«ЗАТВЕРДЖУЮ»
Ректор Волинського національного університету імені Лесі Українки,
професор Анатолій ЦЬОСЬ
_____
«___» _____2025 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук

ВИТЯГ З ПРОТОКОЛУ № 1

міжкафедрального семінару кафедр міжнародних відносин та регіональних студій та міжнародних комунікацій та політичного аналізу Волинського національного університету імені Лесі Українки про наукову новизну, теоретичне та практичне значення результатів та рекомендацію дисертації Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук

ПРИСУТНІ:

Члени кафедр: професор кафедри міжнародних комунікацій та політичного аналізу, д. політ. н., проф. Карпчук Н. П., завідувач кафедри міжнародних відносин та регіональних студій д. геог. н., проф. Коцан Н.Н., д. політ. н., проф. Тихомирова Є. Б., декан факультету міжнародних відносин, д. політ. н., проф. Шуляк А. М., к. істор. н., доц. Моренчук А.А., к. політ. н., доц. Кулик С.М., к. політ. н., доц., докторант Михалюк Н.Ю., ст. лаб. Гаврилюк С. І.

Запрошені: завідувач кафедри політології та публічного управління д. політ. н. Бусленко В.В., д. політ.н., проф. Ярош О.Б.

Науковий консультант – Шуляк А. М., д. політ.н., проф., декан факультету міжнародних відносин, Волинський національний університет імені Лесі Українки.

Голова засідання – професор кафедри міжнародних комунікацій та політичного аналізу, д. політ. н., проф. Карпчук Н. П.

Секретар засідання – доцент кафедри міжнародних відносин та регіональних студій, к. політ. н. Кулик С. М.

ПОРЯДОК ДЕННИЙ:

1. Обговорення докторської дисертації кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук.

СЛУХАЛИ: про рекомендацію дисертації кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук.

ВИСТУПИЛИ:

Голова засідання, професор кафедри міжнародних комунікацій та політичного аналізу, д. політ. н. Карпчук Н. П.: Пропонується до обговорення дисертації кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук.

Тема дисертації Вознюк Є.В. «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» була затверджена на засіданні Вченої Ради Східноєвропейського національного університету імені Лесі Українки, протокол № 6 від 26.12.2015 р. Науковий консультант – декан факультету міжнародних відносин, д. політ. н., проф. Шуляк А. М. Робота виконана на кафедрі міжнародних комунікацій та політичного аналізу ВНУ ім. Лесі Українки. Дисертація подається до розгляду на міжкафедральний семінар вперше.

Зазначу, що Вознюк Є.В. у 2011 р. у результаті публічного захисту в спеціалізованій вченій раді Інституту світової економіки і міжнародних відносин НАН України дисертації «Порівняльний вимір гендерної політики України та Росії» здобула науковий ступінь кандидата політичних наук за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку. Рішенням президії Вищої атестаційної комісії України від 31.05.2011 року

(протокол №59-06/5) підтверджено дипломом кандидата політичних наук ДК № 065215

На підставі ознайомлення із текстом дисертації можу констатувати, що є усі формальні підстави для розгляду питання про її рекомендацію до захисту на спеціалізованій вченій раді за 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку.

Якщо немає заперечень, пропоную перейти безпосередньо до обговорення дисертації. Слово для викладу основних положень роботи надається Вознюк Є.В.

Кандидат політичних наук, доцент, завідувач кафедри міжнародних комунікацій та політичного аналізу Вознюк Є. В.:

Вельмишановна пані головуюча, шановні члени кафедр, присутні!

Маю честь представити до Вашого розгляду дисертаційну роботу на тему: «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку».

Актуальність дослідження інформаційного тероризму зумовлена зростанням загроз інформаційному суверенітету держав у добу гібридних війн і глобалізованого інформаційного простору, де неконтрольовані потоки даних створюють сприятливі умови для маніпуляцій, дезінформації та підриву політичної стабільності. Інформаційний тероризм, на відміну від класичного, діє через символічне насильство, маніпуляцію масовою свідомістю та делегітимацію інституцій, виступаючи складовою гібридної війни й інструментом «м'якої сили навпаки». У сучасних міжнародних відносинах він розглядається як міждисциплінарний феномен, що поєднує елементи безпекових студій, комунікацій, психології та міжнародного права, вимагаючи нових підходів до протидії. Особливої актуальності проблема набула в контексті російсько-української війни, де масовані інформаційні атаки супроводжують військові операції, спрямовані на деморалізацію суспільства, підрив довіри до державних інституцій і дестабілізацію внутрішньополітичної ситуації, що зумовлює необхідність посилення інформаційної стійкості України та формування ефективних стратегій захисту.

Метою дослідження є аналіз теоретико-методологічні підходи до вивчення інформаційного тероризму, визначити його характерні риси, форми прояву та загрози для національної й міжнародної безпеки, а також дослідити практики протидії інформаційному тероризму на глобальному, регіональному та національному рівнях

Об'єкт дослідження – система міжнародної безпеки в умовах інформаційної епохи. *Предметом дослідження* виступає феномен

інформаційного тероризму як форми деструктивного інформаційного впливу та його вплив на безпекове середовище сучасних держав і міжнародних інституцій.

