ЗАТВЕРДЖУЮ

Ректор Національного університету цивільного захисту України, генерал-лейтенант служби цивільного захисту, д.держ.упр., професор

_____ Володимир Садковий

"___" _____ 2022 р.

ВИСНОВОК

Національного університету цивільного захисту України про дисертацію на здобуття наукового ступеня доктора наук з державного управління Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі», за спеціальністю 25.00.02 – механізми державного управління

ВИТЯГ

з протоколу № 11 розширеного засідання
навчально-науково-виробничого центру
від 03 червня 2022 р.

Присутні:

Ректор НУЦЗУ генерал-лейтенант служби цивільного захисту, д. держ. упр., професор В.П. Садковий, перший проректор НУЦЗУ полковник служби цивільного захисту д. держ. упр., доц. В.В. Коврегін, проректор з наукової роботи полковник служби цивільного захисту д.т.н., проф. В.А. Андронов.

Навчально-науково-виробничий центр: д.держ.упр., проф. С.М. Домбровська.

Кафедра публічного адміністрування у сфері цивільного захисту: д.держ.упр., проф. С.В. Майстро, д.держ.упр., проф. І.О. Крюков, к.е.н., доцент Ю.Г. Батир, к.держ.упр. І.М. Лопатченко.

Кафедра менеджменту: д.держ.упр. Н.А. Леоненко; д.держ.упр., доц. О.В. Поступна.

Науковий відділ з проблем управління у сфері цивільного захисту: д.держ.упр., проф. В.Ю. Стрельцов, к.держ.упр. С.А. Мороз.

Науковий відділ з проблем управління державною безпекою: д.держ.упр., с.д. А.Л. Помаза-Пономаренко.

Кафедра управління та організації діяльності у сфері цивільного захисту: к.держ.упр. Н.М. Карпеко.

Члени спеціалізованої вченої ради Д 64.707.03 Національного університету цивільного захисту України: д.держ.упр., проф. Е. В. Щепанський, д.держ.упр., проф. В.В. Сиченко, д.держ.упр., проф. Ю.Д. Древаль, д.держ.упр. доц. М.А. Ажажа, д.держ.упр., проф. А.В. Ромін.

Присутні на засіданні – 19 осіб, зокрема 14 докторів наук і 3 кандидатів наук за профілем поданої на розгляд дисертації.

Слухали: доповідь Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління.

Тема затверджена Вченою радою Національного університету цивільного захисту України (далі – НУЦЗУ), протокол № 4 від 17 грудня 2020 р.

Науковий консультант – завідувач кафедри публічного адміністрування у сфері цивільного захисту навчально-науково-виробничого центру Національного університету цивільного захисту України, д.держ.упр., проф. Майстро С.В.

Доповідь здобувача:

Шановний Голово! Шановні присутні!

Вашій увазі пропонуються результати дисертаційного дослідження на тему: **«**Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі**».**

Зовнішня і внутрішня ефективність публічного сектора може значно підвищитися за рахунок використання нових інформаційно-комунікаційних технологій, проте сучасні тенденції в цій сфері можуть також призвести до появи нових викликів та нових проблем. Очевидно, що частота і масштаби кібератак будуть збільшуватися, в тому числі й на публічний сектор. Шкідливе програмне забезпечення, інсайдерські робочі місця, бот-мережі, DDoS-атаки, кібершпіонаж і кібертероризм ставатимуть все більш витонченими і, як і раніше, наноситимуть фінансову, репутаційну та інші види шкоди, а також створювати загрозу національній безпеці. Тому у даний час кібербезпека – це глобальна проблема, яка потребує глобальної відповіді, але це також локальна проблема, що вимагає локального реагування. Відтак, кожна сучасна публічна організація зобов’язана проявляти ініціативу і реалізовувати політики, що підвищують рівень кібербезпеки. Від цього залежить не тільки її власна безпека, але і безпека всього публічного сектора, держави і суспільства в цілому.

Тому метою дослідження було визначено теоретико-методологічне обґрунтування забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Об’єкт дослідження – формування та реалізація державної політики у сфері кібербезпеки, а предмет дослідження – забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Кібербезпека охоплює широкий набір практик: оцінка ризиків і

тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; забезпечення системної реактивності на кібератаки. Впровадження систем кібербезпеки має важливі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Виходячи з цього, кібербезпеку слід розглядати як суспільне благо. Було зазначено, що три важливі переваги випливають із управління кібербезпекою як суспільним благам: системний підхід до безпеки, спільна відповідальність між різними стейкхолдерами, розвиток співпраці у сфері кібербезпеки.

