Київський столичний університет імені Бориса Грінченка

Факультет суспільно-гуманітарних наук

Кафедра політології та соціології

Допущено до захисту

Зав. кафедри Т.К.Пояркова

«___»_____ 2025 р.

УДК 355.48(581)"1979/1989"

Кваліфікаційна робота бакалавра

НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ (2014-2024 рр.)

рівень вищої освіти: перший (бакалаврський)

галузь знань: 05 «Соціальні та поведінкові науки»

спеціальність: 052 «Політологія»

Погромський Михайло Вікторович,
4 курс, ПОЛ-1-21-4.0д,
Факультет суспільно-гуманітарних наук

_____

Підпис

Науковий керівник:
Панасюк Леонід Валерійович
Доктор політичних наук, доцент

_____

Підпис

Київ 2025

ЗМІСТ

ВСТУП

Актуальність дослідження обумовлена необхідністю аналізу гібридних загроз національній безпеці України в умовах військової агресії Російської Федерації (2014-2024 рр.). Національна безпека є фундаментальною складовою існування держави, яка забезпечує її суверенітет, територіальну цілісність і стабільний розвиток. В умовах сучасного світу загрози національній безпеці набувають комплексного та гібридного характеру, що поєднує військові, політичні, економічні, інформаційні та кібернетичні виклики. Україна, яка з 2014 року зіткнулася з військовою агресією Російської Федерації, стала об’єктом масштабної гібридної війни. Ця війна виявила вразливі аспекти системи національної безпеки України, водночас стимулювавши значні трансформації у цій сфері. Гібридні загрози, що постають перед Україною, включають військові операції без офіційного оголошення війни, економічний тиск, кібернетичні атаки, використання інформаційної пропаганди та дезінформації для впливу на суспільну свідомість. Ці виклики ставлять перед Україною надзвичайно складні завдання, вирішення яких є критично важливим для збереження її суверенітету та інтеграції до європейського і світового співтовариства. Метою цього дослідження є аналіз гібридних загроз, які вплинули на національну безпеку України у 2014–2024 роках, оцінка існуючих механізмів протидії цим викликам та визначення стратегій їх удосконалення. Важливе значення в цьому контексті має вивчення досвіду інших держав, що успішно протидіяли гібридним загрозам, та його адаптація до українських реалій.

Метою цього дослідження є аналіз гібридних загроз з боку Російської Федерації, які вплинули на національну безпеку України у 2014–2024 роках, оцінка існуючих механізмів протидії ним викликам та перспектив їх удосконалення.

Завданнями роботи є:

- визначення змісту та основних елементів національної безпеки держави;
- систематизація основних підходів розуміння явищ «гібридні загрози», «гібридна війна»;
- аналіз гібридних загроз для України з 2014 по 2024 рік;
- аналіз державної політики у протидії гібридним загрозам:
- дослідження ролі інформаційної безпеки та стратегічних комунікацій у забезпеченні національної безпеки: як державні інститути реагували на інформаційні атаки та маніпуляції;
- аналіз зовнішньої політики України у контексті протидії гібридним загрозам та у зміцненні національної безпеки

Об’єктом дослідження є система національної безпеки України.

Предмет дослідження – гібридні загрози національній безпеці України та механізми протидії таким загрозам.

Ключові слова: гібридні загрози, конфлікт, комплексний підхід, вплив, російсько-українська війна, виклики.

Методи дослідження: системний підхід, аналіз і синтез, контент-аналіз, порівняльно.аналітичний метод.

Об’єм роботи складається з основного аналітичного матеріалу обсягом близько пятидесяти сторінок, висновків та списку використаних джерел і літератури.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1. Поняття національної безпеки: теоретичні засади.

У теоретичних засадах поняття національної безпеки зумовлено, перш за все, суспільно обмеженою формою яка поєднує в собі територію, мову, культуру і менталітет. Не приховуючи очевидне, слід зазначити, що безпека національного суверенітету - перш за все, явище по природі своїй багатогранний механізм, що базується одразу на декількох аспектах, що включають у себе такі види забезпечень як: правові, економічні, військові, інформаційні, соціальні, культурні, у деяких випадках навіть екологічні фактори.

Національна безпека відіграє найважливішу роль у працездатності і захищеності державних інтересів і підтримки її існування на міжнародній арені серед інших країн. У цілісності певної держави зацікавлена не тільки одна країна, а й багато інших, адже деструктив однієї держави несе за собою незворотню кризу, дестабілізацію, масштабні неврегулювання, конфлікти інтересів тощо.

Базовими ознаками національної безпеки є:

- Економічна самодостатність.
- Захист прав і свобод громадян.

- Гарантування громадського порядку та правопорядку.
- Обороноздатність країни та її здатність протидіяти загрозам.
- Захист суверенітету та територіальної цілісності держави.
- Забезпечення політичної стабільності

Слід зазначити, що невід'ємною частиною будь якого національного забезпечення є чотири основні підходи:

- Системний підхід - поєднує у собі конгломерат багатьох механізмів захисту і регулювання національної безпеки, завдяки чому утворюється один єдиний елемент.
- Ризик-орієнтований підхід - приділення усієї уваги на пошук, виявлення і передбачення загрози.
- Функціональний підхід - розподіл і делегування повноважень на різні рівні, такі як стратегічний, тактичний і оперативний.

-Суб'єктивно-об'єктивний підхід - ідентифікує об'єкт (громадяни і держава) та суб'єкт (економіка, ресурси та суверенітет)

Говорячи мовою наукових досліджень, можна привести пару прикладів з дослідників робіт, таких як О.В.Белова, який визначив що явище національної безпеки полягає у формах захисту як від внутрішніх загроз, так і від зовнішніх [2, с. 67].

В той же час інший дослідник національної безпеки, В.П. Горбулін прослідкував, що національна безпека складається з певних механізмів, які забезпечують, перш за все, незалежність, суверенітет та розвиток довготривалої перспективи держави в умовах глобалізації.

Виходячи з робіт обох дослідників, можна виокремити 6 основних стовпів, які забезпечують повний захист держави як від внутрішньої загрози, так і від зовнішньої.

1. Політична безпека - забезпечення територіальної цілісності.

2. Економічна безпека - запобігання кризам, сталий економічний вплив на інші держави, контроль над стратегічними галузями, стабільність, розподіл фінансової відповідальності.

3. Військова безпека - розвиток збройних сил, чітке військове самоврядування на всіх рівнях обороноздатності.

4. Соціальна безпека -гарантована добробуту громадян всіх верств суспільства, забезпечення культурного розвитку, надання пільг і структуровано надана соціальна допомога кожному громадянину.

5.Екологічна безпека - запобігання природних катаклізмів, слідкування екологічних норм, дотримання екологічної стабільності.

6.Інформаційна безпека - захист особистих даних кожного громадянина, контроль інформаційного трафіку, запобігання кібератакам з зовнішньої і внутрішньої сторони.

Слід також визначити основні загрози, які включають у себе два види:

внутрішня загроза і зовнішня.

до зовнішніх загроз входить:

- військова агресія сусідніх країн
- санкції, економічні війни
- транснаціональна злочинність і теракти
- втручання у внутрішні справи держави

До зовнішніх загроз входить:

- політична конфліктність у середині держави
- не нормалізоване державне управління
- корупція
- дезінформування і кібератаки

Спираючись на законодавчу частину такої теми як “Національна безпека”, можна звернути увагу на окремий пункт у Законі України “Про

національну безпеку України”, у якому наведені чітки принципи, механізми і напрями забезпечення національної цілісності. [11, с. 230]

Основною метою державного управління в області національної безпеки України є:

- розвиток Збройних сил
- стабілізація економічної ситуації
- мінімізація корупції
- забезпечення інфопростору
- налагодження міжнародних відносин на політичному рівні

Державна політика у сфері національної безпеки

Продовжуючи використовувати матеріал з законодавчих аспектів, слід згадати і про відповідні законодавчі акти, стратегічні документи та звіти, що підкреслюють науковий професіоналізм моєї роботи і розглядання такої теми як “Національна безпека України”

Значну долю внеску у розвиток та реалізацію політики національної безпеки відіграють

- Рада національної безпеки
- Служба безпеки України

-Міністерство оборони України

-Національна поліція

У той же час основними завданнями державного забезпечення політики у сфері національної безпеки є

- зміцнення обороноздатності та розвиток Збройних сил
- формування та вдосконалення економічної ідентичності
- підвищення ефективності державного саморегулювання
- розвиток міжнародного співробітництва.
- удосконалення механізмів національного стратегічного планування

Варто згадати, що історія України сама по собі складається з ряду історичних прикладів ефективного застосування сфер національної безпеки

1. Період козацтва.

Одна з найперших діяльності у сфері захисту територіальної цілісності України. Впровадження перших актів і використання обороноздатності на міжнародному рівні.

2. Акт проголошення незалежності України 1991 року.

Один з найвдаліших прикладів застосування механізмів забезпечення національної цілісності держави після розпаду Радянського союзу.

Відмовившись від ядерної зброї у 1994 році в обмін на гарантований захист з боку Росії, Англії і США ніс у собі дуже дорослий і серйозний характер для світового політичного гравця, який у майбутньому матиме незворотні наслідки.

3. Революція гідності 2013-2014

Один з найкривавіших етапів становлення української самоідентифікації - революція гідності у великих і маленьких містах України в 2013-2014 роках. Для кожного, хто спостерігав за подіями тих років, залишились на довгий час натхнення і бойовий настрій. Для всього світу Революція гідності стала прикладом не тільки як зберегти власну країну, а ще й автономності народа , готовність захищати цілісність своєї країни навіть в умовах повної дестабілізації.

4. Військовий конфлікт з Росією (2022 - ??)

Найяскравішим прикладом порушення суверенітету однієї країни іншою, є повномасштабне вторгнення Росії в Україну в лютому 2022 року.

Заподіявши всі елементи захисту для збереження української держави на всіх рівнях, були застосовані такі механізми військового спротиву як: Збройні сили, економічна підтримка армії і громадян, кібербезпека тощо.

Аналізуючи матеріал дослідження, можна зробити висновок, що багатовимірність такого явища як національна безпека завжди носила в собі важкий, розкладений на багато деталей комплекс, що працює виключно за допомогою правильного застосування кожного з механізмів використання національного забезпечення.

1.2. Гібридні загрози: сутність, типологія та інструменти.

Сутність гібридних загроз полягає, передусім, у комплексності спільних загроз для певної країни, які не несуть у собі відкритий збройний конфлікт або пряме збройне вторгнення, порушуючи при цьому територіальну цілісність держави, в той час як інші засоби ведення гібридних війн включають у себе не менш рушійні пошкодження і наслідки.

Поділити гібридні загрози можна на кілька типів

- Військові загрози

Застосування регулярних військ, найманців, угрупування. Пропагування і провокування до дій, що дестабілізують ситуацію всередині держави. Диверсійні дії і партизанські рухи.

- Інформаційні загрози

Психологічні кібератаки у соцмережах, ЗМІ, підрив довіри до уряду, розсилання провокативних або дезінформуючих повідомлень.

-Політичні загрози

Підтримка сепаратистських угруповань, маргінальних рухів і колаборанство. Маніпуляція виборчими процесами та політичними рішеннями, пропускання іноагентів у ряди політичних посадовців і приймачів політичних рішень.

-Економічні загрози

Застосування корупційних схем для дестабілізації економіки, будування бар’єрів стратегічних ресурсів та інфраструктурних проектів, тиск за допомогою санкційних маніпуляцій в області торгових відносин.

-Кібернетичні загрози

Шантажування особистими даними громадян або можновладців, присвоєння іншим особам конфіденційних даних, запуск вірусних програм у соцмережах.

В інструментах гібридних загроз чітко прослідковується комплексний, ніби командно відпрацьований механізм, що застосовує для досягнення своєї мети такі механізми:

- Засоби інформаційного впливу

Розповсюдження фейкових новин, дезінформують пости в соцмережах, у інформаційних кампаніях застосовуються боти або підкуплені коментатори, створення альтернативних наративів для маніпулювання суспільною думкою.

- Політичний тиск

Лобіювання підконтрольних політичних сил через інтереси громадян і суспільства.

Маніпулювання дипломатичним тиском та впливом на міжнародні організації. Фінансування та просування опозиційних рухів і партій.

- Економічний тиск

Активне ведення нелегального, тіньового бізнесу, підштовхування до уникнення податків, просування неліцензованого ринку , контрабанда.

- Кібернетичні засоби

Застосування троянів, поширення анти суверенних наративів, атаки на власні обігові засоби, хакерські атаки на ЗМІ, банківські системи на мас-медіа.

Приклади застосування інструментів для ведення гібридних загроз

Для підкріплення вищеописаних тез пропоную ознайомитись з прикладами застосування інструментів до кожного засобу

- Військова загроза

Підтримка сепаратиських угруповань на Сході України 2014 року:

Поширення на активне закликання до вступу до рядів військ ЛНР і ДНР.

Робота найманців з інших країн для дестабілізації і провокування української армії. - Економічні маніпуляції, шантажування газової промисловості

- Політична агресія

Втручання у процеси виборів і підтримка опозиційних блоків. Нарощування і агресії до діючої влади і прозелітизм (агресивне нав’язування політичних або релігійних поглядів)

- Кібернетичні атаки на енергосистему у 2015 році

Необхідно згадати і про застосування інструментів гібридної агресії на прикладах інших країн та застосування кібернетичних атак Росією по відношенню до США у 2016 році, який завдавав перешкод виборам, а саме: взлом Демократичної партії і її серверів, витік даних і шантажування оприлюдненням секретними матеріалами, атаки на банківські системи та соціальний рух громадян США.

Вплив економічної сили та фінансування політичних організацій і окремих груп, що поширюють опозиційні наративи. Активне дезінформування та використання соціальних мереж як інформаційного поля для особистих загарбницьких цілей, просування антиурядових ідей і агресивних та девіантних упереджень.

Не можна обійти стороною і 2008 рік у Грузії, коли Росія застосувала такі елементи гібридної агресії як:

- Вторгнення: введення військ і збройне вторгнення у Південну Осетію і Абхазію.
- Кібератаки на Грузинські урядові сайти
- Пропагування “грузинського геноциду”

На відміну від Грузії, по відношенню до Європейського союзу Росія

використовувала не тільки традиційні інструменти ведення агресивної політики та розпалювання гібридних загроз. Враховуючи потужний потенціал країн Європейського союзу, вона вирішила діяти менш відкрито та застосовувати холодну стратегію

1. Поширення фейків - намагання підірвати довіру до європейського об’єднання та співдружжя, що спричинило б вагоме падіння рейтингу лідерів держав ЄС. На думку багатьох “жертв” російського кібернетичного та інформаційно психологічного тиску, в процесі застосування даного методу ведення гібридної агресії по відношенню до ЄС, велика кількість людей казали, що їхні родичі та друзі все частіше застосовують у їхньому буденному лексиконі наративи, які поширювала Росія під час атак.
2. Шантажування енергетичною промисловістю

Як і у багатьох випадках, де прослідковується застосування енергетичного маніпулювання, країна, що веде агресивну політику в сторону іншої, частіше за все обирає шлях, який тисне одночасно на декілька об’єктів забезпечення комфортних для існування людей умов.

У випадку з російською агресією в бік передових європейських держав, вона тиснула на енергетичні канали, шантажуючи перекриттям постачання газу через “Газпром”

3. Фінансова та фізична підтримка радикальних партій.

Фінансова допомога агресивно налаштованих на європейських лідерів осіб (як впливових політичних фігур, так і звичайних громадян).

Розв’язання рук прибічникам російської держави, нарощування імперських настроїв на територіях Європейського союзу, активне розміщення російської пропаганди у соціальних мережах та на телебачені.

Підсумовуючи все вищесказане, можна підбити підсумки простими словами, а саме: застосування методів ведення гібридної агресії з розвитком технологій і масової психології людей дедалі змінюють напрям і спосіб використання даних інструментів.

Здійснювати опір та протистояти цим загрозам можна, якщо застосовувати комплексний підхід, що сполучає у себе розвиток технологічних та кібернетичної сфери управління, міжнародну підтримку та допомогу з боку союзних держав. Знаходження компромісу або дипломатичний підхід. Боротьба з дезінформацією. Зворотна диверсія, обхід гібридних загроз зі сторони та перенесення потенційної агресії на територію злочинної держави.

Професійне розглядання такого частого явища, як гібридні загрози для однієї країни з боку іншої, змушує навести приклади не тільки ті, де суб’єктом застосування елементів гібридної агресії є Росія, а й інших країн, які у певний історичний момент пішли шляхом негативно налаштованого настрою.

Для досягнення стратегічних цілей застосовується не тільки економічний, військовий, соціальний, кібернетичний та екологічний метод, а ще й метод приниження однієї соціальної групи зі сторони іншої. Одним з прикладів застосування саме такого методу є Китай.

Розглядаючи сучасні (нещодавні) приклади ведення гібридних війн і загроз, можна помітити, що під впливом непрямої агресії та військовим тиском опиняються не тільки країни з менш розвинутою армією, економікою, політичною підтримкою та соціальним устроєм.

Під ударом опиняються і такі країни як Китай.

Пропоную ознайомитись з сучасними методами ведення гібридних військових операцій на прикладі даної країни.

Перш за все, почнемо з того, як застосовує інструменти гібридної агресії безпосередньо сам Китай.

- Кібератаки (ми вже знаємо що це один з найпопулярніших засобів у сучасному світі)

Проте на відміну від інших держав з агресивним впливом на оточуючий світ, варто помітити, що Китай розпалює мілітарні настрої проти США, Росії, та інших країн з потужним важелем і впливом.

- Не часто можна зустріти такий метод, як “сіра зона” у військовій активності. Повільне, поступово наростаюче узурпаторство інших територій у Південно Китайському морі, використання цивільного флоту для особистих цілей.

- Окремо слід зазначити, що у випадку з Китаєм, застосування інформаційного впливу є на порядок агресивнішим і відкритішим. Є суттєві різниці між “стилями” у веденні гібридних загроз в області інформаційних атак. Якщо США і Росія застосовує інформаційний вплив з перспективою на довгі роки, яка принесе свої плоди через пару десятиліть, то Китай обрав метод швидкого, різкого нападу на інформаційно-психологічне сприйняття політичного життя у громадян певної країни.

Приклад з Тайванем у 2022 році став тому найяскравішим прикладом.

