Голові разової спеціалізованої вченої ради
Харківського національного університету
імені В.Н. Каразіна професору
Валентині ШАМРАЄВІЙ
майдан Свободи 4, м. Харків, 61022

РЕЦЕНЗІЯ

офіційного рецензента – доктора політичних наук, доцента, завідувача кафедри міжнародних відносин Навчально–наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу» Наталії ВІННИКОВОЇ на дисертаційну роботу Олександри ЗІНЧЕНКО на тему «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» з галузі знань 05 «Соціальні та поведінкові науки»на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія».

Обґрунтування вибору теми дослідження.

Сучасний розвиток держав характеризується глобалізаційними процесами й стрімким прогресом інформаційних технологій, які, поряд з перевагами, породжують нові виклики. Одним із таких викликів є кібертероризм, що становить серйозну загрозу для національної безпеки як України, так і інших держав Європейського регіону.

Кібертероризм охоплює атаки на критичну інфраструктуру, поширення дезінформації, спроби дестабілізації суспільства та втручання у державне управління. В умовах російської збройної агресії проти України ця загроза набула особливої гостроти: кібератаки стали складовою сучасної гібридної війни, спрямованої на підрив обороноздатності, дестабілізацію економіки та завдання шкоди цивільному населенню. Сукупність зазначених обставин свідчить про те, що тема рецензованого дисертаційного дослідження є надзвичайно актуальною та суспільно значущою.

Характеристика основних положень роботи.

Структурно робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. Треба відмітити, що кожен із розділів має наукову новизну та є значущим у контексті розвитку політичної науки.

У першому розділі здійснено ґрунтовний теоретичний аналіз базових категорій — «кібертероризм», «кібербезпека», «національна безпека держави». Авторка пропонує нове наукове осмислення кібертероризму як політичного концепту, що вимагає специфічного реагування з боку державних інституцій і міжнародного співтовариства.

Другий розділ присвячено дослідженню досвіду впровадження комплексних систем кібербезпеки в окремих державах Європейського регіону. Проведений аналіз дозволив авторці окреслити ключові компоненти, які доцільно імплементувати в українську модель захисту кіберпростору. Особливої уваги заслуговує її пропозиція переглянути застарілі правові норми та адаптувати їх до сучасних міжнародних стандартів і актуальних геополітичних викликів.

Слушною та своєчасною є також ідея авторки щодо необхідності реформування української урядової команди реагування на комп'ютерні надзвичайні події (CERT-UA), зокрема в таких критично важливих секторах, як охорона здоров'я, енергетика, державне управління та електронні комунікації. Запропонований секторальний підхід дозволяє забезпечити більш ефективний розподіл відповідальності та підвищити рівень оперативного реагування.

Особливої уваги заслуговує розроблена авторкою національна програма кіберосвіти, яка є надзвичайно важливою для сучасної України. Формування цифрової обізнаності населення, підвищення рівня цифрової грамотності та підготовка професійних кадрів — усе це є передумовою для формування сталого суспільного імунітету до кіберзагроз.

У третьому розділі досліджено трансформацію загроз у кіберпросторі України в умовах російського повномасштабного вторгнення. Авторка

аргументовано виділяє два найбільш уразливі сектори — енергетичну інфраструктуру та систему електронної охорони здоров'я, — які визначено як життєво важливі для забезпечення функціонування держави. Запропоновані підходи до підвищення їх кіберстійкості мають як теоретичну, так і практичну значущість.

Високу наукову цінність має пропозиція авторки щодо закріплення поняття ядерної кібербезпеки в міжнародно-правовому полі. Це нове стратегічне бачення є особливо важливим для України та всього європейського простору, враховуючи ризики, пов'язані з ядерною енергетикою в умовах воєнної агресії та цифрових загроз.

Окрему увагу в дисертаційному дослідженні приділено аналізу стану кібербезпеки в сфері електронної охорони здоров'я (eHealth) України. Авторка обґрунтовано підкреслює, що медична цифрова інфраструктура в умовах війни є не менш уразливою, ніж енергетика чи оборона, оскільки атаки на системи електронного здоров'я мають прямий вплив на життя й здоров'я населення. У роботі визначено конкретні вектори посилення кіберзахисту eHealth-сектору, зокрема розробку та імплементацію спеціалізованих нормативно-правових актів, посилення міжвідомчої координації, а також створення незалежних аудитів цифрової стійкості медичних систем.

Авторка також акцентує на необхідності підвищення кіберграмотності медичних працівників і розробці спеціалізованих протоколів реагування на кіберінциденти в закладах охорони здоров'я. Важливим елементом є ідея інтеграції українських стандартів кіберзахисту eHealth у європейську нормативну площину, що відкриває перспективи для формування спільного цифрового безпекового простору в галузі охорони здоров'я.

Загальним висновком дисертації є встановлення прямого зв'язку між національною та регіональною безпекою, що вимагає скоординованого підходу до вирішення багатовекторних викликів кібервійни. Авторкою обґрунтовано запропоновано низку практичних ініціатив, зокрема ідею

створення посади кіберомбудсмена як незалежного наглядача за правами громадян у цифровому просторі.

Особливої ваги набувають запропоновані авторкою нові соціально-політичні концепції — такі як «кіберсоціальна адаптація» та «кіберімунітет», що становлять інноваційний підхід до забезпечення кіберстійкості держави та суспільства. Вони демонструють авторське бачення сучасної кібербезпеки як багаторівневої взаємодії технічних, нормативних, інституційних, політичних та соціальних компонентів.

Загальний акцент у роботі зроблено на потребі уніфікації правових підходів, розширенні міжнародної співпраці та спільній відповідальності європейських держав у протидії кібертероризму. Методологія дослідження вирізняється об’єктивністю, чітким формулюванням мети та завдань, логічним добором методів, системною обробкою даних, їх верифікацією та критичним аналізом.

На підставі вищезазначеного можна зробити обґрунтований висновок про наявність у дисертації логічно узгоджених і внутрішньо послідовних результатів, які цілковито відповідають сформульованим цілям і завданням дослідження. Авторка продемонструвала глибоке розуміння сутності проблематики кібербезпеки та її політичного виміру, запропонувавши низку концептуально виважених і практично орієнтованих рекомендацій, здатних сприяти модернізації національної політики у сфері кіберзахисту.

Зокрема, у роботі обґрунтовано доцільність створення нових інституцій, здатних забезпечити цілісну та ефективну систему реагування на сучасні кіберзагрози. Окрема увага приділяється необхідності оновлення чинної нормативно-правової бази з урахуванням транснаціонального характеру кіберзлочинності та сучасних міжнародних стандартів. У дисертації також запропоновано імплементацію концепції ядерної кібербезпеки як стратегічно важливої складової безпекової політики України, а також окреслено напрями посилення кіберзахисту в секторі eHealth. Авторка подає детально аргументовані пропозиції щодо реформування кіберінфраструктури у

критичних секторах, що надає роботі прикладної значущості та відкриває простір для подальших політичних рішень у цій сфері. Дисертаційне дослідження повністю відповідає вимогам до наукової роботи, підготовлене державною мовою у вигляді рукопису. Робота має чітку структуру: титульний аркуш, анотацію, зміст, основну частину (вступ, три розділи, висновки), список використаних джерел. Загальний обсяг дисертації — 271 сторінка, з яких 203 сторінки приділено основній частині, бібліографія налічує 348 найменувань.

Усе це свідчить про самостійну, цілеспрямовану й плідну працю над темою, а також про вагомий особистий внесок авторки в розробку актуальних наукових підходів і практичних рішень у сфері протидії кібертероризму. Разом із тим, окремі положення викликають наукову дискусію або потребують подальшої конкретизації та змістовного уточнення.

Дискусійні положення та рекомендації до змісту дисертації

1. У методологічній частині роботі авторка акцентує на важливості застосування ціннісно-нормативного підходу в дослідженні впливу кібертероризму на суспільство, і зокрема громадську довіру до державних установ (с. 77-78). Водночас у дослідженні не представлені результати ані суспільної оцінки кіберзагроз чи механізмів протидії ним, ані показники кіберграмотності чи кібергігієни громадян у контрольній групі країн, обраних для аналізу. У дисертації домінує опис інфрастурктур кібербезпеки та аналіз нормативно-правової бази.

2. На жаль, у роботі недостатньо приділено уваги такій гостроактуальній темі в контексті кіберерозризму та кібербезпеки як експоненціальне впровадження технологій Штучного Інтелекту. Ця проблема прямо корелює з питаннями, порушеними в дисертаційному дослідженні. Авторка лише поверхнево вказує на дотичність цих технологій до загального контексту кібербезпеки: с. 35, с. 57, с.113, с. 150. Доречним було б проаналізувати, які загрози для національних цифрових систем несуть великі

мовні моделі з відкритим кодом, і які заходи впроваджують уряди для їх нейтралізації.

