ІНСТИТУТ ПІДГОТОВКИ КАДРІВ
ДЕРЖАВНОЇ СЛУЖБИ ЗАЙНЯТОСТІ УКРАЇНИ

Станіславський Тарас Володимирович

УДК 35.075.5-027.555:007

МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

25.00.02 – механізми державного управління

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня

кандидата наук з державного управління

КИЇВ – 2020

Дисертацією є рукопис.

Робота виконана в Інституті підготовки кадрів державної служби зайнятості України

Науковий керівник – доктор наук з державного управління, професор **СЕМЕНЧЕНКО Андрій Іванович,**
Національна академія державного управління при Президентові України,
директор Інституту вищих керівних кадрів.

Офіційні опоненти: доктор наук з державного управління, професор **ДОВГАНЬ Валерій Іванович,**
Національна академія Державної прикордонної служби України імені Богдана Хмельницького,
головний науковий співробітник науково-дослідного відділу;

кандидат наук з державного управління
ХЛАПОНІН Дмитро Юрійович,
Державний університет телекомунікацій,
доцент кафедри публічного управління та адміністрування.

Захист відбудеться *20 серпня 2020 року* о *15.00* годині на засіданні спеціалізованої вченої ради Д 26.891.02 Інституту підготовки кадрів державної служби зайнятості України за адресою: 03038, м. Київ, вул. Нововокзальна, 17, к. 201.

З дисертацією можна ознайомитись у бібліотеці Інституту підготовки кадрів державної служби зайнятості України (03038, м. Київ, вул. Нововокзальна, 17).

Автореферат розісланий *16 липня 2020 року*.

Вчений секретар
спеціалізованої вченої ради М. З. Масик

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Сьогодення вимагає від кожної країни відповідності своїх спроможностей у захисті конституційних прав та свобод своїх громадян, особливо у тих сферах суспільних відносин, де застосовність продукції інформаційно-комунікаційних технологій (ІКТ) має визначальний вплив на життєво важливі послуги, ведення бізнесу, безпеку всіх видів комунікацій, життєдіяльності громадян, суспільства та держави. Крім того, проникнення таких технологій у повсякденне життя вимагає нових знань в новому середовищі – кіберпросторі, від якого слід очікувати не тільки великої кількості сервісів та благ, а й розвитку існуючих та створення нових загроз. Ці загрози пов'язані із застосуванням механізмів несанкціонованого втручання в роботу систем та порушення безпеки інформації, яку вони обробляють, постійний розвиток індустрії розроблення та широке використання різного роду шкідливого та уразливостей широковживаного програмного забезпечення, застосування спеціальних операцій у кіберпросторі на об'єкти критичної інформаційної інфраструктури тощо.

Пильна увага суспільства до питань впровадження ІКТ в широкий спектр суспільних відносин, щоденно зростаюча небезпека від їх використання робить актуальним завдання системного дослідження національної системи кібербезпеки, її вад, обґрунтування напрямків та завдань щодо її модернізації.

Серед негативних факторів впливу на національну систему кібербезпеки доцільно виділити насамперед такі: майже повний імпорт продукції ІКТ за наявності в Україні достатньої кількості висококваліфікованих розробників програмного забезпечення; низька координованість виконання загальнодержавних проєктів інформатизації; неефективне бюджетування забезпечення кібербезпеки; низький рівень усвідомлення завдань і цілей кібербезпеки майже всіма суб'єктами її забезпечення та недбале ставлення або нехтування виконанням вимог із кібербезпеки; низька кібербезпекова культура на всіх ланках та в усіх сферах суспільного та особистого життя.

З іншого боку, на сьогодні в Україні наявні фактори для забезпечення відповідності кібербезпеки сучасним вимогам та передовим світовим практикам ЄС та НАТО, їх країн-членів.

Нормативно-правові аспекти систем кібербезпеки розглядалися у працях К. Александера (Alexander K.), Дж. Ліпмана (Liepman, J), В. Мазурова, Р. Олдрича (Aldrich R.), Є. Старостиної, М. Шмітта (Schmitt M.), А. Щетилова, Аквілса А. Алмансі (Aquiles A. Almansi).

Вітчизняними науковцями здійснювались дослідження різних аспектів забезпечення кібербезпеки України: І. Дороніним (щодо державного органу з формування єдиної політики у сфері кібербезпеки), В. Кравцем (виміри оцінки кібербезпеки на різних рівнях через глобальний, національний та галузевий індекс кібербезпеки), Л. Дешко та К. Бондарєвою (застосування механізмів, визначених Будапештською конвенцією про кіберзлочинність, Угодою про реалізацію Трастового фонду Україна – НАТО, Україна – ЄС), І. Забарою (укладення двосторонніх, регіональних і універсальних міжнародних угод з

інформаційної та кібербезпеки), Р. Лук'янчуком (міжнародне співробітництво за участі НАТО), В. Бурячком, В. Богушем (критерії якості підготовки кадрів у сфері кібербезпеки), В. Гурковським (методологічний аспект визначення змісту безпеки як об’єкта державного управління в умовах глобального інформаційного суспільства), В. Довганем (державне управління в електронному урядуванні та реформування системи надання електронних послуг, сутність і структура кадрової безпеки), Д. Дубовим (дослідження терміносистеми та аналізу стану утворення національної системи кібербезпеки та стратегічних аспектів кібербезпеки, державно-приватного партнерства та взаємодії), В. Петровим (формування національної системи кібербезпеки України, співробітництво України з НАТО), А. Семенченком (стан та напрямки розбудови національної системи забезпечення кібербезпеки) тощо.

На теренах нашої держави дотепер спеціалісти достатньо займалися дослідженням окремих проблем державного управління розвитком національної системи кібербезпеки, що обумовило актуальність проведення комплексного дослідження щодо механізмів публічного управління у сфері кібербезпеки.

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» (2018 – 2023 рр.)” (ДР № ДЄ №01118 U 003561), в яких автором проведено комплексне дослідження розвитку механізмів публічного управління у сфері кібербезпеки.

Мета і завдання дослідження. Метою дисертаційного дослідження є обґрунтування теоретико-методологічних засад розвитку механізмів публічного управління у сфері кібербезпеки та розроблення практичних рекомендацій органам влади щодо їх впровадження.