Принижуючі, агресивні наративи у бік тайванців, звертання уваги на розміри двох країн, демонстраційний показ збройної сили Китаю перед Тайванем, поширення “планів” по захопленню територій, розповсюдження історій про минуле перебування у складі Китаю - це все один з недавніх прикладів ведення гібридної агресії, яка не переросла у більш масштабні наслідки.

- Економічне домінування перед іншими країнами грає одну з найвагоміших ролей на політичній арені. Одна з найперших країн у списках найбагатших держав, що своїм впливом перекриває інші економічні еліти.

Не можна обійти стороною той факт, що у питаннях сторонніх, не торкаючи Китай війнах, він воліє зберігати нейтралітет задля збереження свого фінансового ричагу. Чи можна цей хід розглядати як ще один з методів ведення гібридної війни? Так. Адже коли приходить момент “оскалювати” зброю у сторону іншої держави, він нагадує про свій нейтралітет і небажання приймати участь у військових справах потенційної “жертви”, аби тиснути на неї іншими шляхами.

Китай, в свою чергу, не веде відкритої збройної війни по відношенню до Тайваню з метою уникнення санкцій та втрати політичної довіри з боку інших фінансово передових країн.

Порівняння з Україною

Порівнюючи даний приклад з Україною, можна знайти спільні риси і характери. Попри те, що Росія не вела повномасштабної війни з Україною, вона застосовувала на її території ті ж методи з ідентичними цілями і причинами. Однак, якщо провокування зі сторони Китаю до Тайваню не дає змогу досягти своєї мети через обережність і стратегічний підхід, то у випадку з Російською агресією, вона досягла своєї політичної мети (якщо розглядати повномасштабне вторгнення як одну з основних цілей Росії під час ведення гібридної війни)

Причини і сутність

Одна з сутностей поширення військової непрямої загрози - прояв унікальних рис і “характеру” країни, яка розпалює агресію та розглядає іншу країну як бажану для розширення власних територій. Військовий потенціал має чималий вплив на настрої всередині сусідніх держав, а це завжди задовольняє лідерів держав з девіантним характером та стилем.

Ті, хто мають агресивно налаштовані погляди у бік іншої соціальної (національна приналежність, раса, етнічне походження, соціальний клас тощо), завжди викликають, перш за все, зацікавленість у тих, кого не торкнуться ці погляди. В обставинах, коли одна країна проявляє домінування над іншою, у неї завжди знайдуться прихильники та військові, економічні та політичні союзники. Не зважаючи на розвиток технологій і сучасне самовиховання кожного окремого індивіда, докорінно знищити або зупинити цю споконвічну людську сутність неможливо.

Югославська гібридна війна і порівняння її з Україною

У 2000 році економічна ситуація Югославії під проводом Мішолевича досягла таких незворотних наслідків, що його режим ослаб до мінімуму і, як результат, стало причиною його падінню.

Країни Заходу сприяли тому, аби санкції наскільки стиснули фінансові можливості Югославії, що в результаті почалась гіперінфляція і “невиліковна” криза.

Незважаючи на зовнішні фактори, Мілевич, останній очолювач Югославії перед її розпадом (до речі, під впливом не тільки зовнішню гібридну загрозу, а й внаслідок військового прямого втручання, що являє собою наступним кроком після гібридних загроз, про які говорити меться далі), поєднував декілька ключових аспектів у боротьбі з гібридною агресією.

Наведемо пару прикладів, які він застосував задля уникнення загрози своєї країни.

- Внутрішні фактори

Нестабільність політичної ситуації.

Мишлевич вів боротьбу безпосередньо з опозиційно налаштованими організаціями у Сербії, які вели свою політику проти його влади.

Вимагаючи політичних реформ у бік демократичних змін і розвитку ліберальної реконструкції, вони влаштовували безліч мітингувальник актів,

які він, Михалевич, активно утисків і, застосовуючи агресивні методи, розганяв.

- Економічна нестабільність

Запровадження санкцій не вплинули на нескореність Мішолевича і не збили його зі шляху боротьби з зовнішніми гібридної загрози. Штучно підтримуючих валюту, він певний час забезпечував економічне життя громадян і це викликало, хоч і не на довгий час, підтримку з боку малої частини суспільства колишньої держави.

- Тиск міжетнічних груп

Війна у косово зродила між двома сусідніми країнами етнічну ворожнечу один до одного. Бачачи, як розпалюється між косовцями і югославцями неприязнь, міжнародні прихильники ідеї розвалу Югославії підхопили один з найвагоміших ричагів у розв'язанні активної війни середини Югославії.

Порівняння з Україною

Дуже вдалий приклад, як одна і та сама причина для конфлікту може розгорнути перед політичними “глядачами” різні сценарії і кінцеві результати війни. Порівнюючи причини і методи боротьби проти зовнішніх гібридних загроз, можна винести, що незалежно від схожих і протилежних причин для агресії, є певні методи, які застосовувались тисячоліттями для боротьби як гібридних загроз, так і відкритої збройної агресії.

Одним з найяскравіших прикладів української боротьби з російською пасивною агресією є антиросійські наративи, що розповсюджувались у навчальних закладах, школах, університетах тощо.

Патріотична агітація і національне виховання дітей. Введення молодшого покоління у політичну ситуацію дало свої плоди через роки, коли під час повномасштабного вторгнення молоді люди першими

вступили у ряди збройних сил і територіальної оборони у кожному місти України.

Розпалювання патріотичного настрою, слід зазначити, поширювалось передусім через засоби масової інформації.

- Американські настрої і курс у НАТО Порошенко з 2014 року

Не оминути і те, що історія українського виборювання незалежності свого суверенітету є дуже довгим, моментами важким і цікавим.

Міжпартійна боротьба Блоку Петра Порошенка і Опозиційної платформи за життя під проводом Медведчука є гарним прикладом, як внутрішня нестабільність країни грає на руку ворогу, що тільки починає вести гібридну, слизьку агресивно налаштовану війну. Зважаючи на те, як різноманітно хитався внутрішній стовп політичної стабільності України, можна чітко визначити, що ті методи які застососували українські діячі, доволі дієві і працюючі.

Підтримка західних союзників у наданні гуманітарної допомоги і збройної сили. Політичні симпатії європейських партнерів, яка свого часу суттєво відтермінувала початок відкритої збройної війни проти України.

Міжусобні конфлікти між Зеленським і Порошенко у 2019 році стали одним з ключових етапів розвитку історії України.

Поділення на два табори хоч і стало “ідеальним моментом” для початку активної гібридної загрози з боку Росії, проте не мало своїх результатів певний час.

Антиросійська пропаганда на міжнародному рівні виявилась дуже “болючою” не тільки для російського народу, а й чинної агресивної влади РФ, адже зриваючи маску непереможної армії і відчуваючи на собі висміювання з боку багатьох країн, їхні мілітаристичні настрої похитнулись і це завдало суттєвої шкоди для окупаційної сторони.

Чи можна вважати, що застосування методів боротьби проти гібридних загроз вживаючи “сили” засобів масової інформації дієвими? Дивлячись на те, який це мало наслідок на довгий час, багато хто погодився з цим твердженням, проте велика кількість людей помітила і зворотній наслідок. Активне введення інформаційної війни проти агресора викликає такі самі сумніви з часом, коли один інструмент не підкріплюється іншим, а саме видимими наслідками, починаючи від економічного стану, закінчуючи військовими наслідками.

Про застосування методів боротьби проти гібридної агресії можна сказати те, що комплексний тиск на всіх напрямках значно дієвіший, коли задіяні всі сили, такі як економічні, інформаційні, соціальні, кібернетичні - результат буде значно видиміший.

Наголошуючи про сутність гібридних загроз, варто звевернути увагу на те, що розглядати таке явище як гібридна військова агресія є багатогранним, неохопним, поділеним на багато аспектів і деталей, і об’єднуючи всі ключові моменти його роботи, можна виокремити основні положення, завдяки яким введення анти гібридної війни буде значно ефективнішим.

Неодноразово ми наголошували, що завдяки комплексному підходу можна вирішити і зупинити більшість руйнівних наслідків під тиском зовнішньої гібридної агресії.

“Соціокультурні аспекти гібридних загроз”, робота, автором якої є Красін Данило Сергійович, стверджує, що класифікувати гібридні загрози доволі важко, проте застосовуючи такі інструменти як кібернетичні сили у купі з інформаційним тиском можна досягти значно більших результатів, аніж використання тільки економічної нестабільності і санкцій.

Автор навів цікаву і нетипову таблицю моделі асиметричної війни, де послідовно йдуть такі механізми, як Інформація, за нею розвідка, далі дипломатія, наступний крок - економіка, за нею політика,

законодавство, культура, технологія, психологія, мораль і завершується все військовими засобами.

Це одна з моделей, яку створив автор. Проте якщо розглянути її детальніше, то можна побачити, що автор розставляє цю послідовність різними способами. Якщо у першому варіанті ми бачимо, що послідовність аспектів гібридних загроз у даній моделі є простою і не переплітаючою, то існує інша, де відчутна різниця у послідовності, через яку не важко помітити, як деякі механізми пов’язані між собою більш важким поєднанням.

Автор наполягає на тому, що політика, психологія, законодавство і мораль - витікаючі фактори саме з такого механізму як інформація.

І не дивно, адже сприйняття інформаційних хвиль впливає переважно на ті ділянки психологічних “зон”, які найбільш підвладні до рішучих змін і чутливих ділянок свідомості. Застосування інформаційної сили проти схильних до емоційних потрясінь людей - сильніша за військову зброю, адже якщо у першому варіанті людина прирівнює себе до того місця у соціумі, до якого прагне бути в очах оточуючих, то то в другому варіанті людина, скоріш за все, відчує розчинення серед масової загрози, де місце індивіда - найвіддаленіша точка, що розпливається серед інших, не відчуваючи на собі прямого впливу збройної агресії.

Мораль, яка є одним з витікаючим інформаційної сили, тисне безпосередньо на людське індивідуальне виховання і власні упередження, те сприйняття моралі, що виховувалось у певної людини роками, за мить може перетворитись на незначне “правило поведінки” що стоятиме для нього на рівні з інструктажем техніки безпеки і етичної культури. У масштабах багатоосібного суспільства дуже важко поширювати ту мораль, яка призводить до масового добробуту, в той час як “брудна” і аморальна, снобічна поведінка приверне набагато більше зацікавлених поглядів.

Можна висунути твердження, що поєднуючи між собою мораль і інформаційне поглинання можна вивести той тип індивіду, який ідеально підходить для впливу гібридної агресії. Вживання до добробуту в сучасному світі завжди має протилежний результат, тож використати цей метод у досягненні своєї мети було б доволі стратегічно правильним.

Людина, що заперечує моралізм серед тих, хто поширює духовний розвиток, буде завжди мати перед собою титанічний спротив і соціальну зацікавленість, як вже було сказано вище.

Законодавство - одне з найдавніших мірил що визначає рівень моральності серед людства. Те право, що було висунуте під тиском пригніченої моралі (Макіавеллізм), породило серед груп індивідів погляди, що несуть в собі протилежні настрої, адже досягти балансу між моральністю і моральністю - неможливо.

Позбавлене моральних норм законодавство викликатиме страх і небажання бути підкореним (на перший час) серед тих, чия мораль знаходиться нижче “волі до влади” людей.

Враховуючи всі вищевказані імперативи, можна вивести, що однією з невід'ємних рис можно владного діяча, що схильний до ведення і розпалювання агресивної гібридної загрози є аморальність.

Поглиблений розбір причин гібридних загроз і їхніх методів

- Метод інтелектуальної переваги

Над жертвою гібридної агресії цей метод, що притаманний для країн з багатим мілітарним досвідом, працює на глибоко психологічне сприйняття ворога. Підтримка лояльних каналів і вигідних для агресора джерел з території суб’єкта грає на емоціях жертви. Жертва ніби відчуває, що є альтернатива і компроміс, завдяки якому вона потенційно зберігає себе і залишається в безпеці.

- Тиск на емпатію

Один з хитрих методів для завоювання довіри серед бажаних для ворога кіл суспільства. Тиснучи і маніпулюючи задоволенням таким людських потреб як фізіологічні, соціальні, психологічні і духовні, можна переманити чималу кількість людей на інший бік.

Одним з найефективніших способів це штучно створити ті умови, при яких людина, залишившись без можливостей закрити всі базові потреби, сама проявлятиме бажання зробити все, аби отримати необхідне для її існування. Кажучи про моральність, що тісно переплітається з емпатією (що, до речі, дуже рідко можна вважати чимось схожим), можна з легкістю згадати випадки, коли ворон тиснув не тільки на інтелектуальний прояв переваги, а й на жалість. Російські війська у березні 2022 року, опинившись без їжі і води, часто звертаються до жителів тих місць, де вони перебували.

Якщо відсторонитись від ситуативного сприйняття даної картини, то людина з холодним розумом побачить, що спираючись на емпатію, житель, до якого звернулась людина по допомогу, скоріш за все, допоможе їй, і у концепції гібридної загрози це дуже допоможе для досягнення цілей, поставлених ворогом.

- Позбавлення засобів масової інформації

Жителі окупованих Росією територій України в 2022 відчули, що відсутність можливості бути проінформованим дуже тисне на їхній емоційний стан. Як і у випадку з голодом, позбавлена їжі людина готова вдаватись навіть на послуги ворога, аби задовольнити необхідну потребу.

Викривлена інформація діяла на споживачів саме так, як і планувала країна агресор.

Хтось піддавався впливу ворога через страх, хтось через бажання отримати бажане, хтось через власну схильність до швидкої зміни точки зору.

Аспектний погляд на гібридні зовнішні загрози

Тетяна Рева у своїй статті "Гібридні загрози та гібридні війни: сутність та аспекти" розглядає гібридні загрози як комплексне явище, що поєднує в собі різні методи впливу, включаючи військові, економічні, інформаційні та інші. Особлива увага приділяється аналізу сутності гібридних загроз та їхнім аспектам у контексті сучасних міжнародних відносин.

• В роботі, у свою чергу, подається наступне визначення: "Гібридна загроза – це загальний термін, що охоплює широкий спектр наявних негативних явищ та тенденцій (тероризм, міграція, піратство, корупція, етнічні конфлікти тощо), які адаптивно та системно використовуються для досягнення політичних цілей."

Розкладаючи гібридні війні на основні складові та виокремлюючі детальні механізми і сутності, автор приводить декілька етапів розв’язання гібридних війн, що переростають у активні збройні конфлікти.

- Війна без обмежень

Необмежена війна – це підхід, який визначає нову війну як необмежену комбінацію технологій, засобів впливу та методів.

Автор підкреслює, що аналізує сучасні війни як результат розвитку війни. Цей метод поділяє на чотири покоління, які були характерні для різних епох та визначається ключовими факторами, зокрема: людський ресурс, вогнева міць, стратегія та тактика, мережа. Основним ресурсом у першому поколінні війн була чисельність військ, тобто людські ресурси, друге покоління визначалось зброєю та її вогневою потужністю, третє – розробкою стратегії та тактики, а четверте – системою мереж.

3. Комбінована війна, що характеризується асиметрією, активним використанням та координацією діяльності нерегулярних і регулярних сил (ресурсів) [С. 3-4]

Автор зазначає: “Гібридна війна спрямована на використання національних вразливостей через політичну, військову, економічну, соціальну, інформаційну та спектр інфраструктури. Тому як мінімум національні уряди повинні проводити самооцінку критичних функційі вразливості в усіх секторах, і регулярно підтримувати його.

- Гібридна війна використовує скоординовані військові, політичні, економічні, цивільні та інформаційні (MPCI) інструменти влади, які поширюються далеко за військовою сферою. Національні зусилля повинні зміцнювати традиційні діяльність з оцінки загрози для включення нетрадиційних політичних економічні, цивільні, міжнародні (PECI) інструменти та можливості. Важливо,цей аналіз повинен враховувати, якими можуть бути ці засоби нападу сформований у пакет синхронізованих атак, адаптований до конкретного уразливості своєї цілі.
- Гібридна війна є синхронізованою та систематичною – відповідь повинна бути бути теж. Національні уряди повинні встановити та запровадити процес, щоб керувати та координувати національний підхід до самооцінки та загрози аналіз. Цей процес має спрямовувати всебічне міждержавне управління зусилля з розуміння, виявлення та реагування на гібридні загрози.
- Гібридні загрози є міжнародною проблемою – реагувати потрібно до. Національні уряди повинні координувати послідовний підхід між собою, щоб зрозуміти, виявити та реагувати на гібрид війна за їхні колективні інтереси. Багатонаціональні структури –бажано використовувати існуючі інститути та процеси – має бути розроблено для сприяння співпраці та співпраці через кордони.

“Наше спільне розуміння гібридної війни є недорозвинені і тому заважає нашому датність стримувати, пом'якшувати та протидіяти цій загрозі

З огляду на цю точку зору, розуміння супротивника гібридної війни не піддається виключно до традиційного аналізу загрози на основі його можливостей і намірів для а ряд важливих причин.

- По-перше, гібридна війна використовує більш широкий набір інструментів і методів MPECI які зазвичай не розглядаються в традиційних оцінках загроз.
- По-друге, він націлений на вразливі місця в суспільстві так, як це робимо ми не традиційно думати про.
- По-третє, він синхронізує свої засоби новими способами. Наприклад, by only дивлячись на різні інструменти влади, якими володіє ворог, неможливо передбачити, як і в якій мірі вони можуть синхронізувати для створення певних ефектів. Таким чином, функції можливості супротивника гібридної війни, хоча й важливі, але будуть не обов’язково надавати правильну інформацію, щоб зрозуміти проблема.
- По-четверте, гібридна війна навмисно використовує неоднозначність, креативність і наше розуміння війни, щоб зробити напади менш «помітними». Це пов'язано з той факт, що їх можна налаштувати, щоб залишатися нижче певного виявлення та таким чином, пороги відповіді, включаючи міжнародно-правові пороги перешкоджають процесу прийняття рішення та ускладнюючи реагування на атака гібридної війни. • По-п'яте, пов'язано і, мабуть, більше, ніж звичайні типи війни, кампанію гібридної війни можна не побачити, доки вона не буде вже активно розвивається, і руйнівні наслідки вже почалися проявляючись і знижуючи здатність цілі до захисту себе.”

Отже, підсумовуючи все неведене вище, можна узагальнити, що гібридні війні це не тільки про агресивний тиск, психологічна, емоційна і економічна напруга, за яким стоять лише девіантна аморальна поведінка і неприйнятті суспільством бажання. Це, у другорядну чергу, ще й про пошук нестандартних підходів, у яких замішані багато осіб, це, власне

кажучи, ціла рушійна сила зупинити яку можна тільки такою ж самою комплексною силою.

