УДК 339.986:355.019
DOI: https://doi.org/10.31617/zt.knute.2021(118)02
JEL Classification: F51, O38, H12

КАЛЮЖНА Наталія
д. е. н., професор, професор кафедри світової економіки
Київського національного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
E-mail: n.kalyuzhna@knute.edu.ua
ORCID: 0000-0003-0513-705X

ІНТЕНСИВНІСТЬ ГІБРИДНИХ ЗАГРОЗ НАЦІОНАЛЬНИМ ЕКОНОМІКАМ

Обґрунтовано, що високий руйнівний потенціал гібридних загроз потребує визначення критеріїв інтенсивності їхнього впливу на національну економіку з метою подальшого оцінювання ризиків реалізації загроз для держави-об'єкта гібридної агресії. Інтерпретовано взаємозв'язок базових понять ризикології у контексті дослідження соціально-економічних процесів. На підставі визначення специфіки гібридних загроз систематизовано їхні ключові характеристики та структуровано деструктивний вплив на національну економіку. Доведено, що ескалація гібридних загроз для економічно слабких та уразливих держав до рівня реальної небезпеки є практично невідворотною, якщо їхні інтереси конфліктують з амбіціями провідних геополітичних акторів.

Ключові слова: гібридна загроза, небезпека, ризик, деструктивний вплив, ескалація, критерій, інтенсивність, ймовірність.

Постановка проблеми. Трансформація сучасних обрисів міждержавних конфліктів відбувається у напрямі набуття ними ознак гібридизації з можливістю ескалації до форми гібридної війни, яка надає змогу досягати очікуваних результатів за умов мінімізації військового втручання або навіть його відсутності. На відміну від очевидних загроз, що чинить національному суверенітету держави пряме військове втручання, гібридні загрози важко піддаються ідентифікації та мають власну логіку виникнення й ескалації. Ключем до розуміння джерел витоку й реалізації гібридних загроз є їхній розгляд як інструменту політико-економічного тиску, засобу реалізації геополітичних амбіцій провідних акторів світової політики з метою забезпечення національних економічних інтересів. Прихований характер ускладнює реагування держави-об'єкта гібридної агресії на її виклики, що може призвести до суттєвих негативних наслідків для розвитку національної економічної системи. Окрім того, до гібридних загроз важко застосувати механізми стримування та упередження, що зумовлює необхідність проактивного реагування на підставі ґрунтовної оцінки потенційного впливу гібридного протистояння на розвиток національної економіки.

Аналіз останніх досліджень і публікацій. Проблеми своєчасного виявлення гібридних загроз і розробка заходів щодо мінімізації

© Калюжна Н., 2021

ризиків їхньої реалізації перебувають у фокусі дослідження як закордонних [1–3], так і вітчизняних [4–7] науковців. Беззаперечним визнають фахівці першочерговість завдання ідентифікації ключових зон уразливості та асоційованих з ними ризиків у контексті вироблення ефективної стратегії протидії гібридній агресії [1, с. 8]. З метою ідентифікації гібридних загроз та оцінювання ступеня їхнього впливу на державу-об'єкт агресії активно використовується теорія управління ризиками, яка останнім часом отримала поширення у вітчизняному науковому середовищі, передусім – у контексті дослідження загроз національній безпеці держави в інформаційній площині.

Проблематика упередження ризиків і захисту кібернетичного простору України як найуразливішої з огляду на гібридні загрози сфери національної безпеки розглядалася у працях учених [8–11]. Зокрема, М. Алексєєв [8] використовує апарат ризикології для дослідження механізмів нейтралізації кібернетичних загроз і пропонує методику кількісного оцінювання інформаційних ризиків. Учений В. М. Телелим [9] розглядає модель оцінювання вразливості систем з критичною кібернетичною інфраструктурою через реагування на деструктивний вплив загроз. Динаміку ескалації деструктивного інформаційного процесу залежно від рівня інтенсивності інформаційних загроз досліджено авторами П. М. Сніцаренком, Ю. О. Саричевим, П. Д. Рогов [10]. Розгляд інформаційної сфери як ключового операційного простору гібридної війни є цілком виправданим, але водночас гібридні загрози характеризуються набагато більшим спектром дестабілізуючих заходів, які держава-ініціатор агресії застосовує в усіх можливих сферах протистояння. Високий руйнівний потенціал гібридних загроз потребує розвитку методичних підходів до визначення інтенсивності їхнього впливу на національну економіку незалежно від сфери прояву та специфіки певної сфери гібридного протистояння.

Метою статті є обґрунтування критеріїв інтенсивності впливу гібридних загроз на національну економіку задля подальшого оцінювання ризиків реалізації загроз для держави-об'єкта гібридної агресії.

Матеріали та методи. Методи аналізу та синтезу використано для визначення взаємозв'язку базових понять ризикології у контексті дослідження соціально-економічних процесів; математичне моделювання – для формалізації критерію інтенсивності деструктивного впливу гібридних загроз на національну економіку; графічне моделювання – для наочного представлення динаміки ескалації деструктивного впливу гібридних загроз. Дослідження виконано на основі наукових видань, матеріалів Державної служби статистики України та європейських аналітичних служб.

