербезпеку та запобігання кризам і реагування. Наголошено, що ЄС та НАТО мають володіти однаковою інформацією щодо загроз, бо лише у взаємодії робота буде більш ефективною. Українська нормативно-правова сфера також має прописати у документах, які регламентують роботу з НАТО (іншими організаціями) стратегію взаємодії з гібридними загрозами, враховуючи, що офіційно Україна наразі не є членом НАТО [3].

Окрім вищезначеного, ЄС щороку робить звіт про хід виконання Спільної рамкової програми 2016 р. протидії гібридним загрозам та Спільного повідомлення 2018 р. щодо підвищення стійкості і зміцнення можливостей протидії гібридним загрозам. На момент написання статті, було вже зроблено 6 відповідних звітів. Зокрема важливою темою останнього звіту була гібридна політика Кремля, їх атаки по дезінформації європейського суспіль-

ства у зв'язку з розв'язаною Москвою війною проти України [4].

В перспективі, подібні звіти мають стати традицією і для українського суспільства, але в умовах воєнного часу, на наш погляд це є недоречним, адже несе нові виклики системі національної безпеки. Водночас, має бути на державному рівні утворені відповідні комісії, в поза воєнний час можливо з наданням імен експертів, але в умовах війни, експерти мають лишатися інкогніто. Відповідна комісія мусила б оцінювати гібридні загрози (можливо навіть доречним є окремий орган). Звісно СБУ наразі займається відповідною діяльністю, але європейський досвід лише посилив би систему національної безпеки у протидії гібридним загрозам.

Також важливо звернути увагу на Стратегію безпеки ЄС ухвалену у 2020 р. На відміну від двох попередніх стратегій, а саме «Безпечна Європа в кращому світі» (2003 р.) і «Сильніша Європа. Глобальна стратегія зовнішньої політики та політики безпеки Європейського Союзу» (2016 р.), в цій стратегії приділено значно більше уваги гібридним загрозам. Зокрема, з чотирьох розділів Стратегії, частина друга під назвою «Боротьба з загрозами, що розвиваються» була приурочена саме гібридним загрозам.

Комісія та Високий представник у цій Стратегії висвітлили підхід ЄС до гібридних загроз, який об'єднує зовнішній і внутрішній аспекти у безперервний процес. Цей підхід охоплює широкий спектр заходів – від раннього виявлення, аналізу, інформування, підвищення стійкості та запобігання до кризового реагування та управління наслідками. Також передбачає подальше посилення співпраці у сфері розвідування з компетентними службами держав-членів через EU INTCEN, оптимізацію потоків інформації з різних джерел у країнах-членах та агентствах ЄС (ENISA, Європол, Frontex, Комісія, НФС) та забезпечення безперервної співпраці між ЄС і НАТО. Таким чином, Стратегія 2020 р. визначає підходи, які вже були розроблені в документах 2016 та 2018 рр.

Як вказує А. Хміль відповідно до Стратегії 2020 НФС 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 гібридних загроз НАТО та Центром передового досвіду з протидії гібридним загрозам [10, с. 98–99; 1].

Окремо хочеться згадати про таку гібридну загрозу, як прикордонний тиск, яка в першу чергу стосується сучасних відносин з Білоруссю. Загальновідомо, що Білорусь активно підтримує політику Кремля, надала плацдарм для першої хвилі атак на початку 2022 р., наразі підтримує армію РФ, проводячи з нею «навчання». Останнє власне і відносить до категорії прикордонного тиску, адже змушує відтягнути війська з більш вагомим плацдармів, адже невідомо чи відбудеться нова атака з боку цієї держави (окрім спроб проникнення російських ДРГ). Такі питання частково вже окреслені у договорі про функціонування ЄС, тому Україна має законодавчо визначити стратегії прикордонної політики стосовно держав-сусідів. Адже деякі з них підтримують ворожу нашій державі політику.

Тоді як ЄС активно займається у сфері протидії гібридним загрозам та їх досвід буде досить важливим для України, то стратегії ООН є менш вдалимими. З одного боку, саме ООН мусило б захистити Україну від гібридних атак Кремля, проте єдина прописана стратегія ООН – стратегія санкцій є недостатньо ефективною, адже відбувається підтримка агресора іншими державами та поступово в масштабах такої держави, як РФ, є потенціал для хоча й нетакого якісного, але все-таки заміника деяких санкційних продукцій.