Наукова новизна одержаних результатів. У процесі дослідження були здобуті результати, новизна яких конкретизується у таких положеннях:

Уперше:

•запропоновано концептуалізацію поняття інформаційної стійкості. У сучасних умовах гібридної війни та інформаційної конфронтації дедалі більшого значення набуває цей концепт, який розглядається як ключова складова національної безпеки та соціальної згуртованості. Під *інформаційною стійкістю* розуміємо здатність держави, інституцій і громадянського суспільства протистояти зовнішнім і внутрішнім інформаційним загрозам, включаючи дезінформацію, маніпуляції, пропаганду та інші форми інформаційного впливу, що мають на меті дестабілізацію політичного, соціального або культурного середовища. Інформаційна стійкість є комплексним міждисциплінарним феноменом, який включає технічні, організаційні, нормативно-правові, освітні та психологічні складові;

•обґрунтовано новий підхід до протидії інформаційному тероризму, що полягає у виокремленні та теоретичному узагальненні *трикомпонентної моделі забезпечення інформаційної стійкості,* яка охоплює стратегічні комунікації (як інструмент консолідації національного наративу, формування довіри до держави та нейтралізації ворожих інформаційних операцій), медіаосвіту (як чинник формування критичного мислення, інформаційної гігієни та здатності до самостійної ідентифікації інформаційних загроз) та цифрову безпеку (як складова частина інформаційної оборони держави. що включає технологічні та організаційні засоби кіберзахисту, у тому числі на основі національного і міжнародного співробітництва). Уперше здійснено системний аналіз взаємозв'язку між стратегічними комунікаціями, медіаосвітою та цифровою безпекою як ключовими інструментами у структурі національної та міжнародної інформаційної безпеки в умовах гібридних загроз;

•здійснено комплексне міждисциплінарне дослідження *міжнародного тероризму в умовах глобалізації,* в якому запропоновано нову концептуалізацію інформаційного тероризму як автономного феномена, що поєднує риси когнітивної війни, кібертерору та ідеологічної агресії. Визначено інституційні, цивілізаційні та правові аспекти інформаційної агресії, виявлено її вплив на структури міжнародної безпеки, політичну стабільність і правовий режим міжнародного гуманітарного права. Обґрунтовано необхідність перегляду засад міжнародного права та безпеки в контексті викликів інформаційної епохи;

•здійснено аналіз унікального українського досвіду протидії інформаційному тероризму в умовах повномасштабної гібридної агресії, що

триває з 2014 року та інтенсифікувалася після 2022 року. Уперше на основі системного підходу досліджено, як держава, перебуваючи в умовах постійного зовнішнього інформаційного тиску, змогла сформувати *цілісну модель інформаційного спротиву,* що поєднує інституційні, технологічні, суспільні та дипломатичні інструменти. У роботі обґрунтовано нові компоненти української інформаційної стійкості – алгоритмічну протидію фейкам, мобілізацію цифрового громадянського суспільства (зокрема волонтерських ініціатив, кіберспротиву), які ще не були належним чином осмислені в науковій літературі. Досвід України розглядається як перспективна модель, що вже частково імплементується в політики безпеки ЄС, НАТО та окремих країн. Запропоновано авторське бачення українського кейсу як джерела універсальних рішень, придатних до адаптації в інших регіонах, які зазнають інформаційного терору. У цьому контексті акцентовано на необхідності міжнародно-правової інституалізації механізмів боротьби з інформаційним тероризмом із урахуванням українського внеску як одного з головних орієнтирів для формування глобальної стратегії цифрової безпеки;

•запропоновано нову інтерпретацію терористичних атак 11 вересня 2001 року не лише як воєнного виклику, а як переломного моменту у трансформації глобальної парадигми безпеки, що започаткував якісно нову еру інформаційно-психологічного, асиметричного і неконвенційного протиборства. Переосмислено роль подій 11 вересня як тригера для еволюції нових типів конфліктів – від традиційного терору до інформаційних та проксі-війн. Доведено, що гасло «боротьби з тероризмом» стало основою для формування нових стратегічних доктрин, які легітимізували втручання в інші країни поза рамками колективної безпеки.

У результаті дослідження ми дійшли до таких *висновків.*Концепт тероризму у контексті теорії міжнародних відносин постає як надзвичайно складне, багатовимірне і водночас політично чутливе явище, яке має не лише безпековий, а й глибокий соціальний, інформаційний та ідеологічний вимір. Відсутність універсального визначення тероризму обумовлюється як об'єктивною складністю феномена, так і політичними інтерпретаціями, що впливають на концептуалізацію самого поняття. Тероризм трансформувався від державного інструменту терору до інструмента недержавних та транскордонних акторів, ставши формою асиметричної боротьби за політичні, ідеологічні або релігійні цілі. У сучасних умовах його механізми охоплюють не лише фізичне насильство, а й системні інформаційні кампанії, що формують атмосферу страху, недовіри та нестабільності. Окрім того, зростання ролі кіберпростору, мас-медіа та соціальних мереж значно підсилило здатність терористичних організацій впливати на глобальні процеси. Теоретичні парадигми міжнародних відносин –

неореалізм, неолібералізм, конструктивізм – по-різному інтерпретують тероризм: як засіб впливу у світі анархії, як загрозу, що вимагає міжнародної координації, або як соціальний конструкт, що формується під впливом дискурсивних практик. Такий міждисциплінарний підхід дозволяє більш комплексно оцінювати природу тероризму, зокрема його еволюцію, типологію, механізми функціонування та способи легітимації. Загалом, концепт тероризму має розглядатися як динамічне поняття, що розвивається у відповідь на трансформації міжнародного безпекового середовища, соціальних конфліктів та інформаційних технологій. Його аналіз є необхідною передумовою для формування ефективної національної та глобальної стратегії протидії терористичним загрозам та посилення архітектури міжнародної безпеки.