Поняття кібербезпеки у цілому та в публічному секторі зокрема безпосередньо пов’язане з феноменом інформаційного суспільства та електронного врядування, що з’явилось внаслідок розвитку інформаційного суспільства. Електронне врядування ґрунтується на трьох «стовпах»: довірі, прозорості та підзвітності, які є нерозривно взаємопов’язаними. З іншого боку, на сучасний світ у цілому та публічне управління зокрема впливають процеси глобалізації. Виходячи з цього, а також враховуючи особливості публічного сектора, для нього було визначено п’ять основних викликів щодо забезпечення кібербезпеки: публічному сектору властива велика ступінь оперативної незалежності та «ізольованості» між різними його частинами, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб’єктами поза органами публічної влади, тому визначення безпеки публічного сектора має бути розширеним та переосмисленим; поведінка людини, раціональна або нераціональна, є стрижнем кібербезпеки, тому необхідними є заходи для формування безпечної поведінки у кібепросторі; існує зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою, тому необхідним є забезпечення тут певної рівноваги; користувачі електронного уряду потребують такого ж кіберзахисту від органів публічної влади, як органи публічної влади потребують захисту від третьої сторони, тому важливим є налагодження партнерства щодо забезпечення кібербезпеки.

Концептуальні засади забезпечення кібербезпеки в органах публічної влади складають, з одного боку, виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний), з іншого боку – дії, необхідні для забезпечення кібербезпеки. Людський вимір є найбільш фундаментальним і, у той же час, найбільш слабким елементом кібербезпеки, оскільки хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх, а недостатня поінформованість і недостатні знання роблять людей найбільш вразливою ланкою в порівнянні з іншими. Організаційний

вимір зосереджений на інститутах всередині кіберпростору, це функціональна структура, яка контролює кіберпростір, і зміцнення цього виміру може відбуватись за двома напрямами: стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури; стратегічні дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору. Інфраструктурний вимір є середовищем, яке створює кіберпростір, без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому.

За останній час загрози кібербезпеці в публічному секторі постійно зростають і стають більш складними, і певним чином це пов'язано із впроадженням соціальних мереж і Gov 2.0 у діяльність публічних організацій, які намагаються стати більш відкритими і прозорими. Однак, незважаючи на загрози органи влади на всіх рівнях, і особливо місцеві органи влади, повинні продовжувати впроваджувати і сприяти розробці нових технологій і рішень Gov 2.0, щоб залишатися надійними постачальниками публічних послуг та інформації. Тим не менше, органи влади повинні робити це обережно, стратегічно, маючи відповідну політику, розробляючи необхідні керівні принципи, використовуючи відповідні технологічні інструменти та навчання персоналу для захисту від загроз кібербезпеки. Наявність відповідної політики та керівних принципів у сфері кібербезпеки також є позитивним сигналом для громадян, нагадуючи про основоположну природу Gov 2.0 як про рух до відкритої, прозорої та безпечної арени діяльності публічних організацій. Громадяни в світі Web 2.0 очікують інтеграції таких технологій в свої взаємодії з публічними структурами, але як і раніше існують основні проблеми конфіденційності та обміну інформацією.

З урахуванням нових кіберризиків та більш складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Проте незважаючи на те, що ці стратегії та політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Проте доведено, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпка і на рівні організацій. Виходячи з цього було запропоновано модель інституційної кібербезпеки, яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації), та відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість.

Запропонована модель інституційної кібербезпеки забезпечує загальний підхід, за допомогою якого кожна організація може адаптувати дану модель до

власних потреб безпеки для розвитку своїх можливостей із забезпечення кібербезпеки. Для досягнення цієї мети було визначено основні принципи інституційної кібербезпеки, що випливають із запропонованої моделі, і до яких належать такі: підхід до кібербезпеки повинен бути холістичним; слід застосувати гнучкий стиль управління; слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками; на додаток до координації діяльності публічних, приватних, академічних та неурядових організацій, міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки; у забезпеченні кібербезпеки мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова; важливим є встановлення балансу між кібербезпекою та застосовністю ІТ-продуктів і технологій.

Поступова, але послідовна мілітаризація та централізація управління посилюється в країнах, які є головними об'єктами кібератак, таких як США чи країни ЄС. Тому в цих країнах підходи до забезпечення кібербезпеки найбільше нагадують підходи неореалізму, з точки зору якого, фокус зосереджений на державах, а влада та безпека розглядаються як функції відносної вигоди від конкуруючих суперників. Однак, неореалізм не розпізнає загрози та можливості для більшої цілісності систем, які представляють недержавні актори та технології. Зробити це можна з позицій соціального конструктивізму, який вміє аналізувати спільне сприйняття як всередині, так і поза суспільством, і вміє розпізнавати як функцію ідентичності в динаміці національної безпеки, так і те, як ці сприйняття впливають на безпеку. Проте неореалістичний та соціально-конструктивістський підходи обидва розроблені як інтерпретації традиційної міжнародної безпеки, і по суті, жоден з них не включає інформаційні технології у свій дискурс. Уникнути цього недоліку дозволяє кібервестфаліанство, яке базується на розвитку можливих або ймовірних майбутніх технологій, і стверджує, що державна централізація Інтернету в багатьох країнах, спільно з розвитком цих майбутніх технологій, призведе до появи національних «кібермеж». Однак ця теорія не приділяє уваги ролі, яку відіграють чи можуть відігравати окремі громадяни та їх поведінці у кіберпросторі. Кібервестфаліанство також дещо обмежене за своїм обсягом (кіберпростір) та підходом до рішень (технологія). Воно також не враховує економічну, політичну та військову динаміку між великими, середніми та регіональними державами. Усунути ці проблеми може певним чином теорія інтерсекційності, якщо її застосувати до кіберзбезпеки. Враховуючи зазначене було визначено, що теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, який містить елементи інтерсекційності, неореалізму, соціального конструктивізму та кібервестфаліанства.