Результати дослідження. Оцінювання інтенсивності гібридних загроз потребує аналізу понятійно-категоріального апарату сфери дослідження з метою розгалуження сутності понять «загроза», «небезпека», «ризик». Наявна термінологічна невизначеність зумовлюється складністю введення чітких критеріїв для віднесення явищ і подій

політичної, економічної та соціальної природи до тієї або іншої категорії. Намагання конкретизувати сутність базових понять ризикології у контексті перебігу економічних процесів отримали значне поширення у сфері безпекознавства – у ході дослідження як економічної безпеки суб'єктів господарювання [12–14], так і держави [15; 16] або економічних систем загалом [17]. І навіть до уточнення термінологічного апарату вдаються науковці під час дослідження саме гібридних загроз розвитку національних економік [5; 6]. Така увага пояснюється необхідністю прогнозувати ймовірність настання деструктивних (зокрема гібридних) для системи економічної безпеки подій та оцінювати потенційні втрати з метою мінімізації негативних наслідків. Авторське розуміння сутності та взаємозв'язку понять ризику, загрози й небезпеки збігається з підходом, викладеним у праці Є. Рудніченко та проілюстрованим простим прикладом [12, с. 192]: якщо розглянути гіпотетичну ситуацію виходу човна в море, він перебуватиме у стані *потенційної небезпеки* (мінливе зовнішнє середовище), а в разі появи на його шляху айсберга виникає реальна *загроза*, тобто відбувається об'єктивізація небезпеки й її перехід у *реальну*. У цій ситуації команда човна свідомо вирішує прийняти *ризик* (спроба оминути айсберг, що може призвести до зіткнення) або уникнути його (пошук безпечнішого шляху). Результатом рішення продовжувати рух (свідоме прийняття ризику) можуть стати як здобутки (економія часу та ресурсів), так і втрати (руйнація човна й загибель команди). Залежно від результату прийняття рішення можна або подолати загрозу та повернутися у вихідний стан потенційної небезпеки, або настане реальна небезпека через непоборний характер загрози та / або невідповідну реакцію на її виникнення. Цікавим є той факт, що термін «ризик» у давніх варіантах сучасних мов означає близькі поняття: *risicare* (італ.) – лавірувати між скелями, *risquer* (франц.) – оминати скелю, тобто етимологічні коріння знаходяться в часах первісного мореплавства у прибережних водах, коли зіткнення зі скелею означало катастрофу судна [6, с. 21].

Як свідчить наведений приклад, ризик – це категорія, яка пов'язана з розумінням суб'єктом прийняття рішення його потенційних втрат. Ситуація ризику передбачає можливість оцінки ймовірності настання певних несприятливих подій та їхніх наслідків на основі статистичних даних або попереднього досвіду. Ризик є неусувною об'єктивною характеристикою функціонування та розвитку економічних систем в умовах невизначеності зовнішнього середовища, а результатом прийняття рішення щодо протидії впливу загрозливим факторам оточення (або навпаки, влучного використання сприятливої ситуації) можуть виявитися як здобутки, так й збитки. Щодо визначення ризику – уточнюючи трактування, яке розглянуте у праці Є. Рудніченко [12, с. 192], пропонуємо розуміти його як об'єктивно-суб'єктивну категорію, що пов'язана з певною мірою невизначеності результату внаслідок прийнятого рішення як реакції на загрозливу ситуацію та вимірюється ймовірністю подальшого несприятливого розвитку подій.

Повертаючись до прикладу з виходом човна в море, бачимо, що ситуація ризику є наслідком виникнення об'єктивізованої загрози (айсберг), що робить потенційну небезпеку реальною, та вимагає реакції у вигляді прийняття ризику або його уникнення. Можна погодитися з науковцями, які вважають, що загроза – це причини, явища, події, умови, які можуть перешкоджати досягненню цілей та завдань суб'єкта господарювання [13], наслідок небезпеки як об'єктивізований чинник потенційно негативної дії [12], небезпека на стадії переходу з потенційної можливості в дійсність [15]. Власне поняття небезпеки пропонуємо розуміти як можливі (*потенційна небезпека*) або дійсні (*реальна небезпека*) явища, події та процеси, які порушують рівновагу економічної системи, завдають шкоди її функціонуванню та призводять до негативних наслідків.

За умови запропонованого трактування сутності та взаємозв'язку базових понять ризикології (*рис. 1*), джерелом ризику для сталого функціонування й розвитку соціально-економічної системи та її незмінним атрибутом виступають *загрози*. Виходячи з розуміння загроз як обставин, що можуть виявитися причиною порушення стабільного перебігу соціально-економічних процесів, можемо констатувати їхній ймовірнісний характер: обставини (події, явища, умови тощо), що є загрозливими для системи, можуть бути *реальними* (такими, що вже відбулися) або *потенційними* (такими, що очікуються з огляду на тенденції розвитку подій).

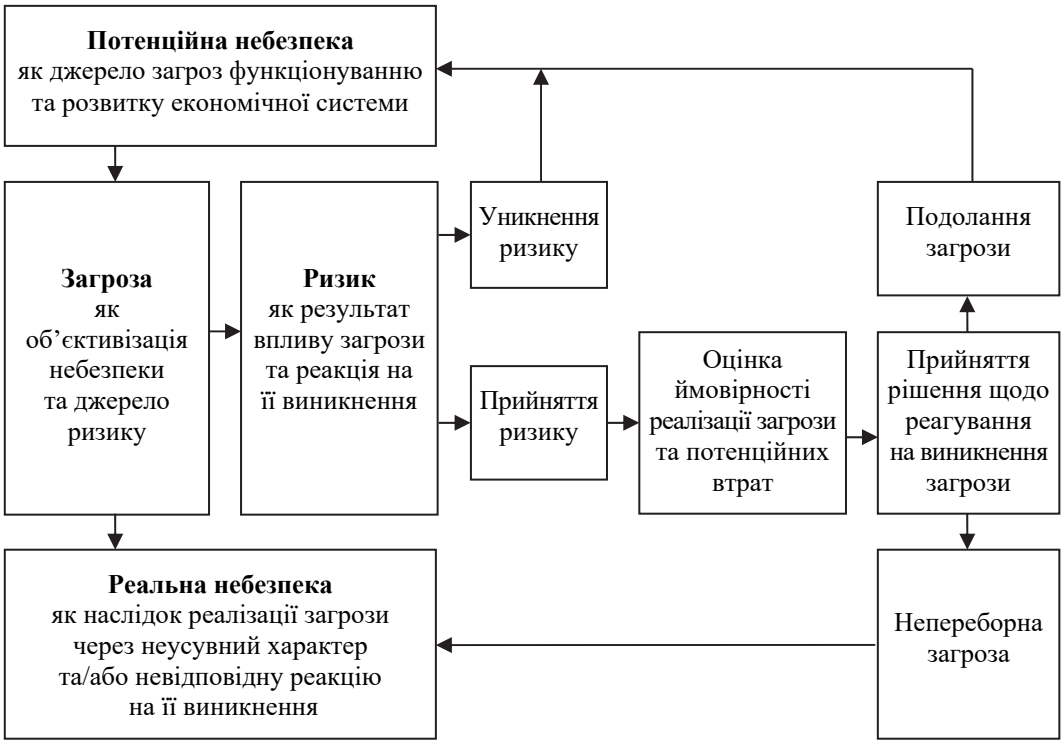

Рис. 1. Інтерпретація взаємозв'язку базових понять ризикології у контексті дослідження соціально-економічних процесів

Джерело: складено автором.