3. Дисертаційне дослідження переважно сфокусовано на аналізі державних механізмів регулювання проблем кібербезпеки і боротьби з кібертероризмом. Водночас варто було б включити в спектр аналізу акторів, що є «джерелом» кібертероризму, їхні політичні мотиви, методи кібератак. У дисертаційні роботі це питання переважно розкривається в огляді російських кібератак на кіберпростір України.

4. Текст дисертації перевантажений англомовними абревіатурами назв установ без розшифрування, що ускладнює сприйняття інформації. На приклад, «Зокрема, **CERT– SE, FM CERT** та інші команди мають акредитацію Trusted Introducer, що підтверджує їх високий рівень професіоналізму і здатність до оперативної взаємодії з європейськими командами» с. 119; «…у Німеччині функціонує мережа організацій **CERT/CSIRT**, що реагують на кіберінциденти та аналізують загрози» с. 110; «Ще одним індексом, який вимірює кібербезпеку, є **NCSI**» с. 135 і т.п.

Наведені зауваження не применшують загальної позитивної оцінки дослідження, а навпаки – відкривають простір для подальших наукових розвідок у цій тематиці, зокрема в контексті практичної імплементації політик кібербезпеки і боротьби з кібертероризмом.

Дисертаційна робота «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» Олександри ЗІНЧЕНКО, подана на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія, є самостійною, завершеною, науково-дослідницькою роботою, відповідає вимогам наказу Міністерства освіти і науки України №40 від 12.01.2017 року «Про затвердження Вимог до оформлення дисертації» (зі змінами), «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України №44 від 12 січня 2022 р . (зі змінами

від 03.05.2024 р. № 507), не містить ознак порушення академічної доброчесності, а тому авторка дисертації – Олександра ЗІНЧЕНКО, за умови успішного захисту, заслуговує на присудження наукового ступеня доктора філософії з галузі знань 05 Соціальні та поведінкові науки зі спеціальності 052 Політологія.

Офіційний рецензент:
доктор політичних наук, доцент,
завідувач кафедри міжнародних відносин
Харківського національного
університету імені В. Н. Каразіна Наталія ВІННИКОВА

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 14:25:01 13.08.2025

Назва файлу з підписом: Рецензія Вінникової Н.А. на дисертацію Зінченко О.І..pdf
Розмір файлу з підписом: 215.4 КБ

Перевірені файли:
Назва файлу без підпису: Рецензія Вінникової Н.А. на дисертацію Зінченко О.І..pdf
Розмір файлу без підпису: 181.4 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ВІННИКОВА НАТАЛІЯ АНАТОЛІЇВНА
П.І.Б.: ВІННИКОВА НАТАЛІЯ АНАТОЛІЇВНА
Країна: Україна
РНОКПП: 2985107184
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 14:25:00 13.08.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000004614A9011AEE8C06
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підписаний PDF-файл (PAdES)
Формат підпису: З повними даними для перевірки (PAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.08.04 13:00

Голові разової спеціалізованої вченої ради
Харківського національного університету
імені В.Н. Каразіна професору
Валентині ШАМРАЄВІЙ
майдан Свободи 4, м. Харків, 61022

РЕЦЕНЗІЯ

офіційного рецензента доктора політичних наук, доцента, професора кафедри політології Харківського національного університету імені В. Н. Каразіна Тетяни КОМАРОВОЇ на дисертаційну роботу Олександри ЗІНЧЕНКО «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону», подану на здобуття наукового ступеня доктора філософії з галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 – Політологія.

Обґрунтування вибору теми дослідження.

Дисертаційна робота Олександри ЗІНЧЕНКО присвячена надзвичайно актуальній та складній у теоретичному й практичному сенсі проблемі, яка пов’язана з сучасними безпековими викликами — протидією кібертероризму в умовах трансформації систем національної та регіональної безпеки в Європі. З огляду на динамічні трансформації у сфері міжнародної безпеки, цифрової глобалізації та загострення гібридних конфліктів, кібертероризм перетворився на один із центральних факторів політичного ризику для демократичних держав.

Авторка цілком слушно зазначає, що нині в Європейському регіоні відсутнє єдине розуміння політичної природи кібертероризму, як і достатня міждержавна координація з протидії цим викликам, особливо в умовах гібридної агресії проти України.

Актуальність обраної теми дослідження зумовлена системною переоцінкою безпекових парадигм у сучасному європейському політичному просторі. У контексті поліцентричної архітектури загальноєвропейської

безпеки, де домінують трансформаційні процеси, пов’язані з міграційними викликами, технологічною уразливістю і цифровим суверенітетом, проблема кібертероризму постає як одна з найменш концептуалізованих, хоча і найнебезпечніших форм підриву державного суверенітету.

Зважаючи на відсутність усталених політичних механізмів протидії таким загрозам у межах національних держав і наднаціональних утворень (ЄС, НАТО), запропоноване авторкою дослідження є спробою закласти політичні основи осмислення цієї категорії не лише як інструменту гібридної війни, але і як окремого політичного явища, що трансформує саме розуміння національної безпеки в цифрову епоху.

Особливу увагу в роботі приділено теоретичній рефлексії над поняттям «кібертероризм», яке розглядається не лише як техніко-безпекова категорія, а передусім як політичне явище — з його інституційними, ціннісними та комунікативними вимірами. Саме тому спроба комплексного політичного аналізу цієї проблематики є надзвичайно своєчасною та заслуговує на високу оцінку.

Загальна характеристика дисертаційної роботи.

Дисертаційна робота складається з анотацій (українською та англійською мовами), вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації —271 сторінка, з яких 203 сторінки приділено основній частині, список використаних джерел налічує 348 найменувань.

У вступі дисертації обґрунтовано актуальність теми дисертаційного дослідження, визначено мету, завдання, об’єкт та предмет дослідження; зазначено використані методи дослідження; сформульовано наукову новизну, отриманих результатів та їхнє практичне значення; надано інформацію щодо апробації результатів дослідження, кількості публікацій за темою дисертації; зазначено структуру дисертації.

У першому розділі дисертації «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» здійснено

теоретико-методологічний аналіз понять «кібертероризм», «кібербезпека» та «національна безпека держави». Авторкою обґрунтовано необхідність оновлення змісту терміна «кібертероризм» у законодавстві України та його закріпленні на регіональному рівні, модернізації його визначення, а також трансформації підходів до розуміння кібербезпеки з урахуванням європейських стандартів.

Запропоновано нові політичні концепти — «кіберсоціальна адаптація» та «кіберімунітет» — як інструменти підвищення стійкості суспільства до цифрових загроз. Розглянуто важливість міждисциплінарної методології, гармонізації правових підходів і міжнародної співпраці, а також надано практичні рекомендації щодо впровадження систем проактивного моніторингу та посади кіберомбудсмена.

У другому розділі дисертації проаналізовано досвід країн Європейського регіону з високим рівнем захисту від кібератак та визначено можливості його адаптації в Україні. Виявлено фрагментарність і неефективність чинної нормативно-правової бази, що стримує формування цілісної стратегії кіберзахисту. Обґрунтовано необхідність гармонізації законодавства України з міжнародними стандартами, реформування CERT-UA та впровадження секторального підходу до кіберзахисту.

Запропоновано трансформацію Антитерористичного центру України в структуру, здатну протидіяти як фізичним, так і кіберзагрозам, що сприятиме посиленню ролі держави у міжнародній безпековій політиці. Окрему увагу приділено «Національній програмі кіберосвіти», спрямованій на подолання кадрового дефіциту в умовах війни.

У третьому розділі дисертації досліджено вплив повномасштабного вторгнення Російської Федерації на кібербезпекову ситуацію в Україні та Європі, зокрема загострення загроз для критичної інфраструктури. Особливий акцент зроблено на енергетичному секторі та системі електронної охорони здоров’я, які визначено як найбільш уразливі до кібератак. Розкрито концепцію «ядерної кібербезпеки» як стратегічного напряму міжнародної безпеки та

обґрунтовано необхідність її закріплення у правовому полі. Проведено порівняльний аналіз стану кіберзахисту електронної охорони здоров'я в Україні та окремих європейських країнах, визначено ключові напрями вдосконалення. Підкреслено взаємозалежність національної та регіональної безпеки, необхідність уніфікованих правових підходів, зміцнення інституційних структур і розвитку міжнародної співпраці задля підвищення стійкості до кібертероризму.

Висновки логічно випливають зі змісту роботи, узагальнюють основні результати дослідження та відповідають поставленим завданням. Вони мають як теоретичне, так і практичне значення, зокрема для формування оновленої національної політики кібербезпеки України, удосконалення нормативно-правової бази та розробки інституційних механізмів протидії кібертероризму. Запропоновані авторкою концепції, моделі та програми можуть бути використані органами державної влади, міжнародними організаціями та науковими установами для посилення стійкості національних і регіональних систем безпеки в умовах зростаючих цифрових загроз.