Для досягнення поставленої мети було визначено такі завдання:

– систематизувати існуючі теоретичні основи та удосконалити категорійно-понятійний апарат у сфері кібербезпеки;

– здійснити порівняльний аналіз національних та міжнародних механізмів публічного управління у сфері кібербезпеки, визначити тенденції їх розвитку, узагальнити досвід провідних країн світу та їх об’єднань у цій сфері;

– удосконалити нормативно-правовий та організаційно-технічний механізми розвитку системи кібербезпеки, зокрема, механізм періодичного проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

– запропонувати в межах державно-приватної взаємодії у сфері кібербезпеки мотиваційний механізм впровадження та застосування засобів систем кіберзахисту на об’єктах критичної інформаційної інфраструктури та в інформаційно-телекомунікаційних системах, де обробляються національні інформаційні ресурси;

– розробити рекомендації державним органам щодо підвищення рівня кібербезпеки.

Об'єкт дослідження – публічна політика у сфері кібербезпеки.

Предмет дослідження – механізми публічного управління забезпечення кібербезпеки в сучасних умовах.

Методи дослідження. Для виконання поставлених завдань дослідження використано загальнонаукові та спеціальні методи:

– діалектичний – при виявленні та дослідженні взаємозв'язків між суб'єктами/об'єктами-учасниками процесів забезпечення кібербезпеки, визначенні кіберзагроз та кіберінцидентів, що впливатимуть на безпеку функціонування об'єктів кіберзахисту, також у процесі розроблення нормативно-правових та організаційно-технічних механізмів забезпечення кібербезпеки;

– емпіричні (спостереження, порівняння, вимірювання) – при зборі інформації під час аналізу норм національних законодавств у сфері кібербезпеки, статистичних даних про динаміку зміни індикаторів кібербезпеки, способів їх отримання, затребуваності, термінів чинності та використання результатів заходів із кіберзахисту, кількості інформаційно-телекомунікаційних систем об'єктів критичної та критичної інформаційної інфраструктури та інші дані;

– узагальнюючий і порівняльний – для оцінки діючого механізму державного регулювання кіберзахистом та дослідження можливостей апробації міжнародного досвіду;

– суб'єктно-об'єктний – для удосконалення механізму державного регулювання кіберзахистом;

– методи синтезу та узагальнення – для формування пропозицій щодо удосконалення системи публічного управління кіберзахистом в Україні, розробленні пропозицій щодо осучаснення системи кібербезпеки в умовах все більш широкого впровадження продуктів ІКТ у повсякденну діяльність громадянина, суспільства та держави.

Методологічною базою дослідження є наукові праці вітчизняних і зарубіжних учених, зокрема офіційні публікації міжнародних організацій. Інформаційну та емпіричну базу дослідження сформували нормативні документи органів державної влади, статистичні та соціологічні дані, матеріали, опубліковані в періодичних виданнях та мережі Інтернет.

Наукова новизна одержаних результатів полягає в обґрунтуванні, поглибленні та розробці теоретико-методологічних засад та практичних рекомендацій державним органам щодо розвитку механізмів публічного управління у сфері кібербезпеки.

У результаті проведеного дослідження сформульовано низку положень, що мають важливе теоретичне і практичне значення, а саме:

уперше:

– доведено на основі результатів порівняльного аналізу часткову 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 й 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 оцінюються спроможності в 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 кібероборонi;

– правовий механізм забезпечення кібербезпеки, спрямований на підвищення ефективності заходів з кіберзахисту, організації належного обміну

інформації про кіберінциденти та кібератаки, зокрема, в інформаційно-телекомунікаційних системах, де обробляється інформація з обмеженим доступом, шляхом внесення змін до Закону України "Про основні засади забезпечення кібербезпеки України", 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 рівні, запровадження яких буде сприяти систематизації законодавства у цій сфері;

– організаційно-технічний механізм підвищення якості робіт зі 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 розбудови державно-приватної взаємодії у сфері кібербезпеки шляхом внесення змін до ліцензійних умов щодо надання послуги в галузі технічного захисту інформації, що не становить державної таємниці, з оцінювання її захищеності, 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 вдосконалення механізмів оцінки

відповідності у сфері захисту інформації за результатами аналізу базових правових та організаційних механізмів ЄС та НАТО щодо процедур сертифікації у 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 одержаних результатів. Практичне значення отриманих результатів полягає в тому, що теоретичні положення, висновки та рекомендації, розроблені автором і запропоновані у дисертації, вже реалізовані та можуть надалі використовуватись для вдосконалення комплексного механізму публічного управління у сфері кібербезпеки, що сприятиме результативності заходів з кіберзахисту.

Наукові висновки й теоретичні положення дисертаційної роботи фактично доведені до рівня конкретних пропозицій і практичних рекомендацій для використання в публічному управлінні. Зокрема, результати дослідження та запропоновані автором рекомендації щодо внесення змін до законодавства у сфері інформатизації використані в практичній діяльності 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 площадок, безпосередньо залучених до виконання завдань із забезпечення кібербезпеки державних органів (довідка про впровадження № 19/2/1-1497 від 28.11.2019), підтримкою Державного управління справами пропозицій щодо законопроєкту № 9166 від 04.10.2018 "Про внесення змін до Закону України "Про Національну програму інформатизації"" (довідка про впровадження № 01-13/12/1663 від 05.09.2019), про який за результатами розгляду законопроєкту Головним науково-експертним управлінням Апарату Верховної Ради України підготовлено висновок про можливість його прийняття за основу, а також щодо формування системи кібербезпекових заходів та їх реалізації в інформаційній діяльності місцевих органів державної виконавчої влади (довідка про впровадження №07-34/2615 від 04.09.2019).

Особистий внесок здобувача. Дисертаційна робота є завершеним самостійним науковим дослідженням автора, що містить теоретичні положення, практичні розробки, висновки та пропозиції, які одержано й сформульовано особисто автором. У комплексі вони дають можливість вирішення важливого наукового завдання щодо удосконалення та реалізації механізмів публічного управління забезпечення кібербезпеки в сучасних умовах.