Погоджуючись з результатами, викладеними у праці [16], зазначимо, що залежно від характеру загрози (*реальна або потенційна*) мінімізація ризиків для стабільного функціонування будь-якої соціально-економічної системи залежить від адекватного оцінювання та використання можливостей протидії *(рис. 2*).

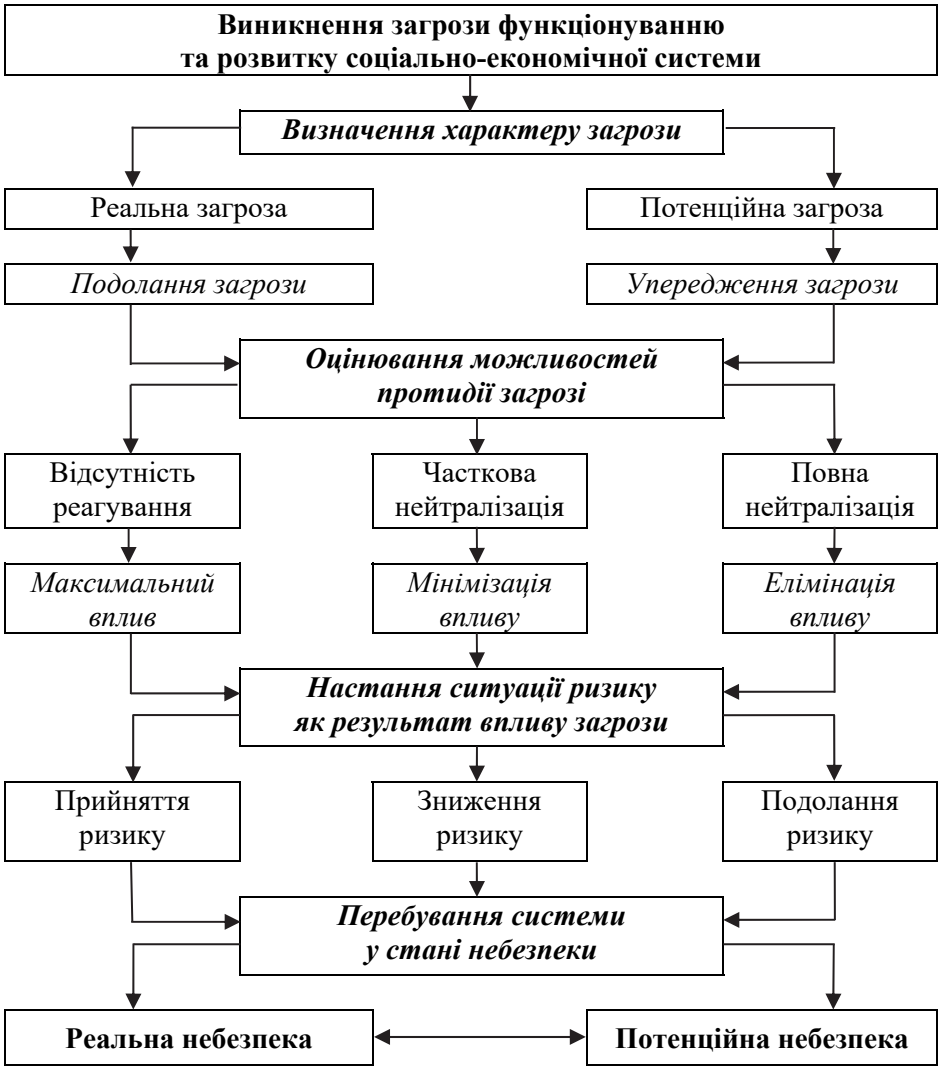

Рис. 2. Схема реагування на виникнення загрози функціонуванню та розвитку соціально-економічної системи

Джерело: складено автором за [16, с. 9–10].

Критеріями для вибору вектора поведінки є ймовірність реалізації загрози та потенційні збитки від її реалізації. Відповідно до результатів аналізу ситуації, суб'єктом управління може бути прийнято рішення про відсутність реагування, часткову або повну нейтралізацію загрози. З огляду на результативність застосованих заходів зазначимо, що загроза може бути або повністю нейтралізована (*елімінація впливу*), або усунута лише частково (*мінімізація впливу*). У разі відсутності належних управлінських дій загроза реалізується, стаючи джерелом ризику та об'єктивізованою небезпекою для розвитку соціально-

економічної системи. Тобто стан потенційної небезпеки, притаманний функціонуванню будь-якої відкритої соціально-економічної системи, перетворюється на реальну небезпеку як наслідок реалізації загрози через неусувний характер та / або невідповідну реакцію на її виникнення.

Гібридні загрози як актуальні виклики для національних безпекових систем мають свою специфіку, яку варто враховувати за формування системи заходів щодо реагування на їхнє виникнення та ескалацію. Поняття гібридних загроз (*hybrid warfare threats*), за визначенням науковців та аналітиків, це:

- продемонстрована противником здатність до одночасного застосування традиційних і нетрадиційних засобів залежно від потреби для досягнення своїх цілей [18];
- централізоване і контрольоване застосування різноманітних відкритих і таємних тактик, що впроваджуються військовими та невійськовими засобами [19];
- явище, що виникає внаслідок зближення та взаємозв'язку різних елементів, які в сукупності утворюють більш складну та багатовимірну загрозу [20];
- поєднання традиційних і нетрадиційних методів, які використовуються суб'єктами впливу для досягнення конкретних цілей, залишаючись на рівні нижче порогу формально оголошеної війни [21].