Зв'язок дисертації з науковими програмами, планами, темами, грантами.

Наукове дослідження було виконано здобувачем на кафедрі політології філософського факультету Харківського національного університету імені В.Н. Каразіна під керівництвом, доктора політичних наук, професора, завідувача кафедри політології Олександра ФІСУНА. Дисертаційне дослідження є складовою науково-дослідної роботи кафедри політології Харківського національного університету імені В.Н. Каразіна за темою «Реформування політичної системи України у порівняльній та глобальній перспективі». У межах цієї НДР автором комплексно проаналізовано кібертероризм як один із ключових чинників, що впливають на політичну стабільність, ефективність інститутів влади та процеси реформування політичної системи. Дослідження охоплює вивчення правових, інституційних

та технологічних механізмів протидії кіберзагрозам у державах Європейського регіону, що дало змогу сформувати рекомендації для інтеграції сучасних стандартів кібербезпеки у вітчизняну систему публічного управління. Отримані результати можуть бути використані для зміцнення стійкості політичної системи України, підвищення її здатності адаптуватися до глобальних викликів цифрової епохи та забезпечення національної безпеки.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Наукова обґрунтованість висновків і пропозицій підкріплена аналізом значного масиву джерел — як наукової, так і нормативної літератури, міжнародних документів, політичних стратегій та реальних прикладів європейської практики. Залучення джерел англомовного наукового дискурсу та стратегічних документів інституцій ЄС та НАТО свідчить про належний рівень академічної підготовки дисертантки та її здатність працювати із матеріалом високої складності.

Основні положення та ідеї дисертаційної роботи висвітлено на міжнародних наукових конференціях та у 4 статтях, опублікованих у наукових фахових виданнях України, та наукових виданнях віднесених до категорії А, індексованих в Scopus та WoS.

Особливу увагу в роботі приділено теоретичній рефлексії над поняттям «кібертероризм», яке розглядається не лише як техніко-безпекова категорія, а передусім як політичне явище — з його інституційними, ціннісними та комунікативними вимірами і ґрунтується на системному осмисленні трансформацій сучасної політики безпеки, зокрема в контексті гібридних загроз і цифрової вразливості європейських демократій.

Авторка аргументовано доводить, що в умовах глобалізації цифрових технологій та гібридного характеру сучасних загроз кібертероризм набув ознак самостійної форми політичного насильства, що здатна підірвати функціонування інститутів державної влади, критичної інфраструктури,

демократичних процедур. Важливо, що авторка не обмежується технологічною або кримінологічною площиною проблеми, а наполягає на її політичному змісті: кібертероризм постає як деструктивний фактор політичної боротьби, що здатний впливати на легітимність влади, змінювати політичну комунікацію та модифікувати систему безпеки.

Найвагоміші наукові результати, що містяться в дисертації.

Робота має високий рівень теоретичної новизни. До важливих результатів належить введення нових політичних понять, таких як наприклад «кіберсоціальна адаптація», «кіберімунітет», а також обґрунтування необхідності створення інституту «кіберомбудсмена». Усі ці поняття ґрунтуються на глибокому аналізі реальних процесів і можуть бути корисними не лише для академічної дискусії, а й для практичного державного управління. Авторка не просто формулює теоретичні положення, а й демонструє можливі шляхи їхнього втілення в національну політику.

Робота авторки вирізняється комплексним підходом до дослідження проблематики кібертероризму та кібербезпеки. Авторка здійснила системний аналіз поняття «кібертероризм», уточнила його структурні елементи та запропонувала власне визначення, що враховує політичний, соціальний та технологічний аспекти цього явища. На основі вивчення досвіду України та європейських країн сформовано концепцію загальноєвропейського стандарту боротьби з кібертероризмом, що забезпечує координацію дій держав у запобіганні та протидії загрозам. Також розширено і уточнено поняття кібербезпеки як комплексного стратегічного процесу, що охоплює захист національного суверенітету, критичної інфраструктури, прав і свобод громадян у кіберпросторі.

Робота відзначається високою міждисциплінарністю, поєднуючи правові, політичні, технічні та соціальні аспекти проблеми. Авторка обґрунтовано запропонувала оновлення національної політики кібербезпеки, реформування CERT-UA, інтеграцію кібертерористичної складової в діяльність Антитерористичного Центру, а також розвиток нормативно-правової бази для

захисту критичної інфраструктури, включно з атомними об’єктами та сектором eHealth. Вперше сформульовано концепти «ядерної кібербезпеки» та «кібербезпеки eHealth», що є важливим внеском у розвиток міжнародної безпеки та національної політики у сфері кіберзахисту.

Особливу наукову значущість роботи становить пропозиція формування інтегрованої моделі забезпечення кібербезпеки України, яка включає компоненти інтеграції, адаптації, інновацій та кіберосвіти, а також ініціативи щодо міжнародного співробітництва, включно з ратифікацією Третього Додаткового Протоколу до Будапештської Конвенції та створенням міжнародного «кібертрибуналу».

Таким чином, дослідження авторки робить вагомий внесок у розвиток теоретичних та практичних засад державної політики і міжнародного співробітництва у сфері кібербезпеки, формує нову політичну парадигму протидії кібертероризму та є актуальним у контексті сучасних загроз національній і міжнародній безпеці.

Практичне значення результатів дисертаційного дослідження.

Практичне значення дисертаційного дослідження полягає у можливості використання його результатів для вдосконалення національної системи кібербезпеки та підвищення ефективності державної політики у сфері протидії кібертероризму. Розроблені авторкою концепції та рекомендації дозволяють впроваджувати комплексні заходи щодо захисту критичної інфраструктури, удосконалення нормативно-правових актів, а також організаційної структури державних органів, відповідальних за кібербезпеку.

Запропоновані інноваційні підходи можуть бути використані у практичній діяльності органів державної влади, міжнародних організацій і наукових установ для підвищення стійкості держави та суспільства до сучасних кіберзагроз. Вперше сформульовані принципи «ядерної кібербезпеки» та «кібербезпеки eHealth» забезпечують наукову основу для створення ефективних заходів захисту стратегічних об’єктів і життєво важливої

інформації, що має безпосереднє значення для національної безпеки та міжнародної співпраці у сфері кіберзахисту.

Таким чином, результати дослідження можуть бути застосовані для розробки стратегій, стандартів і практичних рішень, що дозволяють Україні підвищити рівень захищеності держави та громадян у цифровому середовищі та забезпечити активну участь у формуванні міжнародної системи кібербезпеки.

Дотримання академічної доброчесності.

Дисертація Олександри ЗІНЧЕНКО відповідає вимогам щодо академічної доброчесності, має чітко структуровану систему джерел, посилань, авторських положень. Вона є результатом самостійної, глибокої та масштабної роботи, що поєднує теоретичну складність із практичною значущістю. Матеріали дисертації можуть бути використані у діяльності органів державної влади, зокрема для вдосконалення стратегії кібербезпеки, підготовки проєктів нормативно-правових актів та розробки навчальних курсів із політичної кібербезпеки у закладах вищої освіти.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Дискусійні положення та зауваження до змісту дисертації.

1. Систематизація європейських стандартів кібербезпеки та окреслення їхніх ключових елементів заслуговує на позитивну оцінку, оскільки створює основу для подальшого наукового аналізу. Водночас доречно було б розглянути шляхи адаптації цих стандартів до українського політичного, правового та соціокультурного середовища, зокрема з урахуванням рівня довіри громадян до

державних інституцій, особливостей управлінської культури та кадрових ресурсів у сфері кіберзахисту.

2. Розкриття ролі держави як інституційного гаранта політичної стабільності в умовах цифрових трансформацій є важливим аспектом дослідження. Разом із тим, більш детальне висвітлення взаємодії держави з громадянським суспільством, приватними технологічними компаніями та міжнародними структурами могло б поглибити розуміння механізмів протидії кіберзагрозам та забезпечення балансу між безпекою й демократичними свободами.

3. Порівняння моделей державного управління кібербезпекою в країнах із різними політичними режимами могло б додатково підсилити аргументацію дисертації. Такий підхід дозволив би оцінити інтеграційний потенціал європейських стандартів у національні системи з урахуванням рівня демократичності, централізації влади та взаємодії з громадянським суспільством, а також посприяв би формулюванню більш практично орієнтованих рекомендацій.

Проте означені зауваження в цілому не впливають на результативність, завершеність та загальну позитивну оцінку виконаної дисертаційної роботи, а також не знижують наукової та практичної цінності отриманих результатів.

Загалом дисертація підготовлена на високому науково-теоретичному рівні, висловлені зауваження здебільшого стосуються складності та багатогранності досліджуваної проблеми і жодним чином не применшують наукової та практичної цінності дисертаційної роботи. Означені дискусійні питання можуть бути предметом для подальших наукових досліджень здобувача.

Загальні висновки про дисертаційну роботу.

