НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ

ШАЙХЕТ Сергій Олегович

УДК 351:86:659.3/.4:004:005.346](477)

МЕХАНІЗМИ РЕАЛІЗАЦІЇ СЕРВІСНО-ОРІЄНТОВАНОЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

25.00.02 – механізми державного управління

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата наук з державного управління

КИЇВ – 2019

Дисертацією є рукопис.

Робота виконана в Національній академії державного управління при Президентові України.

Науковий керівник – доктор наук з державного управління
КАРПЕНКО Олександр Валентинович,
Національна академія державного управління при Президентові України,
завідувач кафедри інформаційної політики та цифрових технологій.

Офіційні опоненти: доктор наук з державного управління, професор
СТЕПАНОВ Віктор Юрійович,
Харківська державна академія культури Міністерства культури України,
декан факультету управління та бізнесу;

кандидат наук з державного управління
БРИЧУК Костянтин Григорович,
директор ТОВ "Печерськ", головний редактор газети "Печерськ", м. Київ.

Захист відбудеться *9 вересня 2019 року о 12 годині* на засіданні спеціалізованої вченої ради Д 26.810.02 Національної академії державного управління при Президентові України за адресою: 03057, м. Київ, вул. Антона Цедіка, 20, к. 212.

Із дисертацією можна ознайомитись у бібліотеці Національної академії державного управління при Президентові України (03057, м. Київ, вул. Антона Цедіка, 20).

Автореферат розісланий *29 липня 2019 року.*

Вчений секретар
спеціалізованої вченої ради **М.Г.Цедік**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Цифрові трансформації сучасності внаслідок появи нових технологій та зміни ролі інформації в суспільному розвитку спричинили комплекс проблем, серед яких на особливу увагу заслуговує ефективне забезпечення взаємодії держави та суспільства, що зумовлюється зміною основних суб'єктів політичного, економічного та соціального процесів у глобалізованому просторі. Інформаційні переваги держави використовуються як ресурс у боротьбі за впливи на світовій арені. З огляду на це актуальним постає питання захисту інформаційних систем, мереж та їх даних, що в сукупності становлять невід'ємну частину стратегій інформаційної безпеки країни. Всі ці фактори засвідчують, що стан та рівень інформаційної безпеки в суспільстві вимагають більш ефективної державної політики в інформаційній сфері, яка є основою реалізації базових цінностей його інформаційного розвитку і важливою складовою частиною стратегії національної безпеки, спрямованої на зміцнення політичних, соціальних та економічних інститутів.

Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 25 лютого 2017 р. № 47/2017, визначено базові пріоритети державної політики в інформаційній сфері. Одним з таких пріоритетів, пов'язаних із забезпеченням відкритості та прозорості держави перед громадянами, є розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування. Адже від ефективності інформаційної безпеки багато в чому залежить можливість розвитку механізмів сучасної демократії в Україні, підвищення ефективності державного управління, рівня національної незалежності з огляду на розв'язану Російською Федерацією збройну агресію, що супроводжується інформаційною війною.

Зважаючи на те, що феномен інформації та цифровізації має невичерпний ресурс для підвищення ефективності державного управління, національні інтереси у сфері захисту інформації повинні стати невід'ємною частиною загальної стратегії розвитку держави. Це дає змогу вектор підвищення ефективності державного управління спрямувати в бік активного впровадження цифрових технологій у діяльність органів публічної влади всіх рівнів на основі сервісної моделі управління.

У процесі замовлення будь-якої державної послуги замовник, яким є юридична чи фізична особа, може отримати її в цифровому вигляді за умови дотримання вимог інформаційної безпеки, які встановлюються державою і є обов'язковими для суб'єктів господарювання, що здійснюють сервісну діяльність з використанням інформаційно-комунікаційних систем. Ефективне забезпечення організації інформаційної безпеки органів влади складається із захисту державних інформаційних ресурсів, даних та інформаційно-комунікативної інфраструктури, інструментарію протидії кіберзлочинності, здійснення правоохоронної діяльності в кіберсфері. Організація інформаційної безпеки стає важливою складовою подальшого розвитку сервісної держави в напрямі розширення переліку управлінських послуг.

Проблеми інформаційної безпеки знайшли відображення у працях таких відомих учених, як Л.Борисова, Н.Вінер, О.Євтушенко, Я.Жарков, О.Карпенко, Б.Кормич, О.Литвиненко, В.Ліпкан, Я.Малик, В.Морозова, В.Світлична, В.Степанов, О.Степко, О.Юдін та ін. Сучасне інформаційне протиборство досліджене в роботах Д.Дубова, інформаційні війни як складова гібридної війни розглядалися в працях В.Горбуліна, В.Кравченка, О.Курбана, Є.Магди та Г.Почепцова. Теоретичним підґрунтям дисертаційної роботи стали українські та зарубіжні нормативно-правові акти у сфері державного управління, інформології та національної безпеки, а також фундаментальні та прикладні наукові праці О.Васильєвої, В.Воротіна, В.Голубь, В.Гошовської, О.Дзьобань, І.Драгана, О.Іваницької, Т.Іванової, М.Кантока, Т.Лукіної, В.Овсяннікова, О.Олійник, П.Орлова, О.Петроє, Л.Приходченко, В.Семенова, В.Цимбалюка та Н.Чалої. Питання кібербезпеки як складової інформаційного захисту держави в сучасних умовах розкрито в роботах В.Бурячка, В.Бутузова, Г.Гранта, Р.Грищука, Т.Запорожець, М.Калдора, М.Кофмана, М.Ландлера та Е.Хендерсона.

Актуальність дисертації визначається недостатньою розробкою механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України, які, незважаючи на досить велику кількість праць зарубіжних та українських науковців, окремо не розглядалися та не були предметом окремого дослідження в галузі науки державного управління.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилося в межах комплексного наукового проекту Національної академії державного управління при Президентові України "Державне управління та місцеве самоврядування" (ДР № 0119U002827) у рамках науково-дослідних робіт: кафедри державної політики та суспільного розвитку за темою "Аналіз державної політики" (ДР № 0115U004062) (дисертантом визначено теоретичні засади формування сервісно-орієнтованої державної політики у сфері інформаційної безпеки України); кафедри інформаційної політики та цифрових технологій за темою "Цифрові стратегії країн ЄС як основа формування сервісно-орієнтованої державної політики України" (ДР № 0117U002857) (здобувачем досліджено організаційні механізми реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки).

Мета і завдання дослідження. *Метою* дисертаційної роботи є обґрунтування теоретичних засад та практичних рекомендацій щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України.

Для досягнення мети було поставлено такі *завдання*:

– розкрити сервісну сутність та визначити базові терміни понятійно-категоріального апарату інформаційної безпеки як складової національної безпеки держави;

– систематизувати нормативно-правову базу регулювання сфери інформаційної безпеки в Україні;

– узагальнити зарубіжний досвід упровадження моделей реалізації інформаційної безпеки як сервісу захисту національних інтересів (на прикладі країн ЄС та США);

– охарактеризувати сучасний стан кібербезпеки та розглянути перспективи її розвитку в Україні;

– установити концептуальні засади моделювання системи інформаційної безпеки в умовах гібридної війни;

– обґрунтувати механізми реалізації концепції “Community Policing” в Україні як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади і населення громад у контексті децентралізації влади та реформування правоохоронних органів;

– розробити рекомендації щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України.