Міжнародний тероризм у сучасному світі є не лише загрозою безпеці, а й складним глобалізаційним феноменом, що виявляє глибокі суперечності між цивілізаціями, політичними системами та соціальними устроями. Його витоки та еволюція значною мірою зумовлені асиметрією глобального розвитку, геополітичними імперативами провідних держав, спробами збереження домінування західної моделі, а також ігноруванням культурної ідентичності «інших» світів. Водночас, тероризм виступає реакцією на виклики сучасної глобалізації, в якій не всі учасники мають рівні можливості доступу до ресурсів, розвитку та самореалізації. Тож для подолання тероризму необхідне не лише вдосконалення силових і безпекових механізмів, а й нова парадигма глобальної взаємодії – заснована на повазі до цивілізаційного плюралізму, справедливості, інклюзивності й етичної відповідальності глобальних лідерів.

Інформаційний тероризм став невід'ємною та надзвичайно небезпечною складовою міжнародного тероризму в умовах цифрової доби. Його вплив поширюється не лише на інфраструктуру, а й на свідомість суспільства, використовуючи інструменти масових маніпуляцій, кіберзлочинів та спеціальних інформаційних операцій. Як показав аналіз наукових підходів, це явище охоплює низку форм – від психологічного тиску і дезінформації до кібернападів на критичні об'єкти держав. Небезпека інформаційного тероризму полягає в його невидимості, швидкості поширення та здатності руйнувати довіру до влади, інституцій і цінностей. У сучасному світі, де межа між війною і миром розмита, інформаційна зброя часто є не менш потужною, ніж фізична. Тому боротьба з інформаційним тероризмом має стати пріоритетом як для національної безпеки, так і для міжнародного співробітництва, що вимагає оновлення правових механізмів, розвитку цифрової стійкості, створення ефективної системи реагування на інформаційні загрози.

Проблема тероризму сьогодні виходить за межі питань безпеки і стає індикатором структурних вад світового порядку. Досвід подій 11 вересня 2001

року, подальших збройних операцій і міжнародних санкційних механізмів свідчить про обмежену дієвість переважно силових або суто правових підходів. Навпаки, боротьба з тероризмом має здійснюватися не лише через нейтралізацію його безпосередніх носіїв, а й шляхом ліквідації причин — бідності, соціального відчуження, релігійної нетерпимості, викривленої глобалізації та нерівності доступу до ресурсів.

Усе це обумовлює необхідність переходу від концепту «реакції» до концепту «упередження», що передбачає синергію зусиль національних держав, міжнародних організацій, громадянського суспільства та наукової спільноти. Без цього говорити про реальну протидію терористичній загрозі – лише ілюзія. Тероризм не є окремим злом, а радше – симптомом глибших хвороб сучасної цивілізації. Отже, стратегія боротьби з ним має бути частиною ширшої доктрини глобальної безпеки, справедливості та стійкого розвитку.

Сучасна епоха характеризується стрімкою еволюцією форм воєнних дій, що виходять за межі традиційної «гарячої» війни та охоплюють широкий спектр асиметричних, інформаційних, медійних і проксі-конфліктів. Війна четвертого покоління, гібридна війна, iWar, медіа-війна, асиметричні та посередницькі війни дедалі частіше використовуються як ефективні інструменти впливу в умовах, коли відкриті бойові дії стають політично та економічно невигідними для глобальних акторів. Ці форми конфліктів орієнтовані не лише на військове послаблення противника, а й на підрив його внутрішньої стабільності, ідентичності, економіки, легітимності влади та морального духу населення.

Отже, у XXI столітті саме інформаційна війна визначає нову парадигму глобального конфлікту, і країни, які не готові до активної інформаційної самооборони та стратегічних комунікацій, ризикують втратити не лише контроль над власним інформаційним простором, а й суверенітет. Ефективна протидія цим загрозам потребує національної інформаційної доктрини, розвитку цифрового опору, критичного мислення громадян та тісної міжнародної кооперації.

Інформаційна зброя стала одним із ключових інструментів сучасного конфлікту, здатним завдавати значної шкоди державам без фізичного втручання. Її специфіка полягає у використанні дезінформації, маніпулятивних наративів, кібероперацій, психологічного впливу, фейків і спеціальних інформаційних операцій, які спрямовані на підрив морального духу, дестабілізацію політичної ситуації, ослаблення державного управління та ерозію суспільної довіри. У контексті гібридної війни Росії проти України інформаційна зброя стала стратегічним засобом впливу: зокрема, через поширення пропаганди, підрив довіри до державних інституцій, делегітимацію збройних сил, а також стимулювання паніки, зневіри та розколу всередині суспільства. Такий тип зброї

не потребує значних матеріальних витрат, але має високий рівень ефективності завдяки цифровим технологіям, соціальним мережам та глобальному інформаційному простору. Використання інформаційної зброї також змінює традиційні уявлення про воєнні конфлікти – стирається межа між миром і війною, цивільним і військовим, обороною і нападом. У цих умовах держави повинні розвивати спроможність до ідентифікації, нейтралізації та попередження інформаційних атак, зміцнювати цифрову стійкість, стратегічні комунікації та навички інформаційної гігієни громадян. Отже, інформаційна зброя становить загрозу національній безпеці на рівні, зіставному із застосуванням традиційних форм збройної сили, що потребує адекватних заходів реагування як у внутрішній, так і в міжнародній політиці безпеки.