Слід зазначити, що ключовою особливістю гібридної загрози є те, що війна компенсує межі війни та миру, які дозволяють війні Гібрид- залишатися поза юридичною реакцією глобальної спільноти. Внаслідок інтегрованого використання гібридного обладнання на, держава зловмисника - це створення напруги в державі - ціль нападу (соціальна, політична, політична тощо) пояснює без пояснення відкритих конфліктів, які не виключають можливості вищої ескалації. Ризик недооцінки навчання противника та оборонних заходів може призвести до незадекларованих війн та катастрофічних майбутніх результатів та майбутніх результатів політичних та економічних систем , спрямованих на гібридні атаки.

Регіональні інтереси в галузі інтересів політичних та економічних регіонів можуть в кінцевому рахунку стати об'єктом гібридних атак. Загалом, провокаційний тип гібридного конфлікту полягає в тому, що рівень напруги нав національному об'єкті нападу DAS зберігається на рівні, який виключає законну законну втручання інших країн та міжнародних організацій прямого конфлікту(так звана гібридна невизначеність «). Тому дуже важливо забезпечити формат коаліції для припинення гібридних атак, які повинні бути гармонії з обмеженнями, накладеними об'єктними станами.

Ризики гібридної війни

Враховуючи активне використання різних методів ведення неконтактних війн, різні експертні групи, що досліджують таке явище як гібридна війна стверджують, що більше 50% успішних технік ведень гібридної агресії є :

- мотивування громадян України отримати друге громадянство на прикордонних територіях – 53%;

- поширення контенту, що контролюється країною-агресором у близьких до бойових дій містах – 51%;
- Створення та підтримка (включаючи фінансові проекти) для полегшення соціально -політичної ситуації, довіри національного лідерства та призначення населення в цивільний дискурс (включаючи фінансові проекти).
- Провокаційна медіа -діяльність, контрольована зловмисниками через приховування остаточного бенефіціара - 8%. • Вплив на уявлення про населення, яке не довіряє Міністерству органів внутрішніх справ, організацій та працівників - 9%. Наступні загрози свідчать про значні ризики (0-50%):
- Вплив на обізнаність Міністерства внутрішніх справ через цільову довіру, спрямовану на зміцнення довіри до політичної еліти держави.
- Використання цільової інформації та психологічних маніпуляцій - 3%.
- Просування менеджерів (включаючи несани) в міжнародних організаціях - 2% кандидатів (лояльність до окупантів).
- Введення соціально -економічної напруженості за допомогою бізнес обладнання: утворення негативних поглядів у населення 39%.
- Просування позитивних та руйнівних розповідей про органи та працівників Міністерства внутрішніх справ через інформацію - 1%. • Використання компромісів для сприяння індивідуальним рішенням (Національне, Міністерство внутрішніх органів відмови) -

0%. • Використання компромісу для усунення позицій працівників у системі внутрішніх питань -38%.

- Впровадження всебічної інформаційної кампанії для штучної поляризації та радикалізації суспільства з використанням хвилювання громадян - 5% - з цього питання:

- Ціни на газ, виборці, інша енергія - 8%.
- Державна політика ОРДЛО - 8%. • "Невдалі реформи" - 1%.

Разом з тим, орієнтування на ризики привертає увагу не лише на оцінювання ризиків поширення гібридних загроз, а й на рівні шансів та спроможностей протидії гібридним загрозам.

Важливою особливістю оцінки ризику в гібридній системі боротьби з загрозами в області громадської безпеки та цивільного захисту є оцінка його здатності протистояти ідентифікованим гібридним загрозам - внутрішніми факторами, що характеризують різні аспекти системи карального правосуддя (оцінка поточних фактичних умов). [с. 69-70]

Приклад оцінки ризиків гібридних загроз в Україні

Українсько-Угорські відносини були напружені через ряд міжусобних нюансів, включаючи права українських угорських меншин та війну проти України. Таку політичну напругу розпалюють, як правило, наділені інформаційним впливом на міжнародних споживачів. Беручи до уваги те, що угорська влада цілком належить російській стороні, можна легко зробити висновок, що російська психологічна гібридна загроза проникає навіть з країн-оплічників.

Угорська політика нерідко займає позиції, більш вигідні для Російської Федерації. Інформаційний простір Угорщини є вразливим до зовнішнього впливу, особливо щодо питань національної ідентичності та інтерпретації історичних подій. Це створює сприятливі умови для поширення дезінформації та інформаційних кампаній, спрямованих на посилення суспільних протиріч в Україні.

Економічні відносини між Україною та Угорщиною на даний момент не демонструють наявності конкретних прикладів використання економічних інструментів як засобу гібридного впливу, однак така загроза потенційно існує.

У більшості досліджень гібридних загроз проти України основна увага зосереджена на ризиках з боку Росії. Наразі немає достовірних даних про систематичне або масштабне застосування гібридних методів впливу на Україну з боку Угорщини. Для формування об'єктивної оцінки потенційних ризиків доцільно залучати аналітичні центри, що спеціалізуються на питаннях національної безпеки.

На сьогодні ймовірність збройної агресії Угорщини проти України оцінюється як вкрай низька. Відносини між двома державами, попри окремі політичні та історичні суперечності, залишаються у межах дипломатичного врегулювання. Основними предметами напруги є питання прав національних меншин, трактування історичних подій та співпраця Угорщини з Росією в енергетичній сфері. Водночас Угорщина є членом НАТО та Європейського Союзу, що суттєво обмежує можливості для відкритої агресії проти України через міжнародні зобов'язання та можливі санкції з боку партнерів

Збройна ескалація з боку Будапешта є малоймовірною також через економічну залежність Угорщини від ринку ЄС та небажання порушувати існуючий баланс безпеки у регіоні. Наразі більша загроза виходить не від прямої військової агресії, а від політичного та інформаційного тиску в контексті гібридних загроз. Беручи до уваги сукупність політичних, економічних та військових факторів, ймовірність збройного конфлікту між Угорщиною та Україною можна оцінити на рівні приблизно 1–3%.

Ключові напрями протидії гібридним загрозам, що застосовуються в Україні та на міжнародному рівні (без конкретизації у відсотках):

1. Інформаційна безпека та заходи проти дезінформації:

- Підвищення рівня медіаграмотності громадян: Реалізація освітніх ініціатив, спрямованих на розвиток критичного мислення та навичок виявлення недостовірної інформації.

- Сприяння розвитку незалежних і професійних медіа: Створення умов для забезпечення суспільства об'єктивними та достовірними інформаційними джерелами.

- Формування системи моніторингу та аналізу інформаційного середовища:

Виявлення проявів інформаційних атак та розробка заходів для їх нейтралізації.

1. - Удосконалення законодавчого регулювання у сфері інформаційної безпеки: Протидія поширенню неправдивого та незаконного контенту через запровадження ефективних правових норм.

- Розвиток стратегічних комунікацій: Забезпечення оперативного та достовірного інформування громадськості й міжнародної спільноти для протидії ворожим інформаційним впливам.

2. Кібербезпека:

- Зміцнення захисту критично важливої інфраструктури: Посилення стійкості інформаційних систем органів державної влади, енергетичної галузі, фінансових установ та інших об'єктів, що мають стратегічне значення.

- Розвиток національних кібер спроможностей: Формування спроможностей щодо виявлення, нейтралізації та реагування на кіберзагрози.

- Розширення міжнародної співпраці у сфері кібербезпеки: Налагодження обміну інформацією та проведення спільних заходів із міжнародними партнерами.

- Підвищення рівня кібер грамотності серед фахівців і населення.

3. Політико-дипломатичні механізми:

- Міжнародна взаємодія та зміцнення підтримки: Активне залучення міжнародної спільноти до процесів стримування агресії.

- Запровадження санкцій та інших форм міжнародного тиску на державу агресора.
- Вжиття дипломатичних заходів з метою мирного врегулювання конфліктних ситуацій.
- Забезпечення внутрішньополітичної стабільності та суспільної консолідації: Підвищення рівня національної єдності у відповідь на зовнішні загрози.

4. Сфера оборони та безпеки:

-Підвищення рівня боєготовності Збройних Сил України: Посилення оборонного потенціалу держави.

-Розвиток розвідувальних та контррозвідувальних можливостей: Виявлення та нейтралізація діяльності противника.

-Забезпечення захисту критичної інфраструктури від фізичних атак і диверсій.

-Організація територіальної оборони та підготовка населення до активного опору.

-Економічна стійкість:

-Диверсифікація економічних зв'язків і зменшення залежності від держави агресора.

-Розвиток національного виробництва та підтримка підприємництва.

-Зміцнення енергетичної безпеки держави.

Протидія корупційним схемам та тіньовій економіці як факторам внутрішньої нестабільності

6. Соціальна стійкість:

Формування й підтримка національної ідентичності та патріотичних настроїв.

Соціальний захист ветеранів війни та осіб, які постраждали внаслідок конфлікту.

Гарантування доступу населення до базових соціальних послуг і підтримка вразливих верств суспільства.

Висновок

Гібридні загрози є складним і багатовимірним явищем, що поєднує військові, політичні, економічні, інформаційні та кібернетичні інструменти для досягнення стратегічних цілей без прямого оголошення війни. Вони спрямовані на підрив державної стабільності, ослаблення національної безпеки та розкол суспільства.

Досвід України, яка протистоїть гібридній агресії з 2014 року, доводить, що ефективна боротьба з такими загрозами потребує комплексного підходу. Важливими напрямами протидії є посилення інформаційної та кібербезпеки, розвиток оборонного сектору, забезпечення економічної та енергетичної стійкості, а також зміцнення національної єдності та соціальної згуртованості.

Водночас, міжнародна підтримка, тісна співпраця із союзниками, активна дипломатія та законодавче удосконалення мають вирішальне значення у протистоянні сучасним викликам. Гібридні загрози вимагають постійної адаптації державної політики та здатності швидко реагувати на зміну характеру атак.

Таким чином, боротьба з гібридними загрозами — це довготривалий процес, який вимагає не лише технологічної готовності, а й сильної національної ідентичності, громадянської свідомості та єдності всього суспільства.

1.3. Особливості гібридних загроз у сучасних геополітичних умовах

У XXI столітті такі поняття як війна і безпека докорінно змінилася під впливом розвитку і модернізації застосування інструментів для ведення гібридних війн. Є певна різниця між класичними збройними конфліктами, сучасними гібридними операціями, беручи за основу комплексний вплив на суспільство і державу, застосовуючи певну метаморфозу як мілітаризованих інструментів залякування, так і невійськові засоби тиску. Саме цим визначається одна з головних особливостей гібридних загроз — їхня багатовекторність та важкість для ідентифікації на початковому етапі.

Центральною метою гібридних загроз полягає у намірах нанести шкоду не лише військовій структурі, а й головним частинам політичної, фінансової, соціальної та інформаційної систем країни. Учасники гібридної війни застосовують дипломатичні шляхи, медіа-простор, економічні важелі, кібератаки та підривну діяльність, створюючи ситуацію постійної нестабільності без офіційного оголошення війни. Це ускладнює міжнародне реагування, адже традиційні механізми безпеки часто виявляються неготовими до таких нетипових викликів.

Іншою важливою рисою гібридних загроз є активне використання інформаційного простору. Пропаганда, дезінформація, фейкові новини, маніпуляція суспільною думкою стають одними з головних інструментів впливу. У міжнародних відносинах це проявляється у спробах змінити уявлення громадян інших країн про реальні події, дискредитувати уряди та міжнародні організації, розпалити ворожнечу й розділити суспільства за політичними, національними або релігійними ознаками.

Гібридні загрози, у більшості, несуть в собі латентний, прихований характер. Кроки ворожої країни завуальовані під нешкідливі дії, під внутрішні проблеми "постраждалої" країни, що дає можливість безкарно уникнути відповідальності на міжнародній арені. Анонімність і прихованість виконавців стає чималою перешкодою для колективної відповіді, а також створює проблеми у визначенні юридичного підґрунтя

для використання справедливих дій у відповідь на міжнародну агресію, таких як санкції чи силові операції.

Міжнародні організації у боротьбі проти злочинних дій масштабного характеру зазначають, що гібридна агресія носить в собі масований характер і, очевидно, використовується як національними, так і недержавними “акторами”. Не беручи до уваги передові країни, що володіють більш небезпечними інструментами для ведення важких гібридних операцій, утворюються нові суб'єкти — терористичні групи, наймана армія, окремі хакерські угруповання. Це допомагає ворогу заплутати сліди і залишитися спійманим, звідки і відходять додаткові виклики для цілісності міжнародної спільноти.

Іншою притаманною рисою гібридних атак у новочасних міжнародних відносинах є багатовекторність у визначенні межі між миром і війною. Багато операцій відбуваються у "сірій зоні", яка унеможливлює відповідь на питання, чи перебувають країни у стані збройного конфлікту. Це дозволяє агресорам уникати відповідальності згідно з нормами міжнародного права і в той же час крок за кроком виконувати поставлені завдання.

Міжнародній спільноті не залишається нічого, крім пошуку спільної громадської безпеки у випадку розгортання безконтактних загро. Одним з головних шляхів полягає у “загартуванні” країн до важких військових умов, при яких покращується здатність залишатись продуктивним і об'єднуватись попри потужний тиск. Пріоритетною метою є взаємозв’язок між державами, обмін інформацією про потенційні загрози, розвиток юридично-правової основи з метою уникнення шкоди від кібератак та дезінформаціного впливу, а також вдосконалення рівня усвідомлення громадян.

За таким принципом гібридні загрози в сучасних міжнародних відносинах стають рушійною силою на шляху до задоволення політичних апетитів не підбігаючи до використання регулярної армії. Такий підхід деформує основну складову конфліктів, наполягаючи від агресора покірності, проактивності та тісної міжнародної співпраці для збереження миру і стабільності.

Колективна безпека під час гібридної агресії

Концепція колективної безпеки у всі часи була базовою для міжнародного устрою і стабільності. Попри все, з розповсюдженням і розвитком гібридних загроз, консервативні методи до забезпечення колективної безпеки потребують значної модерніфікації. Гібридні загрози, які поєднують у собі військові, політичні, економічні, інформаційні та кібернетичні елементи, вимагають від держав учасниць спільних, узгоджених і про активних дій.

Однією з ключових особливостей гібридних загроз є їхня прихованість і поступовість. Учасник, що застосовує гібридні методи, намагається уникнути прямої військової конфронтації, натомість обираючи тактику "розмитого" впливу, що ускладнює застосування положень міжнародного права чи статутів міжнародних організацій. Тому для ефективної відповіді необхідна не лише політична воля держав, а й висока оперативність та гнучкість механізмів колективної безпеки.

Передову роль у боротьби з гібридними загрозами грають міжнародні організації, насамперед Організація Північноатлантичного договору (НАТО) та Європейський Союз. У відповідь на нові виклики НАТО ще у 2016 році офіційно визнала гібридні загрози одним із головних викликів безпеці та ухвалила концепцію, згідно з якою гібридна атака може розглядатися як підстава для застосування колективної оборони відповідно до статті 5 Вашингтонського договору.

Міжнародна безпека в умовах неконтактної агресії передбачає локалізацію зусиль у різних сферах:

Інформаційна безпека: Обмін інформації розвідки, координація протидії де інформаційним кампаніям, зміцнення стратегічних комунікацій.

Кібербезпека: Спільні навчання з реагування на кібератаки, заснування центрів кіберзахисту, допомога у зміцнені кіберінфраструктури держав-учасників.

Економічна безпека: Узгодження санкційної політики щодо агресорів, запобігання економічному шантажу та підтримка економічної стійкості союзників.

Військова підтримка: Проведення спільних військових навчань, посилення оборонних спроможностей на загрозливих напрямках, розвиток сил швидкого реагування.

Важливість і значення до військових протидій гібридним загрозам полягає у обміні бойовим досвідом і модернізацією методів між країнами. Держави, що стали жертвами циї загроз, як Україна, Литва чи Естонія, надають важливу інформацію про механізми виявлення та нейтралізації гібридних впливів. Співпраця між країнами у сфері кібербезпеки, розвідки, оборони критичної інфраструктури стає основою сучасної колективної безпеки.

В той же час боротьба з гібридними загрозами ускладнюється паралельними поглядами між країнами в плані забезпечення і протидій загрозам. Протилежні засоби до виявлення небезпеки та аналізу ризиків можуть затримувати хід і розвиток спільного плану. З цієї ж причини уникнення гібридних загроз ґрунтується не тільки посиленням збройного потенціалу, а й досконалості волі до політичних рішень та єдності, солідарності та взаємної довіри серед країн учасниць.

Не дивлячись на це, у наш час велике значення у сапортизації суспільної безпеки полягають у взаємовідносинах між політичними “гравцями” та з іншими міжнародними учасниками. Зміцнення партнерських відносин з НАТО і Європейським Союзом, ООН, ОБСЄ відкриває простір для більш комплексних підходів та масштабних протидій у вигляді викликів .

Як можна визначити, спільна безпека у сьогоднішніх дипломатичних стосунках не обмежується суто військовою силою і покриває багато суспільно-політичних сторін кожної з країн, починаючи від протидій з інформаційними загрозами до підтримки медіа-простору, від допомоги у гуманітарних потребах до зміцнення і поширення “таборів” з активістами проти загроз. Поєднуючи між собою кожен з елементів боротьби з неконтактною агресією, виходить саме комплексний грамотний підхід.

Регулярна демонстрація підкріплення власних робіт посиланнями на роботи інших авторів на тему “Особливості гібридних загроз в сучасних міжнародних відносинах”, пропоную підсилити мою аргументацію працею

Ф. Хоффмана, який стверджував, що гібридні загрози — це "синергія традиційних військових сил із нерегулярними тактиками та сучасними інформаційними операціями" [Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars, 2007, p. 14]. Автор наголошує, що неконтактна агресія складається з політичного і соціального тиску, економічного шантажу (санкції, перекриття постачання товарів для підтримки промислових галузей тощо), кібернетичні загрози та ведення агресивної політики проти певної країни.

Ключові особливості у роботі Ф. Хоффмана сучасних гібридних загроз і порівняння їх з державною політикою України Хоффман ілюструє не схожий на інші підходи і методи роботи та впливу гібридних безконтактних загроз, ідея якої полягає у застосуванні елементів нерегулярної збройної агресії, консервативної війни, класичного тероризму

та кооперaційної злочинності у своїй роботі "Conflict in the 21st Century: The Rise of Hybrid Wars" (2007).