Таким чином, дисертація містить вагому наукову новизну, поєднує аналітичну глибину з прагматичною спрямованістю, відповідає актуальним викликам і повністю відповідає вимогам, що висуваються до дисертаційних

досліджень на здобуття ступеня доктора філософії зі спеціальності 052 – Політологія.

Отже, дисертація Олександри ЗІНЧЕНКО «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» є завершеним самостійним дослідженням, що має значну наукову, практичну та суспільну цінність. Дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 р. № 44) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Зважаючи на це, вважаю, що Олександра ЗІНЧЕНКО заслуговує на присудження наукового ступеня доктора філософії з галузі знань 05 «Соціальні науки та поведінкові» зі спеціальності 052 – Політологія.

доктор політичних наук, доцент,

професор кафедри політології
філософського факультету
Харківського національного університету
імені В. Н. Каразіна

Тетяна КОМАРОВА

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 15:42:48 14.08.2025

Назва файлу з підписом: РЕЦЕНЗІЯ_Комарова _Т_Г_ дисертація_ Зінченко_ О_І.pdf.p7s
Розмір файлу з підписом: 290.7 КБ

Перевірені файли:
Назва файлу без підпису: РЕЦЕНЗІЯ_Комарова _Т_Г_ дисертація_ Зінченко_ О_І.pdf
Розмір файлу без підпису: 271.9 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Комарова Тетяна Геннадіївна
П.І.Б.: Комарова Тетяна Геннадіївна
Країна: Україна
РНОКПП: 2591114188
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 15:42:19 14.08.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF9704000000A249980072545B04
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в одному файлі (CAdES enveloped)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.08.04 13:00

Голові разової спеціалізованої вченої ради
Харківського національного університету імені В.Н. Каразіна
професору Валентині ШАМРАЄВІЙ
майдан Свободи 4, м. Харків, 61022

ВІДГУК

офіційного опонента, доцента кафедри цивільного права і процесу Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», доктора юридичних наук, доцента **Філінович Валерії Вікторівни** на дисертацію Зінченко Олександри Ігорівни на тему *«Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону»* на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія», галузь знань 05 «Соціальні та поведінкові науки».

I. Обґрунтування вибору теми дисертаційного дослідження.

Актуальність дисертаційної роботи передусім пов'язана із поширенням явища кібертероризму як однієї із проблем сучасності, адже його масштаби зростають надзвичайно швидко. Таке явище є транскордонним, а тому політичні та юрисдикційні механізми окремо взятої країни є недостатніми і неефективними, отже потребують удосконалення та доповненням міжурядовими через створення спільних та єдиних стандартів боротьби. Запропонована дисертаційна робота саме й присвячена дослідженню відповідних прогалин як політичного, так і правого впливу для протидії кібертероризму, розробленню нових технологій безпеки через створення спеціальних підрозділів у структурах безпеки та розвиток ефективної міжнародної співпраці.

Запропоновані в дисертації новації як-то уніфікація діючої термінології з метою повного визначення нормативних дефініцій «кібертеротизм», «кібербезпека», осучаснення їх з урахуванням нових проблем та викликів, є слушними та нагальними. Також є науково обґрунтованими та новими тези та пропозиції із розроблення міждисциплінарної методології вивчення кібертероризму, гармонізації правових підходів та посилення міжнародного співробітництва у цій галузі, зокрема пропозиції щодо створення національних підрозділів кіберполіції, оновлення наявних стратегій кібербезпеки та активний моніторинг критичної інфраструктури.

Вбачаються новаторськими сформульовані в дисертації ідеї започаткування посади «кіберобмудсмена» як уповноваженого представника держави, діяльність

якого полягатиме в захисті суспільних інтересів, прав та свобод громадян у цифровому просторі, а також пропозиції з унормування нового Третього Протоколу до Будапештської Конвенції про Кіберзлочинність 2001 року, через включення до його змісту деталізації феномену кібертероризму, його характеристик, криміналізацію та політичного інструментарію протидії.

Заслуговує на увагу запропонована у дисертації гіпотеза щодо необхідності розроблення та впровадження «Національної програми кіберосвіти в Україні». Така програма, на думку авторки, має бути спрямована на системну підготовку та підвищення рівня обізнаності фахівців різних сфер діяльності щодо безпечної та ефективної роботи в цифровому середовищі. Особливо актуальним є охоплення цією програмою таких категорій, як медичні працівники, фінансисти, економісти, фахівці енергетичної галузі, технічні працівники, юристи та інші спеціалісти, діяльність яких передбачає використання інформаційних технологій і доступ до критичних даних. Запровадження подібної програми дозволило б підвищити рівень кіберстійкості держави загалом, сприяло б формуванню культури кібербезпеки у суспільстві та забезпечило б реалізацію державної політики у сфері цифрової трансформації з урахуванням викликів кібертероризму.

Таким чином, проблематика, піднята у дисертаційному дослідженні, є надзвичайно актуальною та відповідає сучасним потребам розвитку держави, а запропоновані у роботі ідеї, гіпотези та аргументи відзначаються науковою новизною та практичною значущістю.

II. Характеристика дисертаційної роботи, оцінка її практичної значущості та наукової новизни.

Дисертаційна робота виконана на кафедрі Політології Філософського факультету Харківського національного університету імені В.Н. Каразіна.

Робота містить вступ, три розділи та список використаних джерел. В структурі дисертації маються таблиці та рисунки, які зрозуміло доповнюють та розкривають тематику дослідження. Кожний розділ дисертації супроводжується висновками та висвітлює новизну і наукову цінність виконаних досліджень.

Запропонована структура викладення матеріалу свідчить про детальне опрацювання наукових джерел, публікацій, досліджень тощо. Кожен розділ та

підрозділ роботи є цілісним та закінченим, не повторює зміст та аргументацію, між тим сукупно створює розуміння єдності думки до сприйняття змісту предмета дослідження.

Так, у вступній частині дисертаційної роботи детально та аргументовано висвітлено актуальність обраної теми, визначені мета та завдання дослідження.

Перший розділ надає виклад та пояснення теоретичним та методологічним основам дослідження кібертороризму. В ньому розкривається та зосереджується на аналізі міжнародних та національних підходів до визначення кібертероризму та звертається увага на важливості змін у різних видах нормативно – правових актів, які регулюють спільну політику в державах, на наявності розриву між науковим уявленням та діючими правовими нормами.

Одночасно наводиться висновок, що визначення поняття кібертероризму по цей час залишається предметом політико – правових та фахових дискусій, що ускладнює вироблення шляхів протидії йому, адже відсутність уніфікованого підходу призводить до розриву між науковою теорією і позицією державних політиків. На підтвердження такого висновку в дисертації здійснений глибокий аналіз праць відомих науковців та політиків за обраною темою, їхній досвід, запропоновані формулювання та тлумачення політичних та юридичних категорій, які є дотичними досліджуваному поняттю, проаналізовані схожі та відмінні риси, зокрема й виходячи із направленості атак та відповідних цілей кебертерористичних посягань.

Достатньо новітньою є систематизація та характеристика методів, які застосовуються у кібертероризмі, зокрема злам або перехоплення даних з інформаційних систем держав, намагання отримати несанкціонований доступ до конфіденційної інформації або пошкодити мережеві системи, створення шкідливих програм. З огляду на таке, детально аналізується поняття кібертероризму в історичній площині та виходячи із його розуміння на національній основі в різних країнах Європейського регіону. В цьому розділі також наводиться достатньо поглиблений аналіз регламентів та директив Європейського Союзу, окремих законодавчих актів Німеччини, Франції, Великої Британії, Нідерландів тощо, аналізується їх історичний досвід, напрацювання, спільні та відмінні риси в правовому регулюванні предмету дослідження. Дослідниця надає свій вибір

рекомендацій, який би дозволив, не зважаючи на різноманітність концепцій формулювання національних термінології, все ж таки досягти максимальної її уніфікації та розробити єдину концепцію із кібербезпеки.

Цей розділ також містить детальний опис методологічних основ дослідження проблематики протидії кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону.

Переходячи до аналізу другого розділу, слід зазначити, що він містить декілька підрозділів, об'єднаних завданням та напрямком викладу змісту цього розділу. Так загалом розділ присвячений аналізу механізмів протидії кібертероризму держав Європейського регіону, а також внеску безпосередньо України в європейську систему кібербезпеки. Зокрема аналізуються наявні інструменти боротьби із кіберзагрозами як-то діяльність Агентства з мережевої та інформаційної безпеки ЄС ENISA, яке виконує постійний моніторинг мереж, проводить оцінку ризиків, надає консультаційну підтримку.