Як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні – кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб'єктів, які зазнають впливу певної форми влади. З'ясовано при цьому, що в основі концепції влади є два «виміри». Перший

вимір – це види соціальних відносин, за допомогою яких впливає (та реалізується) спроможність суб'єктів, а другий вимір – специфіка цих соціальних відносин. Зазначені два виміру разом створюють чотири типи влади: примусова, інституційна, структурна, продуктивна. Стосовно кібербезпеки примусова влада надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

На даний час поширюється створення середовищ, де публічний і приватний сектор активно та успішно співпрацюють – іноді як клієнт і постачальник, іноді через нагляд і дотримання, іноді як партнери. Ці домовленості зазвичай переслідують спільні цілі отримання певних позитивних результатів, але в деяких випадках партнерські відносини формуються як захисна відповідь спільним противникам. Саме така мета партнерства є головною у сфері забезпечення кібербезпеки. Публічно-приватне партнерство як захисна модель покладається на те, що кожен учасник вносить щось унікальне в партнерство, що може пом'якшити його слабкі сторони та посилити його сильні сторони. Для партнерств, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов'язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор, у свою чергу, створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки. Виходячи з цього, і враховуючи наявні проблеми у даній сфері було обґрунтовано основні принципи публічно-приватного партнерства у сфері забезпечення кібербезпеки, а саме: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства.

Доповідь закінчено. Дякую за увагу!

Запитання:

1. Домбровська С.М. д.держ.упр., проф.: У Вашій роботі йдеться про сучасні особливості формування та реалізації державної політики у сфері кібербезпеки. Чим зумовлені ці особливості?

Відповідь здобувача: Дякую за запитання. Дані особливості зумовлені тими викликами, з якими державна політика у цілому стикається в умовах сучасного інформаційного суспільства. Можна визначити три таких основних виклики: перше – формування і реалізація державної політики відбувається в

умовах високої невизначеності; друге – збільшується кількість акторів державної політики і не всі вони є публічними; третє –збільшується важливість урахування соціально-культурних особливостей під час формування і реалізації державної політики.

2. Ромін А.В. д.держ.упр., проф.: З Вашої доповіді та реферату можна зрозуміти, що у своїй дисертації Ви приділили увагу дослідженню зарубіжного досвіду стосовно забезпечення кібербепеки у публічному секторі. Які основні висновки Ви зробили з аналізу цього досвіду?

Відповідь здобувача: Дякую за запитання. Аналіз зарубіжного досвіду показує, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх розглянутих держав, але дана сфера у різних державах відрізняється за трьома показниками: перший – яким чином держави визначають свій референтний об'єкт, тобто що саме потрібно захищати; другий – яким чином держави сприймають основні загрози та ризики; третій – які підходи використовуються для визначення джерел загроз та ризиків.

3. Поступна О.В. д.держ.упр., доц.: Яким чином Ви визначаєте поняття «цифрове врядування»?

Відповідь здобувача: Дякую за запитання. Цифрове врядування – це використання в публічному управлінні повною мірою можливостей, що надають існуючі ІКТ, для заохочення участі громадян у публічному управлінні та формуванні й проведенні політики, підвищення прозорості, підзвітності та довіри до органів влади. Його слід відокремлювати від електронного врядування.

4. Леоненко Н.А. д.держ.упр.: У своїй дисертації Ви крім інформаційного суспільства згадуєте також мережеве суспільство. Поясніть, будь ласка, як Ви розумієте це поняття і навіщо його розглядаєте.

Відповідь здобувача: Дякую за запитання. Дане поняття ми розглядаємо так само, як його розуміє відомий науковець Мануель Кастельс. Він у своїй праці «Становлення мережевого суспільства» визначає, що мережі складають нову соціальну морфологію суспільств, а дифузія мережевої логіки істотно змінює роботу і результати в процесах виробництва, влади і культури. Таким чином, ми розглядаємо мережеве суспільство як суспільство, що ґрунтується на горизонтальних соціальних зв'язках і головну роль у якому відіграють не ієрархічні моделі, а соціальні мережі. Подібне розуміння дало можливість запропонувати заходи із забезпечення кібербезпеки в публічному секторі з урахуванням впливу різних акторів на дану сферу.

5. Лопатченко І.М. к.держ.упр.: У своєму виступі Ви посилались на результати соціологічного дослідження. Уточніть, будь ласка, основні характеристики цього дослідження.