У наукових статтях, опублікованих спільно зі співавторами, внесок здобувача був найбільшим. Так, у статті [1] його особистий внесок полягає в

аналізі та зіставленні положень Закону України “Про основні засади забезпечення кібербезпеки України” та Стратегії кібербезпеки України з іншими нормативно-правовими актами, визначено їх недоліки та позитивні моменти, запропоновано схему нормативно-правового забезпечення розбудови національної системи кібербезпеки та кіберзахисту України, визначено найактуальніші для прийняття законопроєкти, їх основні цілі та завдання, пропозиції до формування переліку об’єктів критичної інфраструктури за галузевим принципом.

У статті [2] особистий внесок полягає в авторському визначенні термінів, відповідно до місця огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури в комплексному огляді сектору безпеки та оборони, розроблена система принципів, основних завдань, суб’єктів та об’єктів його проведення, запропоновано самооцінювання ефективності заходів із кіберзахисту об'єкта огляду та його зміст як невід’ємну частину стану огляду кіберзахисту, надано пропозиції до вибору системи показників огляду.

Ідеї та розробки, що належать співавторам, у дисертаційній роботі не використовувалися.

Апробація результатів дослідження. Основні положення дисертаційного дослідження були презентовані та обговорені на міжнародних і всеукраїнських науково-практичних конференціях, зокрема: “Науково-практичне забезпечення децентралізації надання послуг в об'єднаних територіальних громадах” (м. Київ, 18 квітня 2018 р.); “Освітньо-наукове забезпечення складових сектору безпеки і оборони України” (м. Хмельницький, 15 листопада 2018 р.), “Організаційно-управлінські та психологічні аспекти сучасного ринку праці України” (м. Київ, 29 жовтня 2019 року); “Інформаційні технології та взаємодії” (IT&I 2019) (м. Київ, 20 грудня 2019 р).

Публікації. Наукові результати дисертаційного дослідження опубліковано в 9 наукових працях, зокрема: 4 статях, опублікованих у фахових виданнях з державного управління, 1 публікація в іноземному виданні та 4 тезах доповідей – у збірниках матеріалів науково-практичних заходів.

Структура та обсяг дисертації. Дисертація складається з переліку умовних позначень, вступу, трьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 211 сторінок, з них 181 сторінка основного тексту. Робота налічує 16 рисунків, 3 таблиці та 2 додатки. Список використаних джерел включає 225 найменувань на 29 сторінках.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовано вибір, актуальність і стан розробки теми дисертаційної роботи, подано її загальну характеристику, вказано на зв’язок дисертації з науково-дослідними роботами, визначено мету, завдання, об’єкт, предмет, охарактеризовано методологічну базу, наукову новизну та практичну значущість одержаних результатів, наведено дані щодо апробації та опублікування результатів дослідження.

У **першому розділі** – *“Теоретико-методологічні засади розвитку механізмів державного управління забезпечення кібербезпеки”* – проведено аналіз терміносистем, визначених у документах Європейського Союзу, США, Міжнародної організації зі стандартизації, Міжнародного союзу електрозв’язку та зіставлено з національною терміносистемою.

Проведено аналіз правових механізмів розвитку кібербезпеки в Україні та стану стратегічного управління розвитком кіберзахисту критичної інформаційної інфраструктури України, здійснено систематизацію сукупності законодавчих актів з розвитку кібербезпеки та кіберзахисту. Визначено основні недоліки існуючої редакції Стратегії кібербезпеки України та запропоновано загальні напрями її вдосконалення:

– більш чітке визначення цілей, завдань та заходів стратегії, часових рамок їх виконання;

– формулювання конкретних вимірюваних результатів;

– вдосконалення підходів до організації виконання Стратегії;

– передбачення розроблення та прийняття відповідної державної цільової програми забезпечення кібербезпеки з метою визначення, зокрема, бюджетування відповідних заходів.

Доведено, що серед позитивних результатів прийняття Стратегії є те, що її основні ідеї та підходи враховано при розробці Закону “Про основні засади забезпечення кібербезпеки України”. У ній достатньо конкретно та обґрунтовано сформульовано перелік сучасних загроз кібербезпеці, документ включено в систему стратегічних документів, які визначають розвиток сектору безпеки та оборони, насамперед Закону України “Про національну безпеку України”.

Здійснено аналіз основних положень Закону України “Про основні засади забезпечення кібербезпеки України”, який показав, що в ньому ретельно виписані складові системи забезпечення кібербезпеки, їх функції та завдання, але недостатньо чітко визначена організація їх взаємодії. Практика застосування його норм вказує на необхідність посилення саме цієї частини закону, більш чітке виписування норм, які забезпечили б утворення екосистеми кібербезпеки України. Водночас сфера дії закону не поширюється на системи, де циркулює інформація, яка становить державну таємницю, і вимагає пошуку нових організаційних форм та технічних механізмів, використання яких забезпечило б належний рівень безпеки мереж та інформації, яка в них обробляються.

Основні завдання щодо координації основних суб’єктів національної системи кібербезпеки України, до переліку яких увійшли майже всі суб’єкти сектору безпеки і оборони України, Національний банк України, покладені на робочий орган Ради національної безпеки та оборони України у сфері кібербезпеки – Національний координаційний центр кібербезпеки (далі – Центр). З огляду на це основною формою роботи цього Центру стало прийняття на своїх засіданнях доручень для інших державних органів. Особлива увага в цій системі органів визначена для Держспецзв’язку – спеціально уповноваженого центрального органа виконавчої влади у сфері спеціального зв’язку та захисту інформації, який для вирішення завдань кібербезпеки застосовує механізми

законодавства захисту інформації. Враховуючи, що кібербезпека є специфічною підмножиною безпеки інформації, існуючі вади механізмів сфери захисту інформації знайшли своє повторення при вирішенні завдань кібербезпеки, основною з яких є наявність завдання, проте відсутність норми щодо регулярного перегляду запроваджених механізмів захисту інформації новим загрозам. Обґрунтовано, що ця проблема в подальшому призвела до руйнації сутності комплексної системи захисту інформації (КСЗІ) – системи, яку треба постійно підтримувати в адекватному загрозам стані – відповідності безпеки інформації, яка з використанням механізмів КСЗІ досягається за повної статичності вже створених, досліджених, налаштованих та введених в експлуатацію КСЗІ по відношенню до нових загроз безпеці інформації, яку вони обробляють, що несумісно з реальним забезпеченням кібербезпеки в умовах постійного змінення кіберпростору.