На підставі опрацювання та аналізу значної кількості кібератак на критичну інфраструктуру країн Європи, їх особливостей, предмету посягання, використаного інструментарію тощо, наводяться висновки ефективності використання країнами європейського регіону відповідних засобів реагування, зокрема правових. Є вкрай ґрунтовним проведені аналіз та оцінка кібербезпеки за відповідними «індексами кібербезпеки», серед яких названі GCI, що виданий Міжнародною Спілкою електрозв'язку (МСЕ), та NCSI, розроблений Естонським департаментом інформаційних систем (RIA). На підставі наведених індексів проведений аналіз на угрупування декількох країн Європейського регіону та на підставі його висновків розроблені гіпотези їх прийнятності для України, зокрема запропоновано вжити відповідні організаційні заходи, розширити інституційний складник, удосконалити нормативно-правову базу та підвищити рівень координації між державними і приватними організаціями.

Також детально та поглиблено вивчені діяльність та ефективність утворених в Україні органів та інституцій, уповноважених реалізовувати мету уникнення кіберзагроз, якими названі Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), Національний координаційний центр кібербезпеки

при Раді Національної безпеки і оборони, Міністерство цифрової трансформації України, Центр реагування та комп'ютерні надзвичайні події України тощо.

Представленим аналізом доведені основні елементи стратегії посилення їх ефективності та взаємодії через уніфікацію законодавства, розмежування повноважень у вигляді галузевого розподілу, розширення компетенції саме Антитерористичного центру України.

Третій розділ дисертації наводить дослідження проблематики протидії впливу кібертероризму на елементи критичної інфраструктури в України, серед яких зазначені сфера електронної охорони здоров'я та атомна енергетика. Енергетична інфраструктура України розглядається через призму загрози не лише окремої країни, але й всього Європейського регіону загалом, враховуючи транскордонну дію кібертерористичних посягань, а тому пропонується запровадження новітніх адаптивних концепцій захисту, здатних інтегрувати політичні стратегії із сучасними технологіями кібербезпеки. Центральними ідеями відповідної Концепції кіберзахисту ядерно та радіаційно небезпечних об'єктів інфраструктури наводяться механізми дистанційного управління, що може бути активований у випадку фізичного захоплення ядерного об'єкту та який здатний забезпечити уникнення сценаріїв катастрофічного втручання у його роботу, та динамічне шифрування, тобто постійна заміна ключів доступу.

Особливо звертає увагу ідеї застосування ДНК людини, так званий генетичний маркер, для підтвердження її особистості при доступі до систем управління, а також інтегрування технологій, які зчитують емоційні та стресові показники людини в процесі взаємодії із системою, що, на думку дослідниці, може стати непереборним бар'єром для будь-якої спроби несанкціонованого доступу. Наведені ідеї є новаторськими та при їх реалізації гарантують уникнення катастрофічних наслідків при несанкціонованому втручанні у роботі небезпечних ядерних об'єктів.

Також цей розділ присвячений аналізу роботи електронних систем у галузі охорони здоров'я та створення належних умов їхнього захисту. Досліджуючи запроваджені у Європейському регіоні загалом, та в Україні зокрема, об'єкти та системи, які забезпечують відповідні сервіси та роботу медичних закладів, лабораторій, центрів надання екстреної допомоги тощо, успіхи щодо їх цифровізації

та її переваги, одночасно наголошується на проблемах у разі кібертерористичних посягань на них.

Цей підрозділ дисертаційної роботи досліджує проблематику балансу між необхідними та достатніми засобами втручання та інформативності про пацієнтів та одночасно захист від розголошення таких даних. Так запроваджена та діюча система електронної охорони здоров'я (eHealth) стала ключовим напрямком цифрової трансформації медичних послуг. Одночасно, не зважаючи на наявність достатньої кількості ухвалених актів правового регулювання, європейських ініціатив, які спрямовані на структуризацію та реформування системи eHealth, вони не містять прямих положень про забезпечення кібербезпеки. Отже в дисертації розкривається необхідність пояснення сутності поняття «кібербезпеки електронної охорони здоров'я» та його складників, а також формулюється визначення «кібербезпека в eHealth» та з урахуванням зазначеного пропонуються відповідні зміни до законів України «Про кібербезпеку» та «Основ законодавства України про охорону здоров'я».

Також представляє науковій інтерес проведене в цьому розділі дисертаційної роботи глибоке дослідження досвіду європейських країн а галузі забезпечення кібербезпеки eHealth, відповідних інституцій та актів, імплементація їх до вже діючих нормативних актів. Ґрунтовно описується політична складова проблематики забезпечення захисту eHealth в умовах стрімкого розвитку технологій та визнається необхідність розглядати її як елемент національної безпеки, адже без захисту від кібератак всі зусилля дієвості зручної та ефективної системи цифровізації охорони здоров'я будуть зруйновані.

Кібербезпека eHealth розглядається як пріоритетний напрямок політичної стратегії кібербезпеки держави в цілому та пропонується для реалізації її дієвості запровадження в тому числі кримінальної відповідальності для посадових осіб, відповідальних за забезпечення належного рівня кібербезпеки саме в галузі охорони здоров'я.

Цікавим є звернення особливої уваги в дисертаційному дослідженні на необхідності удосконалення заходів та засобів реагування у сфері забезпечення кібербезпеки в галузі охорони здоров'я в умовах триваючого воєнного стану в Україні, а саме запровадження апробованих на досвіді Великої Британії та Естонії

систем виявлення та запобігання вторгненням (IDS/IPS), які дозволяють виявляти аномалії в реальному часі та які наразі відсутні в України на рівні державних медичних платформ. Авторкою пропонується та вважається доцільним розроблення та впровадження державної стратегії кібербезпеки eHealth, яка б передбачала впровадження IDS/IPS та її інтеграцію до діючої. Також пропонується повне шифрування конфіденційних даних в системі eHealth та розроблення для цього державних регламентів.

Також дисертаційна робота містить підсумовуючий розділ, який надає спільні висновки за всіма розділами досліджень. Такий розділ систематизує та узагальнює окремі висновки за розділами, відповідає загальному змісту дисертації.

Останнім розділом представлений список використаних джерел, який містить інформацію про 348 вивчених та опрацьованих статей, праць, досліджень тощо.

III. Оцінка наукової цінності

У дисертації представлений новий та альтернативний підхід до визначення поняття «кібертероризм», виявлені прогалини його сучасного правового регулювання із наведенням детальних та опрацьованих висновків, в тому числі через детальний аналіз його історичних змін та географії формулювання.

Одночасно наводиться наукова необхідність введення у політичний та правовий обіг нових термінів «кіберсоціальна адаптація», «кіберімунітет». Запропонована термінологія доповнює та конкретизує ті явища, правова природа яких є наразі неврегульованою.

З урахуванням самостійного дослідження найбільш вразливих до кібератак систем, є новим та прогресивним запропонований «вектор кіберстійкості в eHealth» та окреслення сутності його елементів, якими називаються зокрема створення посади «кіберомбудсмена», децентралізація архітектури самої eHealth через розділення серверів та вузлів, повне шифрування даних, перепрограмування функціоналів та програмного забезпечення, використання міжмережевих екранів, створення резервних систем та ін.

Також презентовано доволі цікаві науково ідеї створення підземної розгалуженої системи керування ядерними станціями із кількома пунктами управління через створення галузевого центру CERT-UA (робоча назва CERT-NE –

група реагування на кіберзлочини України з ядерної енергетики) та можливість так званого «заморожування» можливості використання апаратної техніки станції кіберзлочинцями, а також створення новітньої структури на основі кооперації МАГАТЕ та ENISA, як потужної міжнародної платформи за для можливості синхронізації та координації їх дій для розв'язання проблем комплексної безпеки ядерних об'єктів.

З урахуванням розширення та ускладнення кіберзагроз, їх збільшення якісно та сутнісно, вдається цінним та науково доведеним концепт запровадження на міжнародному рівні на базі Міжнародного кримінального суду ООН та/або Міжнародного суду ООН формування самостійного Міжнародного суду у справах злочинів у кіберпросторі у вигляді «кібертрибуналу».

На національному рівні ініційовано перетворення Антитерористичного Центру, який наразі зосереджений лише на боротьбі із фізичними аспектами тероризму, через інтеграцію до його функцій повноважень із кібербезпеки, та об'єднання цих двох аспектів в його діяльності, що є стратегічно та політично привабливим, адже забезпечить як концентрацію, так і ефективність функціонування, універсальність заходів та підбор спеціалістів.

IV. Обґрунтованість висновків і рекомендацій, сформульованих в дисертації

Дисертація Олександри ЗІНЧЕНКО є послідовною, системною та змістовною роботою. Подання та викладення опрацьованого матеріалу є чітким та відповідає задачам дослідження. Дослідженням змісту роботи доводиться вивчення значного пласту наукових робіт, технічних та юридичних документів, яким надані самостійні оцінки та тлумачення.

Також взяті до уваги твердження відомих політиків та науковців й запропоноване осучаснення до умов сьогодення їх методологічне ставлення до проаналізованої проблематики.

Дисертація виконана із дотриманням всіх складових щодо застосування відомих та сталих методів та методологій, які перелічені та достатньо повно розкритий механізм та порядок їх застосування.