У сучасному цифровому середовищі інформаційна стійкість перетворюється на ключовий інструмент протидії інформаційному тероризму, який ускладнює безпекову ситуацію, підриває демократичні інституції та порушує суспільну згуртованість. Комплексний аналіз показав, що загроза інформаційного тероризму проявляється не лише через кібернапади чи фейки, а й через деструктивний вплив на політичну культуру, громадянську активність і довіру до державних інституцій.

Інформаційна стійкість охоплює широкий спектр заходів – від розвитку стратегічних комунікацій і медіаграмотності до забезпечення цифрової безпеки й інституційного контролю за дотриманням інформаційних прав. Центральним елементом у протидії деструктивним впливам виступає синергія між державними структурами, громадянським суспільством і технічними інструментами, спрямованими на виявлення, блокування й нейтралізацію інформаційних атак.

Особливу роль у зміцненні інформаційної стійкості відіграють: медіаосвіта та критичне мислення, що формують у громадян здатність розпізнавати маніпуляції та фейки; інституційна спроможність держави, включно з роллю омбудсмена або інформаційного комісара, у захисті інформаційних прав; інструменти ЄС (Hybrid Toolbox, Cyber Diplomacy Toolbox тощо), які слугують ефективною моделлю багаторівневої протидії гібридним загрозам; цифрова безпека та нормативне регулювання, що забезпечують технологічний і правовий захист національної інформаційної інфраструктури.

Досвід України та країн ЄС підтверджує ефективність комплексного підходу, що поєднує превентивні, просвітницькі, нормативні й технічні засоби. У цьому контексті створення незалежного інституту Інформаційного комісара в Україні є логічним кроком до конституційного закріплення інформаційної демократії та адаптації до європейських стандартів. Отже, інформаційна стійкість має розглядатися як стратегічна категорія національної безпеки, що

забезпечує здатність суспільства й держави протистояти інформаційним загрозам, зберігати соціальну згуртованість, посилювати громадянську відповідальність і формувати безпечне інформаційне середовище в умовах гібридної війни та цифрових трансформацій.

У XXI столітті інформаційні технології стали основою глобальної взаємодії, економічної діяльності та державного управління. Водночас цифровізація зумовила зростання кіберзагроз, що ставить під сумнів безпечність і стійкість національних інформаційних інфраструктур. Аналіз міжнародного досвіду свідчить, що успішна інформаційна політика потребує поєднання кількох ключових елементів: ефективного нормативно-правового регулювання, належної організації системи управління, розвитку цифрової грамотності населення та впровадження інструментів кіберстрахування.

Росія, Китай, а також недержавні актори, зокрема терористичні угруповання, активно адаптують ці моделі до власних стратегічних цілей, що створює серйозні виклики для традиційної системи міжнародного права та безпеки. Такі війни часто залишаються нижче порогу офіційного оголошення конфлікту, що ускладнює міжнародне реагування та відкриває простір для правового нігілізму. Водночас західні демократії, з огляду на високу вразливість до втручання у свої відкриті суспільства, змушені шукати нові моделі стійкості – від реформування інформаційної політики до запровадження систем протидії кіберзагрозам і гібридним операціям.

Поширення таких форм війни свідчить про глибоку трансформацію безпекового середовища XXI століття, в якому ключову роль відіграють не лише військові ресурси, а й технологічна перевага, інформаційний контроль, психологічний вплив та здатність до адаптивного мислення. Це вимагає оновлення концепцій національної та міжнародної безпеки, міжвідомчої координації, стратегічних комунікацій і консолідації зусиль демократичного світу задля ефективного реагування на новітні виклики та загрози. США демонструють системний підхід до інформаційної безпеки, зокрема завдяки ухваленню стратегій кіберзахисту, створенню спеціалізованих державних інституцій (CERT, DHS, C3), розвитку цифрової освіти та співпраці з приватним сектором. Суттєве значення має й баланс між захистом персональних даних і забезпеченням інформаційної безпеки в межах загальнодержавної стратегії. Європейський Союз формує комплексну політику кібербезпеки через директиви, мережі CERT, агенцію ENISA, а також заохочення міждержавної кооперації у сфері кіберзлочинності. Успішні приклади Естонії, Франції та Норвегії демонструють ефективність поєднання правового регулювання, інституційної стійкості та стратегічного планування.

У результаті дослідження зроблено висновок, що ключовими чинниками ефективної інформаційної безпеки є: наявність чіткої законодавчої бази та стратегій кіберзахисту; інтеграція державних, приватних і міжнародних зусиль; розвиток цифрової грамотності населення; створення спеціалізованих органів реагування на кіберінциденти; посилення міжнародного співробітництва в межах глобальної цифрової екосистеми. Зважаючи на гібридні загрози, що постійно еволюціонують, та зростаючу інтенсивність кібератак, забезпечення інформаційної безпеки стає не лише технічним викликом, а й пріоритетом державної політики й міжнародної співпраці.

У контексті зростання ролі цифрових технологій та кіберпростору як рушія соціально-економічного розвитку, проблема інформаційної безпеки набула глобального значення та стала предметом стратегічної уваги держав. Аналіз практик Японії, Китаю та Індії дозволяє зробити низку важливих висновків щодо закономірностей та особливостей національних підходів до забезпечення інформаційної безпеки.