Вітчизняні науковці під час дослідження сутності та особливостей гібридних загроз найчастіше апелюють до їх трактування згідно зі Стратегічною концепцією НАТО від 2010 р. [18], у якій гібридна загроза визначається як продемонстрована противником здатність до одночасного застосування традиційних і нетрадиційних засобів залежно від потреби для досягнення своїх цілей [4–7; 11]. Достатньо «розмите» визначення гібридних загроз цілком виправдовується специфікою заходів гібридного протистояння як таких, що є необмеженими у просторі, часі та формах прояву, що безумовно ускладнює як процес ідентифікації гібридних загроз, так і розробки адекватних своєчасних заходів реагування на їхнє виникнення та ескалацію. Крім розмаїття використовуваних засобів гібридної агресії, варто звернути увагу й на синхронність їхнього використання у різних сферах (військова, економічна, інформаційна тощо) та високу ймовірність виникнення синергетичного ефекту від одночасної реалізації.

Синергетичний ефект (від грецьк. *synergetikos* – спільний, узгоджений, діючий) – це сумарний ефект, який полягає у тому, що за взаємодії двох або більше факторів їхня дія суттєво переважає ефект кожного окремого компонента у вигляді простої їхньої суми. Інтерпретація синергетичного ефекту в контексті дослідження гібридних війн полягає в тому, що комплекс (система) загроз, які створюються одночасно у ключових сферах гібридного протистояння, має набагато більшу руйнівну силу порівняно з простою сумою його складових, що обумовлює їхню особливу небезпеку для політико-економічної системи держави-об'єкта агресії. Так, Р. Тіеле (*R. Thiele*) ґрунтовно прописує, що

гібридна війна є конструкцією з неявно пов'язаних елементів, які насправді є частинами задуманої мозаїки [1, с. 6]. У своїй праці Бусол [5, с. 10] зауважує на високій ефективності використання практики комбінованих дій комплексного характеру з метою нарощування протестного потенціалу з боку суспільства, зокрема диверсій у критичній інфраструктурі, кібератаки, резонансні вбивства.

Окрім синхронності використання засобів гібридної агресії, що забезпечує ефект синергії (підсилення), важливою ознакою гібридних загроз є їхня спрямованість на експлуатацію найслабкіших та уразливих сторін супротивника. Для України такими слабкостями, на думку західних аналітиків, варто визнати [18]: слабке врядування та неефективні національні інститути, корупцію, брак довіри й підтримки безпекових та оборонних структур від населення, присутність значного відсотка російськомовного населення, критичний рівень залежності від російського імпорту й постачання енергоносіїв.

На підставі аналізу специфіки гібридних загроз і виходячи з розуміння гібридності як результату поєднання відмінних форм, можемо визначити такі *характерні риси гібридних загроз*: комбінація традиційних і нетрадиційних засобів з метою отримання синергетичного ефекту; адаптивність стратегії застосування; динамічність і всеосяжність; синхронізація та системність заходів; розмаїття форм і методів (дипломатичних, військових, економічних, технологічних, інформаційних тощо); одночасність запровадження у різних сферах; охоплення всіх сфер і процесів функціонування об'єкта гібридної агресії за умови орієнтованості на найуразливіші аспекти.

Повертаючись до проблематики оцінювання інтенсивності гібридних загроз на підставі теорії управління ризиками, варто зупинитися на їх ключовій особливості, яка полягає в балансуванні на межі війни та миру, що дає змогу гібридній агресії залишатися поза межами правового реагування з боку світової спільноти. Результатом комплексного використання державою-агресором гібридних інструментів є створення в державі-об'єкті агресії напруги (соціальної, політичної, економічної тощо) без проголошення відкритого конфлікту, що не виключає ймовірності його переходу в будь-який момент на вищий щабель ескалації. Ризик недооцінки повільної підготовки та оборонних заходів супротивника може призвести до програшу в непроголошеній війні та катастрофічних майбутніх наслідків для політико-економічної системи держави, проти якої спрямована гібридна агресія. З цього приводу О. Ю. Бусол ґрунтовно зазначає [5, с. 12], що феномен гібридних загроз полягає в тому, що за їхньої реальної наявності у непідготовлених до такого виду ведення війн держав створюється ілюзія відсутності війни, хоча насправді така ситуація є новим видом загроз національній безпеці. Будь-яка держава, яка перебуває у сфері політико-економічних інтересів провідних геополітичних акторів, може в певний момент виявитися об'єктом гібридної агресії під приводом захисту прав національних меншин, вирішення міжконфесійних протиріч, урегулювання етнічних конфліктів тощо. Окремо варто звернути увагу

на стрімке поширення гібридних загроз *в економічній площині*. Активізація тенденцій неопротекціонізму, посилення конкурентної боротьби на світових ринках, зростання ролі транснаціонального капіталу у світовій економіці збільшують уразливість економічно слабких держав і створюють додаткові загрози гібридного характеру для їхнього економічного суверенітету.

З огляду на зазначені категорії ризикології можна констатувати, що будь-яка держава в сучасному глобалізованому світі перебуває у стані потенційної небезпеки, оскільки може стати об'єктом торговельної дискримінації та стороною гібридного конфлікту в економічній площині. Перебування держави у стані потенційної небезпеки варто розглядати як найнижчий (найприйнятніший) рівень деструктивного гібридного впливу на національну економіку. Джерелом такого впливу можуть виявитися як актуальні тенденції у світовому економічному просторі (наслідки коронакризи, поширення політики імпортозаміщення, цінова нестабільність на сировинних ринках тощо), так і вади національної економічної системи (неефективне управління ключовими економічними активами, корупція, сировинна структура імпорту, енергозалежність економіки тощо). Якщо ці обставини використовує на свою користь держава – ініціатор гібридного протистояння, то гібридна загроза набуває об'єктивізованого характеру, та відбувається її проєкція на національну економіку держави-об'єкта.