Об’єкт дослідження – сервісно-орієнтована державна політика у сфері інформаційної безпеки.

Предмет дослідження – механізми реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України.

Методи дослідження. Багатоаспектність об’єкта дослідження зумовила застосування комплексу принципів і методів загальнонаукового й спеціального характеру, взаємодоповнюваність яких забезпечила об’єктивність і достовірність результатів дослідження. Методологія роботи поєднує засади системного, структурного, синергетичного підходів в їх диференційованому використанні залежно від обраного аспекту аналізу проблеми. Так, застосування системного та структурного підходів у дослідженні сервісної сутності інформаційної безпеки дало змогу забезпечити її всебічний розгляд у системі національної безпеки, а також її ролі в належному функціонуванні кіберсередовища в умовах сучасних цифрових трансформацій. З допомогою синергетичного підходу (що доповнює системний і структурний) у процесі аналізу інформаційної безпеки як сервісу було визначено багаторівневість її структурної ієрархії та динаміки, що є іманентним потенціалом самоорганізації. Емпіричний метод було використано для аналізу моделей інформаційних стратегій та концепцій інформаційної безпеки країн світу, компаративний – для виявлення спільних і відмінних рис у розробці стратегій кібербезпеки США та країн ЄС. В основу розробки рекомендацій щодо використання кращого світового досвіду для реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки покладено метод експертного оцінювання та моделювання.

Наукова новизна отриманих результатів полягає в обґрунтуванні теоретичних засад та практичних рекомендацій щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України. З огляду на це у дисертаційній роботі:

уперше: запропоновано та обґрунтовано сукупність механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України в контексті розбудови цифрового суспільства, базовими серед яких визначено: нормативно-правові (нормативно-правове забезпечення, що регламентує інформаційно-безпекову та кіберсфери); організаційно-технологічні (технічне і технологічне забезпечення інформаційно-комунікативної інфраструктури органів публічної влади відповідно до міжнародних стандартів у галузі інформаційної безпеки); ресурсно-

управлінські (ресурсно-управлінське забезпечення: запровадження загальнодержавної системи управління інформаційною безпекою, яка складається з підсистемних засобів, заходів та важелів впливу); програмно-цільові (державні програми реалізації інформаційної безпеки; регіональні та місцеві програми державно-приватного партнерства у сфері виробництва цифрових технологій захисту інформаційно-комунікативної інфраструктури та інформаційного простору, які спрямовані на усунення непрозорості владно-суспільних відносин та протидію маніпулятивним впливам на масову свідомість/підсвідомість; державні програми з підготовки, спеціалізації та підвищення кваліфікації фахівців галузі знань "Публічне управління та адміністрування" у сфері інформаційної безпеки та цифрових технологій);

удосконалено:

– алгоритм процесу організації інформаційної безпеки системи органів державної влади шляхом виокремлення двох взаємопов'язаних складових, одна з яких відповідає за змістове (інформаційне) наповнення контенту державних цифрових (електронних) ресурсів, а друга – за безпекове провадження цієї інформації (створення безпечних умов для доступу, отримання, передавання, обміну та захисту інформації незалежно від її контенту);

– підходи щодо визначення пріоритетів державної політики у сфері інформаційної безпеки України з урахуванням забезпечення відкритості та прозорості держави перед громадянами як клієнтами органів влади із застосуванням механізмів сервісно-орієнтованого державного управління;

– інструментарій взаємодії Національної поліції, місцевої влади та населення в об'єднаних територіальних громадах у контексті децентралізації влади та реформування правоохоронних органів шляхом реалізації в Україні концепції "Community Policing" як сервісу провадження інформаційної безпеки щодо забезпечення ефективної співпраці громадян з представниками органів правопорядку;

набули подальшого розвитку:

– понятійно-категоріальний апарат науки державного управління у сфері сервісно-орієнтованої державної політики в частині введення в науковий обіг авторських дефініцій: "інформаційна безпека – стан захищеності від завдання шкоди життєво важливим інтересам суспільства, держави та громадянина через недостовірність поширюваної інформації, порушення її цілісності та доступності (сприяння несанкціонованому обігу), а також через вплив на масову свідомість (підсвідомість, несвідомість), що спричиняє негативні наслідки шляхом застосування інформаційних, психологічних (маніпулятивних), цифрових та кібернетичних технологій"; "реалізація державної політики у сфері інформаційної безпеки – сукупність нормативно-правової, організаційно-інституційної та ресурсно-управлінської діяльності органів публічної влади, спрямованої на досягнення стану захищеності потреб громадян, суспільства та держави в отриманні, обробленні, збереженні, поширенні та захисті інформації"; "сервісно-орієнтована державна політика у сфері інформаційної безпеки – діяльність органів публічної влади для забезпечення функціонування сервісної держави, яка спрямована на досягнення

захищеності (убезпечення) потреб громадян, суспільства та держави в отриманні, обробленні, збереженні та поширенні інформації";

– теоретичне осмислення застосування лексичної конструкції "забезпечення безпеки", що потрапила в українську мову з російської внаслідок буквального перекладу словосполучення "обеспечение безопасности" і має семантичну емотивність мовної одиниці, яка є свідченням спадковості патерналізму взаємовідносин у соціумі, що не відповідає європейській моделі контракціонізму "надання, реалізації або провадження безпеки", для якої характерна сервісна орієнтованість владних структур і яка є більш вмотивованою для сучасного стану цінностей українського суспільства.

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки. Зокрема, основні теоретичні положення, запропоновані висновки та рекомендації використано:

– Державним агентством з питань електронного урядування України у процесі підготовки проекту Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки, схваленої Розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р, зокрема розробниками концепції враховано науково обґрунтовані пропозиції щодо використання сервісної моделі реалізації проектів цифрових трансформацій у сфері громадської та інформаційної безпеки (довідка про впровадження від 12 жовтня 2018 року № 1/06-1-2120);

– Комітетом з питань інформатизації та зв'язку Верховної Ради України в процесі підготовки Закону України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 р. № 2163-VIII, зокрема при підготовці ст. 1. "Визначення термінів" враховано пропозиції щодо трактування термінів "кібербезпека", "кібератака", "кіберзагроза" та "кіберзахист" (довідка про впровадження від 7 лютого 2019 року № 04-21/14-54 (25379);

– Горностаївською районною державною адміністрацією Херсонської області, зокрема Сектором юридичної, мобілізаційної роботи та взаємодії з правоохоронними органами враховано рекомендації щодо реалізації концепції "Community Policing" при розробці муніципальної програми безпеки та вирішенні інформаційно-безпекових завдань місцевої громади (довідка про впровадження від 18 лютого 2019 року № 1-20-469/0/19/609.1).