Проведений аналіз організаційного механізму управління виконання Стратегії кібербезпеки України вказує на його недостатню спроможність забезпечення завдань із реалізації Стратегії. Суб'єкти кібербезпеки, які не є основними суб'єктами національної системи кібербезпеки України, залишаються осторонь розроблення щорічних планів, Національний координаційний центр кібербезпеки належної участі у стратегічному та щорічному плануванні заходів майже не бере. Вимог та правил з розроблення та оформлення пропозицій до переліку заходів, які б доводили їх відповідність основним цілям Стратегії кібербезпеки України та розвивали б результати заходів, запланованих/виконаних у попередніх роках, не встановлено. Проведений аналіз показує, що заходи з реалізації Стратегії кібербезпеки України мають різну тривалість. За такої умови в період 2016-2018 рр. заходів із реалізації 41% завдань Стратегії взагалі не планувалося. Вірогідність їх втілення до кінця терміну дії Стратегії вкрай низька. Також одним із факторів неуспішного виконання Стратегії є стислий термін планування заходів, який складає один рік і зазвичай закінчується після початку планування видатків державного бюджету України на наступний рік, а фінансування виконання заходів здійснюється за рахунок коштів, передбачених у державному бюджеті на утримання відповідних державних органів.

З метою якісного формування переліку об'єктів критичної інформаційної інфраструктури (комунікаційні й технологічні системи об'єктів критичної інфраструктури, технологічна інформація) визначено органи, які можуть виступати галузевими регуляторами, мали б змогу визначати та відповідати за належну взаємодію з об'єктами критичної інформаційної інфраструктури, встановлювати вимоги обов'язкові до опрацювання цими об'єктами з урахуванням своєї специфіки та рівня зрілості щодо кібербезпеки.

У другому розділі – *"Механізми взаємодії складових національних систем кібербезпеки"* – розглянуто еволюцію національних систем забезпечення кібербезпеки та стратегії кібербезпеки країн-членів ЄС та інших країн; наведено узагальнення характеристик та оцінювання результатів виконання стратегій кібербезпеки в країнах-членах ЄС. Зіставлено зміст стратегій інших країн та

Стратегії кібербезпеки України за такими спільними для більшості країн-членів ЄС ознаками:

– визначення структури управління кібербезпекою;

– визначення механізму (найчастіше державно-приватне партнерство), який дозволяє всім відповідним державним та приватним зацікавленим сторонам обговорювати та погоджувати різні питання політики кібербезпеки та регулювання у цій сфері;

– окреслення та визначення необхідних політичних та регуляторних заходів, чітке визначення ролей, обов'язків та прав приватного та державного сектору;

– встановлення цілей, засобів розвитку національних можливостей та необхідної правової бази для участі в міжнародних зусиллях щодо зменшення наслідків кіберзлочинності;

– визначення критичної інформаційної інфраструктури (КІІ), включаючи ключові активи, послуги та взаємозалежності;

– розроблення або покращення планів готовності, реагування та відновлення заходів щодо захисту таких об’єктів КІІ (наприклад, національних планів дій у надзвичайних ситуаціях, кіберзахисті та усвідомленні ситуації).

– визначення системного та інтегрованого підходу до національного управління ризиками.

Проведений аналіз Національної кіберстратегії Сполучених Штатів Америки, яка була опублікована у вересні 2018 року, принципово відрізняється за своєю суттю від усіх інших розглянутих національних стратегій кібербезпеки європейських країн. Цей документ поряд з питаннями кібербезпеки містить систему підходів та бачення подальшого розвитку політики США в кіберпросторі. Основними положеннями цієї кіберстратегії є:

– сприяння посиленню механізмів міжнародної координації та обміну інформацією;

– розвиток потенційних механізмів притягнення до суду кіберзлочинців з іноземним базуванням;

– “підштовхування” інших країн до прискорення їхньої допомоги в розслідуванні та дотримання будь-яких двосторонніх або багатосторонніх угод чи зобов'язань;

– надання допомоги країнам-партнерам у розбудові їхньої спроможності протистояти кримінальній кібер-діяльності;

– продовження будування потенціалу боротьби з кіберзлочинністю, що сприяє посиленню міжнародного співробітництва в галузі правоохоронних заходів у цьому напрямі;

– прагнення поліпшити міжнародне співробітництво в розслідуванні злочинної кібер-активності, включаючи розробку рішень потенційних бар'єрів для збирання та обміну доказами;

– керування розробленням взаємно сумісних та взаємовигідних систем з метою заохочення ефективного транскордонного обміну інформацією для цілей правоохоронних органів та зменшення бар'єрів у координації;

– наполягання на ефективному використанні існуючих міжнародних інструментів, таких як Конвенція ООН проти транснаціональної організованої злочинності;

– працювання над розширенням міжнародного консенсусу на користь Конвенції про кіберзлочинність Ради Європи (Будапештська конвенція); підтримка більшого прийняття Конвенції.

За результатами аналізу порівняння та зіставлення встановлено, що в Стратегії кібербезпеки України скоріше присутні структура управління кібербезпекою, механізми, заходи, ролі (завдання) її реалізації і, частково, обов'язки, цілі розвитку національних можливостей та визначення об'єктів критичної інфраструктури, але відсутні права суб'єктів кібербезпеки, засоби досягнення цілей, плани готовності, реагування та відновлення, заходи щодо захисту КІІ, системний та інтегрований підходи до національного управління ризиками.

Розглянуто механізми та напрями міжнародного співробітництва України у сфері кібербезпеки з Європейським Союзом, США, НАТО та визначено їх загалом незадовільну ефективність, за винятком реалізації Трастового фонду Україна-НАТО у сфері кібербезпеки.