Комплексна дія даних елементів роботи гібридних загроз становлять:

1. "Скупченість" засобів впливу

Застосування збройних сил і військового потенціалу не являє собою єдиний підхід, який визначає сутність гібридної загрози. Включаючи у себе такі інструменти ведення гібридної агресії як інформаційний тиск, економічна загроза, політична дестабілізація, кібернетичні атаки - це, в свою чергу, як зазначає автор, гібридні актори, що можуть одночасно використовувати регулярні і нерегулярні сили, об'єднуючи можливості різних рівнів протистояння" [Hoffman F. G., 2007, p. 16].

2. *Прозорий перехід від миру до війни*

З давніх часів війна і мир перебували між чітко визначеними кордонами. У випадку гібридних загроз ці рамки розмежовуються і країни, як правило, не відчувають емпатію один до одного, відкидаючи прямий відлік своїм діям, починають поширювати ворожі наративи у мас-медіа і розгортати інформаційні кампанії. Хоффман наголошує, що гібридні атаки створюються у випадках, коли юридична сторона держави втрачає свою силу, що значно ускладнює міжнародну реакцію.

За словами Є. Магди, "гібридні загрози в міжнародних відносинах спрямовані на підрив внутрішньої стабільності держав, використовуючи комбінацію військових та невійськових методів, таких як інформаційна пропаганда, диверсії та економічний тиск. Важливим елементом таких загроз є маніпуляція громадською думкою через контрольовані медіа", що підлягає під наратив про те, що першочерговою дією у боротьби проти зовнішньої гібридної загрози є воля народу до несприйняття негативних епітетів про власне існування

К. Галеотті ж в свою чергу підкріплює значення цих слів таким висловом: "Сірі зони у міжнародних відносинах, де гібридні методи

дозволяють агресору діяти без формального перетину червоних ліній, ускладнює правову оцінку та міжнародну реакцію”. [Galeotti M. The Modern Russian Way of War: Threats, Strategies and Tactics, 2022, p. 27],

Таким чином, зовнішня непряма агресія залишається по статусу слабкішою за пряму військову агресію, проте не позбавлена рушійних наслідків.

3. Асиметрія і адаптивність

Гібридні загрози є багатогранні: їхні “гравці” моментально проявляють резильєнтність доходів агресора, поєднуючи стратегії залежно від змін ситуації на полі бою або в політичному середовищі [Hoffman F. G., 2007, p. 20].

Порівняння з державною політикою України

Ідея Хоффмана прямо пересікається з ситуацією в України до протидії гібридним загрозам, особливо після 2014 року.

1. Реакція на багатовекторність агресії у відповідь на гібридну агресію з боку Російської Федерації. Україна має різновидні шляхи у подоланні цих загроз, що включають у себе посилення обороноздатності, формування стратегічної інформаційної політики, дипломатичний тиск і запровадження економічних санкцій. Це відповідає концепції Хоффмана про необхідність швидкого реагування на різні типи загроз. Прикладом є тактика національної безпеки України від 2020 року, де наголошується на важливості "забезпечення стійкості держави до багатовимірних гібридних загроз". [Стратегія національної безпеки України, 2020, с. 7]

2. Висвітлення конфлікту позбутого мети

Україна неодноразово наголошує на гібридному підґрунті конфлікту з Росією — Кремль не погоджується, що військова нестабільність і прямий військовий конфлікт на Донбасі це справа Москви. Це підтримує концепцію Хоффмана про розмитість меж між станами війни та миру.

3. Гнучкість безпекової політики Україна показує приклади адаптивності, створюючи нові кібербезпеки підрозділи, зміцнюючи інформаційну сферу, наприклад, через Центр стратегічних комунікацій при РНБО, та розвиваючи територіальну оборону. Ці кроки гармонують із поглядом Хоффмана на важливість швидкого реагування на гібридні загрози.

Порівняння підходу Ф. Хоффмана з державною політикою України показує, що українські стратегії насправді втілюють ключові ідеї, запропоновані теоретиком. Україна розглядає гібридні загрози як складні та багатовимірні явища, які вимагають одночасного використання усіх державних ресурсів, що співвідноситься з сучасними поглядами на природу конфліктів у XXI столітті. Разом з тим, на відміну від західної традиції, де акцент робиться на попередженні гібридних атак, досвід України має яскраво виражений акцент на стримуванні та протидії вже існуючій агресії.

Концепція гібридної війни в інтерпретації Євгена Магди та її взаємодія з державною політикою України.

Підхід Євгена Магди до гібридної агресії

Євген Магда - один з авторитетних українських аналітиків у сфері гібридних загроз, і який написав чимало робіт, однією з яких є монографія "Гібридна війна: вижити та перемогти" (2015). Магда не є послідовником західної ідеї боротьби проти гібридних загроз, а розглядає гібридні війни не тільки як збройне зіткнення, а й послідовне, тривале залучення у державу-агресора, її суспільство, культурний простір і політичну систему з метою утилізації національної ідентифікації.

Основні ідеї концепції Євгена Магди

1. “Гібридна війна як новий вимір агресії “, - зазначає Магда, “Гібридна війна — це не лише воєнний конфлікт, а перш за все боротьба за свідомість громадян, нав’язування чужих наративів, дискредитація

інституцій і підрив довіри до держави. Метою агресора є примусити країну внутрішньо капітулювати, не усвідомлюючи, що вона вже перебуває у стані війни. Головною особливістю підходу Магди є акцент на інформаційному, ціннісному та гуманітарному вимірі гібридної агресії".

2. Ціль — руйнація ідентичності, наголошує він. Головна мета гібридної загрози є національна самовизначеність, мова, історія та культура. Завдяки пропаганді й інформаційній атаці, ворог має спробу замилювати державну солідарність, поширюючи хибну версію походження народу і альтернативну історію. Це особливо проявляються в діях РФ на Сході України та в Криму.

"Інформаційна зброя — головний інструмент, як зазначав у своїй книзі Магда, що наводить приклади масового використання інформаційної зброї Росією, від фейкових новин до масштабних кампаній у соцмережах.

Гібридна війна ведеться щодня через телебачення, Інтернет і публічну думку" - [Магда Є., 2015, с. 39].

3. Ідея Магди полягає також і у тому, що тривалість і довгочасність конфлікту, що перетворюється на гібридну війну — це не тимчасовий стан, а постійна форма, у якій агресор одержимий зробити все, аби жертва не визнала себе як окремий суб'єкт. У випадку України це бажання Росії тримати її у "сірій зоні", позбавляючи змоги самостійного вибору геополітичного вектору.

Порівняння з державною політикою України

Вивчаючи структуру такого явища як гібридна загроза, з 2014 року (особливо після 2022-го) Україна чітко визнає, що війна триває не лише за територію,а й за свободу, ідентичність, права, ідеї і нації. Це пересікається з ідеями Магди. В оновлених концепціях національної безпеки фіксується пріоритет національної стійкості, інформаційної гігієни та боротьби з фейками й пропагандою. Інституційна реакція на інформаційну ворожість України створила Центр стратегічних комунікацій при РНБО,

модернізувала закон про ЗМІ та підсилила роль мовної політики — все це працює на захист інформаційного простору, що цілком відповідає рекомендаціям Магди. Активізація культурної політики Держава почала активно підтримувати українську культуру, історичну пам’ять, книговидавництво та україномовний контент. Це також засіб протидії гібридному впливу через гуманітарний ричаг.

Отже, концепція гібридної війни в інтерпретації Євгена Магди значно розвиває розуміння загроз, особливо в гуманітарних та інформаційних аспектах. Вона змушує звернути увагу на тому, що гібридна агресія — це не лише матеріальне протистояння з застосуванням зброї, але й боротьба за народність, за світогляд нації. Теперішня політика України, особливо після повномасштабного вторгнення

Російської Федерації у 2022 році, чітко формується і розвивається за ідеями Магди: це включає зміцнення стійкості суспільства, підтримку національної ідентичності та захист від інформаційного впливу. В той же час, думки Магди не лише підтримуються в практичних діях, а й стали методологічним підґрунтям для формування української стратегії безпеки.

Особливості сучасної гібридної війни в інтерпретації Марк Галеотті

У своїй праці The Modern Russian Way of War британський історик і експерт із російських збройних сил Марк Галеотті описує специфіку російського підходу до війни у XXI столітті, особливо в контексті так званої «гібридної» агресії. Автор не використовує термін «гібридна війна» як догму, натомість наголошує, що Кремль мислить у категоріях «не-лінійної війни», де немає чітких меж між війною та миром, між військовим і цивільним, правдою й маніпуляцією.

1. Конфлікт як постійний стан

Галеотті визначив: “Сучасна російська стратегія виходить із базового припущення: війна не є винятком, вона — норма міжнародних відносин. Для російських еліт, за його словами, Захід веде «приховану

війну» проти Росії ще з 1990-х років, тому Кремль лише «відповідає» на цю агресію. У цьому світогляді мир — це лише форма війни іншими методами, де боротьба триває через політичний вплив, енергетику, пропаганду, дипломатію”.

Такий метод кардинально відрізняється від західного, де війна, як правило, розглядається як радикальний наслідок гібрих загроз. Російська концепція, за Галеотті, більш цинічна і гнучка, і саме в цьому — її небезпека для ліберальних демократій, які не завжди готові діяти за подібною логікою.

2. Багаторівнева агресія

Галеотті підкреслює, що Кремль вдається до «глибокої війни» (deep operations), яка включає:

Інформаційні впливи (фейки, медійні маніпуляції, дезінформація);

Кібероперації (втручання у вибори, атаки на інфраструктуру);

Підкуп і підтримка політичних маріонеток;

Парамілітарні формування (як ПВК або «зелені чоловічки» у Криму);

Правова та дипломатична атака (створення альтернативного міжнародного дискурсу).

Це дозволяє Росії маскувати реальний масштаб конфлікту, змушуючи Захід вагатися щодо адекватної відповіді. Водночас такий підхід вимагає високої координації — тут автор визнає, що в Росії вона часто імпровізована, а не централізована.

3. Вразливість відкритих суспільств

Галеотті застерігає: багатовекторна тактика Кремля формується на ударах по вразливим місцем демократичних форм, зокрема: свободи слова — для поширення дезінформації;

політичної слабкості— для поширювання проросійських наративів; економічної лібералізації — для фінансового впливу на окремі сектори;поляризації — для розколу суспільств.

Ці інструменти досконало працюють у випадках «низької інтенсивності», коли військові методи ще не залучені, проте держава починає тріскати з самої середини.

4. Український контекст

Беручи до прикладу Український сценарій, концепція Галеотті сповнюється особливим значенням. Він бачить конфлікт на Донбасі та агресивну узурпацію Криму як приклад успішної реалізації гібридного конфлікту. У випадку з Кримом було застосовано такі інструменти, як куплений референдум, поширення ворожої для громадян Криму пропаганди, кібератаки, залучення місцевих бойовиків як прикриття для регулярної армії РФ.

Галеотті наголошує, що Україна певний час не відчувала потенційну руйнівну силу і потенціал гібридної агресії, а Захід вбачав у цьому конфлікті виключно як місцеву проблему, а не як прихований план Москви. Успішність гібридних загроз по природі своїй формуються саме таким чином: прихованість майбутніх намірів.

Попри все, автор виділяє пару ключових моментів: з плином часу в Україні розвинулась резистентність, що почала створювати особисті анти гібридні структури, що включає в себе нову українську армію, національні структури, активацією інформаційної політикою та реформи у сфері медіа. За словами Ґалеотті, війна 2022 року зруйнувала ілюзії про «сірі зони», змусивши державу перейти в режим повної мобілізації.

5. Росія — не всемогутній агресор

Відкидаючи звичну формальність, Марк Галеотті змальовує Росію як могутню наддержаву, що здатна домінувати над іншими. Ба більше, він неодноразово говорить про непрофесійні підходи до непрямої гібридної

агресії, її конфліктність між елітами, неспроможність системної солідарності. Такі характерні для Кремля слабкі місця дозволяють демократичним державам взяти собі на замітку, що відкриті політичні ділянки у яких Російська Федерація некомпетентна, можна використовувати як власний шлях до досконалості.

Підсумовуючи все вище описане, та беручи до уваги важливі моменти, можна побачити, як ідея Галеотті дає можливість побачити гібридну загрозу не лише як на бойову дію, а як на суцільну кореляцію, в якому військовий конфлікт — сталий процес. У цьому явищі українська держава постала як активний учасник ще з 2014 року, і її досвід є важливим для відкриття нової етапу розвитку для міжнародної співпраці. Тепер, формуючи національний суверенітет до нових викликів, Україна виливає в реальність прототип тому, над чим працював Галеотті: на зміну бездіяльного прийняття неминучих наслідків гібридних загроз, варто консолідувати всі аспекти державних стовпів, на яких тримається і ґрунтується незалежність країни.

РОЗДІЛ 2.
АНАЛІЗ ГІБРИДНИХ ЗАГРОЗ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ (2014–2024 рр.)

2.1. Нові виклики перед національною безпекою України в умовах російсько-української війни

В умовах нескінченних гібридних загроз Україна перебуває не один десяток років, і це залишає відбитки на стінах її історія, яка формує не тільки незалежність, а й існування нації. Після 2013 року, з перетином РФ кордонів нашої держави, країна потрапила у коло агресивних викликів, що характеризується застосуванням гібридних методів ведення війни. Гібридні загрози торкають неохопгтй спектр дій

— від збройної агресії, інформаційно-психологічних атак, кібератак до економічного тиску та політичної нестабільності, а їхня багатовекторність та комплексний підхід не дає змогу простежити та визначити чіткий спосіб протидії, у якому необхідно застосувати сучасний метод боротьби та аналізувати загрозу національній безпеці.

Метою цього дослідження є аналіз національної безпеки в умовах застосування гібридних загроз, у яких Україна перебуває з 2014 року по сьогодення, з виокремленням основних динамік, механізмів впливу та наслідків для державного суверенітету, цілісності та стабільності. Окремий акцент варто зробити на розвитку понять безпеки в умовах гібридної війни, а також роботі національних структур на міжнародному рівні задля запобігання агресивним викликам.

Актуальність обраної теми ґрунтується на необхідності створення правильної стратегії для досягнення безпеки, яка здатна не втрачати свої права навіть в найскладніших етапах застосування гібридних атак,

нетипові загрози, які не вписуються в традиційні рамки воєнного конфлікту. Аналіз гібридних загроз дозволяє не тільки глибше побачити сутність сучасної війни, але й допомагає трансформації інституційної стійкості України в довгостроковій перспективі.

Хронологія подій і порівняння змін гібридних загроз в Україні у 2014 році з подіями 2022-сьогоденням

У 2014 році світ став свідком незаконної анексії Автономної республіки Крим зі сторони Росії. Злочинна дія, що відбулась в момент ослабленного стану України, базується на бажанні задовольнити свої загарбницькі нахили, посіяти свій вплив серед людей, які вважали себе окремими від України. Гібридність, а саме безконтактність агресії полягає у масовому тиску як на народ україни, так і на весь інший світ.

Говорячи словами професійної аналітики військової оцінки, Росія переступила певний соціально-нормативний кордон, що дозволив багатьом країнам заходу і Європи ніби розв’язати руки і допомагати Україні військовою силою, економічною підтримкою, промисловим запасом та дипломатичним компромісом,

Події після анексії Криму у 2014 році: ескалація на Донбасі

- Початок весни 2014 року: масові проросійські виступи в Донецькій, Луганській, Харківській областях.
- Квітень 2014 — оголошення "ДНР" і "ЛНР", спроби створення "Новоросії".

Застосування інструментів гібридних методів: координація ворожих агентурних груп на території східної частини України під виглядом "ополченців", застосування інформаційних операцій для дискредитації української влади, активізація кібератак.

Порівняння інтенсивності та природи загроз 2014 року та після 2022 року

2014: Росія діяла через "маріонеткові утворення", уникаючи прямої участі; головні методи — провокації, пропаганда, "гібридна війна" у класичному розумінні.

2022: Відкрита агресія повномасштабного характеру, але гібридні елементи не зникли — продовження інформаційних операцій, кібератак на об'єкти критичної інфраструктури, спроби посіяти паніку всередині українського суспільства.

Еволюція методів гібридної війни

В 2014-му ставка робилась на маскування, створення ілюзії "громадянських конфліктів".

Після 2022 року Росія, хоча й діє відкрито, все одно активно використовує гібридні інструменти: енергетичний тиск, спроби розколоти українське суспільство через теми мобілізації, втрат на фронті, економічних труднощів.

Нові форми гібридних загроз після 2022 року

- Залучення штучних інтелектів і бот-мереж для розповсюдження панічних настроїв.
- Підрив гуманітарної безпеки: удари по об'єктах енергетики взимку 20222023 років.
- Посилення пропаганди серед українських біженців за кордоном.

Висновки по блоку

Якщо у 2014 році гібридна війна була переважно замаскованою та обмеженою локальними масштабами, то після 2022 року вона стала глобальною, багаторівневою і стосується не лише фронту, а й тилу, цивільного населення, міжнародної спільноти.

Перехід від хронології подій до аналізу методів гібридної агресії

Розглядаючи інтенсивність гібридної агресії в Україні у період з 2014 року до сьогодення, слід визначити, що на певних етапах конфлікту

відрізнялась не лише динаміка агресивних дій, але й характер застосованих інструментів впливу. На першому етапі російської агресії гібридні методи реалізовувалися переважно через збройне залякування без нормативного дозволу участі регулярних сил, підтримку сепаратистських рухів та ведення інформаційної війни. Згодом, особливо після початку повномасштабної війни у 2022 році, спектр застосовуваних засобів суттєво розширився, охоплюючи політичні, економічні, соціальні, інформаційні й навіть культурні сфери.

Гібридна війна як форма агресії передбачає не тільки використання збройної сили, але й комплекс заходів, спрямованих на ослаблення противника шляхом підриву його внутрішньої стабільності, політичної єдності та міжнародної підтримки. Цей механізм особливо чітко проявилася у випадку України. Тактичне “змішування” різних методів,таких як інформаційних, політичних, економічних та гуманітарних інструментів допомогло РФ досягти успішної стратегії багатовекторного тиску при мінімізації прямих витрат і відповідальності на міжнародному рівні.