За отриманими у праці [10, с. 90] результатами надалі пропонується структурувати ескалацію деструктивного впливу гібридних загроз на об'єкт (національну економіку) – від зародження до набуття агресивних форм (*рис. 3*).

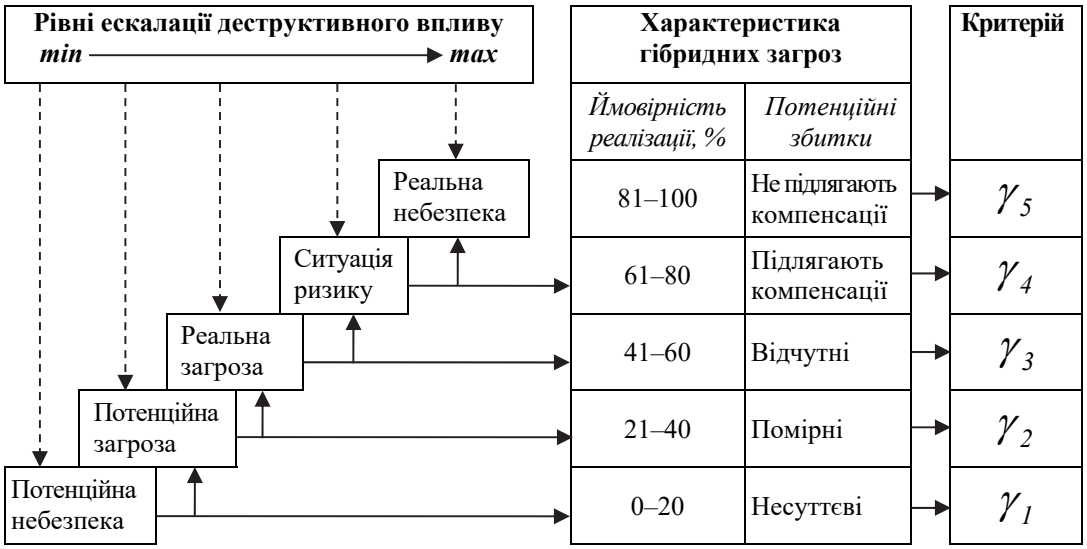

Рис. 3. Динаміка ескалації деструктивного впливу гібридних загроз на національну економіку

Джерело: складено автором.

Відповідно до запропонованого трактування сутності та взаємозв'язку базових понять ризикології (див. *рис. 1*) можуть бути визначені такі *рівні ескалації* деструктивного впливу гібридних загроз на національну економіку:

потенційна небезпека – виникнення у світовому економічному просторі та внутрішньому середовищі держави гібридних загроз як обставин (тенденцій, явищ, подій, процесів тощо), що можуть негативно позначитися на розвитку національної економічної системи;

потенційна загроза – розуміння джерел об'єктивізації зазначених гібридних загроз та очікування негативного впливу на стабільний перебіг економічних процесів у державі;

реальна загроза – настання негативних для розвитку національної економіки обставин у результаті об'єктивізації гібридних загроз;

ситуація ризику – стан невизначеності, що виникає внаслідок реалізації об'єктивізованих гібридних загроз і може призвести до суттєвих порушень у функціонуванні національної економіки;

реальна небезпека – перебування національної економіки у критичному стані як наслідок непоборного характеру гібридних загроз та / або невідповідної реакції на їхнє виникнення.

Узагальнювальною характеристикою деструктивного впливу гібридних загроз на національну економіку варто визнати рівень його інтенсивності γ_i, який передусім залежить від двох ключових характеристик – ймовірність реалізації загроз P_i та потенційні збитки Z_i:

$$\gamma_i = F(P_i, Z_i), \quad i = 1,..,5$$

Головне завдання в контексті упередження впливу гібридних загроз на національну економіку або принаймні мінімізації його наслідків очевидь полягає у визначенні кількісних значень критерію γ_i відповідно до рівнів ескалації деструктивного впливу. Першу характеристику його інтенсивності – ймовірність реалізації гібридних загроз – можна оцінити відсотковими значеннями (*див. рис. 3*). Рівню потенційної небезпеки, на якому перебуває будь-яка національна економіка в сучасному глобалізованому просторі, відповідатиме ймовірність реалізації гібридних загроз як несприятливих для її розвитку обставин у діапазоні від 0 до 20 %. Стан реальної небезпеки характеризуватиметься ймовірністю реалізації загроз на рівні 80–100 %, тобто критичний стан національної економіки є практично неминучим або вже справдився. Щодо другої характеристики деструктивного гібридного впливу – потенційних збитків, – їхня величина варіюється від незначних (рівень потенційної небезпеки) до таких, що не підлягають компенсації (рівень реальної небезпеки). Сполучення значень двох характеристик надає уявлення щодо рівня інтенсивності деструктивного впливу гібридних загроз на національну економіку на цей момент і дає змогу оцінити перспективи подолання негативних наслідків для її розвитку.

Показовим прикладом наростання гібридної загрози, остаточна реалізація якої матиме суттєві негативні наслідки для економіки України, є ситуація з будівництвом російського газогону «Північний потік – 2». Відповідно до запропонованого підходу можна виділити такі рівні ескалації деструктивного впливу загрози на стабільність енергетичної сфери держави та національну безпеку України загалом:

потенційна небезпека – зростання потреб в енергоресурсах з боку європейських країн унаслідок декарбонізації економіки в рамках «зеленого курсу», розвитку відновлювальної енергетики, скорочення видобутку на шельфі Північного моря, імплементації норм Третього енергетичного пакета;

потенційна загроза – початок прокладання Росією «Північного» й «Південного» потоків у 2010 р. з метою збільшення постачання газу до ЄС;

реальна загроза – укладання 22.02.2017 р. угоди між *Nord Stream* 2 *AG* і компанією *Allseas* щодо забезпечення потужностей для морського укладання труб газогону «Північний потік – 2»;

ситуація ризику – тривання будівництва протягом 2016–2021 рр. попри санкції США проти компаній-підрядників, позицію Данії, відмову у звільненні від Газової директиви ЄС, обмежену технічну спроможність РФ у прокладці труби та ін.;

реальна небезпека – підписання 21.07.2021 р. угоди між США та ФРН, що дає згоду завершити будівництво російського газогону.