Особистий внесок здобувача. Робота є самостійно виконаним науковим дослідженням. Усі наукові положення та висновки сформульовано автором дисертації. У працях, виданих у співавторстві, особистий внесок здобувача полягає: в науковому обґрунтуванні недоцільності застосування в науці державного управління мовної конструкції "забезпечення безпеки" [3]; в доведенні необхідності впровадження в Україні концепції "Community Policing" як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади й громад [5]; у дослідженні доцільності використання сервісно-орієнтованого підходу щодо реалізації державної політики у сфері безпеки [6]; в наведенні аргументації щодо небезпечності впливу цілеспрямованих наступальних

інформаційних операцій суб'єктами геополітичного простору на колективну свідомість та "несвідоме" громадян [7]; у здійсненні аналізу тлумачення поняття "управлінські послуги" в дослідженнях галузі науки державного управління [8].

Апробація результатів дисертації. Основні положення, висновки, практичні рекомендації дисертаційного дослідження оприлюднено на таких комунікативних заходах: ІІ Всеукраїнській науково-практичній інтернет-конференції "Актуальні проблеми менеджменту зовнішньоекономічної діяльності підприємств України в контексті євроінтеграційних процесів" (Миколаїв, 2016); Всеукраїнській науково-практичній конференції за міжнародною участю "Реформування публічного управління та адміністрування: теорія, практика, міжнародний досвід" (Одеса, 2016); VIII науково-практичній конференції "Правові аспекти публічного управління: теорія та практика" (Дніпро, 2016); науково-практичній конференції за міжнародною участю "Національні цінності й національні інтереси в системі публічного управління" (Київ, 2017).

Публікації. За темою дисертації опубліковано 10 наукових праць, у тому числі: 5 статей у наукових фахових виданнях з державного управління, одна у зарубіжному науковому періодичному виданні, 4 тези доповідей у матеріалах науково-практичних конференцій.

Структура та обсяг дисертації. Дисертаційне дослідження складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 252 сторінки, з них основного тексту – 211 сторінок. Робота містить 3 рисунки, 1 таблицю та 2 додатки. Список використаних джерел складається з 367 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми, визначено мету, завдання, об'єкт, предмет дисертації; охарактеризовано наукову новизну та практичне значення отриманих результатів; наведено інформацію щодо апробації й публікації результатів дослідження.

У **першому розділі** – *"Теоретичні засади реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України"* – розглянуто поняття інформаційної безпеки як сервісну складову національної безпеки держави, визначено базові складові понятійно-категоріального апарату дослідження сервісно-орієнтованої державної політики у сфері інформаційної безпеки, проаналізовано особливості нормативно-правового регулювання сфери інформаційної безпеки України.

Зазначено, що в умовах геополітичних трансформацій, які визначають характер взаємовідносин держави й суспільства у XXI ст., основним полем боротьби інтересів та протистояння є інформаційний простір як на глобальному, так і на національному рівні. Постійний розвиток інформаційної сфери, який подолав національні кордони держав, приводить до формування інформаційних ресурсів глобального спрямування, які можуть бути використані як у позитивному сенсі, так і з метою справляння маніпулятивних впливів для досягнення певних

цілей, нав'язування цінностей, стандартів поведінки та мислення. Інформаційна безпека являє собою складну, динамічну й цілісну систему, невід'ємними складовими якої є підсистеми безпеки особистості, держави й суспільства.

Установлено, що поняття інформаційної безпеки безпосередньо пов'язане з його основною й визначальною складовою – інформацією та зумовлюваними нею процесами і взаємодіями на різних рівнях і серед визначеного кола суб'єктів та об'єктів. Відповідно до видів інформаційної діяльності виокремлюють такі різновиди провадження інформаційної безпеки: отримання інформації в установленому порядку, забезпечення можливості використання інформації; законне поширення інформації; належне зберігання інформації; захист інформації. Визначено, що інформаційна безпека є системоутворюючим і базовим поняттям, що в цілому визначає й формує стратегічні напрями інформаційної політики держави в означеному напрямі, що зумовлюється функціонуванням нормативно-правових документів, які легітимізують рівні взаємодій різних суб'єктів процесу провадження інформаційної безпеки.

Доведено, що сфера інформаційної безпеки передбачає системну превентивну діяльність органів державної влади з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на формування відповідного рівня довіри до держави, достатнього для подальшого соціального прогресу та належного розвитку інтелектуального потенціалу країни. Аналіз стану сформованості нормативно-правової бази дає підстави стверджувати, що в Україні загалом сформовані всі необхідні правові, адміністративні та економічні умови для розвитку інституту надання послуг з гарантування захисту і реалізації безпеки інформації.

Визначено, що інформаційна безпека є одним з базових механізмів у системі забезпечення національних інтересів України, що зумовлюється нагальною потребою у створенні розвиненого інформаційного середовища українського суспільства. В рамках переходу до моделі сервісно-орієнтованого державного управління важливе місце у сфері провадження інформаційної безпеки відводиться державі не лише в гарантуванні національної безпеки, а й наданні якісних управлінських послуг з інформаційної безпеки в різних сферах суспільного життя. Реалізація державної політики у сфері інформаційної безпеки є сукупністю нормативно-правової, організаційно-інституційної та ресурсно-управлінської діяльності органів публічної влади, спрямованої на досягнення стану захищеності потреб громадян, суспільства та держави в отриманні, обробленні, збереженні, поширенні та захисті інформації. Аналіз основних понять, що утворюють дискурсивне поле сфери інформаційної безпеки в умовах реалізації сервісно-орієнтованої державної політики, дає підстави стверджувати, що під інформаційною безпекою слід розуміти стан захищеності від завдання шкоди життєво важливим інтересам суспільства, держави та громадянина через недостовірність поширюваної інформації, порушення її цілісності та доступності (сприяння несанкціонованому обігу), а також через вплив на масову свідомість (підсвідомість, несвідомість), що спричиняє негативні наслідки шляхом застосування інформаційних, психологічних (маніпулятивних), цифрових та кібернетичних технологій.

Обґрунтовано недоцільність подальшого використання в понятійно-категоріальному апараті науки державного управління словосполучення "забезпечення безпеки" через його тавтологічність, омонімічність та синонімічність. Таке словосполучення має семантичну емотивність мовної одиниці, що свідчить про спадковість патерналізму взаємовідносин у соціумі (від російського аналогу "обеспечение безопасности") та не відповідає типово європейській моделі контракціонізму щодо безпекової діяльності "provide security" ("надання", "реалізації" або "провадження" безпеки), для якої характерна сервісна орієнтованість владних структур, що є більш вмотивованою для сучасних цінностей українського суспільства.

