Голові спеціалізованої вченої ради
Д 26.891.02
Інституту підготовки кадрів державної
служби зайнятості України
Войтович Р.В.

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

кандидата наук з державного управління Хлапоніна Дмитра Юрійовича на дисертацію Станіславського Тараса Володимировича на тему **«Механізми публічного управління забезпеченням кібербезпеки в сучасних умовах»**, представлену до захисту у спеціалізовану вчену раду Д 26.891.02 Інституту підготовки кадрів державної служби зайнятості України на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління

Актуальність теми дисертації, зв'язок з науковими програмами, темами

Однією з необхідних умов успішного формування та реалізацій державної політики у сфері кібербезпеки та кіберзахисту є її ефективне політичне, організаційно-правове, інформаційно-аналітичне, техніко-технологічне, науково-методологічне, методичне та інші види забезпечення, що є однією з причин необхідності розробки нових та удосконалення існуючих механізмів публічного управління в цій сфері в умовах динамічного зростання кількості, складності та непередбаченості кіберзагроз та кіберінцендентів, де традиційні методи, підходи, способи їх нейтралізації та зменшення негативних наслідків є неефективними.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота проводилася в межах науково-дослідних робіт Інституту підготовки кадрів державної служби зайнятості України за темою кафедри публічного управління та адміністрування – «Модернізація та підвищення ефективності публічного управління у сфері зайнятості в Україні в контексті євроінтеграції» (ДР № ДЄ №01118 U 003561), в яких

автором проведено комплексне дослідження розвитку механізмів публічного управління у сфері кібербезпеки.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їх вірогідність

Наукові дослідження, висновки й рекомендації, сформульовані в дисертації, мають достатньо високий рівень теоретико-методологічного та емпіричного обґрунтування, про що свідчить використання широкої джерельної бази за темою дисертації і достатнього масиву аналітичних даних.

Вірогідність наукових положень, висновків, рекомендацій, сформульованих у дисертації Станіславського Т.В., забезпечуються активною апробацією отриманих результатів на науково-практичних конференціях, у тому числі й міжнародній, достатньою географією публікацій, їх глибинністю. Покладена в основу дисертаційної роботи наукова задача отримала достатнє методологічне опрацювання.

Фахове вирішення автором низки наукових завдань в рамках поставленої мети дослідження, адекватність структурно-логічної схеми дослідження визначеній меті, відповідність результатів, викладених у висновках, поставленим завданням та їх новизна дозволила реалізувати авторський підхід до вирішення важливої наукової задачі.

Об'єкт і предмет дослідження відповідають заявленій темі.

Поставлені дисертантом завдання виконані і розкривають мету дослідження. Висновки відповідають поставленим завданням, відповідно відтворюються у авторефераті дисертації.

Таким чином, зміст автореферату й дисертації Станіславського Т.В. свідчать ро їх повну обґрунтованість і вірогідність.

Достовірність та наукова новизна одержаних результатів, повнота їх викладу в опублікованих працях

Достовірність одержаних Станіславським Т.В. науково-практичних результатів обумовлюється глибоким аналізом як вітчизняного, так і закордонного теоретичного надбання, значного обсягу аналітичної інформації,

нормативно-правової бази, апробацією його результатів під час проведення науково-комунікативних заходів.

Наукова новизна одержаних результатів полягає в теоретичному обґрунтуванні та наданні практичних рекомендацій щодо вдосконалення механізмів публічного управління забезпеченням кібербезпеки в сучасних умовах в Україні, а саме:

уперше:

доведено на основі результатів порівняльного аналізу часткова схожість національних стратегій кібербезпеки провідних країн світу та України у цілях та структурі національних систем управління у сфері кібербезпеки, а також відсутність дієвих механізмів реалізації Стратегії кібербезпеки України, обґрунтовано необхідність включення до цих механізмів переліку та планів забезпечення стійкості об'єктів критичної інформаційної інфраструктури, впровадження системного та інтегрованого підходу до управління ризиками у сфері кібербезпеки, що сприятиме підвищенню рівня її результативності;