Від хронологічного огляду подій стає очевидним, що злочинні дії проти України не були у рамках суто військових дій. Навпаки, з часом політичний компонент набуває дедалі більшого значення. Це чітко показувало свою сутність у підтримці політичних рухів, направлених на порушення спокою внутрішньої ситуації, спробах впливу на виборчі процеси, поширенні дезінформації щодо легітимності української влади, а також темами, що піддавались маніпуляціям, ідентичності та історичної цінності. Саме тому аналізування гібридних загроз потребує не лише військово-стратегічного аналізу, але й глибокої оцінки політичних, економічних і соціальних механізмів, які використовувалися для досягнення стратегічних цілей агресора.

У цьому баченні політичної ситуації важливого значення набуває вивчення як прямих, так і непрямий гібридних атак. Їхня природа полягає у зв'язуванні народу чужих тез, створених шляхом обману "спільної історичної долі" та братерських коренів, які насправді переслідували мету нівелювати ідентичність української державності. Крім того, важливою складовою політичної гібридної агресії стала експлуатація економічної і соціальної залежності, яка маскувалася під формат "дружби народів" і "взаємовигідної співпраці".

Подальший аналіз методів ведення гібридної агресії дозволяє глибше зрозуміти як причини, так і наслідки застосування політичних інструментів впливу. Також це дасть можливість простежити еволюцію підходів агресора та адаптацію України до нових викликів у сфері національної безпеки.

Причини ведення політичної гібридної війни

Політична гібридна війна проти України стала логічним продовженням імперіалістичної стратегії Російської Федерації, яка зберігалася після розпаду Радянського Союзу. Незважаючи на формальне визнання України як незалежної держави, російські політичні еліти розглядали її територію як зону своїх "особливих інтересів" і не відмовлялися від спроб зберегти вплив над внутрішніми політичними процесами.

Основною метою розгортання військової гібридної агресії почалось з бажання зі сторони агресора зупинити антирадянський рух в Україні, що мав на меті викорінити на території українською держави та її інтеграції в західні політичні та військові структури. Після підписання “Угоди про асоціацію між Україною та Європейським Союзом” у 2014 році, було зрозуміло, що політична ціль України пересувається у сторону європейської і євроатлантичної групи.

Ця тенденція не пересікається з перспективою, яку Російська Федерація довгий час відбудовувала і направляла, а євроінтеграційні процеси в Україні не задовільняла плани Москви.

Другою не менш важливою причиною стала ідеологічна концепція "русского мира", що безупинно поширювалась кремлівською пропагандою з самих 2000-х років. Внаслідок цього, концепція, яку росіяни розглядали як "єдиний народ", до яких відносини українців і білорусів, була розділена “штучними політичними бар'єрами”. Соціальна гібридна агресія в бік України мала на меті перешкоджати інтеграції України в Європейський союз, а вплив Росії під наративом "відновлення історичної справедливості" та "захисту російськомовного населення", що застосовувався для легітимації дій агресора як на внутрішній арені, так і на міжнародному рівні.

Фінансові інтереси, в свою чергу, не стояли осторонь та відігравали важливу роль у формуванні чинників непрямої збройної агресії. Україна посідає важливу роль у транзитних маршрутах для вивозу ресурсів у ЄС, що значно допомагає Росії у поповненні “казни” та політичного важелю. Втрата контролю над українськими енергетичними та транспортними ресурсами могла призвести до зменшення економічного потенціалу Росії і обмеження її можливостей у зовнішньополітичному вимірі.

Не дивлячись на це, внутрішні політичні чинники у самій Російській Федерації вплинули на активізацію агресивної політики щодо України. Після 2012 року у Росії прослідковувалося збільшення соціального невдоволення, що потягло за собою економічну дестабілізацію, зниженням рівня життя та обмеженням соціальних прав. В умовах наростання внутрішньої нестабільності російське керівництво шукало способи консолідації суспільства навколо "зовнішнього ворога" та підняття патріотичних настроїв. Політична гібридна агресія проти України

стала засобом відвернення уваги населення від внутрішніх проблем та зміцнення авторитарного режиму.

Народні внутрішні незадоволення несло в собі чималиу небезпеку для існування Російської Федерації. Багаторічна інформаційна політика Росії, направлена на створення позитивного образу СРСР та негативного "обличчя" Америки, призвела до збереження у свідомості значної частини російського суспільства уявлень про Україну як "молодшого брата", що потребує "захисту" і "підтримки". Це створювало суспільне підґрунтя для виправдання агресивних дій проти суверенної держави.

Не слід упускати з виду той факт, що гібридна політична агресія дозволяла Російській Федерації запобігти прямої відповідальності перед судовою силою міжнародних інституцій. Застосування безконтактних інструментів, таких як спонсорування нейтрально налаштованих спільнот, маніпулювання громадською думкою, поширення дезінформації, сприяло створенню обставин, у яких дії агресора виглядали як внутрішньополітичні процеси в Україні, а не як зовнішнє втручання. Це ускладнювало формування єдиної позиції міжнародної спільноти та прийняття санкційних рішень.

Ще однією причиною стало прагнення Росії зберегти доступ до стратегічно важливих територій і ресурсів. Анексія Криму, яка стала першим проявом прямої гібридної агресії у 2014 році, забезпечила контроль над Чорноморським флотом та потенційними енергетичними ресурсами на шельфі Чорного моря. Політичні методи подальшого впливу були спрямовані на закріплення цих територіальних здобутків та легітимацію змін через створення "нової реальності", яку агресор намагався нав'язати світовій спільноті.

Отже, причини ведення політичної гібридної війни проти України мають комплексний характер і охоплюють ідеологічні, політичні,

економічні, соціальні та стратегічні чинники. Сукупність цих елементів формувала довгострокову стратегію впливу на Україну, спрямовану на ослаблення її державності, підрив національної єдності та утримання у сфері впливу Російської Федерації.

Методи реалізації політичної гібридної агресії

Способи успішного досягнення цілей завдяки гібридним загрозам є, як ми вже знаємо, комплексним що зберігає в собі використання багатосторонніх методів, направлених на підрив суверенітету, ослаблення національної єдності та досягнення стратегічних цілей агресора без збройної військової інтервенції. Гібридні методи включають в себе механізми традиційного ведення війни з сучасними технологіями інформаційного впливу, економічними маніпуляціями, а також психологічними операціями, що дозволяють реалізовувати зовнішньополітичні цілі з мінімальними втратами для агресора.

Провідним і сучасним способом проведення гібридних компаній є застосування інформаційних атак. Кібернетична атака, сама по собі, має природу дезінформаційності, пропагандистських наративів, маніпулювання громадською думкою і соціальними мережами. Росія неодноманітно використовувала цей спосіб впливу на внутрішню ситуацію в Україні, наприклад, під час Революції гідності та у період після 2014 року. Інформаційна кампанія прагнула меті створити хаос у суспільстві, знищити довіру до уряду та маніпулювати настроями населення. Використовувалися як традиційні ЗМІ, так і цифрові платформи, де здійснювався підрив репутації політичних лідерів, поширення фейкових новин і панічних настроїв, що вело до дестабілізації внутрішньої політичної ситуації в Україні.

Ще одним методом реалізації гібридної агресії є підтримка і фінансування політичних рухів, які виступають проти влади. Росія активно

використовувала ці методи в Україні, зокрема через підтримку проросійських партій, політичних сил і громадських організацій. Це включало фінансування "сепаратистських" настроїв на сході України, організацію проросійських акцій протесту в Криму та на сході України, а також підтримку антикорупційних рухів і політичних опонентів, які були здатні дестабілізувати політичну ситуацію в країні. Така діяльність велася під прикриттям "легітимних" політичних організацій і громадських об'єднань, але насправді служила інтересам агресора, який мав на меті створення внутрішніх політичних потрясінь в Україні.

У рамках політичної гібридної агресії використовувалися також психологічні операції. Зокрема, Росія активно використовувала технології маніпулювання масовою свідомістю через соціальні мережі, створення фальшивих новин, а також використання інтернет-ботів для поширення пропаганди та мобілізації протестних настроїв. Такі операції мають на меті створення враження соціальної нестабільності, непевності та страху, що може впливати на політичні рішення населення та політичних еліт. Психологічні операції включають також вкидання чуток і фейкових новин, що стосуються як внутрішніх проблем країни, так і її зовнішньої політики. Суть таких операцій — це не просто вплив на громадську думку, а й спроба дестабілізувати ситуацію за рахунок створення у населення відчуття безнадійності та нерозуміння того, хто є справжнім ворогом.

Не менш важливим методом реалізації політичної гібридної агресії є застосування нелегітимних, насильницьких дій на території противника, таких як організація масових протестів, громадянських заворушень, залучення військових формувань для підтримки сепаратистських рухів. Росія активно використовувала цей метод в Криму та на сході України. Це включало надання підтримки незаконним збройним угрупованням, таким як "ДНР" і "ЛНР", а також постачання зброї та техніки. Насильницькі дії

створюють відчуття конфлікту і допомагають дестабілізувати ситуацію на території, що стає об’єктом агресії.

Завершуємо методи реалізації гібридної агресії використання дипломатичних маніпуляцій і до єдиного підходу до міжнародних організацій. Росія активно застосовувала двоякі дипломати, які поєднували офіційні заяви про готовність до переговорів із підвищенням напруженості на місцях. Всі ці методи формують гібридну картину агресії, яка, не маючи явного військового характеру, здійснює систематичний вплив на суверенітет та внутрішню політику держави.

Отже, методи реалізації політичної гібридної агресії являють собою складний комплекс різноманітних інструментів, спрямованих на ослаблення державності, підрив національної єдності та реалізацію зовнішньополітичних цілей агресора за допомогою різних засобів, включаючи інформаційні, економічні, психологічні, а також насильницькі й дипломатичні методи.

2.2 Інформаційно-психологічний вплив в умовах гібридної війни: дезінформація, пропаганда

Виклики для подолання гібридних загроз несуть в собі багатошарову структуру, в той час як медіапростір для гібридних загроз можна вважати найкращим середовищем для поширення свого впливу на країни-жертви таким загрозам. «Сьогоднішня гібридна війна розгорнута на всіх можливих напрямках, це не лише інформаційна війна. Це однозначно війна економічна, репутаційна, смислова, людська… На неї повинні працювати всі, хто має вплив на населення: актори, співаки,

письменники, режисери. Воєнні дії створюють лише фон для більш масштабної війни в людському розумінні» [1, с. 264].

Сутність гібридних загроз полягає передусім у інформаційному впливі, тиску на медіа-культурний простір громадян, вплив через соціальні мережі, підрив довіри до влади через ЗМІ та навіть рекламу.

Варто навести приклад таких викликів роботою Оксани Левантович у її праці “ГІБРИДНІ ВІЙНИ XXI СТОЛІТТЯ: НОВІ ВИКЛИКИ ДЛЯ МЕДІА ПРОСТОРУ”. Автор виділяє ключові виклики гібридних загроз через медіапростір, я яких розкривається механізм роботи гібридної агресії, а також звернути увагу на роботи, які сам автор посилається у своїй праці.

Цитата з роботи авторки, у якій вона посилається на роботу іншого видатного політичного аналітика: “Френк Г. Хоффман, колишній офіцер морської піхоти, науковий співробітник міністерства оборони США, наголошував, що у майбутньому «конфлікти будуть мультимодальними (тобто такими, що ведуться різними способами) та багатоваріантними, що не входять в межі простої конструкції ведення збройного конфлікту чи війни. А майбутні загрози можуть більшою мірою бути охарактеризованим як гібридне співвідношення традиційних та нерегулярних стратегій і тактик, це децентралізоване планування та виконання, участь недержавних акторів з використанням одночасно простих та складних технологій»”

Природа викликів гібридним загрозам

Основі виклики через медіа простір поділяються на втрату контролю над інформаційним простором через YouTube, TikTok, Instagram, Facebook тощо. Фейкові новини - один з найсуттєвіших способів впливу на свідомість громади, яскравим прикладом якого є “здача Києва”, шо РФ активно поширювало у 2022 році через ЗМІ. Атаки на довіру, у яких Російська Федерація активно створювала дії Збройних Сил України,

внаслідок чого певна група громадян “відвернулась” від власної причетності до захисту суверенітету України.

Виклики гібридним загрозам несуть характер глобального спротиву, а саме сприйняття таких загроз розпалює у свідомості громадян волю до спротиву зовнішньої агресії. Міненко Є. С. - автор статті “ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЛЮДИНИ УМОВАХ ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ”, що допоміг краще розібратись у специфіці самих викликів гібридним загрозам, зазначив: “Сам термін “гібридна війна” немає єдиного визначення і може трактуватися різними спеціалістами по-різному. Його розуміння та вживання змінюється залежно від контексту та актуальних подій. Також важливо відзначити, що в західних наукових дослідженнях та дискусіях термін “гібридна війна” почав використовуватися приблизно з середини 2000-х років і може мати відмінні підходи та інтерпретації від тих, використовується сьогодні”.

З початку 2014 року Україна стала епіцентром новітнього типу війни, який об'єднує традиційні воєнні дії з інформаційними, політичними, економічними та соціальними засобами впливу. Саме з моменту початку російської агресії, анексії Криму та розгортання конфлікту на сході країни, Україна зіткнулася з форматом загроз, який у науковій, політичній та безпековій риториці дістав назву «гібридної війни».

Російська Федерація не лише здійснила збройну агресію, порушивши міжнародне право та основоположні принципи суверенітету, а й вибудувала цілісну стратегію, спрямовану на підрив стабільності України зсередини. Ця стратегія не обмежувалася використанням військової сили — вона включала маніпуляції у медійному просторі, втручання у політичні процеси, кібератаки, підтримку маріонеткових утворень на тимчасово окупованих територіях, розпалювання міжетнічних та соціальних конфліктів. Такий підхід дозволив агресору уникнути прямої відповідальності за деякі дії та створити атмосферу інформаційної

плутанини, яка гальмувала як внутрішню мобілізацію українського суспільства, так і зовнішню реакцію міжнародної спільноти.

Слід відзначити, що до 2014 року гібридна війна не розглядається як основна форма ведення бойових дій. Однак дії Росії радикально змінили парадигму воєнного мислення у XXI столітті. Агресор застосував методи, що поєднують «м'яку силу» з елементами терору, класичної пропаганди та економічного тиску, створюючи таким чином багатовекторні загрози. Це призвело до того, що питання національної безпеки більше не могло зводитися лише до оборонного сектору — воно стало справою медіа, економіки, культури, освіти і навіть буденної свідомості громадян.

Український досвід став прикладом того, як одна держава може бути змушена реагувати на гібридний наступ у всіх сферах одночасно, формуючи нові підходи до стратегічної комунікації, кіберзахисту, інформаційної політики та державної безпеки загалом. І саме російська агресія стала каталізатором переосмислення поняття загроз: вони перестали бути лише зовнішніми та очевидними. Вони набули рис прихованості, поступовості, багатовимірності, що й дозволяє говорити про гібридний характер сучасного конфлікту.

У цьому підрозділі буде розглянуто, яким чином Російська Федерація стала чинником формування гібридних загроз для України, які саме механізми були використані агресором, та як ці загрози вплинули на безпекову ситуацію в країні та регіоні. Особлива увага продивлятиметься не лише воєнному, але й політико інформаційному виміру російської агресії, який у значній мірі визначає характер сучасної війни та ускладнив традиційні уявлення про мир і конфлікт.

Ефективність застосування інструментів гібридних загроз Російською Федерацією

Ефективність впливу застосування інструментів гібридних загроз в сторону України

Гібридна агресія, здійснювана Російською Федерацією проти України, показала високу ефективність на початкових етапах конфлікту, насамперед через неготовність держави до такого формату загроз. Використання різнорідних інструментів — від дезінформації та кібероперацій до економічного тиску та підтримки сепаратизму — дозволило агресору паралізувати певні елементи національної безпеки України без безпосереднього вторгнення регулярних військ на початковому етапі.

Одним з найефективніших інструментів стала інформаційна війна. Через контрольовані ЗМІ, соціальні мережі, інтернет-ресурси та телеканали, які транслювалися на території України, Росія послідовно формувала альтернативну реальність для частини населення. Особливо ефективною ця стратегія виявилася в Криму та на Донбасі, де інформаційний простір був тривалий час заповнений проросійською риторикою, маніпуляціями на темах "захисту російськомовних", "неонацизму" та "громадянської війни". Як наслідок, значна частина місцевого населення або підтримала сепаратизм, або проявила байдужість до порушення територіальної цілісності України.

Ще одним прикладом ефективного гібридного впливу стали кібератаки. Масштабні хакерські операції, зокрема атаки на енергетичну інфраструктуру (BlackEnergy, Industroyer), електронну пошту державних установ, медіа та фінансовий сектор, довели здатність РФ дестабілізувати критичну інфраструктуру без фізичного втручання. Злам інформаційних систем, фальсифікація документів, витік службової інформації мали не лише безпосередній вплив на функціонування державних органів, а й підірвали довіру громадян до держави.

Політичні інструменти також відіграли важливу роль. Росія активно впливає на політичну ситуацію в Україні як через внутрішніх агентів впливу (окремі політики, партії, аналітичні центри), так і через

зовнішні дипломатичні канали. Створення штучної «суб'єктності» терористичних угруповань на Донбасі дозволяло Росії дистанціюватися від прямих звинувачень в участі у війні, ускладнюючи дипломатичну реакцію Заходу. У міжнародних організаціях Москва систематично блокувала або зводила нанівець ухвалення рішень щодо посилення тиску на неї, маніпулюючи правом вето, двосторонніми домовленостями з окремими державами-членами тощо.

Окремо слід відзначити економічні інструменти гібридної війни, які Росія застосовувала через торговельні обмеження, енергетичну залежність, блокування транзиту, знищення інфраструктури та підрив платоспроможності державних підприємств. Такі дії мали не лише економічний, а й соціальний ефект, сприяючи зростанню напруги в суспільстві, зниженню рівня довіри до влади та створенню вразливого ґрунту для антидержавної пропаганди.

Важливою особливістю гібридного підходу стала спроможність комбінувати інструменти у реальному часі, адаптуючи їх до обставин. Наприклад, військові дії на Донбасі нерідко супроводжувалися потужними інформаційними кампаніями, які дискредитували Збройні Сили України, поширювали фейки про злочини українських військових, або, навпаки, вихваляли бойовиків. Така взаємодія різних форм впливу дозволяє досягати результату без тотального застосування сили.

Загалом ефективність гібридних загроз з боку Росії проявилася в тому, що українська держава змушена була витрачати ресурси одночасно на військову оборону, інформаційний захист, реформування безпекових структур, адаптацію правової системи до нових викликів. Це значно ускладнило процеси державного управління та спричинило значну психологічну, економічну і політичну напругу в суспільстві.