Відповідь здобувача: Дякую за запитання. З метою з'ясування інформації щодо стану кібербезпеки в Україні в сучасних умовах та пошуку шляхів

підвищення рівня захисту кіберпростору в Україні у період з 24 жовтня по 3 листопада 2020 р. автором за сприяння кафедри політології та філософії Харківського регіонального інституту державного управління було проведено всеукраїнське експертне соціологічне опитування. До складу експертної групи увійшли: керівники державних та комунальних підприємств; представники великого і середнього бізнесу, банківських структур; керівники громадських організацій, депутати різних рівнів, працівники органів виконавчої влади та місцевого самоврядування, політичні аналітики; журналісти; експерти з питань кібербезпеки. Загальна кількість респондентів склала 1007 осіб.

6. Ажажа М.А. д.держ.упр., доц.: Для чого може бути використано моніторинг соціальних медіа в діяльності органів публічної влади?

Відповідь здобувача: Дякую за запитання. Моніторинг соціальних медіа може бути використаний органами влади для виявлення тенденцій в суспільстві, наприклад, думки громадян й цільових груп з конкретних питань політики, для спростування неправдивої, доповнення неповної та виправлення такої інформації в соціальних медіа, що була некоректно сприйнята громадянами. Моніторинг може бути також задіяно в репутаційному менеджменті та стратегічній комунікації як засіб пом'якшення опору громадян деяким рішенням органів влади шляхом здійснення впливу на їх точку зору.

В обговоренні дисертації взяли участь:

Крюков О.І. д.держ.упр., проф. (рецензент).

Насамперед хотів би відзначити актуальність обраної теми дослідження, але, у той же час, і її складність. Вважаю, що дисертанту вдалось цілком досягти визначених мети і завдань дослідження, в результаті чого було отримано дуже цікаву з наукової точки зору роботу, результати якої мають і наукову, і практичну цінність.

Разом з тим, слід виділити окремі моменти, які потребують певного корегування та доопрацювання, а саме:

– у другому пункті «уперше» наукової новизни формулювання «розроблено модель», що передбачає вирішення прикладної задачі, доречно змінити на «обґрунтовано модель», що передбачає вирішення теоретичної задачі;

– формулювання «розроблено методологію» в науковій новизні треба замінити на «розроблено методологічний підхід», що є вужчим поняттям та відповідає результатам дослідження;

– необхідно привести у відповідність задачі, пункти наукової новизни та загальні висновки.

Проте в цілому, вважаю, що робота виконана на високому рівні, результати дисертаційного дослідження є оригінальними і містять наукову новизну і безперечно є цінними для державного управління.

Враховуючи це, вважаю, що дисертація Котуха Євгена Володимировичв на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в

публічному секторі» може бути рекомендована до попереднього розгляду спеціалізованою вченою радою та захисту за спеціальністю 25.00.02 – «механізми державного управління».

Леоненко Н.А. д.держ.упр. (рецензент).

Шановні колеги! Безумовно, обрана Котухом Євгеном Володимировичем тема дисертаційного дослідження є актуальною і своєчасною. Структура роботи є логічно послідовною, вона викладена науковим стилем і демонструє високу обізнаність дисертанта з проблематики дослідження. Мета і завдання дослідження досягнуті, що дозволило отримати низку оригінальних результатів, які характеризуються науковою новизною і мають практичну значущість.

Разом з тим дисертаційна робота містить окремі дискусійні положення на які дисертанту слід звернути особливу увагу:

– на нашу думку, доцільно скоригувати об’єкт та предмет дослідження відповідно до спеціальності 25.00.02 – механізми державного управління;

– не визначено, які саме результати дослідження і яким чином можуть бути використані в практичній діяльності органів публічної влади центрального, регіонального та місцевого рівнів;

– на початку загальних висновків необхідно визначити, яку наукову проблему вирішено за результатами проведених досліджень.

Однак, виходячи з високого теоретико-методологічного рівня дисертаційного дослідження, наукової та практичної цінності отриманих результатів, важливості роботи для державного управління, вважаю за необхідне рекомендувати дисертаційну роботу до подання у спеціалізовану вчену раду для її подальшого розгляду та захисту.

Стрельцов В.Ю. д.держ.упр., проф. (рецензент)

Шановні колеги! Цілком поділяю думку, що дисертаційна робота Котуха Євгена Володимировича на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» є актуальною, містить нові обґрунтовані результати, які мають теоретичну і практичну значущість для науки державного управління. Останнє підтверджується впровадженням результатів дисертаційного дослідження в практичну діяльність органів влади. Дисертаційна робота є логічно побудованою, містить авторські пропозиції щодо підвищення рівня кібербезпеки в публічному секторі в Україні.