Показано, що в рамках концепції сервісної держави влада розглядається передусім як джерело, що забезпечує організацію надання послуг для громадян-споживачів, які виступають суспільними замовниками цих послуг. Сервісна діяльність у сфері інформаційної безпеки передбачає розуміння її як процесу, пов'язаного, насамперед, із забезпеченням потреби в отриманні інформації, її передачі, поширенні й захисті, що притаманна як окремим громадянам, так і спільнотам. Метою сучасного реформування галузі державного управління є запровадження сервісно-орієнтованої моделі вироблення державної політики, зокрема досягнення належного рівня інформаційної безпеки в контексті гарантування національної безпеки. Обґрунтовано, що сервісно-орієнтована державна політика у сфері інформаційної безпеки є діяльністю органів публічної влади щодо забезпечення функціонування сервісної держави, яка спрямована на досягнення захищеності (убезпечення) потреб громадян, суспільства та держави в отриманні, обробленні, збереженні та поширенні інформації.

Доведено, що, з одного боку, в Україні створено певну нормативно-правову базу регулювання сервісно-орієнтованої державної політики у сфері інформаційної безпеки, свідченням чого стало введення в дію указами Президента України рішень Ради національної безпеки і оборони України, зокрема Стратегії кібербезпеки України (2016), Доктрини інформаційної безпеки України (2017), а також ухвалення Закону України "Про основні засади забезпечення кібербезпеки України" (2017), у яких визначено принципи та окреслено головні напрями щодо провадження безпекової діяльності органів публічної влади в сучасних умовах загроз та з урахуванням пріоритетності захисту національних інтересів України. Крім того, вживається низка належних заходів щодо гарантування інформаційної безпеки у сфері надання управлінських послуг (як сервісу від імені держави). З другого боку, враховуючи погіршення динаміки впровадження нових законодавчих ініціатив, спостерігається несвоєчасність (втрачається актуальність) нормативного забезпечення потреб інформаційного суспільства, уповільнення темпів розвитку інформаційної інфраструктури з метою створення умов для ефективного запобігання кіберзлочинам, засоби здійснення яких постійно вдосконалюються. Виокремлено такі пріоритетні напрями, що потребують додаткового правового врегулювання побудови системи сучасних і високопродуктивних інформаційно-телекомунікаційних систем та центрів обробки даних щодо: визначення механізму проведення інвентаризації вже створених інформаційно-телекомунікаційних систем та центрів обробки даних, які обслуговують органи державної влади всіх рівнів, а

також забезпечують роботу центрів надання адміністративних послуг; забезпечення правових механізмів передачі в державну власність приватних інформаційно-телекомунікаційних систем та центрів обробки даних, які використовуються органами влади. Забезпечення функціонування цих напрямів (вказаних умов) сприятиме появі повноцінного сучасного сервісу держави, такого, як "надання інформаційної безпеки", оскільки основою сервісної діяльності органів влади в Україні повинна стати ефективна система провадження інформаційної безпеки громадянам – отримувачам управлінських послуг.

У **другому розділі** – *"Сучасний стан реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки: вітчизняний та зарубіжний досвід"* – узагальнено зарубіжні здобутки впровадження моделей реалізації інформаційної безпеки як сервісу захисту національних інтересів (на прикладі країн ЄС та США); проаналізовано сучасний стан кібербезпеки та розглянуто перспективи її розвитку в Україні; визначено концептуальні засади моделювання системи інформаційної безпеки в умовах гібридної війни.

Установлено, що з огляду на стрімкий розвиток цифрових технологій у сфері інформації та комунікації питання інформаційного захисту національних стратегічних каналів та мереж інформації й комунікації останні кілька десятиліть є одним з актуальних у технологічно розвинених країнах світу, в яких захист інформаційних ресурсів та убезпечення від негативного впливу на суспільство стали важливими складниками їх інформаційної політики. Якісні зміни у процесах управління зумовлені, з одного боку, інтенсивним упровадженням сучасних цифрових технологій, а з другого – формуванням сервісної діяльності у безпековій сфері як загальним принципом діяльності органів публічної влади.

Узагальнено кращі світові практики щодо розробки стратегій інформаційної безпеки, і, зокрема, захисту інформаційних систем і даних у середовищі кібербезпеки. Як показує світовий досвід, технологічно та інформаційно розвинені країни, такі, як США, Німеччина, Швеція, Великобританія, Франція, Фінляндія, Польща, пріоритетного значення надають безпеці в середовищі кіберпростору, який являє собою систему технологічного та ресурсно-організаційного порядку. Проаналізовано різні зарубіжні підходи щодо вироблення стратегій кібербезпеки, які дають змогу зрозуміти, що якісна побудова системи захисту та управління інформацією, цифрових мереж різного типу критичної інфраструктури можлива лише за наявності стандартів щодо рівня захисту інформації, які ґрунтуються на визнаних міжнародних стандартах захисту інформації. Досвід цих країн доводить підвищення рівня довіри громадян до влади та ступеня забезпечення потреб від сервісної діяльності органів публічної влади у сфері реалізації інформаційної безпеки.

Визначено, що під кібербезпекою розуміється такий різновид безпеки, що включає процеси формування, функціонування й еволюції кібероб'єктів з метою виявлення кібернебезпечних джерел, які можуть завдати їм шкоди. Складовими кібербезпеки є кібернетичні впливи, розвідка інформаційно-комунікаційних та криптосистем протиборчих сторін, а також захист державою власної інформаційної сфери. Сфера кібербезпеки містить у собі стратегії, принципи та засоби провадження безпеки, гарантії безпеки, підходи до управління ризиками,

практичний досвід захищеності технологій, що в комплексі слугують засобами захисту інформації в кіберсередовищі. Як загрози у сфері кібербезпеки можна виокремити кібертероризм та кібершпигунство, кібервійну, складовими яких є безпосередні кіберінтервенції, що складаються з кібератак та інших втручань. Важливими напрямами діяльності у сфері кібербезпеки є формування конкурентного середовища цифрових комунікацій з можливістю надання послуг із захисту інформації; проведення навчань щодо усунення надзвичайних ситуацій у кіберпросторі; розвиток та вдосконалення системи державного контролю щодо захисту інформації, а також системи незалежного аудиту інформаційної безпеки.

Обґрунтовано, що феномен інформаційної війни в гуманітарному та ціннісно-світоглядному аспектах і вимірах являє собою практично реалізовані заходи цілеспрямованого інформаційного впливу на масову свідомість з метою трансформації усталених світоглядних, морально-ціннісних, поведінкових засад у діяльності членів суспільства; отримання певної інформації і даних з метою економічної, політичної та іншої вигоди і в напрямі, який належить до сфери інтересів ворожої сторони, що здійснює таке втручання.

Доведено, що в процесі розробки концептуальних засад моделювання інформаційної безпеки визначальним є аналіз самого кіберпростору та основних факторів, що впливають на його функціонування. З огляду на це важливими є: створення математичних моделей, що дають змогу отримувати кількісні показники інформаційної безпеки (ступеня загроз інформаційній безпеці, аналізу інформаційних ризиків, оцінки ефективності заходів захисту), розробка спеціальних методів забезпечення стійкості кіберпростору при впливі загроз, що дасть можливість здійснювати аналіз топологічної структури та вироблення рекомендацій щодо її зміни, способів і конкретних алгоритмів їх реалізації; розробка нових методів криптографічного захисту, що базуються не тільки на суто обчислювальних механізмах реалізації стійкості, а й на використанні переваг багаторівневої архітектури зв'язків і великої кількості користувачів, розробка методів реалізації інформаційної безпеки на основі соціальних сервісів для протидії кібератакам із застосуванням спеціальних процедур аналізу групової поведінки. З огляду на стан організації та практичної реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки в рамках реалізації стратегії національної безпеки доцільною є побудова такої концептуальної моделі інформаційної безпеки, що відповідала б як загальносвітовим стандартам і вимогам, так і мала змогу адаптуватися в різних сферах і галузях економіки, фінансів, державного управління, соціальної сфери тощо. Порушене питання вимагає також суттєвого доопрацювання на рівні державного законодавчого вдосконалення структурно-організаційних механізмів реалізації подібних концепцій.