По-перше, у Японії спостерігається розвинена нормативно-інституційна модель, що базується на принципах соціальної відповідальності, сервісного підходу до кіберзахисту та широкого використання механізмів аутсорсингу. Водночас система характеризується високим рівнем державного впливу на інформаційний обіг, включаючи механізми неформального контролю та саморегулювання медіа. Незважаючи на значні досягнення в галузі інформатизації, нормативне забезпечення інформаційних прав громадян залишається обмеженим фрагментарністю правової бази та дефіцитом доктринального осмислення.

По-друге, Китай демонструє стратегічне використання кібербезпеки як елемента зовнішньої політики. Ініціатива «Цифрового шовкового шляху» у рамках BRI передбачає не лише експорт цифрової інфраструктури, а й експорт моделі кіберсуверенітету. Залучення кібербезпечних компаній, тісно пов'язаних із державними органами безпеки, свідчить про використання приватного сектору в інтересах політичного впливу та просування специфічного бачення інтернет-врядування. Такий підхід викликає занепокоєння щодо прозорості, дотримання прав людини та потенційних механізмів цифрового контролю.

По-третє, Індія, маючи статус одного з лідерів у сфері інформаційних технологій, активно розвиває інституційний потенціал у сфері кібербезпеки. Національна політика кібербезпеки, створення галузевих органів (зокрема DSCI), а також зростання державного і приватного інвестування свідчать про прагнення до посилення стійкості у цифровому середовищі. Водночас країна залишається вразливою до кіберзагроз через фрагментарність регулювання, обмежений доступ до якісних IT-рішень та нерівномірність цифрового розвитку.

Загалом, досвід цих країн засвідчує необхідність формування багаторівневої, адаптивної системи інформаційної безпеки, що враховує: комплексність регуляторних механізмів; баланс між безпекою, правами людини і свободою інформації; стратегічне бачення цифрового суверенітету; ефективну координацію між державним, приватним та громадянським секторами; міжнародну співпрацю в галузі цифрової безпеки. Для України ці напрацювання становлять значну цінність у процесі розбудови національної системи інформаційної безпеки. Вивчення підходів Японії, Китаю та Індії дозволяє виокремити ефективні практики, уникнути системних ризиків та сформулювати стратегію цифрової стійкості, що відповідатиме як вимогам національної безпеки, так і цінностям демократичного врядування.

Аналіз підходів країн Латинської Америки до забезпечення інформаційної безпеки засвідчив наявність спільних викликів, серед яких – фрагментарність нормативно-правової бази, нестача координації між інституціями, обмежені технічні ресурси та вразливість до кіберзлочинності. Водночас кожна держава демонструє власну модель реагування на цифрові загрози, яка формується під впливом політичного контексту, рівня цифровізації та наявності інституційної спроможності. Мексика характеризується спробами інституційного оформлення кібербезпеки, однак її політика залишається декларативною через брак міжвідомчої координації, відсутність центрального органу та обмежене впровадження стратегії. Бразилія демонструє децентралізовану, але активну політику, з акцентом на цифрові права, свободу інтернету та публічно-приватне партнерство. Водночас ефективність обмежується регіональною фрагментованістю. Аргентина зробила кроки до посилення кіберзахисту через створення спеціалізованих структур, однак страждає на відсутність інтегрованої стратегії та сталого міжінституційного управління. Колумбія виділяється порівняно системним підходом до формування кіберполітики, активною участю в міжнародному співробітництві та розбудовою інституцій, проте стикається з нестачею ресурсів та нерівномірним впровадженням політик.

У підсумку, ефективне забезпечення інформаційної безпеки в регіоні потребує: створення національних координуючих центрів; уніфікації законодавства відповідно до міжнародних стандартів; розвитку цифрової освіти та обізнаності населення; зміцнення міжнародного співробітництва в межах Латинської Америки; поєднання технічних, правових та організаційних механізмів кіберзахисту. Для України досвід країн Латинської Америки може слугувати джерелом важливих уроків щодо побудови стійкої цифрової інфраструктури в умовах політичної нестабільності, обмежених ресурсів та зростаючих гібридних загроз.

Інформаційна агресія Російської Федерації проти України є системною, комплексною та стратегічно вмотивованою формою гібридної війни, що поєднує пропаганду, дезінформацію, кібероперації, інформаційно-психологічні впливи та маніпулятивні кампанії в цифровому середовищі. Її мета – підірвати політичну стабільність, делегітимізувати державні інститути, ослабити національну єдність і знизити міжнародну підтримку України.

Аналіз засобів та механізмів, що використовуються РФ, свідчить про високу технологічність, адаптивність і мімікрію під демократичні цінності, зокрема свободу слова, плюралізм та відкритість інформаційного простору. В умовах триваючої війни особливо небезпечною є здатність ІПсО формувати викривлену реальність, деморалізувати населення й впливати на громадську думку як в Україні, так і за її межами.

Незважаючи на значні зусилля української держави у сфері протидії – від нормативно-інституційних ініціатив до блокування проросійських ресурсів, зміцнення стратегічних комунікацій і співпраці з міжнародними партнерами – Україна залишається вразливою до інформаційних атак. Ключовими проблемами є низький рівень цифрової освіти, обмеженість незалежних медіа, поширення анонімного деструктивного контенту та повільна реакція на новітні загрози, зокрема з боку генеративного ШІ.