запропоновано авторське визначення термінів, а саме: «кібербезпека – безпека інформації при використанні кіберпростору», який відповідатиме міжнародним термінологічним системам у цій сфері, а також нові терміни: «огляд стану кіберзахисту – процедура періодичного спостереження, вимірювання, аналізу та оцінювання стану і готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем, в яких обробляються та зберігаються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом»; «спостереження стану кіберзахисту – активне, систематичне, цілеспрямоване, планомірне вивчення реального стану кіберзахищеності, за якого оцінюється спроможності у запобіганні кіберінцидентам, виявленні, попередженні та припиненні/ліквідації наслідків кібератак, здатності об'єктів критичної інформаційної інфраструктури до відновлення роботи після кібератак та кіберінцидентів», застосування яких сприятиме підвищенню рівня семантичної інтероперабельності у сфері кібербезпеки;

удосконалено:

з урахуванням результатів узагальнення тенденцій розвитку національних систем кібербезпеки провідних країн світу та їх об'єднань визначено перелік та зміст науково обґрунтованих пропозицій щодо підвищення спроможності України адекватно протистояти загрозам у сфері кібербезпеки та розвитку національної системи кібербезпеки, а саме: налагодження ефективного виконання завдань та впровадження дієвих механізмів взаємодії суб'єктів забезпечення кібербезпеки при кіберінцидентах і кібератаках, розроблення та реалізація заходів щодо підвищення зрілості національної системи кібербезпеки, організація взаємодії при кіберінцидентах та кібератаках між уповноваженими органами України та інших країн (їх об'єднань), продовження підвищення загального рівня кібербезпекових навичок та знань громадян, підприємств та публічних адміністрацій, проведення та впровадження результатів фундаментальних та прикладних досліджень у сфері кібербезпеки з урахуванням впровадження нових технологій (інтернету речей, нейронних мереж та штучного інтелекту, квантових обчислень тощо), розроблення нових надійних криптографічних механізмів для публічного застосування, об'єднання з уповноваженими національними органами інших країн у боротьбі з кіберзлочинністю та впровадження ефективних механізмів оцінки відповідності вимогам з кібербезпеки продукції ІКТ широкого вжитку, посилення спроможностей у кібероборони;

правовий механізм забезпечення кібербезпеки, спрямований на підвищення ефективності заходів з кіберзахисту, організації належного обміну інформації про кіберінциденти та кібератаки, в тому числі, в інформаційно-телекомунікаційних системах, де обробляється інформація з обмеженим доступом, шляхом внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України», а саме, на відміну від існуючого, запропоновано: удосконалення термінології; впровадження норм щодо ідентифікації подій як кіберінциденти, обов'язкових до виконання правил та звітування про результати їх оброблення; поширення сфери дії цього Закону на діяльність, пов'язану з обробленням інформації, що становить державну таємницю, засобами інформаційно-комунікаційних технологій, шляхом введення окремої процедури оцінки

виконання заходів з кібероборони при здійсненні акредитації з безпеки; розширення переліку принципів, на яких ґрунтується забезпечення кібербезпеки шляхом уведення додаткового принципу з проведення на постійній основі періодичного аналізу результативності заходів із забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів силами персоналу цих об'єктів та із залученням уповноважених організацій у цій сфері; запровадження принципів проведення огляду національної системи кібербезпеки та критичної інформаційної інфраструктури; запропоновано авторську ієрархічну модель структури законодавства у сфері кібербезпеки, яка включає стратегічний, оперативний та тактичний рівень, запровадження якої буде сприяти систематизації законодавства у цій сфері;

організаційно-технічний механізм підвищення якості робіт із створення та оцінювання відповідності засобів, процесів і систем, які задіяні для надання життєво необхідних послуг, шляхом розвитку інфраструктури стандартизації у сфері кібербезпеки в Україні, сертифікації за міжнародними стандартами оцінки відповідності, а також визнання сертифікатів кібербезпеки, виданих в країнах Європейського Союзу органами з оцінки відповідності під егідою Європейської агенції з кібербезпеки ENISA, або сертифікатів відповідності, виданих в інших країнах, які є суб'єктами міжнародного договору про визнання сертифікації за стандартами оцінки безпеки ІКТ за «Common Criteria» (ДСТУ ISO/IEC 15 408 «Інформаційні технології. Методи захисту. Критерії оцінки»);