Невідворотний характер загрози у вигляді завершення будівництва та введення в експлуатацію «Північного потоку – 2» може призвести до кризи у сфері енергетичної безпеки України через втрати транзитного потенціалу за відсутності пролонгації контракту з Газпромом після 01.01.2024 р. З часом втрата функцій транзитера та руйнація енергетичної інфраструктури можуть спровокувати ефект доміно в соціальній (зростання цін для населення внаслідок неможливості компенсації дефіциту на внутрішньому ринку, втрата робочих місць через закриття шахт) та зовнішньополітичній (додаткове послаблення суб'єктності, додаткові важелі тиску з боку Росії) сферах. Загалом ситуація з будівництвом російського газогону ілюструє високий рівень гібридності загроз в сучасному геополітичному просторі. У цьому випадку реалізація байпасних російських проєктів інфраструктурного нівелювання транзитної функції газотранспортної системи України («Північний потік – 2», «Турецький потік») відповідає національним інтересам держав-партнерів. Підписання угоди між США та Німеччиною робить завершення будівництва «Північного потоку – 2» практично невідворотним, навіть, попри загрози для України, що підтверджує високий рівень уразливості держав зі слабкою економікою та обмеженою зовнішньополітичною суб'єктністю у випадку, якщо їхні інтереси конфліктують з амбіціями провідних геополітичних акторів.

Висновки. Гібридні загрози як інструмент політико-економічного тиску та засіб реалізації національних інтересів потужних держав світу

мають високий руйнівний потенціал через їхній прихований характер та орієнтованість на найуразливіші сторони об'єкта гібридної агресії. Мінімізація впливу гібридних загроз потребує вироблення адекватної стратегії протидії на підставі оцінювання ймовірності реалізації загроз і розміру потенційних збитків від їхньої реалізації. Інтервальна оцінка критеріїв інтенсивності гібридних загроз дає змогу структурувати їхній деструктивний вплив на національну економіку від мінімального (потенційна небезпека) до максимального (реальна небезпека) рівня ескалації. Структуризація деструктивного впливу гібридних загроз створює підстави для оцінювання ризиків реалізації загроз для держави-об'єкта гібридної агресії залежно від рівня їхньої інтенсивності та подолання негативних наслідків для економіки держави-об'єкта гібридної агресії.

Подальші дослідження мають бути спрямовані на формалізацію лінгвістичних змінних, що описують потенційні збитки на кожному з рівнів ескалації деструктивного впливу гібридних загроз на національну економіку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Thiele R. Hybrid Threats – And how to counter them. ISPSW Strategy Series: Focus on Defense and International Security. 2016. No. 448. pp. 1-12. URL: https://css.ethz.ch/en/services/digital-library/publications/publication.html/eeb48a96-91d3-4d69-8992-576e25cf53d9.
2. Weissmann M. Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*. 2019. № 5(1). pp. 17-26. DOI: 10.2478/jobs-2019-0002.
3. Bajarūnas E., Keršanskas V. Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome. *Lithuanian Annual Strategic Review*. 2018. Vol. 16. pp. 123-170. DOI: 10.2478/lasr-2018-0006.
4. Тригуб О., Місяць М. Феномен гібридної війни в українській та зарубіжній політології. *Наукові праці. Політологія*. 2019. Вип. 312. Т. 324. С. 66-70.
5. Бусол О. Ю. Феномен гібридних загроз національній безпеці. *Юридична Україна.* 2020. № 4. С. 6-15. DOI 10.37749/2308-9636-2020-4(208)-1.
6. Мартинюк В. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Київ: Центр глобалістики «Стратегія XXI», 2018. 106 с. URL: https://geostrategy.org.ua/analityka/doslidzhennya/gibrydni-zagrozy-ukrayini-i-suspilna-bezpeka-dosvid-yes-i-shidnogo-partnerstva/zavantazhyty-pdf.
7. Акімова Л. М. Аналіз гібридних загроз економічній безпеці України: міжнародний досвід та українські реалії. *Інвестиції: практика та досвід*. 2018. № 22. С. 110-115. DOI: 10.32702/2306-6814.2018.22.110.
8. Алексєєв М. М. Методика кількісного оцінювання інформаційних ризиків із застосуванням онтології факторного аналізу. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 2 (69). С. 72-78. DOI: 10.33099/2304-2745/2020-2-69/72-78.

9. Телелим В. М., Даник Ю. Г., Зінченко А. О. Модель оцінювання вразливостей систем з критичною кібернетичною інфраструктурою. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2018. № 2 (63). С. 63-67. DOI: 10.33099/2304-2745/2018-2-63/63-67.
10. Сніцаренко П. М., Саричев Ю. О., Рогов П. Д. Методика оцінки рівня деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури держави. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій*. Київ, 2014. Вип. 1. С. 88-96.
11. Грищук Р. В., Жовноватюк Р. М., Носова Г. М. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2019. № 3 (36). С. 53-58. DOI: 10.33099/2311-7249/2019-36-3-53-58.
12. Рудніченко Є. М. Загроза, ризик, небезпека: сутність та взаємозв'язок із системою економічної безпеки підприємства. *Економіка. Менеджмент. Підприємництво*. *Збірник наук. праць*. 2013. № 25 (1). С. 188-195.
13. Колесніченко П.Т. Загрози, ризики та небезпеки в системі економічної безпеки підприємства. *Науковий вісник Херсонського державного університету. Серія: Економічні науки*. 2017. Вип. 24. Ч. І. С. 56-59.
14. Бойко І. В. Дефініції «ризик», «загроза», «небезпека» як об'єкти наукових досліджень у напрямі економічної безпеки підприємства. *Приазовський економічний вісник*. 2017. Вип. 5 (05). С. 94-97.
15. Олійник О. В. Сутність державної політики забезпечення інформаційної безпеки щодо джерел загроз та інших безпекогенних чинників. *Юридичний вісник*. 2016. № 1 (38). С. 71-78.
16. Барон І. Г. Алгоритм нейтралізації загроз економічній безпеці України. *Перспективні напрямки розвитку економіки, обліку, фінансів та права*: матеріали Міжнар. наук.-практ. конф., 23 серпня 2019 р. Полтава: ЦФЕНД, 2019. Ч. 1. С. 9-10.
17. Романчик Т. В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник НТУУ «КПІ»*. 2020. № 17. С. 257-267. DOI: 10.20535/2307-5651.17.2020.192866.
18. Active Engagement, Modern Defense. NATO's Strategic Concept 2010. URL: https://www.nato.int/cps/en/natohq/topics_82705.htm.
19. Countering Hybrid Treats. Food-for-thought paper. Working document of the European External Action Service of 13.05.2015. URL: https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.
20. Understanding Hybrid Treats. Briefing European parliamentary research service of June 2015. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.
21. Joint communication to the European Parliament and the Council Joint Framework on countering hybrid treats. A European Union response 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