Варто зазначити, що США – єдина країна, яка на законодавчому рівні унормувала взаємодію з Україною у сфері кібербезпеки: Ukraine Cybersecurity Cooperation Act of 2017, який спрямований на просування активної взаємодії між Україною та США у сфері кібербезпеки, насамперед, у забезпеченні відкритості, сумісності, надійності і безпечності Інтернету, зокрема з питань розширення можливостей у сфері кібербезпеки, покращенні здатності України реагувати на підтримувану РФ дезінформацію та пропаганду в кіберпросторі, зокрема через соціальні медіа та інші способи. Пріоритетними напрямками взаємодії цим законом визначено: убезпечення урядових мереж від зловмисних кібер-вторгнень, зокрема таких мереж, які захищають критичну інфраструктуру України; зменшення залежності від російських інформаційно-комунікаційних технологій; розбудова власного потенціалу; розширення обміну інформацією про кібербезпеку та співпраця з міжнародними зусиллями у сфері кіберпростору.

У США прийнятий окремий Закон про поширення інформації про інциденти кібербезпеки, важливим аспектом якого є те, що він визначає індикатори кіберзагроз – показники (технічні дані), які використовуються для виявлення та реагування на кіберзагрози. Водночас в їх визначенні наводиться не конкретний тип кібератаки, а її загальний опис. В українському законодавстві це питання визначено, але не внормовано, що підкреслює відсутність методологічної бази для розроблення єдиної системи норм у напрямку інформування про кіберінциденти, кіберзагрозу та кібератаку. Обґрунтовано доцільність врахування підходу США при формуванні базису для інформування суб'єктів кібербезпеки в Україні.

При аналізі документів НАТО встановлена обов'язковість проведення оцінок виконання заходів згідно з політикою НАТО з кібероборони (NATO

Policy on Cyber Defense (C-M(2011)0042) при акредитації комунікаційно-інформаційних систем для оброблення інформації НАТО з обмеженим доступом.

Досліджено досвід інших країн та їх об'єднань щодо нормативного регулювання, порядку та змісту інформування про кіберінциденти, принципи управління та обов'язкового звітування про їх опрацювання. З'ясовано, що в ЄС обов'язкове інформування про інциденти безпеки інформації встановлені п'ятьма загальними та галузевими актами законодавства ЄС (щодо захисту персональних даних, зокрема компетентними органами; щодо вільного обігу неперсональних даних; щодо електронної ідентифікації та електронних довірчих послуг; щодо мереж електронних комунікацій та послуг; директива про безпеку інформації та мереж), а також стандартом ETSI щодо структури інформації про загрози.

В українському законодавстві обмін інформацією про кіберзагрози на сьогодні унормований частково: Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в ІТС (2008 рік). Це вказує на практичну відсутність державного регулювання цим напрямком, наявна прогалина суттєво впливає на координацію боротьби з кібератаками як на загальнодержавному, так і на галузевому рівнях, та вимагає удосконалення, зокрема для підвищення довіри між суб'єктами в межах державно-приватної взаємодії у сфері кібербезпеки.

У третьому розділі – *"Рекомендації державним органам щодо удосконалення механізмів публічного управління забезпечення кібербезпеки"* – обґрунтовано та розроблено науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури з урахуванням міжнародного досвіду в цій сфері.

Запропоновано такі авторські визначення понять:

"огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури" – процедура періодичного спостереження, вимірювання, аналізу та оцінювання стану й готовності кіберзахисту об'єктів критичної інформаційної інфраструктури, інформаційно-телекомунікаційних систем (ІТС), 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 кіберзахисту, спрямоване на запобігання кіберінцидентам, виявлення, попередження та припинення, ліквідацію наслідків кібератак, здатність об'єктів критичної інформаційної інфраструктури до відновлення роботи після кібератак та кіберінцидентів (стійкості);

"мета огляду стану кіберзахисту" – визначення стану захищеності й готовності державних інформаційних ресурсів та критичної інформаційної інфраструктури до запобігання кіберінцидентам, оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак, ліквідації їх

наслідків, відновлення, функціонування цих об'єктів і систем.

Подано додаткові принципи проведення огляду у сфері кібербезпеки, які базуються на статті 7 Закону “Про основні засади забезпечення кібербезпеки”, а також завдання його проведення: планування; оцінювання затверджених власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури огляду (оцінки) ризиків та відповідних ним політик інформаційної безпеки; наявність на об'єктах огляду систем безпеки інформації або комплексних систем захисту інформації з підтвердженою відповідністю, їх періодичні випробування та модернізація; оцінка ефективності протоколів взаємодії об'єктів огляду; визначення підрозділів безпеки (захисту) інформації та кіберзахисту; оцінка достатності та ефективності заходів кіберзахисту, заходів з управління ризиками для запобігання та мінімізації впливу кібератак та кіберінцидентів; підвищення кваліфікації спеціалістів; визначення та/або вдосконалення критеріїв ризиків; оцінка стану кадрового, фінансового, матеріально-технічного та інших видів забезпечення.

Результати огляду в конкретизованому та деталізованому вигляді повинні враховуватися та відображатись у Стратегії кібербезпеки України, програмах і планах з її реалізації, інших концептуальних, програмних та планових документах ієрархічної системи нормативно-правових актів у сфері кібербезпеки та кіберзахисту, зокрема у відповідних завданнях державних цільових та національних програм.

Водночас актуальною проблемою є обґрунтований вибір системи показників вимірювання стану кіберзахисту об'єктів огляду, яка обумовлена різнотипністю цих об'єктів та різноманітністю складових огляду кібербезпеки (кіберрозвідка, кіберзахист, кібероборона, боротьба з кібершахрайством, протидія кібершпигунству та кібертероризму), їх цілей, інструментів застосування та підсистем показників і індикаторів, методичних апаратів спостереження, вимірювання, аналізу та оцінювання тощо.

Запропоновано мотиваційний механізм як один із першочергових кроків розбудови державно-приватної взаємодії у сфері кібербезпеки: удосконалення ліцензування господарської діяльності у сфері захисту інформації шляхом внесення змін до ліцензійних умов щодо надання послуги в галузі технічного захисту інформації, що не становить державної таємниці, з оцінювання її захищеності.

У межах дослідження існуючих механізмів публічного управління досліджено різні організаційно-технічні механізми визначення стану захищеності інформації та систем, що її обробляють: оцінювання стану захищеності державних інформаційних ресурсів, державний контроль за станом технічного та криптографічного захисту інформації, оцінювання захищеності інформації, що не становить державної таємниці, проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури.