У цьому контексті забезпечення інформаційної безпеки має стати постійним елементом національної безпекової політики. Протидія інформаційно-маніпулятивному впливу РФ повинна спиратися на такі стратегічні підходи: підвищення цифрової та медіаграмотності громадян, формування культури критичного мислення, розвиток незалежних медіа, розширення міжнародної співпраці в межах системи інформаційної безпеки та створення ефективної державної політики з превентивного захисту інформаційного простору. Лише в умовах поєднання інституційної спроможності, громадянської активності та міжнародної солідарності можливе стримування російської інформаційної експансії та збереження інформаційного суверенітету України.

Громадянське суспільство стало одним із ключових чинників забезпечення інформаційної безпеки України в умовах гібридної війни. З початку агресії РФ у 2014 році численні неурядові організації, журналістські ініціативи, OSINT-спільноти та волонтерські об'єднання, зокрема StopFake, Detector Media, InformNapalm, Українські кібервійська, Лабораторія цифрової безпеки, взяли на себе функції моніторингу, спростування дезінформації, цифрового патрулювання та формування контрнаративів. Ці організації оперативно реагують на інформаційні загрози, посилюють спроможності держави, розбудовують цифрову грамотність суспільства, створюють нові стандарти кіберзахисту та сприяють міжнародному визнанню українського досвіду. Участь

громадськості дозволила не лише компенсувати інституційну нестачу державної відповіді, але й запровадити нові практики – від верифікації фактів до мобілізації цифрових волонтерів.

Водночас діяльність громадянського сектору стикається з низкою викликів: фрагментарна координація з державою, нестача фінансування, правова неврегульованість, а також необхідність дотримання етичних і правових норм, особливо у питаннях публікації персональних даних. Окремі приклади, як-от випадок із «Миротворцем», засвідчують ризики відсутності чітких рамок співпраці між державними й недержавними суб'єктами. У сучасних умовах захист інформаційного простору потребує скоординованої взаємодії держави та громадських ініціатив. Необхідним є формування національної стратегії співпраці, розвиток правових гарантій для громадських організацій та розбудова загальнонаціональної мережі цифрової безпеки. Український досвід протидії інформаційному тероризму вже інтегрується в європейські й натівські стратегії безпеки та може бути адаптований іншими державами, які стикаються з подібними загрозами.

Таким чином, українське громадянське суспільство довело свою ефективність як потужний суб'єкт інформаційного спротиву. Його подальше інституціональне укріплення та міжнародна підтримка мають стати пріоритетом у побудові сталої моделі інформаційної стійкості України

Дякую за увагу!

ВИСТУПИЛИ:

Науковий консультант – Шуляк А. М., доктор політичних наук, професор, декан факультету міжнародних відносин, Волинський національний університет імені Лесі України.

(ТЕКСТ ВІДГУ ДОДАЄТЬСЯ)

У цілому докторська дисертація Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук, відповідає вимогам Порядку присудження та позбавлення наукового ступеня доктора наук, який затверджено Постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197 «Деякі питання присудження (позбавлення) наукових ступенів» щодо дисертації для здобуття наукового ступеня доктора політичних наук та може бути рекомендована до захисту.

Рецензенти надали позитивні відгуки на дисертацію та реферат та висловили пропозиції, які носять рекомендаційний характер:

Д. політ. н., проф. Тихомирова Є. Б.: У дисертації було б доречно доповнити аналіз коротким оглядом історії розвитку інформаційних атак у світі. Зокрема, у першому розділі доцільно подати хронологію становлення концепції інформаційного тероризму, а в другому – етапи розвитку його практики, з акцентом на трансформацію терористичних дій у цифрову епоху. Важливо висвітлити події 11 вересня 2001 року як ключову точку переосмислення: з одного боку – каталізатор активного розвитку досліджень тероризму, а з іншого – фактор радикальної зміни ролі медіа у висвітленні терористичних актів, коли поєднання шокового ефекту з політичною пропагандою значно підсилило вплив терористів на масову аудиторію.

Завідувач кафедри політології та публічного управління, доктор політичних наук, професор Бусленко В. В.: Структура дисертації є всеохоплюючою та демонструє прагнення охопити широкий спектр країн і концепцій. Водночас таке розширене бачення (наприклад, аналіз «інформаційного тероризму у країнах Африки й Латинської Америки») подекуди призводить до більш описового характеру окремих розділів. Тому варто було б розглянути можливість поглиблення деяких частин, зокрема у порівняльному аналізі регіонів, що зробило б дослідження ще більш переконливим та збалансованим.

Доктор політичних наук, професор кафедри політології та публічного управління Ярош О. Б.: Висновки дисертації, попри те що вони добре узагальнюють результати, могли б бути посилені шляхом більш чіткого окреслення обмежень дослідження та визначення перспектив подальших наукових пошуків. Доцільно було б окремо зупинитися на таких напрямах майбутніх досліджень, як етичні наслідки застосування ШІ в інформаційній обороні, детальний аналіз алгоритмічної дезінформації та впливу штучного інтелекту на феномен інформаційного тероризму, роль приватних технологічних компаній в управлінні цими процесами, а також довгострокові психологічні ефекти для суспільства. Це дозволило б забезпечити більш комплексний і глибокий аналіз проблематики.

ЗАПИТАННЯ ДО ДИСЕРТАНТКИ ТА ВІДПОВІДІ НА НИХ:

1. К. істор. н., доц. кафедри міжнародних комунікацій та політичного аналізу Моренчук А. А.