мотиваційний механізм, як один із пріоритетних напрямків кроків розбудови державно-приватної взаємодії у сфері кібербезпеки шляхом унесення змін до ліцензійних умов щодо надання послуги у галузі технічного захисту інформації з оцінювання захищеності інформації, що не становить державної таємниці, в яких ціль, сутність та зміст відповідного виду господарської діяльності, на відміну від існуючого механізму (атестація комплексів технічного захисту інформації та експертні оцінювання у сфері технічного захисту інформації) мають відповідати завданням забезпечення кібербезпеки об'єкта, який оцінюється, а персонал ліцензіата, який проваджуватиме такий вид діяльності, має постійно відповідати сучасним вимогам;

набули подальшого розвитку:

наукове обґрунтування удосконалення механізмів оцінки відповідності в сфері захисту інформації за результатами аналізу базових правових та організаційних механізмів ЄС та НАТО щодо процедур сертифікації в сфері кібербезпеки;

обґрунтування необхідності перегляду підходів до формування змісту наступної редакції Стратегії кібербезпеки України в напрямку зосередження на конкретизації стратегічних цілей, завдань, вимірюваності результатів, обґрунтування етапів та строків їх виконання.

Практичне значення і впровадження одержаних результатів дослідження

Наукові висновки і теоретичні положення дисертаційної роботи фактично доведені до рівня конкретних пропозицій і практичних рекомендацій для використання в публічному управлінні.

Так, результати та пропозиції, отримані в дисертаційному дослідженні, знайшли практичне застосування в законотворчій, службовій діяльності центральних та місцевих органів державної влади, зокрема у сфері інформатизації використані в практичній діяльності Міністерства цифрових трансформацій України (правонаступник Державного агентства з питань електронного урядування України) (довідка про впровадження № 1/22-3-1533 від 21.06.2019), щодо змісту щорічних планів заходів з реалізації Стратегії кібербезпеки України, які подаються на затвердження Кабінету Міністрів України Державною службою спеціального зв'язку та захисту інформації України, підвищенні ефективності заходів з реалізації цієї стратегії основними суб'єктами національної системи кібербезпеки, узгодженості з результатами виконання заходів у попередні роки, створенні та дооснащенні технологічних майданчиків, безпосередньо залучених до виконання завдань із забезпечення кібербезпеки державних органів (довідка про впровадження № 19/2/1-1497 від 28.11.2019), підтримкою Державним управлінням справами пропозицій щодо законопроекту № 9166 від 04.10 2018 «Про внесення змін до Закону України «Про Національну програму інформатизації», про який за результатами розгляду

законопроекту Головним науково-експертним управлінням Апарату Верховної Ради України підготовлено висновок про можливість його прийняття за основу (довідка про впровадження №01-13/12/1663 від 05.09.2019), а також щодо формування системи кібербезпекових заходів і їх реалізації у інформаційній діяльності місцевих органів державної виконавчої влади (довідка про впровадження Київо-Святошинської районній державній адміністрації Київської області (№07-34/2615 від 04.09.2019).

Повнота отриманих результатів дослідження. Основні наукові результати, висновки та рекомендації дисертаційної роботи викладені у 5 наукових працях, із них: 1 стаття – у зарубіжному спеціалізованому виданні, 4 статтей – у вітчизняних наукових фахових виданнях, 4 тези доповідей – у збірниках матеріалів науково практичних заходів.

Опубліковані наукові праці повною мірою розкривають основні наукові положення дисертації, що становлять наукову новизну і винесені на захист.

Оцінка оформлення дисертації та змісту автореферату.

Структура дисертації логічно побудована і сприяє розкриттю теми дослідження, виконанню поставлених завдань, кожен наступний розділ чи підрозділ органічно пов'язаний з попереднім і доповнює його. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Дисертація та автореферат оформлені відповідно до вимог Міністерства освіти і науки України, що висуваються до такого виду наукових робіт. Зміст автореферату ідентичний основним положенням дисертації.

Висновки повністю відповідають сформульованим завданням та змісту самої роботи та випливають з її основних положень. Дисертант стисло формулює основні результати дослідження, які викладені у тому числі і у структурній частині автореферату.

Предметна спрямованість дисертаційної роботи повністю відповідає паспорту спеціальності 25.00.02 «Механізми державного управління».

Зауваження та дискусійні положення щодо змісту дисертації.

Загалом дисертаційне дослідження здійснено на високому науково-теоретичному рівні. Проте, оскільки деякі його положення є дискусійними, що пов'язано із означенням дисертантом власної позиції щодо окремих досліджуваних проблем, варто зробити певні зауваження та побажання з метою подальшого удосконалення обумовленої проблематики.