При оцінюванні стану захищеності державних інформаційних ресурсів здійснюється детальний аналіз мереж і систем з точки зору потенційного зловмисника. Суть тесту полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. У процесі тестування роль

зловмисника відіграє спеціаліст, який повинен визначити рівень захищеності, виявити вразливості, ідентифікувати найбільш вірогідні шляхи зламу й визначити наскільки добре працюють засоби виявлення і захисту інформаційної системи від атак на підприємстві.

Завдання оцінки – виявлення вразливостей інформаційної системи та їх використання з метою отримання несанкціонованого доступу чи здійснення несанкціонованого впливу на інформацію для демонстрації наявності вразливостей і існування високоймовірної загрози інформаційної системи; оцінка поточного стану системи захисту інформації інформаційної системи; вироблення рекомендацій щодо підвищення ефективності захисту інформації в інформаційній системі

Державний контроль за станом технічного та криптографічного захисту інформації передбачає проведення в межах інспектування аналізу та виявлення порушень вимог законодавства у сфері захисту інформації. За результатами проведення контролю складається акт з виявленими порушеннями та вимогами щодо їх усунення. Неусунення порушень, викладених в акті, має результатом заборону оброблення в системі інформації, вимога щодо захисту якої встановлена законом.

Реалізація перших двох механізмів здійснюється Державною службою спеціального зв'язку та захисту інформації України.

Третій механізм – оцінювання захищеності інформації, яка не становить державної таємниці. Цей механізм регулюється шляхом ліцензування господарської діяльності в галузі технічного захисту інформації, може застосовуватись шляхом залучення підприємства ліцензіата в галузі технічного захисту інформації. Відповідно до Переліку видів господарської діяльності, які підлягають ліцензуванню, цей механізм передбачає атестацію комплексів технічного захисту інформації та експертні оцінювання у цій сфері. Ліцензійними умовами провадження цього виду діяльності передбачена, зокрема, наявність нормативних документів технічного захисту інформації (НД ТЗІ). Основним з них є НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. Згідно з цим НД ТЗІ критерієм є відповідність архітектури та параметрів програмно-апаратних засобів об’єкта оцінювання чіткому регламенту – комплексній системі захисту інформації (КСЗІ). За результатами такого способу оцінювання видається експертний висновок (є власником замовника експертизи та, зазвичай, не публікується). Експертний висновок є підставою для видачі атестата відповідності КСЗІ. Згідно з Законом України “Про захист інформації в ІТС” наявність такого атестата є умовою оброблення в системі інформації з обмеженим доступом або інформації, вимога щодо захисту якої встановлена законом.

Четвертий механізм – незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури забезпечує функціонування системи такого аудиту, а визначення вимог і порядку його проведення здійснює Кабінет Міністрів України. Проведення аудиту визначається суб’єктами забезпечення кібербезпеки, а організація його проведення покладається на

власників/розпорядників об’єктів критичної інфраструктури. Держспецзв’язку забезпечує впровадження такого аудиту, встановлює вимоги до аудиторів, порядок їх атестації, проводить такий аудит. Всі аспекти вказаного аудиту щодо банківської системи визначає Національний банк України. Водночас незалежний аудит діяльності основних суб’єктів національної системи кібербезпеки здійснюється щороку згідно з міжнародними стандартами.

За результатами аналізу цих механізмів запропоновано: на даному етапі розширити коло суб’єктів, що на законодавчих підставах, не вступаючи в конфлікт з положеннями статті 361 КК України (незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж), за згодою власника системи та, за необхідності, за погодженням з уповноваженими органами будуть здійснювати оцінювання захищеності державних інформаційних ресурсів, за результатами яких будуть видаватися відповідні рекомендації. Вимоги до суб’єктів проведення оцінювання за ліцензованим видом діяльності, його цільова функція та зміст перевірок постійно мають відповідати рівню можливих загроз в кіберпросторі.

Надалі запропоновано забезпечити поступове злиття обох видів оцінювань та їх трансформацію й об’єднання в незалежний аудит інформаційної безпеки за міжнародними стандартами та передовими практиками.

У процесі досліджень розроблено пропозиції до Законів України “Про основні засади забезпечення кібербезпеки України”, “Про Національну програму інформатизації”, “Про телекомунікації”, а також на основі аналізу міжнародного досвіду розроблено пропозиції щодо удосконалення розвитку системи національної стандартизації у сфері кібербезпеки.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне наукове завдання, яке полягає в теоретико-методологічному обґрунтуванні механізмів публічного управління у сфері кібербезпеки в сучасних умовах. Результати, одержані в процесі проведення досліджень, дозволяють зробити такі висновки:

1. Доведено необхідність приведення національної терміносистеми сфери кібербезпеки відповідно до міжнародних терміносистем задля поліпшення розуміння її сутності, забезпечення семантичної інтероперабельності, удосконалення взаємодії суб’єктів національної системи кібербезпеки між собою та з міжнародними організаціями в цій сфері, насамперед з НАТО та ЄС. Запропоновано авторське визначення термінів “кібербезпека”, “огляд стану кіберзахисту”, “спостереження стану кіберзахисту”, які адаптовані до аналогічних понять, визначених у терміносистемах цих міжнародних організацій.

2. Доведена відносна схожість національних стратегій кібербезпеки провідних країн світу та України у цілях та структурі національних систем управління кібербезпекою та обґрунтовано доцільність використання міжнародного досвіду у сфері безпеки мереж та інформаційних систем, який може бути імплементований в українському законодавстві лише в загальних та

спільних завданнях та підходах, зокрема для визначення українських інституцій задля взаємодії з міжнародними партнерами на всіх рівнях (міжнародний, загальнонаціональний, регіональний, секторальний (галузевий)).

Визначено основні тенденції розвитку систем кібербезпеки країн ЄС та США, а саме: збільшення ефективності виконання завдань з кібербезпеки та, найголовніше, впровадження дієвих механізмів їх взаємодії при кіберінцидентах і кібератаках; підвищення зрілості елементів національних систем кібербезпеки; вдосконалення взаємодії з уповноваженими органами інших країн та їх об'єднань, зокрема у боротьбі з кіберзлочинністю та впровадженні ефективних механізмів оцінки відповідності вимогам з кібербезпеки продукції ІКТ широкого вжитку (за стандартами та рекомендаціями ISO/IEC, ETSI, ENISA, NIST, COBIT тощо) та визнання результатів таких оцінок, здійснених відповідними органами інших країн; подовження 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; посилення спроможностей у кібероборони.