За змістом, дослідження є цілісним фундаментальним розглядом проблематики кібертероризму в більшості в політичному контексті, водночас торкається й правової складової, як цілком необхідної для повного розуміння відповідного явища та надання йому фахового аналізу.

В дисертації представлені запропоновані авторські поняття, концептуальні ідеї й новаторські цінності, серед яких особливо слід виділити саме дефініції «кібертероризм» та «кібербезпека». Такі оновлені визначення усувають науково з'ясовані прогалини та суттєво доповнені автором необхідним змістом. Вивчений та поданий матеріал є достовірним, містить посилання на його джерела, а достовірність результатів і висновків доводиться публікаціями та апробацією.

Дисертація структурована, має логічне та послідовне викладення матеріалу, а аналізом її тексту доводяться наукові результати, обґрунтованість та достовірність. Розкриття обраної теми досягнуто завдяки в тому числі вивченню та аналізу значного обсягу наукових робіт, статей, монографій, джерел публічної інформації.

Вбачається, що впровадження наукових ідей дисертації, наприклад «Національної програми кіберосвіти в Україні» надасть практичну можливість окреслити окремі напрямки підготовки спеціалістів, в тому числі в критично важливих сферах життя та за для максимальної продуктивності в цифровому робочому середовищі.

Науковий аналіз результатів не викликає сумнівів у їхній достовірності та науковій обґрунтованості.

V. Оформлення дисертації та академічна доброчесність

Дисертаційна роботі Олександри ЗІНЧЕНКО відповідає всім необхідним вимогам щодо її оформлення, структури і змісту, так як це передбачено в «Порядку присудження ступеня доктора філософії та скасування разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 №44) та наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації».

Робота виконана державною мовою, має необхідні та виокремлені в самостійні структури відповідні розділи та підрозділи.

В тексті дисертації міститься повний та деталізований перелік використаних джерел, який включає наукові та власні публікації, із зазначенням авторів таких публікацій та місця публікації.

Використані джерела інформації є тісно пов'язаними із темою дисертації.

Ознайомившись із протоколом перевірки дисертаційної роботи на наявність запозичень в Інтернет ресурсах, можливо констатувати, що робота виконана самостійно, є унікальною, цитати, думки, ідеї інших авторів мають відповідні посилання, які оприлюднені у списку використаних джерел.

VI. Завершеність дисертаційної роботи

Дисертація Олександри ЗІНЧЕНКО є завершеною, самостійною та цілісною науковою працею, у якій простежується глибоке розуміння авторкою обраної проблематики та комплексне бачення шляхів її вирішення. Структура роботи є чіткою та послідовною, всі розділи логічно взаємопов'язані, кожен з них доповнює попередній та формує єдиний науковий концепт дослідження. Така структура забезпечує цілісне сприйняття матеріалу, дає змогу простежити хід наукової думки здобувачки від постановки проблеми до формування практичних висновків та пропозицій.

Використана у дисертації термінологія є коректною, послідовною та відповідає сучасному стану наукових досліджень у галузі права, політології та кібербезпеки. Це свідчить про високий рівень теоретичної підготовки авторки, її вміння працювати з категоріальним апаратом та сформулювати власне бачення складних міждисциплінарних понять. Висновки роботи мають як глибоке теоретичне обґрунтування, так і практичне спрямування, що надзвичайно важливо для сучасної науки, орієнтованої на вирішення прикладних проблем державної політики та правозастосовної практики.

Текст дисертації викладено грамотної діловою українською мовою із дотриманням норм наукового стилю та юридичної техніки викладу. Це забезпечує ясність, логічність і доступність поданих матеріалів як для науковців, так і для практиків у сфері права, публічного управління та кібербезпеки.

Про завершеність, ґрунтовність та високу наукову цінність роботи свідчить наявність у тексті фундаментальних авторських концепцій, обґрунтованих нових

дефініцій, а також пропозицій, що мають практичну спрямованість. Авторкою окреслено конкретні шляхи імплементації сформульованих наукових положень у законодавчу, правозастосовну та управлінську практику. Важливо, що дослідження поєднує у собі не лише теоретичний аналіз актуальної проблематики, а й пропонує реальні механізми впровадження сформульованих висновків та рекомендацій, що є особливо цінним у сучасних умовах посилення кіберзагроз та потреби у їх правовому та політичному врегулюванні.

Таким чином, дисертаційна робота є вагомим внеском у розвиток науки та практики у сфері протидії кібертероризму, а її результати можуть бути використані як у подальших наукових дослідженнях, так і у практичній діяльності органів державної влади, сектору безпеки та оборони, а також у навчальному процесі закладів вищої освіти.

VII. Апробації та публікації

Основні результати та положення дисертаційної роботи Олександри ЗІНЧЕНКО викладені у 20 наукових публікаціях, серед яких 3 статті у наукових фахових виданнях України, що відповідають вимогам МОН України до публікацій за темою дисертаційної роботи, а також стаття у науково-періодичному виданні, яке індексується у міжнародних наукометричних базах даних Scopus та/або Web of Science Core Collection, що підтверджує високий рівень наукових результатів, їх апробацію у вітчизняному та міжнародному науковому середовищі, доводить достовірність отриманих висновків та свідчить про практичну значущість дослідження у контексті розвитку сучасної науки та вирішення актуальних проблем протидії кібертероризму.

VIII. Загальні висновки. Зауваження та пропозиції.

Дисертація Олександри ЗІНЧЕНКО є завершеною науково-дослідницькою роботою, має наукову новизну та практичну значимість.

Зміст повністю відображає основні наукові положення дисертації, яка оформлена відповідно до вимог та положень чинного законодавства.

Попри безперечну актуальність теми дисертаційного дослідження та високий рівень опрацьованості низки теоретичних і практичних аспектів проблеми, деякі положення роботи викликають застереження або потребують уточнення.

1. У дисертації подано авторські визначення понять «кібертероризм», «політичний кіберкарантин», «кібербезпека», «кіберімунітет», «кіберсоціальна адаптація», «кіберомбудсмен», «ядерна кібербезпека», «кібербезпека eHealth» тощо. Водночас більшість із них мають надмірно розширений зміст, що ускладнює їх нормативне застосування або емпіричну верифікацію. Деякі терміни (зокрема «кіберсоціальна адаптація», «кіберомбудсмен») не мають усталеного вживання у сучасному політологічному дискурсі. Доцільним є їх закріплення у системі вже існуючої національної політичної та правової термінології. Це дозволить уникнути можливих колізій при їх подальшому правозастосуванні та сприятиме впровадженню запропонованих категорій у нормативно-правову базу.

2. Окремі ідеї, запропоновані авторкою, зокрема: створення міжнародного кібертрибуналу, укладення «Конвенції про взаємні кіберзобов'язання», запровадження «кіберкарантину» тощо є надзвичайно амбітними та інноваційними. Водночас, на нашу думку, у висновках доцільно додати елементи обережності або застереження щодо складності їх імплементації на практиці, а також окреслити потенційні механізми "дипломатичного" забезпечення таких ініціатив.

3. У другому розділі роботи було б доцільно додати короткий аналіз практики Європейського суду з прав людини у справах, що стосуються втручання у кіберпростір, особливо у контексті балансу між захистом національної безпеки та дотриманням прав і свобод людини. Такий огляд посилив би правовий аспект дослідження та його міждисциплінарність.

4. У дисертації запропоновано створення посади кіберомбудсмена, що є безумовно новаторською ідеєю, однак потребує додаткового обґрунтування щодо співвідношення його функцій та повноважень з існуючими інститутами омбудсмена в Україні, зокрема Уповноваженим Верховної Ради України з прав людини, для запобігання дублюванню повноважень та визначення оптимальної моделі правового регулювання.

Дисертаційне дослідження має значну теоретичну та практичну цінність, а окремі концептуальні положення — інноваційний характер. Водночас, зауваження, висловлені вище, мають на меті вдосконалити наукову цілісність, точність формулювань і методологічну завершеність роботи. З огляду на викладене, зазначені зауваження **не знижують** загального позитивного враження від наукової праці та не впливають на висновок про її відповідність вимогам до дисертацій на здобуття ступеня доктора філософії.

На підставі проведеного аналізу вважаю, що дисертаційна робота Зінченко Олександри Ігорівни «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» має високий рівень актуальності, відзначається достатньою повнотою викладення результатів дослідження у наукових публікаціях здобувачки, належним обсягом, якісним оформленням, чітким термінологічним апаратом та коректним стилістичним викладенням матеріалу. Робота відповідає вимогам, визначеним «Порядком присудження ступеня доктора філософії та скасування разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 №44), а також наказом Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», і її авторка заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 052 «Політологія», галузь знань 05 «Соціальні та поведінкові науки».