Разом із тим, з часом ефективність гібридних впливів Росії почала знижуватись. Українське суспільство стало більш стійким до маніпуляцій,

державні інституції адаптувалися до умов гібридної війни, було розпочато масштабні реформи у сфері безпеки, ЗМІ, оборони та цифрової безпеки. Проте важливо визнати, що саме початкова ефективність гібридних загроз дозволила Росії здобути низку тактичних переваг і затягнути конфлікт на роки.

- *Ефективність боротьби з гібридними загрозами, розпаленими Росією*

З початку агресії у 2014 році Україна стикнулася з необхідністю протидіяти нетиповим, асиметричним викликам, які не охоплювали лише військову площину.

В умовах гібридної війни держава була змушена оперативно реформувати свої безпекові структури, адаптуватися до нової природи загроз і вчитися діяти одночасно в інформаційному, кібернетичному, економічному та дипломатичному вимірах.

Одним із ключових досягнень у боротьбі стало поступове вибудовування стійкої системи стратегічних комунікацій. Після 2014 року було заборонено трансляцію низки російських телеканалів, обмежено доступ до соціальних платформ, що використовувалися для пропаганди, а українські медіа стали більш чутливими до викликів інформаційної безпеки. Згодом з'явилися незалежні платформи з перевірки фактів (наприклад, StopFake), а журналістська спільнота стала активним гравцем у боротьбі з дезінформацією.

На фронті кібербезпеки Україна досягла значного прогресу. Було створено Національний координаційний центр кібербезпеки при РНБО, а держава почала активно співпрацювати з західними партнерами та НАТО у сфері протидії кібератакам. Хоча загроза з боку Росії залишається, Україна більше не є настільки вразливою, як у 2015 році, коли атаки виводили з ладу цілі енергетичні блоки.

У військовій площині було проведено реформу Збройних Сил України: суттєво зросла боєздатність армії, покращено систему управління, командування та логістики. Перехід до стандартів НАТО сприяв уніфікації процедур і підвищенню мобільності. Окрім того, широке залучення добровольчих підрозділів та формування територіальної оборони стали відповіддю на децентралізований характер гібридної загрози.

Незважаючи на досягнення, боротьба з гібридними загрозами залишається складною і потребує постійної адаптації. Росія змінює тактику, знаходить нові точки тиску — від релігійного впливу до економічної дестабілізації. Водночас сам факт виживання української держави в умовах тривалого гібридного тиску вже є свідченням ефективності її спротиву. Україна поступово перетворилася на майданчик для формування нових підходів до протидії гібридній агресії, які вивчають та переймають інші держави.

На розквіті військово-політичних технологій (серед яких і гібридні загрози), психологічний важіль набув такої ваги, що встигнути за їхнім розвитком стає дедалі важче. Історія сучасної російсько-української війни, що бере свій початок з 2014 року, яскраво засвідчила той факт, що центральна тенденція криється не лише на полі бою, а й у свідомості людей. Інформаційне поле і сприйняття реальної ситуації – деформоване, штучно спотворене, і у більшості випадках служить зброєю. Використання цього інструменту несе в собі не менш руйнівний характер аніж застосування звичайних озброєнь. Дезінформація, фейки, пропагандистські посили до громади, направлені на підірвання віри, розкол суспільства, посіяти страх або недовіру до влади, — це стало невід’ємною частиною стратегії ворога.

Специфіка сьогоднішній інформаційних війн розкривається в її можливості до зміни форми та все проникності. Під дією цифрового захоплення людства навіть звичайний громадянин, позбавлений військової

підготовки, легко стає учасником інформаційної боротьби — як ціль, як передавач або навіть як носій ворожих наративів. Це створює нову реальність, у якій критичне мислення та інформаційна гігієна стають не розкішшю, а умовою виживання суспільства.

Україна стала яскравим прикладом, як цілеспрямовані інформаційно-психологічні операції можуть впливати на громадську думку, виборчі процеси, внутрішню політичну стабільність та міжнародний імідж перед іншими державами. У перші роки після окупації Криму і початку бойових дій на Донбасі кремлівській пропаганді вдалося посіяти розбрат не лише серед українців, а й у світовій спільноті. Ворожа сторона активно використовував як звичні для нас джерела(телебачення, газети), так і нові – соціальні мережі, інтернет-ресурси, ботоферми. "Альтернативні точки зору" стали маскуванням ворожих гачків і транслювались у формі “спотворених” фактів, конспірології, емоційно заряджені меседжі, які підірвали довіру до офіційної інформації.

Дезінформація і “фейкові новини” це явище, яке по своїй суті потребує більш глибокого аналізу не лише з точки зору політичної науки, а й психологічної та дослідницької. Необхідно акцентувати увагу не тільки на результати впливу, а й зрозуміти його внутрішні механізми: яким чином маніпулювати свідомістю, як формуються фейкові наративи, на які емоції робиться ставка, і які соціальні групи є найбільш вразливими до впливу. Питання в тому, як інформація стає зброєю — і як захиститися від неї.

У цьому підрозділі розглядатимуться основні форми та методи дезінформації, роль пропаганди в сучасному гібридному конфлікті, приклади впливу на українське суспільство у 2014–2024 роках. Особлива увага буде приділена аналізу конкретних кейсів, а також стратегіям протидії на рівні держави й громадянського суспільства. Також буде висвітлено, чому інформаційна безпека стала складовою національної безпеки України.

Приклади дезінформаційних кампаній та їхній вплив на свідомість українського суспільства

Одним із найяскравіших (якщо не найуспішнішим) прикладів інформаційної кампанії з боку Російської Федерації став період анексії Криму у 2014 році. Протягом декількох тижнів російські ЗМІ масово транслювали меседжі про нібито «загрозу життю російськомовного населення», «неонацистський переворот у Києві» та «легітимність кримського референдуму». Пропаганда апелювала до страху, історичної пам’яті (особливо до Другої світової війни) та етнічної ідентичності, створюючи враження нагальної небезпеки, яка виправдовує будь-які дії з боку Росії. Ці наративи активно транслювалися як всередині самої РФ, так і на окупованих територіях, а через супутникове телебачення — і на значну частину південного сходу України.

Методи медійного контенту, який просуває ворожа країна, зіграла потужну роль на частину українського народу — в першу чергу на ту спільноту, яка протягом десятків років знаходилась під впливом російського культурного простору. У баченні світу цих людей ґрунтувалась альтернатива до українського інформаційного поля, в якій РФ виглядала як «захисник», а Україна — як «вороже середовище». Це призвело до масової підтримки анексії серед частини кримчан і створило ґрунт для подальших дій у східних регіонах України.

Другим не менш впливовим прикладом можна вважати початок конфлікту на Донбасі, коли з російських і проросійських джерел ширилася інформація, яка не відповідає дійсності про «розп’ятого хлопчика в Слов’янську», «карателів» із ЗСУ. Антиукраїнські ЗМІ, на які йшла левова частка бюджету РФ були ефективними в досягненні своєї мети. Російські журналісти використовували базову психологічну реакцію людини на жорстокість і несправедливість, наслідком чого стала деморалізація меншин, підвищення рівня тривожності, зміцнення стереотипів, а в

окремих випадках — відкритий спротив українським військовим силам з боку місцевих мешканців.

Окремої уваги заслуговує кампанія дискредитації українських військових. Через соціальні мережі та проросійські ЗМІ поширювались повідомлення про мародерства, аморальну поведінку, корупцію в армії тощо. Часто ці матеріали супроводжувалися емоційними заголовками, маніпулятивними фото або відео, що виривалися з контексту. Метою було знищити довіру до Збройних Сил України як до захисника. У відповідь на це українські медіа, волонтерські організації та держава почали формувати власний інформаційний фронт, зокрема створювати проекти на зразок «ІнформНапалму», «StopFake», «Баба і кіт», які перевіряли інформацію і давали змогу суспільству бачити фейки в реальному часі.

Період пандемії COVID-19 допоміг агресору і став ще однією нагодою для РФ активізувати інформаційні атаки. У 2020–2021 роках поширювалась інформація про так звані «лабораторії США в Україні», небезпечність вакцин, «таємні експерименти над українцями» тощо. Метою даних інформаційних кампаній була підірвати довіру до міжнародних партнерів, дискредитувати українську владу й підірвати єдність у суспільстві. Попри спростування цих заяв міжнародною науковою спільнотою, фейки спричиняли хвилі паніки, сприяли поширенню антивакцинаторських настроїв і послабленню дисципліни в періоди епідемічної загрози.

Найагресивнішим етапом російської пропаганди став період повномасштабного вторгнення на територію України, де кремлівська сторона мала набагато більше простору для поширення ще більших інформаційних атак. Протягом перших тижнів окупанти активно поширювали меседжі про «капітулюючу владу», «здачу Києва», «дружнє ставлення до росіян у південних регіонах». Особливо активно діяли проросійські Telegram-канали, які подекуди випереджали офіційні

джерела, створюючи в людей відчуття невпевненості, недовіри до ЗМІ та хаосу.

Інформаційний вакуум і брак налагоджених комунікацій у перші дні війни дозволили цим джерелам тимчасово впливати на свідомість українців — зокрема, у вигляді паніки, виїздів за кордон, масового скуповування товарів.

Проте варто зазначити й протилежну тенденцію. В умовах воєнного стану українське суспільство продемонструвало високий рівень адаптації до нової інформаційної реальності. За короткий час формувалася культура перевірки інформації, активізувалися ініціативи з медіаграмотності. Зросла довіра до офіційних джерел — насамперед до ЗСУ, Генштабу, Офісу Президента, які почали регулярно й структуровано надавати інформацію. Таким чином, спроби дестабілізувати суспільство шляхом інформаційних атак не лише не досягли мети, а й стали каталізатором нової інформаційної мобілізації.

Окремим фактором впливу стала російська пропаганда щодо міжнародного становища України. Починаючи з 2014 року, систематично просувалися меседжі про «зовнішнє управління», «втрату суверенітету», «невдалі реформи» тощо. Ці заяви транслювались через низку проросійських політичних діячів, блогерів, телеканалів. Суспільний ефект від них був неоднозначний: частина людей дійсно втратила віру в здатність держави до змін, інші — активніше почали підтримувати євроінтеграційний курс як опір зовнішньому тиску. У підсумку російська дезінформація часто спрацьовувала не завдяки правдоподібності, а завдяки повторюваності й апеляції до емоцій.

Врешті решт, інформаційно-психологічний вплив як елемент гібридної війни суттєво вплинув на формування суспільної думки в Україні протягом останнього десятиліття. Він сприяв як поширенню недовіри й дезорієнтації, так і — як парадокс — формуванню імунітету проти фейків і

згуртованості в кризових умовах. Український досвід у цьому контексті є унікальним: через постійну інформаційну атаку суспільство навчилося бути критичним, мобілізованим і в певному сенсі — стійким до зовнішнього впливу.

Приклади боротьби проти дезінформації та інформаційно-психологічних атак

Після початку гібридної агресії у 2014 році Україна була змушена не лише відповідати на зовнішні військові виклики, а й вибудовувати власну інформаційну безпеку. Усвідомлення масштабів загрози з боку російської пропаганди стало поштовхом до створення нових інституцій, інформаційних ініціатив, законодавчих змін та просвітницьких кампаній. Спротив дезінформації набув форми багаторівневої стратегії, яка включала як державні, так і громадські ініціативи, що спільно спрямовувались на підвищення рівня медіаграмотності населення та оперативну протидію фейкам.

Однією з перших відповідей держави стало блокування російських телеканалів на території України. Уже в 2014 році Рада національної безпеки і оборони ухвалила рішення щодо обмеження доступу до мовлення, що містить ознаки пропаганди війни, маніпуляцій та розпалювання ворожнечі. Згодом було заблоковано й низку російських сайтів, зокрема соціальні мережі «ВКонтакте» та «Одноклассники», які стали інструментами збирання даних і поширення проросійських наративів. Це рішення викликало багато дискусій, але з часом виявилось виправданим: завдяки обмеженню доступу до джерел токсичної інформації вдалося суттєво знизити рівень її впливу на українську аудиторію.

На громадському рівні однією з ключових ініціатив у протидії дезінформації став проєкт StopFake, заснований 2014 року викладачами та студентами Могилянської школи журналістики. Цей проєкт систематично відстежував фейки, які поширювались у ЗМІ, зокрема російських, і надавав

перевірену інформацію з джерел, яким можна довіряти. StopFake не лише спростував брехливі повідомлення, а й пояснював механізми маніпуляції, тим самим сприяючи зростанню критичного мислення у суспільстві. Проект також набув міжнародного розголосу та став прикладом для подібних ініціатив у інших країнах, які зіткнулись із російським впливом.

Ще одним важливим кроком стало створення Центру протидії дезінформації при РНБО у 2021 році. Центр працює як аналітична й комунікаційна структура, покликана відслідковувати загрози інформаційній безпеці, координувати дії між відомствами, оперативно реагувати на фейки, гібридні впливи та кіберзагрози. У перші місяці повномасштабного вторгнення цей орган став ключовим елементом інформаційного спротиву — зокрема, завдяки публікації щоденних зведень щодо інформаційної обстановки, викриттю фейків і демонтажу ворожих наративів.

Не менш важливим елементом спротиву стала система єдиного голосу — стратегія інформаційної єдності, яку координували з Офісу Президента та Генерального штабу. Вона передбачала чітку й уніфіковану комунікацію від офіційних джерел, що дозволило уникнути плутанини та інформаційного вакууму. Поява офіційних Telegram-каналів, сторінок ЗСУ, ДСНС, МОЗ, Міністерства оборони, які регулярно інформували населення, стала однією з причин зростання довіри до українських інституцій. Зокрема, брифінги Олексія Данілова, Олексія Арестовича та інших речників влади на початковому етапі війни сприяли збереженню спокою та єдності в суспільстві.

Велику роль у протидії інформаційно-психологічним атакам відіграли волонтерські та журналістські ініціативи. Проєкти на зразок «ІнформНапалму» не лише виявляли фейки, а й займаються ідентифікацією російських військових, причетних до злочинів в Україні, збирають докази присутності регулярних підрозділів РФ на Донбасі. Їхня

діяльність стала не лише формою інформаційного спротиву, а й доказовою базою для міжнародних судових інстанцій.

Не можна оминути увагою і просвітницькі програми з медіаграмотності, які почали реалізовуватись як у неформальній освіті, так і в межах громадських ініціатив. Міністерство освіти та науки України, за підтримки міжнародних партнерів, поступово впроваджує елементи медіаграмотності в шкільну програму, зокрема через курси «Критичне мислення», інтеграцію у предмет «Громадянська освіта», а також у формі окремих факультативів. Університети почали включати теми медіаграмотності до курсів з журналістики, права, політології. Водночас НУО на зразок «Інтерньюз-Україна», «Детектор медіа», «Лабораторія цифрової безпеки» проводять тренінги, онлайн-курси, створюють мультимедійні платформи для підвищення інформаційної стійкості громадян.

Одним із сучасних прикладів ефективної інформаційної кампанії став проект «разом», створений у відповідь на спроби Росії посіяти ворожнечу між регіонами України. У межах цього проекту висвітлювалися історії людей з різних частин країни, які спільно боронять державу, допомагають ЗСУ, підтримують одне одного, незалежно від мови чи походження. Такі наративи формували відчуття єдності, солідарності, спільної долі — і цим нейтралізували спроби посіяти розкол.

Платформи на кшталт «Телебачення Торонто», «Української правди», «Суспільного мовлення» та інших незалежних медіа також відіграли важливу роль, створюючи альтернативу для молоді — з гострим гумором, аналітикою, перевіреними фактами. Їхній вплив особливо помітний у міському, освіченому середовищі, де критичне мислення стало частиною інформаційної культури.

Також варто згадати роль міжнародної підтримки. Європейський Союз, НАТО, уряди окремих держав допомагали Україні у сфері

інформаційної безпеки: проводили спільні навчання, підтримували створення спеціалізованих центрів (наприклад, протидії кіберзагрозам), фінансували програми медіаграмотності, а також публічно спростовували наративи російської пропаганди.

Таким чином, боротьба з дезінформацією в Україні з 2014 року набрала системного характеру. Вона об'єднала державу, громадянське суспільство, міжнародних партнерів і самих громадян у спільному спротиві інформаційним загрозам. Хоча виклики залишаються масштабними, зокрема з огляду на зміну форм і каналів впливу (зокрема, через TikTok, YouTube, анонімні месенджери), однак українське суспільство продемонструвало надзвичайну здатність до адаптації й самозахисту. Цей досвід сьогодні вивчається як приклад інформаційної стійкості в умовах гібридної війни.

Ефективність і наслідки боротьби проти інформаційних атак

Боротьба з інформаційно-психологічним впливом упродовж останнього десятиліття стала одним із ключових чинників збереження державності України в умовах гібридної війни. Ефективність цієї боротьби можна оцінити за кількома вимірами — зокрема, у зміні суспільних настроїв, зростанні критичності мислення громадян, підвищенні довіри до українських джерел інформації, а також у стримані впливу ворожих наративів на широкі верстви населення.

Одним із найбільш видимих результатів стало значне зменшення довіри до російських медіа. Якщо ще у 2013 році в деяких регіонах України російські телеканали залишаються основними джерелами інформації, то вже після 2014 року, а особливо після 2022 року, їхній вплив практично зник. За даними соціологічних досліджень Центру Разумкова та Київського міжнародного інституту соціології, понад 85% українців повністю відкидають російські ЗМІ як джерело правдивої інформації. Це демонструє глибоку трансформацію у сприйнятті інформації, зумовлену як

трагічними подіями війни, так і активною інформаційною політикою держави й громадських ініціатив.

Ще одним важливим результатом стало формування в Україні культури інформаційного спротиву. У кризових умовах, коли з перших днів повномасштабного вторгнення РФ поширювались фейки про здачу Києва, масові капітуляції чи знищення військових структур, українці зберігали спокій та довіру до офіційних джерел. Оперативні спростування, якісна інформаційна робота ОК "Північ", ЗСУ, ДСНС, Центру протидії дезінформації та інших структур допомогли уникнути паніки та посилити єдність суспільства.

Боротьба з дезінформацією також сприяла зростанню медіаграмотності, особливо серед молоді та активної частини населення. Громадяни дедалі частіше ставлять під сумнів інформацію з неперевірених джерел, перевіряють факти, звертаються до офіційних платформ і вивчають механізми маніпуляції. Це свідчить не лише про ефективність освітніх кампаній, а й про певну еволюцію суспільної свідомості в напрямі стійкості до впливу.