3. Запропоновано авторську ієрархічну модель структури законодавства у сфері кібербезпеки, яка включає стратегічний, оперативний та тактичний рівні, запровадження яких буде сприяти систематизації та розвитку законодавства у цій сфері, забезпечуючи взаємну узгодженість, зв'язок та відповідність норм існуючих та нових актів законодавства, цілі та завдання їх розроблення.

Обґрунтовано напрямки вдосконалення публічного управління задля підвищення ефективності виконання Стратегії кібербезпеки України, а саме: впровадження механізмів встановлення відповідності змісту щорічних заходів з реалізації Стратегії її цілям, осучаснення принципів планування та контролю за виконанням цих заходів; обґрунтовано розширення кола суб'єктів-учасників виконання щорічних планів заходів з реалізації Стратегії. Наступна редакція Стратегії кібербезпеки України має бути доповненою положеннями щодо запровадження сучасних механізмів стратегічного планування завданнями з формування переліку та планів забезпечення стійкості об'єктів критичної інформаційної інфраструктури, впровадження системного та інтегрованого підходу до управління ризиками кібербезпеці на національному рівні, що сприятиме підвищенню її результативності.

Удосконалено організаційно-технічний механізм підвищення якості робіт зі створення та оцінювання відповідності засобів, процесів і систем, які застосовуються 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”).

Науково обґрунтовано пропозиції щодо змін до Закону України “Про основні засади забезпечення кібербезпеки України”, а саме: відкоригувати існуючі та ввести нові терміни; впровадити перелік подій, які при визначенні їх як кіберінциденти мають обов’язково оброблятися відповідно до встановлених правил, зокрема щодо 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, включаючи волонтерські організації та їх об’єднання; запровадження принципів проведення огляду національної системи кібербезпеки та критичної інформаційної інфраструктури. Крім того, запропоновано зміни до Законів України “Про Національну програму інформатизації” та “Про телекомунікації”, а також, на основі аналізу міжнародного досвіду, розроблено пропозиції щодо удосконалення розвитку системи національної стандартизації у сфері кібербезпеки.

4. Доведено, що утворена в Україні система захисту інформації, зокрема за напрямком ліцензування виду господарської діяльності щодо оцінювання стану захищеності інформації, має слугувати базисом задля розвитку державно-приватної взаємодії (партнерства) у сфері кіберзахисту. Мотиваційним механізмом залучення широкого кола фахової спільноти у сфері кібербезпеки, зокрема «білих хакерів», має бути нормативне врегулювання їх діяльності та визнання результатів здійснених ними оцінок захищеності інформації та інформаційно-телекомунікаційних систем, що в них обробляється. Водночас способом врахування динаміки змін загроз в кіберпросторі для забезпечення довіри до результатів оцінок є запровадження дискусійної панелі при уповноваженому державному органі (наприклад, Держспецзв’язку). Основним завданням такої дискусійної панелі має стати формування вичерпних вимог до змісту заходів з оцінювання захищеності інформації від кіберзагроз, порядку виконання цих заходів, вимог до персоналу та вимог до оцінювання ефективності такого оцінювання.

5. Запропоновано підхід до вибору галузевих регуляторів, що має забезпечити реалізацію секторального принципу до формування як переліку об’єктів критичної інфраструктури, так і вимог з кібербезпеки до таких об’єктів з урахуванням галузевої специфіки та відмінностей, ступеня впровадження та способів оцінки їх реалізації.

6. Запропоновано органам державної влади розширити варіанти застосування огляду кіберзахисту державних інформаційних ресурсів та

критичної інформаційної інфраструктури, а саме не тільки як автономну процедуру та складову комплексного огляду сектору безпеки та оборони, а також передбачити його проведення у складі процедури періодичного проведення огляду національної системи кібербезпеки. Внести відповідні зміни до Закону ОЗКБ, Закону України "Про національну безпеку України" щодо автономного застосування періодичного проведення огляду національної системи кібербезпеки або у складі комплексного огляду сектору безпеки та оборони, Закони України "Про Національну програму інформатизації", "Про телекомунікації".

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Станіславський Т.В. Стратегічне управління розвитком кіберзахисту критичної інформаційної інфраструктури України / І.Б .Жиляєв, А.І. Семенченко, Д.В. Мялковський, Т.В. Станіславський. *Публічне управління та адміністрування в Україні.* Одеса, 2018. №3. С. 44-51.

2. Станіславський Т.В. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури / А.І. Семенченко, Д.В. Мялковський, Т.В. Станіславський. *Інвестиції: практика та досвід*. Київ, 2018. №18 вересень. С. 87-95.

3. Станіславський Т.В. Розвиток міжнародного співробітництва України у сфері кібербезпеки. *Актуальні проблеми державного управління.* 2019. №3(79). С. 58-67.

4. Станіславський Т.В. Стан та удосконалення механізму державного управління виконанням стратегії кібербезпеки України. *Економіка та держава: серія державне управління*. 2019. № 4 (12). С. 99-103.

Статті в зарубіжних виданнях:

5. Improving the planning of events as a key to the effective implementation of the Cybersecurity Strategy of Ukraine. *News of Science and Education*. 2019. №2 (63). P. 18-24.

Праці, які додатково відображають наукові результати дисертації

6. Станіславський Т. Забезпечення кібербезпеки: стан та актуальні завдання нормативного регулювання. *Науково-практичне забезпечення децентралізації надання послуг в об'єднаних територіальних громадах*: матеріали наук.-практ. конф (м. Київ, 18 квіт. 2018 р.). м. Київ: ІПК ДСЗУ, 2018. С. 348-353.

7. Семенченко А. І., Мялковський Д. В., Станіславський Т. В. Огляд кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури: науково-методологічні підходи до організації та проведення. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України*: тези XI Всеукраїнської науково-практичної конференції (м. Хмельницький, 15 лист. 2018 р.). Хмельницький : Вид-во НАДПСУ, 2018. С. 290-292

8. Станіславський Т.В. Розвиток міжнародного співробітництва України у сфері кібербезпеки. *Організаційно-управлінські та психологічні аспекти сучасного ринку праці України:* тези доповідей VIII Всеукраїнської науково-практичної конференції

молодих науковців (м. Київ, 29 жовт. 2019 р.). К. : ІПК ДСЗУ, 2019. С. 150-153.