1. Деякі результати наукової новизни, насамперед такі як, наприклад, удосконалення: "з урахуванням результатів узагальнення тенденцій розвитку національних систем кібербезпеки провідних країн світу та їх об'єднань визначено перелік та зміст науково обґрунтованих пропозицій щодо підвищення спроможності України адекватно протистояти загрозам у сфері кібербезпеки....", "організаційно-технічний механізм..." та "правового механізму забезпечення кібербезпеки..."(стор. 14 дисертації) сформульовано занадто складно та громіздко.

2. Рекомендації (стор.100-103,132-146) щодо удосконалення проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, як одного з основних механізмів формування та виконання Стратегії кібербезпеки України, доцільно було б уточнити стосовно місця, функцій та завдань в цій сфері такого суб'єкту кібербезпеки як Міністерство цифрових трансформацій України.

3. Автор справедливо вказує на одну з головних проблем забезпечення кібербезпеки України (стор.123-125): відсутність ефективного та результативного механізму обміну інформацією про кіберінциденти та кіберзагрози між органами влади, бізнесом та громадянами, але, на наш погляд, недостатньо чітко пропонує підходи щодо розв'язання цієї проблеми.

4. Важливе місце в механізмах міжнародного співробітництва України у сфері кібербезпеки займає двостороння міжнародна взаємодія України з кібербезпеки (стор.86-89 дисертації). На сьогодні такий механізм впроваджено лише з США. В дисертації бажано було б дати пояснення чому такий механізм не запроваджено з іншими країнами НАТО та ЄС, що заважає і визначити шляхи удосконалення цього механізму.

5. В 3 розділі дисертації (стор.165-175) приділено достатньо уваги національному та міжнародному досвіду щодо стандартизації у сфері кібербезпеки, у тому числі, стосовно можливостей та доцільності його застосування з метою удосконалення національної системи стандартизації в цій сфері. В той же час у сформульованих рекомендаціях не запропоновано застосування механізму державно-приватного партнерства в цій сфері, коли за ініціативою недержавних організацій та за підтримки держави створюються незалежні професійні структури в інтересах стандартизації з питань кібербезпеки та кіберзахисту.

6. Виходячи із змісту пропозицій здобувача щодо системи принципів проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури (стор.135-136) вбачається, що він пропонує нові принципи замість загальних принципів забезпечення кібербезпеки. Чи є науково-обгрунтованою заміна всіх 10 загальних принципів забезпечення кібербезпеки на запропоновані принципи?

Загальний висновок про відповідність роботи встановленим вимогам

З огляду на актуальність, новизну, важливість одержаних автором наукових результатів, їх обґрунтованість і достовірність, а також практичну цінність сформульованих положень і висновків, вважаю, що дисертація Станіславського Тараса Володимировича на тему «Механізми публічного управління забезпеченням кібербезпеки в сучасних умовах» є самостійним, оригінальним, завершеним науковим дослідженням, в якому вирішено актуальне наукове завдання, що полягає в комплексному дослідженні теоретичних і практичних засад забезпечення кібербезпеки в сучасних умовах, що має суттєве значення для галузі науки «Державне управління».

Дисертаційна робота відповідає таким науковим напрямам паспорту спеціальності 25.00.02 – теоретико-методологічні засади розроблення та функціонування механізмів державного управління: категорії, закономірності, принципи, методи, концепції, моделі, системи, класифікація; механізми державного регулювання окремих галузей і сфер суспільного життя та їх удосконалення; управління та регулювання діяльності органів та установ

державної влади: аналіз, моделювання й оптимізація; взаємовідносини та взаємодія з громадськістю в системі державного управління; інформаційні технології та інформаційне забезпечення в системах державного управління.

На підставі вище зазначеного можна зробити висновок, що дисертаційна робота повністю відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 із змінами, внесеними згідно з Постановою Кабінету Міністрів України від 19.08.2015 р. № 656, а її автор, Станіславський Тарас Володимирович, заслуговує на присудження наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління.

Офіційний опонент:
кандидат наук з державного управління,
доцент кафедри публічного управління та адміністрування
Державного університету телекомунікацій Д.Ю. Хлапонін

Підпис Хлапоніна Д.Ю. засвідчую:
Проректор Державного університету телекомунікацій
з науково-педагогічної роботи
доктор технічних наук, професор Л.Н. Беркман

“__” _____ 2020р.