На міжнародному рівні українська стратегія протидії інформаційним загрозам отримала визнання та підтримку. Європейські інституції, НАТО, а також численні медіаорганізації розглядають український досвід як приклад активної самооборони в інформаційному просторі. Співпраця з ЄС у рамках стратегічної комунікації, обмін практиками з країнами Балтії, які також мають досвід протидії російському впливу, зміцнили українську позицію як суб’єкта інформаційної безпеки, а не лише об'єкта атак.

Утім, не варто ідеалізувати ситуацію. Ворог продовжує адаптуватись, використовує нові платформи, гібридиз меседжі, що часто подаються під виглядом "громадянського занепокоєння" або "альтернативної думки". Інформаційна війна не завершилась, вона лише

змінила форму. Тому здобутий досвід має стати основою для довготривалої політики інформаційної безпеки, яка включатиме законодавче оновлення, кіберзахист, просвітництво й міжнародну співпрацю.

У підсумку, боротьба України з інформаційними атаками засвідчила не лише ефективність конкретних дій, а й значну зрілість суспільства, здатного протистояти маніпуляціям, зберігати єдність у часи хаосу та чинити опір на інформаційному фронті не менш потужно, ніж на військовому.

2.3. Кіберзагрози як складова гібридної війни

Упродовж останніх десятиліть війна дедалі частіше виходить за межі традиційного бойового поля, набуваючи прихованих і багатовимірних форм. Сучасне протистояння держав дедалі менше нагадує класичні конфлікти минулого, де домінували танки, гармати та авіація. Натомість головною ареною боротьби дедалі частіше стає інформаційний простір, а серед найнебезпечніших видів зброї вирізняються не фізичні ракети, а коли й алгоритми. У цьому контексті кіберзагрози стали ключовим інструментом новітнього типу війни — гібридної, яка поєднує військові, економічні, інформаційні та технологічні засоби впливу.

Поняття гібридної війни охоплює широкий спектр інструментів, що використовуються для досягнення політичних цілей без формального оголошення війни. Вона передбачає гнучке поєднання як відкритих, так і прихованих методів тиску, серед яких особливе місце посідають кібероперації. Атаки на інформаційні системи державних органів, критичної інфраструктури, фінансового сектору та медіа-компаній дедалі частіше використовуються для дестабілізації суспільства, послаблення

обороноздатності та посіву паніки серед населення. При цьому агресор зазвичай маскує свою присутність, діючи руками проксі-груп або через складні мережі анонімних виконавців, що ускладнює притягнення до відповідальності та реагування.

Україна стала одним із перших прикладів того, як кіберзагрози інтегруються у загальну стратегію гібридної війни. Починаючи з 2014 року, держава зазнає безперервного тиску в кіберпросторі з боку Російської Федерації. Від атак на сервере ЦВК, енергетичну систему та медіа-ресурси — до масштабних кампаній з дезінформації та маніпулювання суспільною свідомістю в соціальних мережах. Такі дії не лише створюють безпосередню загрозу національній безпеці, а й демонструють, наскільки тісно цифрова сфера переплетена з політичними, економічними та воєнними вимірами сучасного світу.

З огляду на стрімкий розвиток інформаційних технологій, кіберпростір став не просто новим фронтом, а фундаментальним середовищем боротьби за вплив і перевагу. Успішна протидія кіберзагрозам вимагає не лише технологічних рішень, а й глибокого усвідомлення їхнього місця в системі гібридної війни. Саме це і становить предмет дослідження: з’ясування природи кіберзагроз, їхніх механізмів, цілей, а також шляхів захисту національних інтересів у нових умовах стратегічного протистояння.

Природа кіберзагроз у гібридній війні

Розглядаючи різні види некласичних гібридних загроз, можна виділити одну складну і не менш рушійну частину комплексного методу невійськових видів атак, а саме кібернетичну загрозу : сутність її розкривається у анонімності, важкого морального тиску, агресивній інтервенції та важкого пошуку “хвосту”, але що робить цей вид атаки надзвичайно ефективними. Її природа полягає не лише в пошкодженні інформаційних систем чи порушенні зв’язку, а й у руйнуванні довіри — до

держави, інституцій, фактів, навіть до власного сприйняття реальності. Інформація стає зброєю, а ціль — не лише інфраструктура, а й свідомість громадян.

Природа кіберзагроз проявляється у поєднанні технічного й психологічного методів роботи. З одного боку, це шкідливі програми, віруси, бот-мережі, фішингові атаки, а з іншого — кампанії з дезінформації, маніпуляції громадською думкою, вкидання фейків. Їхня ефективність полягає у швидкому масштабуванні та точковому впливі на слабкі місця соціуму. Варто зазначити, що кіберзагрози рідко виникають хаотично — зазвичай вони мають стратегічну мету, яка виходить за межі конкретного інциденту.

Механізми реалізації кіберзагроз

Метод “кіберпаутини” в технологічному просторі, як правило, здійснюється через кілька основних механізмів. Один з найпоширеніших — атака на критичну інфраструктуру. Такі випадки були зафіксовані в Україні у 2015 та 2016 роках, коли внаслідок хакерських атак частково була паралізована енергосистема. Уразливість енергетичного сектору, банківських систем або транспортної мережі може мати катастрофічні наслідки для функціонування держави.

Соціальна інженерія - другий спосіб застосування кібернетичного методу ведення гібридних загроз — тактика обману, користувача змушують надати конфіденційні дані або виконати дії, які відкривають доступ до системи. Тиск таким способом здійснюється на людський фактор, що часто виявляється слабкою ланкою в безпеці. Слід наголосити про вплив на інформаційне поле через ботоферми, маніпуляцію пошуковими алгоритмами, створення фейкових новинних ресурсів. Держава агресор, знаючи про багаторівневі операції, застосовують кібернетичну загрозу у поєднанні з психологічним важелем тиску (PSYOPS). Такий підхід спрямований на довгострокове ослаблення

супротивника шляхом підриву його внутрішньої стабільності, дискредитації керівництва та сіяння розбрату між громадянами. В умовах демократії ці процеси особливо небезпечні, адже використовують відкритість суспільства проти нього самого.

Мета застосування кібернетичних атак у веденні гібридної війни

Поділенням високотехнологічних загроз (кібернетичних) керує прагнення задовольнити одразу декілька інтересів країни-агресора. З одного боку, це дестабілізація — створення хаосу в суспільстві, підрив довіри до влади та інституцій, порушення звичного ритму життя. Наприклад, злами урядових сайтів у період виборів можуть поставити під сумнів легітимність процесу та призвести до внутрішньополітичної кризи.

З другого - шпигунство, у якому криється здобуття стратегічної інформації, доступ до конфіденційних державних даних або приватних комунікацій. Така інформація може використовуватись для шантажу, дискредитації чи навіть планування воєнних дій.

На додаток, такий метод несе в собі руйнування — прямий вплив на об’єкти інфраструктури з метою їх виведення з ладу. В умовах війни або загострення ситуації атака на енергетичну систему, телекомунікації чи логістику може мати наслідки, порівнянні з бомбардуванням.

І, нарешті, вплив на міжнародну репутацію — через поширення дезінформації про державу на зовнішньополітичній арені, створення образу нестабільної, корумпованої чи неадекватної країни. Це дозволяє ворогові послабити підтримку союзників або підірвати міжнародні санкційні механізми.

Шляхи захисту національних інтересів

Протидію кібернетичним атакам можна назвати успішнеою у тому випадку, коли сили, які були покладені для подолання новітнього методу агресивного впливу на іншу країну, було комбіновано декількома механізмами — технологічними, правовими, організаційними та

освітніми. Передусім, необхідність створити стійку та адаптивну систему кібербезпеки, яка охоплюватиме як державні органи, так і приватний сектор, включає інвестиції в інфраструктуру, постійне оновлення систем захисту, запровадження стандартів кібер гігієни на всіх рівнях.

Не менш важливою дією у при захисті від кібератак криється у розбудові нормативно-правової бази, яка кооперує сферу кібербезпеки та передбачає відповідальність за кібератаки. Питання цифрового суверенітету, збереження персональних даних та прав громадян повинні бути чітко врегульовані з урахуванням міжнародних практик. Також доцільним можна назвати створення спеціалізованих кіберсил у структурі оборонного сектору, що мають можливість не лише захищатися, а й здійснювати превентивні дії.Інформаційна народна освіта грає переважну роль під час масштабних кібератак. І нарешті, міжнародна координація. Оскільки кіберпростір не має кордонів, ефективна протидія кіберзагрозам можлива лише через співпрацю з союзниками, обмін інформацією, участь у спільних ініціатив та оперативному реагуванні на глобальні виклики. Саме тому Україна активно залучається до діяльності в межах ЄС, НАТО та інших міжнародних структур.

Кібернетичні атаки Росії проти України: приклади, протидія та ефективність

Кібер Вимір гібридної війни

Російсько-українська війна стала кривавим прикладом того, що війна, на жаль, дійсно слугує для певних аспектів життя людей двигуном процесу. Жорстокі методи, націлені на досягнення своїх політичних амбіцій і задоволення військових інтересів, вражають масштабом того простору, у якому наділені привілеями групи осіб мають змогу для застосування різноманітних способів для посилення свого потенціалу.

Багаторічні військові зіткнення між обома країнами розвинули в народах вміння розвивати ті сфери, у яких вони по праву вважаються професіоналами, адже беручи до прикладу кібернетичний спосіб нанесення політичної шкоди, не важко виділити той рівень руйнації на життєво необхідні сфери людства.

Впродовж усієї дослідницької роботи судження, які були висунуті на професійний огляд, завжди підкріплюватися прикладами з реального політичного життя.

Розглянувши конкретні ситуації, у яких застосування технологічних методів досягнення військових цілей перейшло у агресивні атаки на, перш за все, духовний стан українського народу, можна зробити висновки, наскільки ефективними можуть бути способи, які не вважаються класичними.

2. Приклади російських кібератак на Україну

2.1. Атака на енергосистему (2015)

Грудень 2015 року став знаковим для хакерів, найнятих Росією, що здійснили кібернетичну атаку на енергетичну інфраструктуру України, внаслідок чого близько 230 тисяч споживачів були позбавлені електроенергії.

Ця подія недарма вважається пам'яткою, адже головною темою дослідницької роботи, у якій розглядається природа гібридних загроз, перш за все вважається комбінованих уражень на психологічний стан людини. Особа, позбавлена ресурсу для задоволення фізіологічних потреб, стає в рази піддатливою, а у крайньому випадку - агресивною, що грає на користь агресору.

2.2. Вірус Not Petya (2017)

Влітку, у середині червня 2017 року вирус NotPetya, поширений через програму M.E.Doc, вразив тисячі користувачів цифрових технологій

в Україні, паралізувавши при цьому роботу урядових ресурсів, банків та підприємств.

2.3. Атака на "Київстар" (2023)

У грудні 2023 року російські хакери здійснили масштабну атаку на телекомунікаційного оператора "Київстар", вивівши з ладу його інфраструктуру та отримавши доступ до персональних даних мільйонів користувачів.

3. *Засоби та інструменти протидії кібератакам*

3.1. Державні структури

Україна створила низку органів для забезпечення кібербезпеки, зокрема CERT-UA та Держспецзв'язок, які координують реагування на кібер інциденти та розробляють стратегії захисту.

3.2. Міжнародна співпраця

Україна активно співпрацює з міжнародними партнерами, зокрема з ЄС, НАТО та США, отримуючи технічну допомогу та обмінюючись інформацією про кіберзагрози.

3.3. Громадські ініціативи

Групи, такі як Український кіберальянс та InformNapalm, здійснюють власні операції проти російських кіберзагроз, збираючи та публікуючи докази агресії.

4. Ефективність протидії та порівняння інструментів

Україна демонструє зростаючу ефективність у протидії кібератакам завдяки поєднанню державних зусиль, міжнародної підтримки та громадських ініціатив. Проте, виклики залишаються, зокрема в сфері захисту критичної інфраструктури та підвищення кібер грамотності населення.

Розглядаючи всі елементи цифрових способів гібридного ураження на країну, попереду якого йде саме кібернетичний фронт війни між Росією та Україною став однією з головних арен сучасного стратегічного

протистояння. Пошкоджена енергосистема, державні установи, фінансовий сектор та критична інфраструктура підтверджують про те, що Росія цілеспрямовано використовує кіберзброю для досягнення політичних і військових цілей. Агресивні дії, показані у даній роботі, завдають, крім матеріальної шкоди ще й підрив довіри громадян до держави, де стабілізування суспільства й ослаблення державного управління.

Україна, попри обмежені ресурси, розвинула резильєнтність (адаптацію) до умов кібернетичної війни, створивши ефективну систему реагування та попередження загроз. Розглянувши детальніше, можна побачити, що суттєву роль у цьому відіграє взаємодія між секторами впливу — об’єднання державних структур, громадянського суспільства та міжнародних партнерів. Проте боротьба з кіберзагрозами вимагає не лише оперативної реакції на атаки, а й системного підходу до підвищення стійкості: кібер освіти, інвестицій у захист інфраструктури, законодавчого регулювання та міжнародної співпраці.

Таким чином, український досвід протистояння російським кібератакам набуває особливого значення як приклад для інших країн, які можуть опинитися в подібній ситуації. У XXI столітті війна ведеться не лише на полі бою, а й у цифровому вимірі — і перемога в цьому вимірі можлива лише за умови постійної готовності, інноваційності та єдності дій.

РОЗДІЛ 3.
СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У сучасному безпековому середовищі гібридні загрози стали визначальним чинником, що суттєво трансформує підходи до національної безпеки. Агресія проти України, розпочата Російською Федерацією у 2014 році, засвідчила, що традиційні механізми безпеки вже не здатні ефективно протистояти викликам, які поєднують у собі як відкриті військові дії, так і приховані, асиметричні форми впливу — інформаційні, кібернетичні, економічні, політичні та психологічні операції. У цих умовах стратегічне планування та формування політики безпеки потребують нової якості: гнучкості, прогнозованості, швидкого реагування і багаторівневої координації.

Розробка ефективних стратегій забезпечення національної безпеки в умовах гібридної війни вимагає системного аналізу як зовнішніх, так і внутрішніх чинників ризику, а також глибокого розуміння природи сучасного конфлікту. Україна, перебуваючи на передовій боротьби з гібридною агресією, змушена постійно адаптуватися до нових викликів, удосконалювати інституційні механізми та використовувати весь арсенал ресурсів — від дипломатії та розвідки до громадянської мобілізації й цифрової безпеки.

У цьому розділі розглядатимуться ключові стратегії, які Україна застосовує для зміцнення власної безпеки в умовах гібридної загрози, а також аналіз ефективності цих стратегій, їх переваг, недоліків та перспектив розвитку у контексті світових тенденцій безпекової політики.

3.1. Інституційна система забезпечення національної безпеки України.

Інституційна система забезпечення національної безпеки України формувалась протягом останніх десятиліть під впливом як внутрішніх політичних трансформацій, так і зовнішніх загроз. Після 2014 року, з початком російської агресії, система набула нового змісту — вона стала орієнтованою на реагування на гібридні виклики, що включають інформаційні та кібератаки, терористичну діяльність, політичну дестабілізацію, економічний тиск, енергетичні загрози тощо. Основу цієї системи становлять державні органи, які реалізують політику безпеки на стратегічному, оперативному та тактичному рівнях.

Рада національної безпеки і оборони України (РНБО) — ключовий координаційний орган у сфері національної безпеки та оборони. Вона визначає пріоритети державної політики, координує діяльність органів виконавчої влади в умовах надзвичайного або воєнного стану, розробляє стратегії, доктрини та плани оборони. Особливе значення РНБО отримала в умовах війни: її рішення часто стають основою для указів Президента щодо мобілізації, санкцій, інформаційної безпеки та кіберзахисту. Саме РНБО ініціювала ухвалення Доктрини інформаційної безпеки України (2017) та Стратегії кібербезпеки (2021), які стали відповіддю на загрози нового типу.

Служба безпеки України (СБУ) виконує функції контррозвідки, боротьби з тероризмом і захисту державної таємниці. В останні роки її роль у забезпеченні кібербезпеки та виявленні інформаційно-психологічних операцій зросла. СБУ розробляє і впроваджує спеціальні оперативно-розшукові заходи щодо нейтралізації шпигунських мереж, викриття диверсій, а також боротьби з внутрішніми колаборантами. В

умовах війни, особливо після 24 лютого 2022 року, її повноваження розширилися, що викликало і дискусії про потребу демократичного контролю над службою.

Міністерство оборони України та Генеральний штаб ЗСУ забезпечують воєнну безпеку. Окрім ведення бойових дій, у повноваження цих структур входить стратегічне планування оборонної політики, розвиток спроможностей сил оборони, міжнародне співробітництво, включаючи наближення до стандартів НАТО. Варто відзначити активну роль ЗСУ у протидії гібридним загрозам, особливо в частині адаптації до змін характеру війни: розвиток військової розвідки, впровадження цифрових платформ типу "Дія.City" для обліку ресурсів, застосування БПЛА, тактичного кібер озброєння тощо.

Міністерство внутрішніх справ України координує діяльність Національної поліції, Державної прикордонної служби, Національної гвардії та Державної служби з надзвичайних ситуацій. Усі ці структури відіграють критичну роль у забезпеченні громадської безпеки, боротьбі з диверсійно-розвідувальними групами, забезпеченні прикордонного контролю та цивільного захисту. Нацгвардія, зокрема, бере участь у підтримці громадського порядку на окупованих територіях, що важливо для стабілізації ситуації після гібридних операцій.

Міністерство цифрової трансформації України стало новим гравцем в інституційній архітектурі безпеки. Його завданням є розвиток цифрової інфраструктури, безпечного кіберпростору, електронного урядування, а також втілення політики відкритих даних. У 2022–2023 роках Мінцифра разом із Держспецзв’язку активно брала участь у побудові кіберзахисної інфраструктури, розвитку ІТ-військ та створенні умов для цифрової мобілізації населення. Український досвід у створенні «армії дронів» чи залученні ІТ-волонтерів (наприклад, група Anonymous Ukraine чи ІТ-армія) став унікальним у світі.