9. Семенченко А.І., Станіславський Т.В. Організаційно-правові механізми огляду кібербезпеки та кіберзахисту державних інформаційних ресурсів та критичної інфраструктури. *Інформаційні технології та взаємодії*: VI Міжнародна науково-практична конференція (IT&I 2019). м. Київ. С. 297-304.

АНОТАЦІЯ

Станіславський Т.В. Розвиток механізмів публічного управління у сфері кібербезпеки. Рукопис.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. Інститут підготовки кадрів Державної служби зайнятості України. Київ, 2020.

У дисертації досліджено національні стратегії кібербезпеки та узагальнено тенденції розвитку систем кібербезпеки провідних країн світу та їх об'єднань, стан розвитку міжнародної взаємодії, визначено перелік та зміст науково обґрунтованих пропозицій щодо підвищення спроможності України адекватно протистояти загрозам у сфері кібербезпеки та розвитку національної системи кібербезпеки.

У дисертації обґрунтовано розвиток механізмів публічного управління у сфері кібербезпеки як пріоритету державної політики в Україні та подано напрями їх удосконалення на основі запровадження комплексного механізму. У роботі здійснено удосконалення категорійно-понятійного апарату у сфері кібербезпеки, запропоновано напрямки удосконалення Стратегії кібербезпеки України та Закону України "Про основні засади забезпечення кібербезпеки України", інших актів законодавства у цій сфері, вдосконалено правовий механізм забезпечення кібербезпеки, організаційно-технічний механізм підвищення якості робіт зі створення та оцінювання відповідності засобів, процесів і систем.

Ключові слова: кібербезпека, взаємодія при кіберінциденті, обмін інформацією про інциденти кібербезпеки, безпека інформації та мереж, сертифікація з кібербезпеки, об'єкт критичної інформаційної інфраструктури, оцінка відповідності у сфері кібербезпеки.

SUMMARY

Stanislavskyi T.V. The development of cybersecurity public administration's mechanisms. Manuscript.

Dissertation for obtaining the scientific degree of The Candidate of Science in Public Administration, by specialty 25.00.02 – Mechanisms of public administration. Ukrainian State Employment Service Training Institute. Kyiv, 2020.

In the Dissertation, National cybersecurity strategies were researched and generalized the trends of cybersecurity systems development in the leading countries and their associations, Ukraine's cybersecurity international cooperation. The list and content of scientifically substantiated proposals for improving Ukraine's ability to adequately confront cybersecurity threats and the development of the national cybersecurity system have been identified.

The dissertation substantiates the development of public governance mechanisms in

the field of cybersecurity as a priority of state policy in Ukraine and presents their improvement directions based on the implementation of a comprehensive mechanism. Improvements of the categorical and meaning apparatus in the field of cybersecurity, are made in the work and presented, directions of improvement of the Cybersecurity Strategy of Ukraine and the Law of Ukraine "On the basic principles of providing of cybersecurity of Ukraine", other acts of the legislation in this sphere, the legal mechanism of ensurance of cybersecurity are improved, the institutional mechanism to create and evaluate the compliance of the ICT products, processes and systems that are involved (applied) on critical infrastructure objects, to ensure the trust of the results of the information security assessments in the information and communication systems the creation of a discussion panel at the authorized state body was proposed. Also, a sectoral approach to the formation of critical infrastructure objects in which critical information infrastructure objects should be identified is proposed, motivational mechanisms as one of the primary steps of development of public-private cooperation in cybersecurity, as well as proposals to public authorities to enhance cybersecurity.

***Keywords*:** cybersecurity, cyber-incident interaction, cybersecurity information sharing, information and network security, cybersecurity certification and assessment of compliance, critical information infrastructure, cybersecurity.

SOMMAIRE

Stanislavskyi T.V. Développement de mécanismes d'administration publique dans le domaine de la cybersécurité. **Sur les droits du manuscrit.**

La thèse de candidat en sciences de l'administration publique sur une spécialité 25.00.02 – mécanismes de l'administration publique. Institut de formation du personnel du Service public de l'emploi de l'Ukraine. Kiev, 2020.

La thèse examine les stratégies nationales de cybersécurité et généralise les tendances des systèmes de cybersécurité des principaux pays du monde et de leurs associations, l'état de la coopération internationale, identifie la liste et le contenu des propositions scientifiquement solides pour accroître la capacité de l'Ukraine à contrer de manière adéquate les menaces dans la sphère de la cybersécurité et le développement du système de la cybersécurité nationale.

La thèse justifie le développement de mécanismes d'administration publique dans le domaine de la cybersécurité en tant que priorité de la politique de l'État en Ukraine et présente des directions pour leur amélioration sur la base de l'introduction d'un mécanisme complet. La thèse améliore l'appareil catégorique et conceptuel dans le domaine de la cybersécurité, suggère des moyens d'améliorer la stratégie de cybersécurité de l'Ukraine et la loi de l'Ukraine "Sur les principes de base de la cybersécurité de l'Ukraine", d'autres lois dans ce domaine, améliore le mécanisme juridique pour la cybersécurité, le mécanisme organisationnel et technique de l'augmentation de la qualité des travaux afin de créer et évaluer la conformité des outils processus et systèmes impliqués.

Mots-clés: cybersécurité, interaction avec les incidents cybernétiques, échange d'informations sur les incidents de cybersécurité, sécurité des informations et des réseaux, certification de cybersécurité, objet de 'infrastructures d'informations critiques, évaluation de la conformité dans le domaine de la cybersécurité.

Підписано до друку 10.07.2020
Формат 148х210 мм. Обл.-вид.арк. 0,9.
Наклад 100 прим.

Свідоцтво серії ДК № 1805 від 25.05.2004
Віддруковано з оригінал-макета в Інституті підготовки кадрів державної служби зайнятості України
03038, м. Київ, вул. Нововокзальна, 17, тел. (044) 536 -14-85