Втім, хотів би звернути увагу на декілька моментів, які потребують уточнення та доопрацювання:

– в тексті дисертаційної роботи надається декілька непов’язаних між собою визначень поняття «кібербезпека», необхідно об’єднати їх в одне розширене поняття;

– треба визначити відмінності запропонованого методологічного підходу до забезпечення кібербезпеки у середовищі Gov 2.0 від вже існуючих;

– потрібно більш чітко прописати, чим забезпечення кібербезпеки в

публічному секторі в сучасних умовах відрізняється від того, як це було раніше.

Однак це не зніжає загальну наукову та практичну цінність отриманих результатів, тому вважаю, що дисертаційне дослідження Котуха Євгена Володимировича за темою «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» має бути рекомендованим спеціалізованій вченій раді для попереднього розгляду та захисту.

Щепанський Е.В. д.держ.упр., проф.

Шановні колеги! Тема дисертаційного дослідження, присвяченого забезпеченню кібербезпеки в публічному секторі в Україні, є дуже актуальною та має важливе значення як для вдосконалення діяльності окремих органів публічної влади, так і державного управління в цілому.

Результати дисертаційного дослідження дали можливість автору обґрунтувати механізми, що спрямовані на підвищення рівня кібербезпеки в сучасних умовах та адаптовані до особливостей українських органів, враховують специфіку їхньої діяльності, що є дуже важливим з практичної точки зору. Як дуже позитивний момент слід відзначити й те, що дисертант не обмежується в своїй роботі суто теоретичними міркуваннями, а підкріплює їх аналізом результатів проведеного соціологічного дослідження.

Тому вважаю, що дисертаційна робота Котуха Євгена Володимировича може бути рекомендованою до подання до спеціалізованої вченої ради для попереднього розгляду та захисту.

Котух Євген Володимирович – здобувач.

Шановний Голово, шановні учасники засідання. Дозвольте виказати слова глибокої та щирої вдячності за згоду розглянути мою дисертаційну роботу. Дякую шановним рецензентам і всім, хто ознайомився з моєю дисертацією та рефератом, взяв участь в обговоренні. Ми обов’язково врахуємо всі зауваження пропозиції та побажання при підготовці та поданні дисертації до спеціалізованої вченої ради.

У результаті експертизи дисертації Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» та повноти публікації основних результатів дослідження

У Х В А Л И Л И:

Дисертація на здобуття наукового ступеня доктора наук з державного управління – кваліфікаційна наукова праця оформлена відповідно до державного стандарту.

Актуальність теми. Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що

займаються питаннями національної безпеки. Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади. Це зумовлює необхідність проведення досліджень щодо розробки механізмів і моделей, визначення принципів забезпечення кібербезпеки у публічному секторі. Вибір теми дисертаційного дослідження Котуха Є.В. також актуалізують процеси впровадження технологій електронного урядування у діяльність органів публічної влади і пов'язані з цим нові виклики та загрози.

Формулювання наукового завдання, нове вирішення якого отримано в дисертації. У дисертації Котуха Є.В. отримано нові науково обґрунтовані результати та запропоновано вирішення актуальної наукової проблеми, що полягає в розробці теоретико-методологічних засад забезпечення кібербезпки в публічному секторі в сучасних умовах. Отримані у процесі дисертаційного дослідження результати підтверджують загальну методологію, покладену в його основу, а реалізована мета і завдання дослідження дали можливість сформулювати у дисертації завершені висновки.

Наукові положення, розроблені особисто здобувачем, та їх новизна. Наукові твердження, що виносяться на захист, розроблені особисто без співавторів здобувачем та викладені в опублікованих наукових працях. Наукова новизна одержаних результатів визначається таким:

уперше:

– обґрунтовано концептуальні засади забезпечення кібербезпеки в органах публічної влади, які поділяються на дві групи: виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний) та дії, необхідні для забезпечення кібербезпеки (побудова онлайн-довіри; розвиток координації, співпраця та кооперація; профілювання кіберстану; сприяння впровадженню систем кібербезпеки; перегляд; створення правового середовища; встановлення стандартів);

– обґрунтовано модель інституційної кібербезпеки, відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість;

– обґрунтовано теоретико-методологічну модель розробки національної стратегії кібербезпеки, яка використовує підходи неореалізму, соціального конструктивізму, інтерсекційності, кібервестфалізму та враховує, що актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці,

атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують інформаційно-комунікаційні технології для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо;

удосконалено:

– методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0, визначено, що вона має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL;

– перелік основних принципів інституційної кібербезпеки до яких віднесено такі: запровадження холістичного підходу до кібербезпеки; використання гнучкого стилю управління у сфері кібербезпеки; впровадження методів постійного вдосконалення діяльності, орієнтованих на управління ризиками; віднесення до базису забезпечення кібербезпеки координації діяльності публічних, приватних, академічних та неурядових організацій разом з міжнародною співпрацею та обміном інформацією; заохочення прозорості, підзвітності, етичних цінностей, свободи слова у кіберпросторі; встановлення балансу між безпекою та застосовністю IT-продуктів і технологій;

– обґрунтування основних принципів публічно-приватного партнерства у сфері забезпечення кібербезпеки, до яких віднесено такі: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства;