ЗАПИТАННЯ: *Шановна дисертантка, скажіть будь ласка, у чому полягає складність сучасного міжнародного тероризму та які фактори визначають його трансформацію?*

ВІДПОВІДЬ: Дякую за запитання! Міжнародний тероризм є складним, динамічним і трансформаційним феноменом, що адаптується до змін глобального безпекового середовища. Попри значні наукові зусилля, рівень теоретичного осмислення та практичного забезпечення боротьби з ним усе ще не

відповідає масштабам загрози, а одновимірні підходи виявляються малоефективними. Серед основних чинників терористичної активності виокремлюють соціально-економічну поляризацію, релігійний фанатизм, ідеологічний радикалізм, прагнення до самовизначення та міжцивілізаційні розломи. Особливу небезпеку становить технологічний тероризм, що використовує зброю масового ураження, кіберінструменти й «сурогатні» війни, поширенню яких сприяє глобалізація. Це зумовлює зміну природи терористичних суб'єктів, появу транснаціональних і гібридних структур та потребу переосмислення концептів війни й безпеки, де тероризм дедалі більше набуває ознак воєнного інструментарію

2. К. політ. н., доц. кафедри міжнародних відносин та регіональних студій Кулик С.М.

ЗАПИТАННЯ: *Яке значення мали теракти 11 вересня 2001 року для трансформації міжнародної безпеки та глобального порядку?*

ВІДПОВІДЬ: Дякую за запитання! Теракти 11 вересня 2001 року стали переломним етапом у розумінні міжнародної безпеки, ролі держав у протидії новим загрозам та засад функціонування глобального порядку. Вперше одна з найпотужніших держав світу – США – зазнала удару на власній території, що продемонструвало асиметричний характер терористичних викликів у добу глобалізації. У відповідь Сполучені Штати розпочали воєнні кампанії в Афганістані та Іраку, які викликали широкий міжнародний осуд через відхід від принципів колективної безпеки та легітимацію концепції «превентивної війни». Ці події спричинили суттєві геополітичні зрушення, серед яких – посилення американської присутності в Центральній Азії та розширення практик інформаційного й пропагандистського впливу. Водночас риторика «глобальної війни з тероризмом» нерідко ставала інструментом виправдання політичних і військових дій, що ігнорували соціальні й культурні витоки самого феномена тероризму.

Голова засідання, проф. кафедри міжнародних комунікацій та політичного аналізу, д. політ. н. Карпчук Н. П.: В ході обговорення дисертаційної роботи до неї не було висунуто зауважень, що стосувалися би самої суті роботи. Отже, можна констатувати, що дисертація кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук, носить оригінальний і завершений характер, є актуальною і самостійною роботою.

Таким чином **міжкафедральний семінар ухвалив:**

1. Дисертаційна робота містить розробки наукової новизни, що надає їй вагомого значення в рамках вирішення політичних проблем міжнародних систем і глобального розвитку.

2. Дисертацію виконано в рамках науково-дослідних робіт факультету міжнародних відносин ВНУ ім. Лесі Українки, а саме «Актуальні проблеми формування та розвитку європейського інформаційного простору» в 2010–2012 рр., «Інформація та комунікація в сучасному світі» у 2012–2014 рр. (держреєстраційний №0112U001779), держбюджетної теми «Інформаційна підтримка транскордонного співробітництва України» у 2013–2015 рр. (держреєстраційний №0113U002221), 2018-2019 рр. НДР «Інформаційна війна як новий вимір геополітичної ривалізації» згідно з наказом Міністерства освіти і науки України від 25.06.2018 р. № 695». Про фінансування спільних українсько-польських науково-дослідних проектів у 2018 р.» (співвиконавець Інститут наук про безпеку Краківського педагогічного університету ім. Національної освітньої комісії) (держреєстраційний №0119U001621). А також міжнародних грантових проєктів програми ERASMUS+ напряму Модуль Жана Моне: 2022-2025 рр. «Стратегічні комунікації ЄС: протидія деструктивним впливам», 2024-2027 рр. – «EU Counteraction to FIMI» (№101172342 ERASMUS-JMO-2024-MODULE).

3. Висновки дослідження знайшли своє підтвердження у 71 публікаціях, серед яких у фахових виданнях України категорії «Б» – 18, закордонних фахових виданнях – 3, з них у виданнях, що індексуються у наукометричних базах Web of Science та Scopus – 7, індивідуальна монографія – 1, розділ у колективній монографії – 2, навчальні та навчально-методичні праці – 3, тези доповідей та інші статті у наукових виданнях – 37.

4. Текст дисертації відповідає спеціальності 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку і вимогам Порядку присудження та позбавлення наукового ступеня доктора наук, який затверджено Постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197 «Деякі питання присудження (позбавлення) наукових ступенів» щодо дисертації для здобуття наукового ступеня доктора політичних наук.

5. Науковий ступінь кандидата політичних наук за спеціальністю Вознюк Є. В. здобула в 2011 р. у результаті публічного захисту в спеціалізованій вченій раді Інституту світової економіки і міжнародних відносин НАН України дисертації «Порівняльний вимір гендерної політики України та Росії».

Відповідно до Порядку присудження та позбавлення наукового ступеня доктора наук, який затверджено Постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197 «Деякі питання присудження (позбавлення) наукових ступенів» щодо дисертації для здобуття наукового ступеня доктора політичних

наук може бути подана для розгляду до спеціалізованої ради із захисту докторських дисертацій з політичних наук.