Запропоновано та обґрунтовано сукупність механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України в контексті розбудови цифрового суспільства, базовими серед яких визначено: нормативно-правові, організаційно-технологічні, ресурсно-управлінські та програмно-цільові.

У **третьому розділі** – *"Удосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України"* –

обґрунтовано механізми впровадження концепції “Community Policing” в Україні як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади і населення об’єднаних територіальних громад у контексті децентралізації влади та реформування правоохоронних органів; визначено інституційно-організаційні механізми упровадження сервісів інформаційної безпеки через адаптацію світових здобутків; запропоновано шляхи модернізації технологій упровадження сервісної діяльності органів влади у сфері інформаційної безпеки; розроблено рекомендації щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України.

Доведено доцільність реалізації в Україні концепції “Community Policing” як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади та населення громад у контексті децентралізації влади та реформування правоохоронних органів. Здійснено фактологічний аналіз досвіду зарубіжних країн щодо реалізації концепції “Community Policing” (на прикладі США, Великої Британії, Кенії, Індії та Японії), сформульовано рекомендації щодо впровадження механізмів її реалізації в Україні, зокрема через: розробку та ухвалення органами місцевої влади відповідних стратегій (програм) безпеки територій; децентралізацію діяльності Національної поліції, наприклад шляхом упровадження інституцій “присутності” поліції “Кобанів” у комплексі з традиційним патрулюванням; застосування сучасних цифрових сервісів для здійснення ефективної боротьби з новими різновидами злочинів; проведення спільного навчання поліцейських і громадян (відкриті діалоги, спільне вирішення безпекових завдань територіальних громад, обговорення “незручних” питань тощо) з метою налагодження комунікації, оперативної взаємодії та забезпечення належного рівня взаємоповаги й допомоги; стимулювання патріотизму та волонтерства для ефективної співпраці громадян з органами правопорядку.

З’ясовано, що реалізація сервісно-орієнтованої державної політики у сфері інформаційної безпеки ґрунтується на переорієнтації з гарантованого права забезпечення захисту інформації на сервісну інформаційну безпеку в сукупності правових, інституційних, ресурсних та організаційних складових чинників та механізмів її реалізації. Пріоритетними напрямами щодо провадження інформаційної безпеки на національному рівні визначено заходи протидії у відповідь на інформаційну агресію щодо України; створення систем оцінювання інформаційних загроз; виявлення та нейтралізацію в межах українського інформаційного простору суб’єктів, які здійснюють підривну інформаційну діяльність проти України; підвищення рівня розкриття кіберзлочинів, забезпечення захищеності об’єктів критичної інформаційно-комунікативної інфраструктури держави та їх ресурсів від кібератак.

Окреслено параметри технічного складника в процесі запровадження сервісних механізмів у сфері інформаційної безпеки. Зроблено акцент на важливому значенні вимог щодо програмно-технічних засобів, які забезпечують доступ до глобальних мереж передачі даних, якості окремих видів послуг та захисту інформації в мережах передачі даних. Доведено, що

вирішення цієї проблематики є можливим з допомогою створення цифрових технологій, що забезпечить інтеграцію інформаційних сервісних систем різноманітними способами та їх організацію щодо охоплення великих обсягів даних і надання при цьому швидкого авторизованого доступу до них максимальній кількості користувачів. Архітектура типової системи управління інформаційною безпекою має включати такі основні компоненти: інтеграційну платформу; апаратно-програмні засоби моніторингу й аудиту; апаратно-програмні засоби захисту інформації; сховище інформації про інциденти інформаційної безпеки; аналітичні інструменти генерації звітів.

Обґрунтовано, що створення безпечного інформаційного простору державного управління здійснюється шляхом формування цілісної системи інформаційної безпеки органів державної влади, для чого необхідним є вирішення таких пріоритетних завдань: створення єдиного репозиторію програмного забезпечення у сфері інформаційної безпеки з метою його належного використання органами державної влади та органами місцевого самоврядування; організація ефективної комунікації, убезпечення передачі інформаційних потоків у кіберсередовищі держави; цифровізація управлінських і технологічних процесів державного управління; централізоване здійснення моніторингу та контролю систем інформаційної безпеки державного управління; забезпечення захисту інформації, яку отримують із зовнішнього середовища органи публічної влади; гарантування належного рівня безпеки і захисту інформаційно-комунікативної інфраструктури органів державної влади.

Зазначено, що для забезпечення реалізації механізмів сервісно-орієнтованої державної політики у сфері інформаційної безпеки першочерговими заходами є: нормативно-правове врегулювання насамперед процедурних питань щодо надання послуг органами влади у сфері інформаційної безпеки; дотримання принципів і напрямів реформування органів публічної влади для здійснення ефективної сервісної діяльності з подальшою практичною реалізацією; делегування повноважень щодо надання управлінських послуг з реалізації інформаційної безпеки соціально відповідальним суб’єктам приватного сектору; встановлення стандартів послуг органів влади у сфері інформаційної безпеки; підвищення відповідальності за порушення прав громадян при здійсненні сервісної діяльності органами влади; запровадження сучасних цифрових форм і засобів надання безпекових послуг.

Запропоновано стратегічні пріоритети реалізації сервісно-орієнтованої державної політики в Україні, а саме: створення умов для гарантування прав на забезпечення законодавчо закріплених потреб громадян суспільства; гарантування законних інтересів та захисту прав користувачів державних сервісів; забезпечення рівноправності кожного на отримання послуг у сфері інформаційної безпеки за єдиними процедурами, а також рівного доступу до отримання послуг органів публічної влади для всіх громадян з урахуванням економічної спроможності різних верств населення.

Установлено, що для реалізації стратегії інформаційної безпеки важливим компонентом є визначення необхідних для цього механізмів, які полягають як в інтегративному розвитку інституційної інфраструктури, нормативно-правовому

регулюванні, так і у вжитті комплексу практичних організаційних заходів з метою запобігання деструктивним впливам та їх нейтралізації, що досягається завдяки координації зусиль органів публічної влади. Для України реалізація сервісно-орієнтованої державної політики у сфері інформаційної безпеки формує перспективи сталого розвитку, який перебуває в площині побудови цифрової економіки та суспільства як базової основи сучасної держави з розвиненими демократичними інститутами.