дістали подальшого розвитку:

– концептуальні положення щодо трактування кібербезпеки як суспільного блага; було визначено, що кібербезпека, маючи три основні складові (інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; забезпечення системної реактивності на кібератаки), забезпечує задоволення публічних інтересів інформаційного суспільства щодо можливості належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології;

– визначення основних викликів для публічного сектора у контексті забезпечення кібербезпеки, до яких віднесено такі: 1) велика ступінь оперативної незалежності та «ізольованості» між різними частинами

публічного сектора, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; 2) важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб'єктами поза органами публічної влади; 3) працівники організацій публічного сектора далеко не завжди демонструють безпечну поведінку у кібепросторі, хоча саме поведінка людини є стрижнем кібербезпеки; 4) зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою; 5) відсутність або неефективність публічно-приватного партнерства щодо забезпечення кібербезпеки;

– узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі, зокрема, з'ясовано, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх досліджених держав, але дана сфера у різних державах відрізняється за тим, як держави, по-перше, визначають референтний об'єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики; відповідно до цих відмінностей держави можна поділити на дві категорії: держави, що мілітаризують питання кібербезпеки, та держави, що криміналізують питання кібербезпеки;

– методологічний підхід до використання різних типів владних відносин у забезпеченні кібербезпеки; визначено, що примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кіберпростором;

– визначення особливостей запобігання та протидії кіберзагрозам у публічному секторі України, зокрема, встановлено, що головними проблемами при цьому є: відсутність чіткого розподілу повноважень між органами виконавчої влади та органами місцевого самоврядування (зокрема, дослідження довело таку ситуацію у сферах боротьби з безробіттям, бідністю, вирішення екологічних проблем, розвитку малого та середнього бізнесу, промисловості тощо); існування та функціонування неадаптивних організаційних структур у системі публічного управління; використання застарілих методів і принципів управління в органах публічної влади (зокрема, відсутність деліберативних практик у діяльності).

Обґрунтованість і достовірність наукових положень, висновків, рекомендацій, які захищаються. Обґрунтованість і достовірність отриманих результатів підтверджуються їх позитивною оцінкою в процесі апробації на конференціях, публікацією результатів дослідження в наукових працях, збірниках матеріалів науково-практичних конференцій. Сформульовані наукові положення, висновки та рекомендації є логічним продовженням сучасних напрацювань вітчизняних та закордонних вчених, присвячених дослідженню

державного управління та місцевого самоврядування, містять нові оригінальні ідеї, що в сукупності вирішують визначені в роботі наукові завдання. В цілому наукові результати, отримані в дисертації, є достовірними, науково обґрунтованими та доказовими.

Публікація основних положень і результатів дослідження.

Монографія:

1. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. – Харків : Колегіум, 2021. – 272 с.

Статті Scopus, Web of Scince:

2. Kotukh Ye.V. Public value management and new public governance as modern approaches to the development of public administration / Oleksandr O. Bryhinets, Ivo Svoboda, Oksana R. Shevchuk, Yevgen V. Kotukh, Valentyna Yu. Radich // Revista San Gregorio (Web of Science Core Collection). – Núm. 42 (2020). Pp. 205-213. http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1568/20-OLAKSANDR/ Особистий внесок здобувача: визначення особливостей концепції «Public value», що має значення для розвитку концепції електронного врядування.

3. Kotukh Ye.V. Spread of virtual communities as a potential threat to state security and sustainable well-being / Viacheslav B. Dziundziuk, Oleksandr A. Kotukov, Dmytro V. Hryn, Eugene V. Kotukh // Rivista Di Studi Sulla Sostenibilita (Scopus). – 2020. – Issue 2. – Pp. 7-18. Особистий внесок здобувача: визначено основні напрями негативного впливу розвитку віртуальних співтовариств як акторів кіберпростору на національну безпеку.

4. Kotukh Y.V. State Information Security Policy (Comparative Legal Aspect) / Y. V. Kotukh, V. B. Dziundziuk, O. M. Krutii, V. P. Solovykh, O. A. Kotukov // Cuestiones Políticas. – 2021. – 39(71). – Pp. 166-186. Особистий внесок здобувача: визначено принципи, на яких має ґрунтуватись державна політика кібербезпеки.

5. Kotukh, Y. V. Cybercrime and subculture of cybercriminals / Y. V. Kotukh, D. V. Kislov, T. S. Yarovoi, R. O. Kotsiuba, O. H. Bondarenko // Linguistics and Culture Review. –2021 – 5(S4). – Pp. 858-869. Особистий внесок здобувача: визначено особливості хакерської субкультури у контексті загрози кібербезпеці.

Статті у наукових фахових виданнях з державного управління:

6. Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки / Є.В. Котух // Теорія та практика державного управління. – 2019. – № 4(67). – С. 40-47.

7. Котух Є.В. Проблеми кібербезпеки в сучасному світі // Актуальні проблеми державного управління. – 2019. – №2(56). – С. 33-38.