Стаття надійшла до редакції 11.08.2020.

Kalyuzhna N. Intensity of hybrid threats to national economies.

Background. *In the context of growing tendencies to hybridize interstate conflicts, hybrid threats become especially important, which, in contrast to direct military threats, are difficult to identify and have their own logic of emergence and escalation. The hidden nature of hybrid aggression and the focus on the most vulnerable parties necessitate a proactive response of the object state based on a thorough assessment of the potential impact of hybrid confrontation on the development of the national economy.*

The ***aim*** *of the article is to substantiate the criteria for the intensity of the impact of hybrid threats on the national economy in order to further assess the risks of threats to the state-object of hybrid aggression.*

Materials and methods. *Methods of analysis and synthesis are used to determine the relationship of basic concepts of risk in the context of the study of socio-economic processes; method of mathematical modeling – to formalize the criterion of the intensity of the destructive impact of hybrid threats on the national economy; method of graphical modeling – to visualize the dynamics of escalation of the destructive effects of hybrid threats. The research was performed on the basis of scientific publications, materials of the State Statistics Service of Ukraine and European analytical services.*

Results. *It is substantiated that the transformation of modern interstate conflicts takes place in the direction of their acquisition of signs of hybridization, provided that it is understood as a process of using various means of pressure, mostly of a non-military nature. It is proved that the high destructive potential of hybrid threats requires the definition of criteria for the intensity of their impact on the national economy in order to further assess the risks of threats to the state-object of hybrid aggression. The author's interpretation of the relationship between the basic concepts of risk in the context of the study of socio-economic processes, which are arranged by the level of escalation in the following order: potential danger, potential threat, real threat, risk situation, real danger. Based on the definition of the specifics of hybrid threats, their key characteristics are systematized and the destructive impact on the national economy is structured. It is substantiated that the generalizing characteristics of the destructive impact of hybrid threats on the national economy should be recognized as the level of its intensity, which is determined by the probability of the threat realization and potential losses. It is proved that the escalation of hybrid threats to economically weak and vulnerable states to the level of real danger is almost inevitable if their interests conflict with the ambitions of leading geopolitical actors.*

Conclusion. *Interval assessment of the criteria for the intensity of hybrid threats allows structuring their destructive impact on the national economy from the minimum (potential danger) to the maximum (real danger) level of escalation. The structuring of the destructive impact of hybrid threats creates a basis for assessing the risks of threats to the state-object of hybrid aggression depending on the level of their intensity and overcoming the negative consequences for the economy of the state-object of hybrid aggression.*

Keywords: hybrid threat, danger, risk, destructive influence, escalation, criterion, intensity, probability.

REFERENCES

1. Thiele, R. (2016). Hybrid Threats – And how to counter them. ISPSW Strategy Series: *Focus on Defense and International Security, 448,* 1-12. Retrieved from https://css.ethz.ch/en/services/digital-library/publications/publication.html/eeb48a96-91d3-4d69-8992-576e25cf53d9 [in English].
2. Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security, 5(1),* 17-26. DOI: 10.2478/jobs-2019-0002 [in English].
3. Bajarūnas, E., & Keršanskas, V. (2018). Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome. *Lithuanian Annual Strategic Review*, (Vol. 16), (pp. 123-170). DOI: 10.2478/lasr-2018-0006 [in English].
4. Trygub, O., & Misjac', M. (2019). Fenomen gibrydnoi' vijny v ukrai'ns'kij ta zarubizhnij politologii' [The phenomenon of hybrid warfare in Ukrainian and foreign political science]. *Naukovi praci. Politologija – Scientific works. Politology,* (Vol. 324, Issue 312), (pp. 66-70) [in Ukrainian].
5. Busol, O. Ju. (2020). Fenomen gibrydnyh zagroz nacional'nij bezpeci [The phenomenon of hybrid threats to national security]. *Jurydychna Ukrai'na – Legal Ukraine, 4,* 6-15. DOI: 10.37749/2308-9636-2020-4(208)-1 [in Ukrainian].
6. Martynjuk, V. (2018). *Gibrydni zagrozy Ukrai'ni i suspil'na bezpeka. Dosvid JeS i Shidnogo partnerstva* [*Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership*]. Kyi'v: Centr globalistyky Strategija XXI. Retrieved from https://geostrategy.org.ua/analityka/doslidzhennya/gibrydni-zagrozy-ukrayini-i-suspilna-bezpeka-dosvid-yes-i-shidnogo-partnerstva/zavantazhyty-pdf [in Ukrainian].
7. Akimova, L. M. (2018). Analiz gibrydnyh zagroz ekonomichnij bezpeci Ukrai'ny: mizhnarodnyj dosvid ta ukrai'ns'ki realii' [Analysis of hybrid threats to Ukraine's economic security: international experience and Ukrainian realities]. *Investycii': praktyka ta dosvid – Investments: practice and experience, 22,* 110-115. DOI: 10.32702/2306-6814.2018.22.110 [in Ukrainian].
8. Aleksjejev, M. M. (2020). Metodyka kil'kisnogo ocinjuvannja informacijnyh ryzykiv iz zastosuvannjam ontologii' faktornogo analizu [Methods of quantitative assessment of information risks using the ontology of factor analysis]. *Zbirnyk naukovyh prac' Centru vojenno-strategichnyh doslidzhen' Nacional'nogo universytetu oborony Ukrai'ny imeni Ivana Chernjahovs'kogo – Collection of scientific works of the Military and Strategic Research Center of the National Defense University of Ukraine named after Ivan Cherniakhovskyi*. Kyi'v*, 2 (69),* 72-78. DOI: 10.33099/2304-2745/2020-2-69/72-78 [in Ukrainian].
9. Telelym, V. M., Danyk, Ju. G., & Zinchenko, A. O. (2018). Model' ocinjuvannja vrazlyvostej system z krytychnoju kibernetychnoju infrastrukturoju [Vulnerability assessment model for systems with critical cyber infrastructure]. *Zbirnyk naukovyh prac' Centru vojenno-strategichnyh doslidzhen' Nacional'nogo universytetu oborony Ukrai'ny imeni Ivana Chernjahovs'kogo – Collection of scientific works of the Military and Strategic Research Center of the National Defense University of Ukraine named after Ivan Cherniakhovskyi*. Kyi'v*, 2 (63),* 63-67. DOI: 10.33099/2304-2745/ 2018-2-63/63-67 [in Ukrainian].
10. Snicarenko, P. M., Sarychev, Ju. O., & Rogov, P. D. (2014). Metodyka ocinky rivnja destruktyvnogo informacijnogo vplyvu na ob'jekty informacijnoi' infrastruktury derzhavy [Methods for assessing the level of destructive information impact on the objects of state information infrastructure]. *Zbirnyk naukovyh prac' Vijs'kovogo instytutu telekomunikacij ta informatyzacii' Derzhavnogo universytetu teleko-munikacij – Collection of scientific works of the Military Institute of Telecommunications and Information Technologies of the State University of Telecommunications*. Kyi'v, (Vol. 1), (pp. 88-96) [in Ukrainian].