ВИСНОВКИ

У дисертаційній роботі вирішено нове наукове завдання, яке полягає в обґрунтуванні теоретичних засад та практичних рекомендацій щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України. Результати, отримані в процесі дисертаційного дослідження, дають підстави сформулювати такі висновки.

1. Розкрито сервісну сутність інформаційної безпеки як складової національної безпеки держави на основі узагальнення теоретичних засад механізмів вироблення сервісно-орієнтованої державної політики. Встановлено, що інформаційна безпека є системоутворюючим і базовим поняттям, що в цілому визначає і формує стратегічні напрями інформаційної політики держави. Зазначено, що реалізація інформаційної безпеки як сервісу полягає в гарантуванні сталого розвитку інформаційного простору, який при цьому має таку систему захисту, що здатна протистояти зовнішнім і внутрішнім загрозам. Стратегія цифровізації як основний магістральний напрям побудови цифрової економіки та суспільства також безпосередньо пов’язана з питаннями інформаційної безпеки, формуванням державної інформаційної політики та здійсненням сервісної діяльності органами публічної влади в контексті забезпечення сталості збереження різного роду інформації та запобігання ризикам щодо стороннього втручання в інформаційно-комунікаційні системи.

Визначено базові складові понятійно-категоріального апарату дослідження сервісно-орієнтованої державної політики у сфері інформаційної безпеки на основі аналізу наукових джерел. Зокрема, введено в науковий обіг авторське трактування понять: “інформаційна безпека” та “сервісно-орієнтована державна політика у сфері інформаційної безпеки”.

Доведено недоцільність подальшого використання в понятійно-категоріальному апараті науки державного управління словосполучення “забезпечення безпеки”, замість якого запропоновано вживати в подальших дослідженнях терміни “надання безпеки”, “реалізація безпеки” або “провадження безпеки”.

2. Систематизовано чинну нормативно-правову базу щодо регулювання сфери інформаційної безпеки в Україні, в результаті чого доведено, що, з одного боку, в Україні створено певну нормативно-правову базу регулювання сервісно-орієнтованої державної політики у сфері інформаційної безпеки, з другого, з огляду на погіршення динаміки впровадження нових законодавчих ініціатив, спостерігаються несвоєчасність (втрачається актуальність) нормативного

забезпечення потреб інформаційного суспільства, уповільнення темпів розвитку інформаційної інфраструктури, з метою створення умов щодо ефективного запобігання кіберзлочинам, засоби здійснення яких постійно вдосконалюються.

Установлено пріоритетні напрями, що потребують додаткового правового врегулювання побудови комплексу сучасних та високопродуктивних інформаційно-телекомунікаційних систем і центрів обробки даних: визначення механізму проведення інвентаризації вже створених інформаційно-телекомунікаційних систем та центрів обробки даних, які обслуговують органи державної влади всіх рівнів, а також забезпечують роботу центрів надання адміністративних послуг; забезпечення правових механізмів передачі в державну власність приватних інформаційно-телекомунікаційних систем та центрів обробки даних, які використовуються органами влади.

3. Узагальнено зарубіжний досвід упровадження моделей реалізації інформаційної безпеки як сервісу захисту національних інтересів (на прикладі країн ЄС та США), в результаті чого виявлено, що лідером у сфері інформаційного захисту та безпеки кіберпростору є США, де вперше було прийнято стратегію національної безпеки з акцентуванням уваги на інформаційній складовій.

Установлено, що основні особливості вироблення сервісно-орієнтованої державної політики у сфері інформаційної безпеки і технологій полягають у розумінні самої галузі інформаційної безпеки як сервісу системи національної безпеки, формуванні і реалізації цілісної системи державного управління, розвитку та підтримці організаційної структури і сформованої необхідної законодавчої бази, яка будується на загальнодержавній стратегії провадження інформаційної безпеки, пріоритетності захисту національного інформаційного простору. Управління інформаційною безпекою в загальній системі державного управління функціонально передбачає забезпечення конфіденційності, цілісності та доступності інформаційних активів. Аналіз нормативних документів та основних положень стратегій США і країн ЄС засвідчив відсутність єдиних стандартів у галузі інформаційної безпеки, оскільки зміст цієї категорії значною мірою зумовлюється внутрішніми та зовнішніми політичними цілями та завданнями конкретної країни.

4. Охарактеризовано сучасний стан та перспективи розвитку кібербезпеки в Україні. Це дає підстави стверджувати, що проблематика вітчизняного досвіду щодо захисту інформації та організації системи інформаційної безпеки й управління нею потребує цілісного доопрацювання як з технологічного боку, так і з законодавчого та інфраструктурного. Важливим завданням є визначення природи різних видів інформаційних загроз, способів та механізмів їх впливу на об’єкти інформаційної безпеки, прогнозування можливих наслідків цих впливів, шляхів і методів їх нейтралізації. Під кібербезпекою розуміється такий різновид безпеки, що вивчає процеси формування, функціонування й еволюції кібероб’єктів з метою виявлення кібернебезпечних джерел, які можуть завдати шкоди критичній інформаційно-комунікативній (кібер) інфраструктурі, а також розробка законів та інших нормативних актів, що регламентують стандарти, вимоги, правила,

рекомендації і методики, виконання яких повинно гарантувати захищеність об’єктів у кіберпросторі від усіх відомих і потенційних джерел небезпеки.

5. Установлено концептуальні засади моделювання системи інформаційної безпеки в умовах гібридної війни. У результаті дослідження виявлено, що інформаційні війни, які розгортаються за певними сценаріями і законами, породжують низку проблем та конфліктів для всіх важливих сфер життєдіяльності суспільств. Виходячи з логіки теоретичної побудови цілісної системи інформаційної безпеки на рівні концептуальних засад її базовими структурними елементами можуть бути: об’єкти безпеки, на які й спрямовуватимуться основні дії щодо виконання цієї функції; суб’єкти безпеки, що включають організації, інституції, служби як державного, так і приватного типу, до визначених функцій і повноважень яких належить убезпечення об’єктів шляхом здійснення практичних дій із запровадження механізмів реалізації інформаційної безпеки. Ця система являє собою поєднання як теоретичних розробок щодо визначення й обґрунтування певного алгоритму, так і практичних дій щодо провадження безпеки шляхом його послідовної реалізації.

Доведено, що в процесі розробки концептуальних засад моделювання інформаційної безпеки важливим є аналіз самого кіберпростору та основних факторів, що впливають на його функціонування. З урахуванням цього важливими є: створення математичних моделей, що дають змогу отримувати кількісні показники інформаційної безпеки (ступеня загроз інформаційній безпеці, аналізу інформаційних ризиків, оцінки ефективності заходів захисту), розробка спеціальних методів забезпечення стійкості кіберпростору при впливі загроз, що дасть можливість здійснювати аналіз топологічної структури та вироблення рекомендацій щодо її зміни, способів і конкретних алгоритмів їх реалізації; розробка нових методів криптографічного захисту, що базуються не тільки на суто обчислювальних механізмах реалізації стійкості, а й на використанні переваг багаторівневої архітектури зв’язків і великої кількості користувачів; розробка методів реалізації інформаційної безпеки на основі соціальних сервісів для протидії кібератакам із застосуванням спеціальних процедур аналізу групової поведінки.