8. Котух Є.В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації / Є.В. Котух // Державне будівництво. – 2019. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/view/65/60.

9. Котух Є.В. Формування систем кібербезпеки в органах публічної влади / Є.В. Котух // Державне управління: удосконалення та розвиток. – 2020. – № 3, березень. – Режим доступу: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf.

10. Котух Є.В. Електронне урядування як нова парадигма публічного управління / Є.В. Котух // Інвестиції: практика та досвід. – 2020. – № 3, лютий. – С. 122-127.

11. Котух Є.В. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації // Вісник НУЦЗ України. Серія: Державне управління. – 2020. – № 2. – С. 564-572.

12. Котух Є.В. Основні виклики врядування у сфері кібербезпеки / Є. Котух, В. Ободяк // Теорія та практика державного управління. – 2020. – № 4 (71). – С. 38-46. Особистий внесок здобувача: визначено характеристики врядування у сфері кібербезпеки та ресурси кіберпростору.

13. Котух Є.В. Кібербезпека як один з пріоритетів національної політики / В.Б. Дзюндзюк, Є.В. Котух // Державне будівництво. – 2020. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/download/90/85. Особистий внесок здобувача: визначено пріоритетні напрями реалізації стратегій кібербезпеки.

14. Котух Є.В. Сучасний стан та проблеми «цифровізації» в Україні / Є.В. Котух, А.С. Довбиш // Актуальні проблеми державного управління. – 2020. – № 2. – С. 25-31. Особистий внесок здобувача: визначено основні проблеми процесу цифровізації в Україні.

15. Котух Є.В. Реалізація національних стратегій кібербезпеки: силовий аспект // Наукові перспективи. – 2021. – № 2(8). – С. 125-136.

16. Котух Є. В. Основні підходи до забезпечення кібербезпеки: досвід країн вишеградської четвірки // Інвестиції: практика та досвід. – 2021. – № 3. – С. 68-74.

17. Котух Є.В. Проблема кібершахрайства та фактори стримування її вирішення органами публічного управління / Є.В. Котух. // Вісник НУЦЗ України. Серія: Державне управління. – 2021. – Випуск 1 (14). – С. 185-191.

18. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз / Є.В. Котух // Актуальні проблеми державного управління. – 2021. – № 1. – С. 48-57.

19. Котух Є.В. Оцінка рівня захисту кіберпростору в публічному управлінні: національний та організаційний виміри / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 1. – С. 31-39.

20. Котух Є.В. Реалізація стратегій кібербезпеки: економіко-політичний аспект / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 2. – С. 171-175.

21. Котух Є.В. та ін. Аудит інформаційної безпеки як необхідна складова управління в державних установах / Є.В. Котух, О.М. Кучма, Д.М. Нехороших, Г.В. Пліс, Г.З. Халімов // Державне будівництво. – 2021. – № 1. – Режим доступу: https://db.kh.ua/index.php/db/article/view/117/110. Особистий внесок здобувача: визначення особливнстей аудиту інформаційної безпеки.

22. Котух Є.В. Типи владних відносин у стратегії кібербезпеки / Є.В. Котух // Інвестиції: практика та досвід. – 2021. – № 11. – С. 98-102.

23. Котух Є.В. Теоретико-методологічна модель розробки національної стратегії кібербезпеки / Є.В. Котух // Наукові перспективи. – 2021. – № 6 (12). – С. 39-52.

24. Котух Є.В. Розвиток публічно-приватного партнерства у сфері кібербезпеки // Інвестиції: практика та досвід. – 2021. – № 13. – С. 76-84.

Інші публікації апробаційного характеру:

25. Котух Є.В. Ризики зростання відкритості публічного сектору та засоби боротьби з ними / Котух Є.В. // Збірник тез XX Міжнародного наукового конгресу «Публічне управління XXI століття: портал можливостей» (м. Харків, 23 квітня 2020 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2020. – С. 103-106.

26. Котух Є.В. Кіберзагрози у сучасному світі / В.Б. Дзюндзюк, Є.В. Котух // International Scientific Integration ‘2020 (Seattle, Washington, USA, November 10, 2020). – Pp. 103-106.

27. Котух Є.В. Проблеми урядування у сфері кібербезпеки / В.Б. Дзюндзюк, Є.В. Котух // Abstracts of scientific papers of IV International Scientific Conference «Science and Global Studies» (Prague, November 30, 2020). – Pp. 25-28.

28. Kotukh Ye. Encryption scheme based on the automorphism group of the Ree function field / Gennady Khalimov, Yevgeniy Kotukh, Svitlana Khalimova // 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France. December 14-16, 2020). – Pp. 1-8.

29. Котух Є.В. Щодо питання реалізації національних стратегій кібербезпеки / Котух Є.В. // Збірник тез XXI Міжнародного наукового конгресу «Публічне управління XXI століття: погляд у майбутнє» (м. Харків, 21 квітня 2021 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2021. – С. 161–165.