Важливою є також роль Громадянського суспільства — волонтерських організацій, медіа, незалежних експертів, які забезпечують додатковий рівень стійкості системи. У співпраці з державними органами вони створюють механізми протидії дезінформації, забезпечують швидкий обмін даними та беруть участь у підготовці безпекових стратегій. Наприклад, організації типу Центру протидії дезінформації чи VoxUkraine відіграють важливу роль у знешкодженні фейків і пропаганди.

Інституційна система національної безпеки України нині є багаторівневою, гнучкою та інтегрованою, проте не позбавленою викликів. Серед основних проблем — обмежене фінансування, дублювання повноважень, фрагментованість міжвідомчої взаємодії та потреба у гармонізації із західними стандартами. Разом з тим, процес її еволюції триває, а війна стала каталізатором глибоких змін, які, за належного управління, можуть суттєво зміцнити державну безпеку.

Використання комплексного підходу у боротьби проти гібридних загроз

Комплексний підхід у протидії гібридним загрозам передбачає поєднання зусиль усіх секторів держави — політичного, військового, інформаційного, економічного, дипломатичного й кіберпростору — для створення єдиної, скоординованої системи реагування. У контексті національної безпеки України це означає посилення міжвідомчої взаємодії між СБУ, РНБО, Міноборони, МВС, Держспецзв’язком та Міністерством цифрової трансформації, а також активну участь громадянського суспільства та міжнародних партнерів. Такий підхід дозволяє не лише оперативно реагувати на загрози, а й запобігати їм через аналітику, раннє попередження, інформаційну гігієну, законодавчі ініціативи та підвищення стійкості критичної інфраструктури. Комплексність також передбачає навчання кадрів, обмін досвідом з країнами НАТО, впровадження

цифрових технологій і стратегічну комунікацію, що дозволяє зменшити вразливість держави до ворожих впливів.

3.2. Світовий досвід протидії гібридним загрозам.

В умовах цифрових технологій гібридні загрози стали одним з найнебезпечніших викликів для національної безпеки держав. Це багатовекторне явище, що поєднує військові, інформаційні, кібернетичні, економічні та політичні інструменти, дозволяє агресорам впливати на цілі держави без прямого оголошення війни. Вивчення досвіду інших країн у протидії гібридним загрозам є важливим чинником для формування дієвої стратегії безпеки, особливо для таких країн, як Україна.

Завдяки попереднім підрозділам ми вже розбирали деякі приклади застосування гібридних загроз спираючись на попередній досвід інших країн, проте і оминути його задля порівняння різних методів і принципів застосування безконтактної агресії - вкрай непрофесійно.

Отже, розберемо деякі приклади ведення гібридних війн і інших країнах.

Естонія: кіберзагрози та інформаційна безпека

Одним із найвідоміших прикладів гібридного впливу стали події в Естонії у 2007 році, коли країна зазнала масштабної кібератаки після рішення влади демонтувати радянський пам’ятник у Таллінні. Протягом кількох днів державні сайти, ЗМІ, банки та інфраструктура були паралізовані. Цей інцидент змусив Естонію переглянути свою політику безпеки, особливо в кіберсфері.

У відповідь було створено Центр кіберзахисту при НАТО в Таллінні (CCDCOE), а сама держава стала піонером у сфері кібероборони. Естонія активно розвиває електронне урядування та застосовує багаторівневу

аутентифікацію для захисту інформації. Також велику увагу приділено медіаграмотності населення: ще зі школи учнів навчають критично сприймати інформацію, розпізнавати фейки та пропаганду.

Фінляндія: суспільна стійкість і загальнодержавна готовність

Фінляндія має спільний кордон із Росією, тому ще з часів Холодної війни серйозно ставиться до гібридних загроз. Її стратегія протидії базується на концепції "всеохоплюючої безпеки" (Comprehensive Security). Це означає, що в процес забезпечення безпеки залучено не лише армію, але й громадянське суспільство, приватний сектор, медіа та освітні установи.

У Фінляндії активно функціонує Центр з підвищення стійкості суспільства до гібридних загроз (Hybrid CoE), створений у 2017 році за підтримки ЄС і НАТО. Центр займається дослідженням тактик гібридного впливу, поширенням кращих практик між країнами-партнерами та навчанням фахівців. Фінська модель також передбачає підготовку населення до кризових ситуацій, у тому числі через інструкції щодо дій у разі інформаційної війни, кібератак або диверсій.

Ізраїль: багаторівнева оборона та превентивні дії

Ізраїль — країна з багаторічним досвідом протидії як традиційним, так і асиметричним загрозам. Особливість його підходу полягає в перевазі технологій та інтелектуальних ресурсів над чисельністю. Гібридна війна в ізраїльському контексті включає протидію тероризму, кібератакам, пропаганді, підривній діяльності з боку інших держав та впливу через арабські медіа.

Держава розвинула ефективну кіберрозвідку (приклад — підрозділ "Unit 8200") та створила умови для швидкого реагування на будь-які форми втручання. В Ізраїлі практикуються превентивні операції — тобто удари по загрозах до їх активізації. Крім того, країна активно

використовує інформаційні кампанії для деморалізації противника й нейтралізації ворожої пропаганди серед свого населення.

США: стратегія стримування та роль технологій

Для Сполучених Штатів гібридні загрози набули актуальності особливо після втручання у президентські вибори 2016 року, коли розвідка США визнала втручання Росії через дезінформаційні кампанії, хакерські атаки та вплив на соціальні мережі. У відповідь уряд США посилив нагляд за кібербезпекою, створивши Кібернетичне командування США (USCYBERCOM), а також розширив можливості Агентства національної безпеки.

Відзначається тісна взаємодія з IT-компаніями (Google, Meta, Microsoft), які зобов'язалися виявляти та блокувати підозрілий контент, пов’язаний із впливом іноземних держав. США також активно інвестують у штучний інтелект і машинне навчання для виявлення дезінформації на ранніх етапах.

Уряд застосовує стратегію стримування: заявляється, що будь-яка спроба гібридного впливу буде розцінена як акт агресії, на який буде відповідь у будь-якій доступній формі — економічній, політичній та військовій.

Польща та країни Балтії: гібридні навчання і стратегічна комунікація

Польща, як і країни Балтії, є одними з найактивніших учасників антиросійської стратегії НАТО. У цих країнах активно проводяться військово-цивільні навчання щодо реагування на гібридні атаки: кібератаки, інформаційні види, провокації на кордоні, атаки на інфраструктуру.

Також було створено Європейський центр стратегічної комунікації НАТО, що аналізує методи інформаційного впливу та розробляє методики захисту. Польща запровадила законодавчі ініціативи, які обмежують

діяльність іноземних ЗМІ, що поширюють пропаганду, а також створила агентства з протидії фейкам.

У країнах Балтії велику увагу приділяють роботі з національними меншинами, які можуть стати об’єктом впливу іноземної пропаганди. Наприклад, у Латвії та Литві активно впроваджуються програми з інтеграції російськомовного населення в політичне та культурне життя держави.

Висновки

Аналізуючи досвід різних країн, можна виокремити кілька ключових принципів ефективної протидії гібридним загрозам:

- Інтеграція зусиль усіх секторів — державного, приватного, освітнього та громадського — задля побудови всеохоплюючої безпеки.
- Підвищення стійкості суспільства, зокрема через медіаграмотність, патріотичне виховання, громадянську освіту.
- Розвиток кібербезпеки як одного з найважливіших елементів захисту у цифрову епоху.
- Превентивні дії та стратегічна комунікація, які дозволяють нейтралізувати загрозу ще до її реалізації.
- Міжнародна співпраця та обмін досвідом між країнами, які вже мають справу з гібридним впливам.

Для України, яка стала жертвою повномасштабної гібридної агресії з боку Росії, цей досвід є не лише цінним, а й необхідним для адаптації. Формування національної системи протидії гібридним загрозам має враховувати багатовимірність сучасної війни та передбачати системні дії в усіх сферах — від інформаційної до гуманітарної.

3.3. Перспективи підвищення ефективності системи національної безпеки України в умовах сучасних гібридних загроз.

Сучасна система національної безпеки України функціонує в умовах тривалої гібридної агресії з боку Російської Федерації, що охоплює не лише військову, але й інформаційну, політичну, економічну, енергетичну, кібернетичну та психологічну сфери. У зв’язку з цим постає необхідність системного перегляду підходів до гарантування безпеки держави та впровадження комплексних реформ, здатних забезпечити стійкість і гнучкість у протидії гібридним викликам.

На основі аналізу сучасного стану системи національної безпеки України, досвіду країн НАТО та ЄС, а також результатів власного дослідження, пропонуються наступні рекомендації:

1. Формування цілісної державної стратегії протидії гібридним загрозам

Україна потребує єдиного стратегічного документу, що визначатиме комплексний підхід до протидії гібридній агресії. Така стратегія має враховувати міжвідомчу координацію, роль громадянського суспільства, інформаційні, кібернетичні та економічні виміри загроз. Необхідно: розробити Оновлену концепцію національної безпеки України, в якій гібридна війна буде визначена як окрема форма загрози; передбачити механізми превентивного реагування, а не лише реактивних дій; встановити чіткі протоколи взаємодії між секторами оборони, внутрішніх справ, СБУ, РНБО, Міні Цифри та іншими.

2. Посилення кібербезпеки та цифрової стійкості

З огляду на постійні кібератаки на українські державні органи, критичну інфраструктуру та об’єкти енергетики, варто: розширити повноваження Державної служби спеціального зв’язку та захисту інформації, створивши постійно діючу мережу моніторингу загроз;

запровадити обов’язкову кібербезпекову сертифікацію для всіх державних установ та стратегічних підприємств; підтримувати розвиток власного програмного забезпечення та зменшувати залежність від іноземних технологій; розвивати систему реагування на інциденти (CSIRT) з оперативною аналітикою.

3. Зміцнення інформаційної безпеки та стратегічної комунікації

Інформаційний фронт є одним із найважливіших у гібридній війні. Тому Україні слід: створити Єдиний центр стратегічних комунікацій, що забезпечуватиме швидке реагування на дезінформаційні кампанії;

проводити медіаграмотні кампанії серед населення, особливо в регіонах, де існує вразливість до ворожого впливу; посилити державну підтримку незалежних ЗМІ, які дотримуються журналістських стандартів;

запровадити моніторинг ворожого контенту в соцмережах за участю фахівців з OSINT та залученням міжнародних партнерів.

4. Переосмислення системи військово-цивільної взаємодії та територіальної оборони

Повномасштабна війна показала необхідність глибокої інтеграції цивільних ресурсів у систему оборони. Для цього слід: переформатувати підготовку резервістів за моделлю країн Балтії (зокрема, створення добровольчих загонів при громадах); розробити локальні плани безпеки для кожної територіальної громади; створити структури кризового управління на місцях із чітко розписаними обов’язками під час надзвичайних ситуацій; залучати громадян до постійних навчань і тренувань, особливо у прикордонних областях.

5. Реформа системи національної безпеки у сфері освіти і науки

Наукова спільнота, освітні заклади та експертні центри мають стати основою аналітичної, концептуальної та прогностичної підтримки безпеки. Рекомендується: створити державну програму дослідження гібридних загроз за участю університетів, think-tank ів, аналітичних центрів; підтримувати наукові розробки у сфері соціальної психології, інформаційних технологій, комунікацій; включити дисципліни з національної безпеки, кібер гігієни та критичного мислення в програми старших класів та університетів.

6. Міжнародне співробітництво і євроатлантична інтеграція

Україна повинна поглиблювати співпрацю з партнерами у сфері безпеки, зокрема: активніше брати участь у спільних навчаннях НАТО та ЄС, з акцентом на протидію гібридним загрозам; використовувати технічну допомогу з кібербезпеки від партнерів для модернізації інфраструктури;

створити спільні центри обміну інформацією про загрози з країнами Балтії, Польщею, Фінляндією; ініціювати навчальні програми для фахівців сектору безпеки за підтримки країн НАТО.

7. Енергетична та економічна безпека як фундамент стійкості

Гібридна війна часто проявляється у формі енергетичного шантажу, диверсій чи фінансових атак. Тому Україна має:

збільшити енергонезалежність через розвиток альтернативної енергетики; запровадити механізми захисту критичної інфраструктури (електростанцій, логістичних вузлів, підприємств оборонпрому); посилити фінансову розвідку для боротьби з відмиванням грошей, що фінансують деструктивні мережі; стимулювати внутрішнє виробництво стратегічно важливої продукції: медичної, оборонної, ІТ-сфери.

8. Гуманітарна політика та внутрішня згуртованість

Суспільна стійкість — це не лише технології, а й відчуття справедливості, рівності, довіри до держави. Тому потрібно: забезпечити ефективну політику реінтеграції окупованих територій, включно з

інформаційною, культурою та освітньою підтримкою; підвищити рівень державної підтримки ветеранів, військовослужбовців та їхніх родин; забезпечити рівний доступ до публічних послуг у всіх регіонах, особливо в прикордонних та постраждалих зонах; підтримувати національну ідентичність через культуру, мову, мистецтво.

Реальність гібридних загроз вимагає від України не лише оновлення законодавчої бази, але й створення принципово нової моделі безпеки — адаптивної, інтегрованої, превентивної. Національна безпека повинна стати справою не лише силових структур, а всього суспільства. Виконання запропонованих рекомендацій дозволить Україні сформувати ефективну, стійку та сучасну систему безпеки, здатну протистояти як традиційним, так і новітнім формам агресії.

ВИСНОВКИ

У ході аналізу національної безпеки України під впливом гібридних загроз усі завдання кваліфікаційної роботи були виконані наступним чином:

1. Ключові елементи та зміст національної безпеки були виокремлені та розкладені на окремі складові. Досліджено, що застосування комплексного підходу є одним з найефективніших методів у забезпеченні національної цілісності держави, де кожен механізм даного підходу працює злагоджено і укупі з іншими чинниками.
2. Основі підходи у розумінні таких явищ як “гібридні загрози” та “гібридна війна” було систематизовано за допомогою таких методів, як порівняльний аналіз, дослідницький метод, шляхом емпіричного підходу, завдяки якому розуміння даних явищ набуло більш детального і лабораторного вигляду.
3. Прослідковано за процесами гібридної загрози для Уаїни з 2014 по 2024 рік, у яких чітко виділяються застосування інформаційної, збройної, кібернетичної, медійної, культурної та економічної агресії.
4. Проаналізовано державну політику України у сфері протидії гібридним загрозам, зокрема розглянуто нормативно-правову базу, інституційні механізми, доктринальні документи. Зазначено позитивні зрушення, однак окреслено й низку проблем, пов’язаних із недостатньою координацією органів влади, фрагментарністю реакцій та запізнілими рішеннями.
5. Досліджено роль інформаційної безпеки та стратегічних комунікацій у забезпеченні національної безпеки. З’ясовано, що інформаційна складова є ключовою у сучасній гібридній війні. Оцінено ефективність заходів, які реалізовувалися державними інституціями у відповідь на ворожі

інформаційні впливи. Виявлено як позитивні приклади протидії дезінформації, так і слабкі місця.

6. Проаналізовано зовнішню політику України у контексті протидії гібридним загрозам та зміцнення національної безпеки. Особлива увага приділялася питанням міжнародної підтримки, інтеграції до НАТО та ЄС, активізації стратегічного партнерства з державами Заходу. Доведено, що зовнішньополітична діяльність стала важливим інструментом зміцнення безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Указ президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»
2. Антонов В.О. Конституційно-правові засади національної оборони України: монографія. наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. 576 с.
3. Антонов В.О. Поняття та зміст системи національної безпеки. Держава і право. 2010. Вип. 48. С. 137–144.
4. Глобальна та національна безпека. авт. кол.: В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін.; за заг. ред. Г.П. Ситника. Київ: НАДУ, 2016. 784 с.
5. Крук С.І. Інституційний розвиток державного управління у сфері забезпечення національної безпеки України : автореф. дис. ... д-ра наук з держ. упр.: 25.00.05. Харків, 2019. 43 с.
6. Мельниченко Б., Фігель Н. Основні підходи до розуміння поняття «національна безпека». Вісник Національного університету «Львівська політехніка». 2021. № 2 (30). С. 68–72.
7. Мотайло О. В. Основні концептуальні підходи до сутності поняття «національна безпека». Право та державне управління. 2019. № 4. С. 288–293.
8. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Вип. 3. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf

9. Пасічник В. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою. Науковий вісник «Демократичне врядування». 2011. Вип. 7. URL: http://nbuv.gov.ua/UJRN/DeVr_2011_7_7
10. Подорожна Т. С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. Аналітично-порівняльне правознавство. 2023. № 6. С. 491–497.
11. Погібко О. І. Воєнна доктрина України – нормативноправове підґрунтя законодавчого забезпечення оборони держави. Прикарпатський юридичний вісник. 2015. № 3. С. 17–24. URL: http://nbuv.gov.ua/UJRN/Pjuv_2015.
12. Про національну безпеку України: Закон України від 21.06.2018 № 2649-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19
13. Редькіна А. Українські національні інтереси й цінності: суспільне усвідомлення та переоцінка. Політичні дослідження / Political Studies. 2023. № 1 (5). С. 144–162. URL: http://pd.ipiend.gov.ua/article/view/280397
14. Рябовол Л.Т. Державний суверенітет: наукові підходи до визначення поняття та ступеня обмежень в умовах глобалізації. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2019. № 3 (43). С. 262–266.
15. Ситник Г. П. Вплив глобалізації на воєнну сферу та принципові особливості сучасних воєнних конфліктів. Науково-інформаційний вісник Академії національної безпеки. 2016. №1-2 (9-10). С. 99–115.
16. Смолянюк В.Ф. Системні засади національної безпеки України. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2018. № 2 (37). С. 107–126.
17. Ткаченко В.І., Смірнов Є.Б., Астахов О.О. Шляхи формування системи забезпечення національної безпеки. Збірник наукових праць Харківського університету Повітряних Сил. 2015. Вип. 2 (43). С. 3–8.

18. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. … д-ра юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет», Ужгород, 2019. 487 с.
19. Ткаля О. В. Національні інтереси та цінності як основа існування і розвитку національної держави. Юридичний науковий електронний журнал. 2022. № 4. С. 58–61. URL: http://lsej.org.ua/4_2022/12.pdf
20. Федченко О. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. Journal of Scientific Papers «Social Development and Security». 2022. Vol. 12, №. 3. С. 128–134.
21. Шевченко М.М. Функції та завдання системи забезпечення національної безпеки України в сучасних умовах. Науково-інформаційний вісник Академії національної безпеки. 2014. № 3–4. С. 14–24.