Визначено сукупність складових механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України в контексті розбудови цифрового суспільства, серед яких базовими є: нормативно-правові, організаційно-технологічні, ресурсно-управлінські та програмно-цільові.

6. Обґрунтовано необхідність реалізації в Україні концепції “Community Policing” як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади та населення об’єднаних територіальних громад у контексті децентралізації влади та реформування правоохоронних органів.

Здійснено фактологічний аналіз досвіду зарубіжних країн щодо реалізації концепції “Community Policing” (на прикладі США, Великої Британії, Кенії, Індії та Японії). Сформульовано рекомендації щодо впровадження механізмів реалізації концепції “Community Policing” в Україні, зокрема через: розробку та ухвалення органами місцевої влади відповідних стратегій (програм) безпеки

територій; децентралізацію діяльності Національної поліції, зокрема шляхом упровадження інституцій “присутності” поліції “Кобанів” у комплексі з традиційним патрулюванням; застосування сучасних цифрових сервісів для ефективної боротьби з новими різновидами злочинів; проведення спільного навчання поліцейських і громадян (відкриті діалоги, спільне вирішення безпекових завдань територіальних громад, обговорення незручних питань тощо) з метою налагодження комунікації, оперативної взаємодії та забезпечення належного рівня взаємоповаги й допомоги; стимулювання патріотизму та волонтерства для ефективної співпраці громадян з органами правопорядку.

7. Визначено шляхи вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України, зокрема обґрунтовано, що загальносвітовими ключовими позиціями стратегій інформаційної та кібербезпеки є побудова урядової моделі, спрямованої на реалізацію кібербезпеки; вироблення належного механізму впровадження сервісів інформаційної безпеки на засадах суспільно-державного партнерства у сфері інформаційної безпеки, а також необхідної державної політики та механізмів регулювання забезпечення кіберзахисту. Загальноєвропейська стратегія кібербезпеки передбачає всебічне сприяння розвитку кібероборони ЄС за допомогою різних засобів, технологій, навчання спеціалізованого персоналу (проведення тренінгів) та розвитку цифрової інфраструктури.

Обґрунтовано, що створення безпечного інформаційного простору державного управління здійснюється шляхом формування цілісної системи інформаційної безпеки органів державної влади, для чого необхідним є вирішення таких пріоритетних завдань: створення єдиного репозиторію програмного забезпечення у сфері інформаційної безпеки з метою його належного використання органами державної влади та органами місцевого самоврядування; організація ефективної комунікації, убезпечення передачі інформаційних потоків у кіберсередовищі держави; цифровізація управлінських і технологічних процесів державного управління; централізоване здійснення моніторингу та контролю систем інформаційної безпеки державного управління; забезпечення захисту інформації, яка отримується із зовнішнього середовища органами публічної влади; гарантування належного рівня безпеки і захисту інформаційно-комунікативної інфраструктури органів державної влади.

Розроблено рекомендації органам публічної влади щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України: центральним органам виконавчої влади запровадити координовану систему ситуаційних центрів у практичну діяльність органів влади у сфері інформаційної безпеки; уповноваженим підрозділам органів влади сформувати та постійно оновлювати ведення інформаційних баз даних; суб’єктам сервісної діяльності забезпечити можливість дистанційного доступу громадян до інформації про порядок та результати отримання послуг з різних напрямів; здійснювати онлайн-ідентифікацію усіх бажаючих при використанні особистих кабінетів на сайтах органів державної влади; застосовувати принцип цифрової взаємодії за допомогою хмарних сервісів, використовувати сервіс-орієнтовану архітектуру як основу для інтеграції інформаційних мереж при

застосуванні сервісного принципу надання інформаційних безпекових послуг; забезпечувати цифрову підтримку операційної діяльності щодо виконання встановлених процедур сервісного обслуговування.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Шайхет С. О. Інформаційна безпека як сервіс належного врядування / Сергій Шайхет // Актуальні проблеми державного управління : зб. наук. пр. ОРІДУ. – Одеса : ОРІДУ НАДУ, 2016. – Вип. 3 (67). – С. 97–101.

2. Шайхет С. О. Інформаційна безпека як сервіс сучасної держави / С. О. Шайхет // Наукові розвідки з державного та муніципального управління : зб. наук. пр. – Київ : АМУ, 2016. – Вип. 2. – С. 228–239.

3. Карпенко О. В. Застосування поняття “безпека” в галузі державного управління: етимологія та сучасне тлумачення / О. В. Карпенко, С. О. Шайхет // Науковий вісник Академії муніципального управління : зб. наук. пр. – Київ : АМУ, 2016. – Вип. 3. – С. 26–35. – (Серія “Управління”). – Авторські с. 28–33.

4. Шайхет С. О. Надання інформаційної безпеки як складова сервісної діяльності органів влади: нормативно-правове забезпечення в Україні / С. О. Шайхет // Науковий вісник Академії муніципального управління : зб. наук. пр. – Київ : АМУ, 2016. – Вип. 4. – С. 184–192. – (Серія “Управління”).

5. Шайхет С. О. Концепція Community Policing як інструмент ефективної взаємодії національної поліції, місцевих органів влади та громад: український та зарубіжний досвід упровадження / С. О. Шайхет, Ю. В. Карпенко // Вісн. НАДУ. – 2018. – № 4 (91). – С. 78–86. – (Серія “Державне управління”). – Авторські с. 80–86.

6. Karpenko O. Services Digitizing in the Sector of Public Policy for Employment Provision and Security / O. Karpenko, N. Savchenko, S. Shaykhet // Economic Paper : Special issue Research of the Ukrainian Economy, Politics, Society and Environment. – Kobe (Japan) : Kobe-Gakuin University (神戸学院経済学論集), 2018. – Vol. 50. – N 3. – P. 89–98. – Авторські с. 95–98.

Праці, які додатково відображають наукові результати дисертації

7. Карпенко О. В. Маніпулятивний вплив на колективну підсвідомість як загроза інформаційній безпеці України / О. В. Карпенко, С. О. Шайхет // Актуальні проблеми менеджменту зовнішньоекономічної діяльності підприємств України в контексті євроінтеграційних процесів : зб. матеріалів II Всеукр. наук.-практ. інтернет-конф., Миколаїв, 26 жовт. 2016 р. – Миколаїв : МНУ ім. В. О. Сухомлинського, 2016. – С. 93–95. – Авторські с. 94–95.

8. Шайхет С. О. Теоретичні аспекти вітчизняної сфери надання управлінських послуг / С. О. Шайхет, А. М. Козубенко // Реформування публічного управління та адміністрування: теорія, практика, міжнародний досвід : матеріали Всеукр. наук.-практ. конф. за міжнар. участю, Одеса, 28 жовт. 2016 р. – Одеса : ОРІДУ НАДУ, 2016. – С. 28–29. – Авторські с. 29.