30. Котух Є.В. Національні стратегії кібербезпеки: економіко-політичний аспект / Є.В. Котух // Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 09.04.2021). – Pp. 49-50.

31. Котух Є. Боротьба з кіберзлочинністю в країнах ЄС / Є. Котух // Матеріали 18-ї регіональної науково-практичної конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 13 травня 2021 р.). – Дніпро : ДРІДУ НАДУ. – С. 114-117.

Наукове значення роботи визначається тим, що у дослідженні автором розроблені й опрацьовані нові підходи щодо підвищення рівня кібербезпеки, реалізація яких дозволить значно підвищити ефективність роботи органів публічної влади за рахунок впровадження новітніх інформаційно-комунікаційних технологій. Одержані у дисертації наукові результати мають значення для розвитку науки державного управління, сприятимуть якісно новому розумінню теорії, методології й практики взаємодії органів влади з громадянами в Україні.

Практичне значення роботи полягає в доведенні низки теоретичних

положень і висновків до конкретних рекомендацій, спрямованих на забезпечення кібербезпеки в органах публічної влади. Основні положення й висновки дисертаційної роботи можуть використовуватися фахівцями, освітянами, науковцями під час написання монографій, підручників, навчальних посібників, створення навчально-методичної літератури з практичними рекомендаціями щодо вирішення проблемних питань забезпечення кібербезпеки у публічному секторі.

Використання результатів роботи. Висновки і рекомендації, викладені в роботі, мають практичне значення і можуть використовуватись органами публічної влади різного рівня для забезпечення власної кібербезпеки. Розроблені автором рекомендації щодо підвищення кібербезпеки впроваджено в діяльність Міністерства фінансів України (довідка від 20 серпня 2021 р. № 20040-03-73/26056), Міністерства молоді та спорту України (довідка від 13 липня 2021 р. № 6090/1), Державної аудиторської служби України (довідка від 13 липня 2021 р. № 001400-16/8764-2021).

Повнота викладу матеріалів дисертації в публікаціях та особистий внесок у них автора. Дисертаційна робота є самостійною науковою працею, теоретичні та прикладні результати якої отримані особисто здобувачем. У дисертації не використовувалися ідеї співвиконавців науково-дослідних робіт, а також результати наукових досліджень співавторів у наукових публікаціях, які опубліковано здобувачем.

Оцінка мови та стилю дисертації. Текст дисертаційного дослідження та реферату відзначається змістовною завершеністю, є доступним для сприйняття, а їх мовностилістичний рівень та оформлення відповідають встановленим до відповідного типу робіт вимогам. Реферат дисертації відображає основні положення роботи.

Відповідність дисертації паспорту спеціальності, за якою вона подається до захисту. Дисертація Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі», яка представлена на здобуття наукового ступеня доктора наук з державного управління, за змістом відповідає паспорту спеціальності 25.00.02 – механізми державного управління.

Характеристика особистості здобувача. Котух Євген Володимирович характеризується як науковець, який здатний самостійно ставити та вирішувати складні наукові завдання, займатися науковими розробками широкого кола споріднених проблем. Під час дисертаційного дослідження він продемонстрував ґрунтовну наукову підготовку, володіння сучасною науковою методологією, що дало можливість реалізувати поставлені мету і завдання дослідження. Для дисертанта притаманні такі особистісні риси, як

наполегливість, працелюбність, схильність до творчого й системного мислення, пошуку нестандартних рішень.

Робота над дисертацією продемонструвала високу наукову культуру та ерудованість дисертанта, здатність коректно, логічно і послідовно викладати матеріал дослідження. Використана методологія дослідження дозволила дисертанту ґрунтовно дослідити та розробити теоретичні засади і надати практичні рекомендації щодо удосконалення забезпечення кібербезпеки у публічному секторі в Україні в сучасних умовах. У цілому, зміст дисертаційного дослідження і наукових публікацій свідчать про те, що Котух Євген Володимирович вільно орієнтується у складних проблемах теорії і практики галузі науки державного управління.

ПОСТАНОВА МІЖКАФЕДРАЛЬНОГО ТЕОРЕТИЧНОГО СЕМІНАРУ:

1. За актуальністю, ступенем новизни, обґрунтованості, наукової та практичної цінності здобутих результатів дисертація Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» відповідає вимогам МОН України та Порядку присудження та позбавлення наукового ступеня доктора наук, що затверджений Постановою КМУ від 17.11.2021 р., №1197.
2. Рекомендувати дисертацію Котуха Є.В. на тему: «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» за спеціальністю 25.00.02 – механізми державного управління спеціалізованій вченій раді для попереднього розгляду і захисту.

Результати голосування присутніх на засіданні докторів наук і кандидатів наук: за – 19, проти – немає, утрималися – немає.

Головуючий на розширеному засіданні, д. держ. упр., проф. Світлана Домбровська

Вчений секретар розширеного засідання, к. держ. упр. Світлана Мороз