Офіційний опонент:
доктор юридичних наук, доцент,
доцент кафедри цивільного права і процесу Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» — Валерія ФІЛІНОВИЧ

Підпис В. Філінович засвідчую
Проректор з наукових досліджень та трансферу технологій
Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», д.т.н., професор — Сергій ГНАТЮК

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 15:24:26 15.08.2025

Назва файлу з підписом: Відгук_ФІЛІНОВИЧ - на Зінченко - KAI (2).docx.asice
Розмір файлу з підписом: 29.2 КБ

Перевірені файли:
Назва файлу без підпису: Відгук_ФІЛІНОВИЧ - на Зінченко - KAI (2).docx
Розмір файлу без підпису: 24.6 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Філінович Валерія Вікторівна
П.І.Б.: Філінович Валерія Вікторівна
Країна: Україна
РНОКПП: 3227518003
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 15:24:22 15.08.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF9704000000A2391A008D05FA03
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.08.04 13:00

Голові разової спеціалізованої вченої ради
Харківського національного університету імені В.Н. Каразіна
професору Валентині ШАМРАЄВІЙ
майдан Свободи 4б м. Харків, 61022

В І Д Г У К

Офіційного опонента – доктора політичних наук, старшого наукового співробітника, завідувача відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень Національного інституту стратегічних досліджень
Дубова Дмитра Володимировича
на дисертаційну роботу Зінченко Олександри Ігорівни на тему
«Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону»
на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія», галузь знань 05 «Соціальні та поведінкові науки».

I. Обґрунтування актуальності обраної теми дисертаційного дослідження.

З огляду на специфіку сьогодення є цілком очевидним зростання загрози терористичних атак із застосуванням технологічних та інформаційних інструментів, технічного прогресу, комп'ютерних мереж та інтернету. Ті надбання еволюційного розвитку людства, яким воно мало намір користуватися за для розвитку та вдосконалення, часто зловмисно використовуються як потужний елемент здійснення політичного впливу та різноманітних гібридних війн, складовою яких виступає сучасний тероризм який майже не віддільний від інформаційних технологій. В сучасних умовах, коли всі сфери життя, мають суттєвий політичний зміст, суто технічними або технологічними засобів стримування як самих кібератак, так й їх наслідків вже недостатньо – це потребує консолідованих зусиль політичного та юридичного змісту та грунтовних дискусій щодо того, які ці інструменти можуть бути застосовані для досягнення бажаного результату.

Особливо актуальним такі дослідження є для сучасної України, яка стикнулась з екзестенційними викликами які ставлять під загрозу саму державність і загрожують життю кожного українця. Цифровізація майже всіх сфер життя потребує сучасних засобів захисту та дієвих запобіжників від протиправних посягань. Представлене дослідження надає детальний опис як відповідним загрозам, так і способам реагування на них, що є високо цінним, адже автор не лише окреслює проблематику, а й рекомендує дієві та різноманітні шляхи подолання відповідних проблем.

Фактично динаміка розвитку ситуації породила наявність очевидного протиріччя: складність цифровізаційних процесів тісно пов'язаних із зростанням кіберзагроз (аж до форм кібертероризму) стикається з відсутністю належного наукового опрацювання цієї проблеми та вироблення відповідних дієвих та науково обгрунтованих рекомендацій. З огляду на зазначене зазначаю, що тема дисертаційної роботи, яка присвячена проблематиці кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону, є нагальною та актуальною і спрямована на вирішення вище вказаного протиріччя.

II. Загальна характеристика дисертаційної роботи.

Дисертаційна робота виконана на кафедрі Політології Харківського національного університету імені В.Н. Каразіна. Загальний обсяг основного тексту роботи складає 203 сторінки, містить вступ, три розділи та список використаних джерел. Письмове дослідження супроводжується структурованими таблицями та рисунками, що полегшує сприйняття поданого автором матеріалу. Кожен розділ дослідження містить висновки автора із зазначенням практичних результатів їхнього застосування, висвітлює новизну та наукову цінність.

У вступі дисертаційної роботи висвітлено актуальність обраної теми, визначені мета та завдання дослідження, також міститься обґрунтування наукової новизни та значення його одержаних результатів.

Розділ 1 дисертації присвячений теоретичним та методологічним основам дослідження кібертероризму та складається із трьох підрозділів

Підрозділ 1.1. присвячено огляду історичних підходів до визначення самого поняття «кібертероризм», окреслення його складових та характеристик, зроблено спробу запропонувати уточнене визначення вказаного терміну.

Підрозділ 1.2. розкриває проблематику ширшого тлумачення «кібербезпеки» як необхідної та безумовної складової у протидії явищу кібертероризму. Глибина опрацювання та географія проаналізованих робіт є суттєвою та свідчить про фундаментальний підхід до їх попереднього вивчення для досягнення цілей роботи. Дисертант приділив особливу увагу аналізу чинних актів міжнародного законодавства, конвенційних та директивних документів.

Підрозділ 1.3. присвячений методологічним основам дослідження проблематики протидії кібертероризму як загрозі національній безпеці. В ньому докладно описуються застосовані автором методи аналізу, зокрема: бібліографічний, історичний, термінологічний, метод нормативно-правового аналізу, ціннісно-нормативний, аксіологічний, аналізу та синтезу, системного аналізу та порівняльний.

Розділ 2 присвячений вивченню механізмів протидії кібертероризму державами Європейського регіону та безпосередньо внеску України до загальної системи безпеки.

Перший (2.1) підрозділ присвячений європейським регіональним засобам протидії кібертероризму та розкриває в тому числі в історичній площині створення та започаткування нормативного регулювання основ боротьби із кіберзлочинністю. Авторка пропонує застосування різноманітних політичних інструментів боротьби та стримування кіберзагроз, створення відповідних універсальних юрисдикцій притягнення до відповідальності та покарання, уніфікацію законодавства, яке б забезпечило ефективність та дієвість вже існуючих юрисдикційних механізмів. Дисертантка також пропонує до розгляду низку авторських концепцій (як то «політичний механізм кіберпосередництва», «політичного кіберкарантину» тощо) які хоч і є подекуди контроверсійними,

однак стимулюють наукову дискусію та можливість до ширшого стратегічного планування.

Підрозділ 2.2. надає детальний аналіз нормативно-правових та інституційних інструментів протидії кібертероризму в державах Європейського регіону. На підставі проведеного аналізу дисертанткою надаються пропозиції до низки національних кібербезпекових документів. Авторкою пропонує розглядати питання кібербезпеки України в межах запропонованої нею «формули забезпечення кібербезпеки», що включає: інтеграцію, адаптацію до загроз, інновації та прогресивну кіберосвіту суспільства. Слушною є пропозиція дисертантки щодо розроблення та впровадження «Національної програми кіберосвіти», яка має включати розроблення єдиного освітнього стандарту з кібербезпеки для всіх спеціальностей; створення доступних навчальних курсів та матеріалів на різноманітних платформах, перепідготовка та сертифікація державних службовців, працівників критичної інфраструктури та приватного сектору; масове інформування населення через засоби масової інформації та просвітницькі заходи. При цьому авторка не лише наголошує та аргументує необхідність такої програми, а достатньо докладно описує та пропонує її структурні складові.

Розділ 3 дисертації присвячений проблематиці протидії впливу кібертероризму на критичну інфраструктуру України (з акцентом на енергетичну інфраструктуру та електронну систему охорони здоров'я) та оцінку викликів воєнного стану на неї.

Так, підрозділ 1 розділу 3 характеризує організацію кібербезпеки енергетичної інфраструктури в України, її теперішній стан та перспективи вдосконалення. Авторка пропонує запровадити спільні стандарти для протидії кібртероризму та інших форм гібридної агресії, спрямованої на ядерні об'єкти.

Підрозділ 2 розділу 3 характеризує кібербезпеку в галузі електронної охорони здоров'я України та авторкою пропонується розглянути можливість глобального політичного партнерства у сфері цифрового здоров'я (GDHP) з метою обміну знаннями, досвідом та найкращими практиками для покращення

здоров’я населення через ефективне використання цифрових технологій. Одночасно звертається увага, на то факт, що цифровізація у сфері охорони здоров’я не може існувати без одночасного забезпечення належного рівня кібербезпеки та наводяться приклади кібератак, їх наслідки та способи ефективного упередження та подолання на досвіді як України так і інших європейських держав. З огляду на те, що сектор охорони здоров’я посідає перше місце в списку хакерських цілей у всьому світі, в дослідженні наголошується, що є нагально необхідним в України розробити законодавчу базу та внести зміни до діючих актів законодавства, які б вичерпно розглядали та регулювали аспекти кібербезпеки в системі електронної охорони здоров’я.

Передостанній розділ дисертаційної роботи деталізує результати дослідження та надає послідовні та змістовні висновки, які сутнісно відображають та відповідають змісту дисертації.

Останнім розділом представлений список використаних джерел, який містить інформацію про 348 вивчених та опрацьованих статті, праці, дослідження тощо.