Протягом десятиліть чотири Женевські конвенції 1949 року та два додаткові протоколи до них 1977 року забезпечували достатньо керівні принципи ведення звичайних війн через *jus in bello* (міжнародне право, що регулює поведінку під час війни). однак, у нинішньому контексті гібридних операцій діють закони війни розпливчасті, а їх застосування недостатньо чітке. Таким чином, ООН і Женевські

конвенції є неадекватними інструментами для деескалації конфліктів сірої зони.

Однією з основних причин цього є непрозорість діяльності, що відбувається в сірій зоні, а також регулярне залучення недержавних структур. Крім того, державний суверенітет ставиться під сумнів міжнародним правом прав людини. Як зазначив Руссо, «зміщення акценту в міжнародному праві з суверенітету на гуманітарні принципи створив розрив між миром і війною, який державні та недержавні актори використовують за допомогою заходів, окрім військових». Крім того, повага до закону, включно з Міжнародним правом прав людини, піддається постійному контролю з часів Другої світової війни. Хоча цей посилений легалізм, безсумнівно, є сильною стороною демократичних суспільств, в епоху соціальних мереж це також є складним завданням. Вигадуються численні неправильні тлумачення закону, і він також використовується як засіб оскарження дій опонентів або, навпаки, використовується для виправдання власних дій.

Деяко неповноцінними є і норми НАТО щодо протидії гібридним загрозам. З одного боку – напад на одну державу-члена НАТО є нападом на все НАТО. Але гібридні загрози досі певною мірою лишаються у сірій зоні, через що хоча і надається відповідна допомога країні-члену, але питання більш активного втручання може бути відхиленою.

Загалом можемо відзначити, що міжнародне право (а власне певні міжнародні організації) закріплюють поступово шляхи боротьби з гібридними загрозами, розуміючи, що у сучасному динамічному світі вони є невід'ємною складовою як відкритої, так і тіньової боротьби. Україна намагається активно використовувати юридичну площину у боротьбі із загрозами, зокрема це було продемонстровано зверненнями до міжнародних судів. Водночас, політика санкцій, яка наразі є найбільш активним засобом міжнародного сприяння у боротьбі із гібридними загрозами, активно застосовується у боротьбі проти російського агресора. Міжнародні спільноти, включаючи Європейський Союз і ООН, вживають різноманітні санкційні заходи проти РФ з метою вплинути на її поведінку та змінити агресивну політику [9].

Ці санкції включають в себе заморожування активів і обмеження видачі віз для окремих російських посадовців та компаній, які мають прямий зв'язок із гібридною агресією в Україні. Покладання фінансового та економічного тиску на РФ в теорії спонукає її до перегляду стратегії та може вимагати змін у її політиці. Але, підтримка останньої з боку низки інших держав робить санкцій не завжди ефективними.

Застосування санкцій стало певною мірою дієвим інструментом, оскільки воно визнано міжнародним співтовариством і базується на загальноприйнятих нормах міжнародного права. Це свідчить про готовність спільноти держав діяти разом у відповідь на гібридні загрози та підтримувати країни, що потерпають від агресії і маніпуляцій з боку РФ.

Окрім того, Україною наразі використовується міжнародна допомога, яка визнана більш як гуманітарною у міжнародному праві. Відповідна допомога вже сприяє відбудові деяких деокупованих територій.

Таким чином, незважаючи на триваючу невирішену дискусію щодо реальної необхідності визначення гібридних загроз, існує міжнародний консенсус щодо того, що гібридні загрози становлять зростаючу проблему безпеки. Міжнародні організації визнають існування гібридних загроз, поступово впроваджують їх у власні нормативно-правові акти, проте наразі гібридні загрози все ще залишаються сферою дій «сірої зони» міжнародного права та можуть тлумачитися по-різному у конкретному випадку. Держави, що застосовують гібридні методи атак, використовують невизначеність міжнародного права у відповідних сферах, тим самим виправдовуючи свої дії тим, що жодного порушення норм не відбулося. Водночас, сьогодні світова спільнота прагне локалізувати відповідний вакуум нормативно-правової сфери, окресливши міжнародні загрози та сфери протидії ним. Поштовхом для цього стала гібридна війна РФ проти України, розпочата у 2014 р. Проте найбільшого успіху на сьогодні досягли у поданій сфері лише ЄС, які ухвалили низку законів, комісій, здійснюють щорічні звіти. Решта міжнародних організацій наразі все ще знаходяться в стадії генези відповідного законодавства. Україна може активно використовувати наявний міжна-

родний нормативно-правовий досвід, адже незважаючи, що саме наша держава найбільше потерпала від гібридних загроз, ЄС більш детально окреслила їх різновиди та сфери, які потребують захисту, як результат, Україна не була готова ні в юридичній, ні в практичній площині до низки гібридних атак, скоєних РФ у 2022 р. Водночас, Україна може надати власний практичний досвід для побудови міжнародних стратегій боротьби з гібридними загрозами, які б стали орієнтиром для усіх демократичних держав у майбутньому.