9. Шайхет С. О. Перспективи нормативно-правового забезпечення сфери захисту електронних комунікацій та протидії кіберзлочинності / С. О. Шайхет // Правові аспекти публічного управління: теорія та практика : матеріали VIII наук.-практ. конф. (Дніпро, 8 груд. 2016 р.). – Дніпро : ДРІДУ НАДУ, 2016. – С. 198–201.

10. Шайхет С. О. Кібербезпека: сучасний стан та перспективи розвитку в Україні / С. О. Шайхет // Національні цінності й національні інтереси в системі публічного управління : матеріали наук.-практ. конф. за міжнар. участю : у 2 т. (Київ, 12 жовт. 2017 р.) / за заг. ред. В. С. Куйбіди, І. В. Розпутенка. – Київ : НАДУ, 2017. – Т. ІІ. – С. 120–123.

АНОТАЦІЯ

Шайхет С. О. Механізми реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. – Національна академія державного управління при Президентові України, Київ, 2019.

У дисертації здійснено обґрунтування теоретичних засад та практичних рекомендацій щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України. Запропоновано та обґрунтовано сукупність механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України в контексті розбудови цифрового суспільства, базовими серед яких визначено: нормативно-правові, організаційно-технологічні, ресурсно-управлінські та програмно-цільові. На основі аналізу досвіду країн Євросоюзу та США в галузі захисту інформації та розвитку стратегій кібербезпеки визначено основні тенденції в комплексному формуванні національної системи інформаційної безпеки. Охарактеризовано сучасний стан та перспективи розвитку кібербезпеки в Україні. Наголошено на необхідності реалізації в Україні концепції “Community Policing” як сервісу провадження інформаційної безпеки та ефективного інструменту взаємодії Національної поліції, місцевої влади та населення об’єднаних територіальних громад у контексті децентралізації влади та реформування правоохоронних органів. Доведено, що створення безпечного інформаційного простору державного управління здійснюється шляхом формування цілісної системи інформаційної безпеки органів державної влади, для чого визначено низку пріоритетних завдань. Розроблено рекомендації щодо вдосконалення механізмів реалізації сервісно-орієнтованої державної політики у сфері інформаційної безпеки України.

Ключові слова: інформація, інформаційна безпека, інформаційний простір, державне управління, кібербезпека, кіберпростір, сервісна діяльність, сервісно-орієнтована державна політика, цифровізація, цифрові технології.

ANNOTATION

Shaikhet S. O. Mechanisms for implementation of service-oriented public policy in the field of information security of Ukraine. – Qualifying scientific work on the rights of manuscripts.

Thesis for a Candidate Degree in Public Administration, specialty 25.00.02 – Mechanisms of Public Administration. – National Academy for Public Administration under the President of Ukraine, Kyiv, 2019.

In the dissertation the substantiation of theoretical principles and practical recommendations for improving the mechanisms of service-oriented public information security policy implementation has been substantiated. The set of mechanisms of service-oriented public information security policy implementation in the context of digital society building is suggested and substantiated; the basic ones among them are: normative-legal, organizational-technological, and resource-management.

The set of mechanisms of implementation of service-oriented state policy in the field of information security of Ukraine in the context of building a digital society is suggested and substantiated. The basic ones among them are: normative-legal, organizational-technological, resource-management, and program-target.

The algorithm of the organization of state authorities system's information security is improved by separating two interconnected components, one of which is responsible for the content of the state digital (electronic) resources, and the other – for the security of this information (creation of safe conditions for access, receiving, transmitting, exchange and protection of information regardless of its content).

The conceptual-categorical apparatus of public administration science was further developed by introduction into the scientific course of the author's interpretation of the terms: "information security", "public information security policy implementation", "service-oriented public information security policy". The inexpediency of further use in the conceptual-categorical apparatus of state-controlled science of the phrase "security" is used in the context of further research, but the term "security", "implementation of security" or "implementation of safety" is suggested in further researches.

The existing legal framework for the information security regulation in Ukraine has been systemized. The priority directions, which require additional legal regulation of construction of the system of modern and high-performance information-telecommunication systems and data centers, are determined. The foreign achievements of implementing information security models as a national interests protection service (on the example of the EU and the USA) have been generalized, resulting in the absence of common standards, since the security category is largely conditioned by internal and external political goals and objectives of a particular country.

It is established that the main features of the development of service-oriented public information security and technologies policy are based on the understanding of the information security industry as a service of the national security system, the formation and implementation of an integrated public administration system, development and support of the organizational structure and the necessary legal

framework. The current state and prospects of cyber security development in Ukraine are characterized, which gives grounds for asserting that the problems of domestic information security experience, information security system organization, and its management require a holistic technological, legislative, and infrastructural revision.

It is proved that in the issue of developing the conceptual foundations of information security modeling it is important to analyze the cyberspace and the main factors influencing its functioning. One of the basic directions is the creation of mathematical models that allows to obtain quantitative information security indicators (degree of information security threats, information risks analysis, assessment of the protection measures effectiveness), the creation of special methods to ensure the cyberspace stability, or its areas under the influence of threats that will enable the implementation: topological structure analysis and the development of recommendations for its change, methods and specific algorithms for their implementation; new cryptographic protection methods, based not only on purely computational mechanisms of the stability implementation, but also on the benefits of multi-level communications architecture and a large number of users; methods of implementing information security on the basis of social services to combat cyber attacks using special procedures for analyzing group behavior.

The necessity of implementation the "Community Policing" concept in Ukraine as an information security service and an effective tool for interaction of the National Police, local authorities, and communities in the context of power decentralization and law enforcement bodies reforming is substantiated. A factual analysis of the experience of foreign countries in "Community Policing" concept implementation (based on the example of the United States, Great Britain, Kenya, India and Japan) has been carried out. Recommendations for the mechanisms of "Community Policing" concept implementation in Ukraine are formulated.

It is proved that the creation of a safe information space for public administration is carried out through the formation of public authorities' integrated information security system, which requires the solving of such priority tasks. Recommendations for improving the implementation mechanisms of service-oriented public information security policy of Ukraine are developed: for the central executive authorities to introduce the application of a coordinated system of situational centers into the practical activities of the information security authorities; for the authorized subdivisions of authorities to form and constantly update the maintenance of information databases; for the service activity entities to provide for citizens the remote access possibility to information about the order and results of receiving services in different directions; to carry out on-line identification for personal cabinets usage on the public authorities sites; to apply the digital interaction principle through cloud services, and as a basis for information networks integration, using the service-oriented principle of providing information security services to use service-oriented architecture; to provide digital support for operating activities in relation to the implementation of established maintenance procedures.

Key words: information, information security, information space, public administration, cybersecurity, cyberspace, service activities, service-oriented public policy, digitalisation, digital technologies.

Підп. до друку 22.07.2019.
Формат 60 х 84/16. Обл.-вид. арк. 1,4.
Ум.-друк. арк. 1,16.
Тираж 100 пр.

Свідоцтво серії ДК № 1561 від 06.11.2003.

Віддруковано з оригінал-макета в управлінні з видавничої діяльності
Національної академії державного управління
при Президентові України
03057, Київ, вул. Антона Цедіка, 20, тел. 456-77-95.