11. Gryshhuk, R. V., Zhovnovatjuk, R. M., & Nosova, G. M. (2019). Gibrydni zagrozy u kiberprostori: faktory vplyvu na pryrodu vynyknennja [Hybrid threats in cyberspace: factors influencing the nature of their occurrence]. Suchasni informacijni tehnologii' u sferi bezpeky ta oborony – *Modern information technologies in the field of security and defence, 3 (36),* 53-58. DOI: 10.33099/2311-7249/2019-36-3-53-58 [in Ukrainian].
12. Rudnichenko, Je. M. (2013). Zagroza, ryzyk, nebezpeka: sutnist' ta vzajemozv'jazok iz systemoju ekonomichnoi' bezpeky pidpryjemstva [Threat, risk, danger: the essence and relationship with the system of economic security of the enterprise]. *Ekonomika. Menedzhment. Pidpryjemnyctvo. Zbirnyk nauk. prac'. – Economics. Management. Entrepreneurship. Collection of scient. works, № 25 (I),* 188-195 [in Ukrainian].
13. Kolesnichenko, P. T. (2017). Zagrozy, ryzyky ta nebezpeky v systemi ekonomichnoi' bezpeky pidpryjemstva [Threats, risks and dangers in the system of economic security of the enterprise]. *Naukovyj visnyk Hersons'kogo derzhavnogo universytetu. Serija: Ekonomichni nauky – Scientific Bulletin of Kherson State University. Series: Economic Sciences,* (Issue 24, Part I), (pp. 56-59) [in Ukrainian].
14. Bojko, I. V. (2017). Definicii' «ryzyk», «zagroza», «nebezpeka» jak ob'jekty naukovyh doslidzhen' u naprjami ekonomichnoi' bezpeky pidpryjemstva [Definitions of «risk», «threat», «danger» as objects of scientific research in the direction of economic security of the enterprise]. *Pryazovs'kyj ekonomichnyj visnyk – Pryazovskyi Economic Herald*, *5 (05),* 94-97 [in Ukrainian].
15. Olijnyk, O. V. (2016). Sutnist' derzhavnoi' polityky zabezpechennja informacijnoi' bezpeky shhodo dzherel zagroz ta inshyh bezpekogennyh chynnykiv [The essence of the state policy of information security in relation to sources of threats and other safety factors]. *Jurydychnyj visnyk – Legal Bulletin, 1 (38),* 71-78 [in Ukrainian].
16. Baron, I. G. (2019). Algorytm nejtralizacii' zagroz ekonomichnij bezpeci Ukrai'ny [Algorithm for neutralizing threats to Ukraine's economic security]. *Perspektyvni naprjamky rozvytku ekonomiky, obliku, finansiv ta prava: materialy Mizhnar. nauk.-prakt. konf. – Promising areas of economic development, accounting, finance and law: materials of Intern. scient. and pract. conf.*, 23 serpnja 2019 r. Poltava: CFEND, (Part 1), (pp. 9-10) [in Ukrainian].
17. Romanchyk, T. V. (2020). Nebezpeka, zagroza, ryzyk: analiz terminologichnogo aparatu teorii' ekonomichnoi' bezpeky [Danger, threat, risk: analysis of the terminological apparatus of the theory of economic security]. *Ekonomichnyj visnyk NTUU «KPI» – Economic Bulletin of NTUU «KPI», 17,* 257-267. DOI: 10.20535/2307-5651.17.2020.192866 [in Ukrainian].
18. Active Engagement, Modern Defense. NATO's Strategic Concept 2010. Retrieved from https://www.nato.int/cps/en/natohq/topics_82705.htm [in English].
19. Countering Hybrid Treats. Food-for-thought paper. Working document of the European External Action Service of 13.05.2015. Retrieved from https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf [in English].
20. Understanding Hybrid Treats. Briefing European parliamentary research service of June 2015. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf [in English].
21. Joint communication to the European Parliament and the Council Joint Framework on countering hybrid treats. A European Union response 2016. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 [in English].