6. В докторській дисертації не використані матеріали й висновки кандидатської дисертації здобувача. Наукові положення і результати, які виносилися на захист у кандидатській дисертації «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку», повторно не виноситися на захист здобувачем наукового ступеня доктора наук.

7. Затвердити висновок, підготовлений докторами наук, професорами Бусленком В.В., Ярош О.Б., Тихомировою Є.Б. у такій редакції:

Тема дисертації кандидата політичних наук, доцента, завідувача кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку» за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку, поданої на здобуття наукового ступеня доктора політичних наук, була затверджена на засіданні Вченої Ради Східноєвропейського національного університету імені Лесі Українки, протокол № 6 від 26.12.2015 р. Науковий консультант – Шуляк Антоніна Миколаївна, доктор політичних наук, професор, декан факультету міжнародних відносин, Волинський національний університет імені Лесі України (м. Луцьк, Україна). Робота виконана на кафедрі міжнародних комунікацій та політичного аналізу ВНУ ім. Лесі Українки. Дисертація подається до розгляду на міжкафедральному семінарі вперше.

Актуальність теми дослідження. Актуальність дослідження інформаційного тероризму зумовлена тим, що він виступає одним із ключових інструментів гібридної війни, здатним дестабілізувати політичні системи, підірвати легітимність влади та створювати загрози міжнародній безпеці без застосування традиційної військової сили. У контексті російсько-української війни його вивчення є критично важливим для зміцнення інформаційної стійкості держави, захисту демократичних інститутів та розробки ефективних стратегій протидії деструктивним інформаційним впливам.

Ступінь новизни та важливість отриманих результатів. Представлені в дисертації положення, структура, концептуальні засади, формування завдань та їх вирішення, узагальнені висновки є результатом реалізації авторських ідей та самостійно виконаної науково-дослідної роботи автора. Наукова новизна дослідження полягає у запропонованій уперше концептуалізації поняття інформаційної стійкості, що визначається як здатність держави, інституцій та суспільства протидіяти комплексним інформаційним загрозам. У роботі обґрунтовано новий підхід до протидії інформаційному тероризму шляхом виокремлення трикомпонентної моделі, що поєднує стратегічні комунікації,

медіаосвіту та цифрову безпеку як взаємопов'язані складові національної інформаційної оборони. Вперше здійснено міждисциплінарне дослідження інформаційного тероризму, у якому його осмислено як автономний феномен глобалізованого світу, що поєднує риси когнітивної війни, кібертерору та ідеологічної агресії. Окрему новизну становить системний аналіз українського досвіду протидії інформаційній агресії, що розглядається як перспективна модель для ЄС, НАТО та міжнародної спільноти. Крім того, запропоновано нову інтерпретацію подій 11 вересня 2001 року як переломного моменту трансформації глобальної парадигми безпеки й початку нової ери інформаційно-психологічних і асиметричних конфліктів.

Теоретичне та практичне значення одержаних результатів. На основі проведеного дослідження сформульовано висновки, що поглиблюють теоретичне розуміння феномену інформаційного тероризму та його місця у системі міжнародної безпеки. Запропоновано міждисциплінарний підхід до аналізу деструктивних інформаційних впливів, розроблено типологію загроз і узагальнено міжнародний досвід протидії. Результати можуть слугувати основою для державної стратегії інформаційної безпеки, підвищення інформаційної грамотності суспільства та зміцнення стійкості до гібридних загроз. Практична цінність роботи полягає також у можливості використання її напрацювань у навчальному процесі та при створенні аналітичних центрів, спрямованих на вироблення україноцентричних наративів і посилення інтеграції в європейський простір.

Апробація результатів дослідження. Особистий внесок здобувача полягає у тому, що наукові положення та результати дисертації були обговоренні на численних наукових конференція різних рівнів – міжнародних, всеукраїнських, регіональних. За темою дисертації опубліковано у 71 публікаціях, серед яких у фахових виданнях України категорії «Б» – 18, закордонних фахових виданнях – 3, з них у виданнях, що індексуються у наукометричних базах Web of Science та Scopus – 7, індивідуальна монографія – 1, розділ у колективній монографії – 2, навчальні та навчально-методичні праці – 3, тези доповідей та інші статті у наукових виданнях – 37.

За затвердження висновку проголосували:

«ЗА» – 13, «ПРОТИ» – 0, «УТРИМАЛИСЯ» – 1.

Результати експертизи та засідання фахового семінару. Рецензенти на підставі експертизи дисертаційного дослідження та наукових публікацій, у яких висвітлені основні наукові відкриття, а також за результатами засідання фахового міжкафедрального семінару, на якому була апробована дисертація,

ухвалили одноголосне рішення – рекомендувати до захисту у спеціалізованій вченій раді дисертацію кандидата політичних наук, доцента кафедри міжнародних комунікацій та політичного аналізу Вознюк Євгенії Василівни «Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку», поданої на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку.

Рецензенти:

Д.політ.н., проф. кафедри міжнародних комунікацій
та політичного аналізу Тихомирова Є. Б. _____

Завідувач кафедри політології та публічного управління,
д. політ. н., проф. Бусленко В.В. _____

Д. політ.н., проф. кафедри політології
та публічного управління Ярош О.Б. _____

Д. політ. н., проф. кафедри
міжнародних комунікацій
та політичного аналізу _____ **проф. Наталія КАРПЧУК**

Секретар _____ **доц. Сергій КУЛИК**

ПІДПИС Н. Карпчук С. Кулика
ЗАСВІДЧУЮ
Вчений секретар університету
«26» 08 2025 р.