III. Наукова новизна та наукова цінність

У дисертації представлені та запропоновані ряд концептуально нових підходів до таких дефініцій як «кібертероризм» та «кібербезпека», а також запровадження нових – «кіберсоціальна адаптація», «кіберімунітет», «ядерна кібербезпека». Запропоновані нові формати політичної взаємодії як-то «кіберімунітет для критичної інфраструктури», «політичний кіберкарантин».

Запропоновано концепт «ядерної кібербезпеки» та необхідність його закріплення в міжнародній системі правового регулювання міжнародних відносин, що може представляти особливу цінність з огляду на важливість та масштабність наслідків подібних загроз, які не є суто національними.

Заслуговує на увагу запропонована ідея створення галузевого центру – Група реагування на кіберзлочини з ядерної енергетики (CERT-NE), оптимізація CERT-UA шляхом розподілу компетенцій через функціональні підгрупи: CERT-

HC – забезпечення кібербезпеки в галузі охорони здоров'я, CERT-NE – забезпечення кібербезпеки в енергетиці, CERT - LR – забезпечення кібербезпеки щодо здійснення правопорядку правосуддя, тримання під вартою, а також цивільного захисту населення, CERT-ECI – забезпечення кібербезбеки електронних комунікацій та інформаційних послуг.

IV. Обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертації

Дисертація О.І Зінченко структурована, логічно та послідовно викладена, не містить термінологічних та текстуальних помилок, тема розкрита широко та зрозуміло, а отримані результати в сукупності надають наукові рекомендації щодо вдосконалення політичної, юридичної, організаційної складових із забезпечення кібербезпеки в Україні, створення ефективних засобів та інституцій із боротьби з кібертероризмом, досягнення цілей зокрема в галузях ядерної кібербезпеки та охорони здоров'я. Достовірність наукових результатів і висновків доводиться та підтверджується науковими публікаціями та апробацією.

V. Апробація результатів дослідження

Основні положення, висновки та рекомендації дисертаційної роботи Зінченко Олександри Ігорівни були оприлюднені під час участі здобувачки у низці науково-практичних конференцій, семінарів, круглих столів, зокрема з проблем національної безпеки, кібербезпеки та міжнародної політики, що дало можливість обговорити результати дослідження з фахівцями відповідної галузі, отримати слушні зауваження та пропозиції щодо їхньої практичної імплементації.

Крім того, результати дисертації знайшли своє відображення у публікаціях здобувачки у наукових фахових виданнях України та зарубіжних виданнях, що засвідчує їхню наукову новизну, достовірність, теоретичну та практичну цінність. Апробація результатів у такому обсязі свідчить про ґрунтовну

перевірку отриманих даних, належний рівень їхної валідації науковою спільнотою та готовність до впровадження у практику державного управління у сфері кібербезпеки та протидії кібертероризму.

VI. Зауваження та пропозиції опонента

Незважаючи на вище зазначене робота не позбавлена низки недоліків:

1. Запропоноване дисертанткою визначення кібертероризму дійсно більш точно описує технологічну складову сучасного тероризму і додає вкрай важливі уточнення щодо мотивів атакуючих, які і трансформують класичні/некласичні злочини у акти терору. Однак запропоноване поняття залишає за межами охоплення низку дій терористів, які можуть бути здійснені ними із застосуванням сучасних технологій та інструментів кіберпростору, як то: вербування прихильників, відмивання коштів чи навіть акцій, які прямо не торкаються об'єктів критичної інфраструктури. У разі запровадження терміну у такій трактовці це може створити складнощі для правоохоронних та контррозвідувальних органів щодо практичних заходів протидії кібертероризму. Крім того, запропоноване визначення «кібертероризму», вочевидь, потребує додаткового опрацювання в т.ч. для забезпечення його відповідності всім наведеним в роботі кейсам які позначені як акти кібертерору.

2. В окремих елементах роботи дисертантка вказує на те, що «масштаби кібератаки та її вплив на суспільство» можуть атрибутувати ту чи іншу кібератаку як акти кібертероризму. Однак запропоноване авторкою визначення не містить відсилок до розуміння масштабів події як фактору атрибуції. Робота б стала більш цілісною якби авторка змогла запропонувати перелік критеріїв та порогових значень (хоча б для рівня політичної атрибуції) які б дозволили відділити різні типи кіберзлочинів від кібертерористичних актів.

3. Хоча Розділ 1 надзвичайно насичений та динамічний, однак з точки зору його сутності (а саме визначення теоретико-методологічних основ дослідження та виявлення не вирішених проблем) він містить значну кількість висновків та рекомендацій які мали б знайти своє відображення в наступних розділах роботи

– це б спростило розуміння тієї методичної бази на яку безпосередньо спирається авторка.

4. Робота лише б виграла якщо дисертантка додатково показала б в своєму дослідженні розуміння кіберзагроз (передусім - кібертероризму) в розрізі класичних та, можливо, нео/пост класичних політичних теорій як додаткового елементу політологічного аналізу.

5. Хоча дисертантка провела дійсно глибокий та всебічний аналіз європейського законодавства, однак окремі його аспекти залишились або слабковисвітленими (наприклад, положення NIS2 Директиви та її впровадження в європейських країнах) або не охопленими (наприклад, Регламент (ЄС) 2021/784 Європейського парламенту та Ради від 29 квітня 2021 року щодо боротьби з поширенням терористичного контенту онлайн). Їх аналіз дозволив би роботі стати більш цілісною з точки огляду сучасних європейських кібербезпекових процесів.

6. Розділ 2 містить широкий огляд практик низки європейських країн щодо побудови власних систем кібербезпеки. Робота б лише виграла, якби такий аналіз був проведений у відповідності до єдиного набору критеріїв/індикаторів, можливо – у формі таблиці. Це б спростило процес аналізу отриманих даних та зробило б можливою об’єктивну оцінку прогресу цих країн на шляху розбудови власної системи кібербезпеки.

7. Для роботи характерні окремі стилістичні та орфографічні помилки, однак які не впливають на загальну якість тексту.

Незважаючи на зазначене можу підкреслити, що висловлені зауваження не зменшують загальної цінності та інноваційності дослідження.

VII. Оформлення дисертації та академічна доброчесність

Дисертаційна робота О.І. Зінченко відповідає всім необхідним вимогам щодо її оформлення, структури і змісту, так як це передбачено в «Порядку присудження ступеня доктора філософії та скасування разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня

доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 №44) та наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації».

Робота виконана державною мовою, має структуровані розділи та підрозділи, є науковою працею на правах рукопису.

Дослідженням змісту дисертаційної роботи встановлено, що вона має необхідні посилання на джерела вивчених та використаних наукових робіт, їхніх авторів та співавторів, дані про їх публікації тощо. В списку використаних джерел міститься повна, достовірна та достатня інформація про такі дані та матеріали, а по тексту роботи є посилання на відповідні наукові праці, які тісно пов'язані із темою дисертаційного дослідження.

Власні дослідження та висновки відповідають аспектам самостійності та індивідуальності, структуровані, послідовні та компетентно висловлені. Аргументація та висновки відповідають наведеному у дослідженні обґрунтуванню.

VIII. Відповідність змісту дисертації ознакам завершеності

Дисертація Зінченко О.І. є завершеною науковою працею, яка має чітку структуру, логічну та термінологічну послідовність, запропонований аналіз та висновки наповнені теоретичними і практичними знаннями, новітніми ідеями та пропозиціями.

IX. Загальні висновки

Дисертація Зінченко Олександри Ігорівни є завершеною науково-дослідницькою роботою, має наукову новизну та практичну значимість.

Зміст повністю відображає основні наукові положення дисертації, яка оформлена відповідно до вимог та положень чинного законодавства.

Дисертаційна робота Зінченко Олександри Ігорівни «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» за актуальністю, змістом та повнотою викладу її результатів у

публікаціях здобувача, обсягом, якістю оформлення, термінологічним та стилістичним викладенням матеріалу відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 №44) та наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», та Зінченко Олександра Ігорівна заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 052 «Політологія», галузь знань 05 «Соціальні та поведінкові науки».

Офіційний опонент,
доктор політичних наук, старший науковий співробітник
завідувач відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень
Національного інституту стратегічних досліджень — Д.В. Дубов

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 09:30:34 18.08.2025

Назва файлу з підписом: vidguk_DDubov_diser_Zinchenko.docx.asice
Розмір файлу з підписом: 47.1 КБ

Перевірені файли:
Назва файлу без підпису: vidguk_DDubov_diser_Zinchenko.docx
Розмір файлу без підпису: 44.1 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ДУБОВ ДМИТРО ВОЛОДИМИРОВИЧ
П.І.Б.: ДУБОВ ДМИТРО ВОЛОДИМИРОВИЧ
Країна: Україна
РНОКПП: 3012416595
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 09:30:34 18.08.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000002EA7C700EA166906
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.08.04 13:00