Список використаної літератури:

1. 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. URL: <https://cutt.ly/7UUC4ao>
2. Countering hybrid threats URL: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en
3. Joint communication to the European parliament and the council. Joint Framework on countering hybrid threats a European Union response : JOIN/2016/018 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>
4. Joint staff working document : Sixth Progress 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*. Brussels, 2022. 33 p.
5. Saarelainen M. Hybrid threats – what are we talking about? *The European Centre of Excellence for Countering Hybrid Threats*. 2017. URL: <https://www.hybridcoe.fi/hybrid-threats-what-are-we-talking-about/>
6. Акімова Л., Лисачок А. Державне регулювання фінансово-економічної безпеки суб'єктів господарювання. ДП «Видавничий дім «Персонал». 2017. № 5. С. 16-28.
7. Гбур З. В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 97–99.
8. Гібридні загрози: чи вистоїть Україна? URL: <https://yvu.com.ua/gibrydni-zagrozy-chy-vystoyit-ukrayina/>
9. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). *Acta*

- de Historia & Politica : Saeculum XXI.* 2021/2022. T. III. C. 91–101.
10. Radchenko, O., Kovach, V., Radchenko, O., Kriukov, O., Sydoruk, L., Sharov, P., & Semenets-Orlova, I. (2021). Principles of natural capital preservation in the context of strategy of state environmental safety. In *E3S Web of Conferences* (Vol. 280, p. 09024). EDP Sciences.
 11. Semenets-Orlova, I. A., & Kyselova, Y. Y. (2018). Multidimensional management contemporary: generation of social meanings for a new collective identities. *Публічне урядування*, (4), 264–273.
 12. Semenets-Orlova, I. (2016). Osvita dlya demokraty'chnogo gromadyanstva/osvita z prav lyudy'ny'yak zasib formuvannya kul'tury'gromadyans' kosti [Education for Democratic Citizenship and Human Rights Education as a means of forming of the culture of citizenship]. *Civic competences in vocational education of civil servants and local government officials*, 66–87.
 13. Shmalenko, I., Yeftieni, N., & Semenets-Orlova, I. (2021, December). Impact of social media influencers on public policy and political discourse. In *International Conference on Social Science, Psychology and Legal Regulation (SPL 2021)* (pp. 88–93). Atlantis Press.
 14. Strigul, M., Khomeriki, O., Yahodzinskyi, S., Romanenko, Y., Semenets-Orlova, I., & Lyasota, L. (2019). Peculiarities of development and dynamics of economism and the commercialization of Ukrainian higher education.

Chub S.V. International regulatory and legal means of combating hybrid threats in the conditions of Russian aggression against Ukraine

In the article, the author analyzed a number of regulatory and legal documents that regulate hybrid threats within the EU and NATO and beyond.

It is noted that the difference between a hybrid threat and a hybrid war should be understood under hybrid threats at the same time. Although the nature of both is the same, hybrid warfare is a more massive phenomenon, both spatially and temporally. It was determined that hybrid threats can be «one-time measures», but they, in turn, can precede more active actions. In addition, hybrid war also includes military aggression, while threats of a targeted military attack are not foreseen (but also do not exclude terrorist actions, armed provocations, etc.). The purpose of the article was to analyze the main international legal acts on countering hybrid threats with an emphasis on their implementation in the Ukrainian strategy of fighting against the Russian aggressor. Emphasis is placed on the documents created by the EU, the UN and NATO, as key players on the international arena in the issue of countering hybrid threats. It was emphasized that the development of the international system for countering hybrid threats took place already against the background of the military aggression of the Russian Federation against Ukraine in 2014, thus, unfortunately, the Ukrainian experience has become advanced for the construction and legislative consolidation of countering the corresponding threats from the alleged aggressors. At the same time, EU and US countries have more quickly assessed their own potential and the degree of relevant dangers, having normatively established mechanisms for countering hybrid threats, which is why the use of similar experience will be effective for Ukrainian society as well.

Key words: hybrid threat, hybrid war, international legal acts, implementation, public administration, national security, mechanisms of public administration.