ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ
ІНСТИТУТ ДЕРЖАВНОГО УПРАВЛІННЯ
Кафедра публічного управління та адміністрування

Володін Сергій Владиславович

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Спеціальність: 074 Публічне управління та адміністрування

АВТОРЕФЕРАТ

магістерської роботи на здобуття наукового ступеня
магістра публічного управління

Миколаїв – 2019

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В Україні, як і в усьому світі, проблеми забезпечення системи безпеки держави, суспільства й особистості все більше виходять на перший план у державній політиці та державному управлінні.

Інформаційна безпека належить до числа пріоритетних цілей сучасної держави і є одним з основних факторів його стабільного розвитку. Очевидно, що системні дефекти та збої у функціонуванні механізмів забезпечення інформаційної безпеки можуть привести до соціально-політичних, економічних і техногенних зрушень, здатних підірвати можливість органів державного управління належним чином здійснювати свої основні функції.

На сьогодні інформаційна безпека суспільства в цілому та його структурних частин є досить актуальною проблемою, що пов'язано з тим фактом, що питання інформації, а особливо соціальної інформації, набули в даний час особливого значення.

Сучасний етап розвитку суспільства характеризує зростаюча роль інформаційної сфери, що виступає важливим чинником суспільного життя та, багато в чому, окреслює подальші перспективи успішного здійснення соціальних, політичних, державних та управлінських перетворень у вітчизняному суспільстві. Крім того це обумовлено й такими основними обставинами як: посилення інтенсивного розвитку інформаційної інфраструктури та, в першу чергу, інформаційно-телекомунікаційних систем, засобів та систем зв'язку, інтеграцією світовий інформаційний простір, а також, подальшою інформатизацією практично всіх без виключення сторін суспільного життя, діяльності державних органів влади та управління, що істотно посилюють залежність ефективного функціонування суспільства й держави від стану інформаційної сфери; індустрії інформатизації, телекомунікації та зв'язку, демократизації тощо. Щодо змістовного плану, то інформаційна безпека є складовою частиною національної безпеки. В її структурі інформаційній безпеці відведено особливе місце, що обумовлено тим, що будь-які види безпеки не можуть бути реалізовані без належного інформаційного забезпечення. Цінність інформації може бути як позитивною, так і негативною, що пояснюється тим, що інформація є універсальним інструментом прогресу людства, глобальним та найбільш дефіцитним ресурсом розвитку сучасного суспільства, однією з головних загальнолюдських та національно-державних цінностей. Інформаційні ресурси та процеси – це першопричина багатьох соціальних конфліктів, криз та посилення напруги у суспільстві. Очевидно, що порушення існуючих інформаційних законів світобудови може виявитися фатальним для існування людської цивілізації, що також підкреслює важливість та актуальність обраної теми дослідження.

Загальні питання, що стосуються генезису інформаційного суспільства, аналізуються у працях В. Абрамов, В. Бегма, К. Варивода, Б. Кормич, В. Політанський та ін. Проблеми комунікації в управлінні досліджують такі науковці, як І. Березовська, К. Беляков, О. Коротич, І. Рамоне та ін. Питання державного управління у сфері безпеки (національної, регіональної тощо), її забезпечення організаційними, інформаційними та іншими методами розглядаються у працях С. Бєлай, О. Вербицький, А. Качинський, З. Коваль, О. Рябоконь та ін. Проте їх наукові праці здебільшого присвячені теоретичним проблемам щодо розвитку інформаційного суспільства, правового регулювання інформаційної сфери з боку держави чи виключно технічним аспектам упровадження інформаційних технологій. У той же час, залишається недостатньо розробленою проблема реалізації інформаційної безпеки держави в умовах становлення інформаційного суспільства з урахуванням їх дихотомічності та необхідності переходу до сучасних принципів публічного адміністрування та міжсекторної взаємодії, що й актуалізує тему дослідження, визначає його мету та завдання.

Нормативно-правову та інформаційну базу дослідження склали нормативно-правові акти, пов'язані з реалізацією державної політики у сфері інформаційної безпеки в Україні, зокрема Міністерством інформаційної політики України, а також наукові

напрацювання в означеній сфері.

Об'єкт дослідження – процес реалізації державного управління у сфері інформаційної політики.

Предмет дослідження – державна політика щодо сфери інформаційної безпеки в Україні.

Мета і завдання дослідження. Метою дослідження є науково-теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення механізмів державної політики у сфері інформаційної безпеки в Україні.

Досягнення визначеної мети зумовило необхідність вирішення таких завдань:

–охарактеризувати сучасні наукові підходи до розуміння сутності інформаційної безпеки;

–з'ясувати зміст інформаційної безпеки і її місце в системі державного управління;

–узагальнити зарубіжний досвід державної політики інформаційної безпеки та можливості його використання у вітчизняних умовах;

–проаналізувати стан дії механізмів державної політики у сфері інформаційної безпеки в Україні;

–визначити шляхи вдосконалення організаційно-правових механізмів державної політики у сфері інформаційної безпеки України;

–обґрунтувати новітні функціонали системи державного управління у сфері інформаційної безпеки України.

Методи дослідження. Цілісність дослідження забезпечують системний підхід. Для теоретичного осмислення різних аспектів проблеми застосовуються аналіз і синтез (можливості адаптації світових зразків в Україні із організації єдиної інформаційно-комунікативної інфраструктури, е-уряду), моделювання (визначення моделі державного регулювання інформаційної сфери суспільства та міжсекторної взаємодії в цій сфері), абстрагування й узагальнення (визначення шляхів удосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки України, порівняння й уточнення новітніх функціоналів системи держу правління нею).

Наукова новизна роботи полягає в тому, що національні інтереси, загрози їм, управління цими загрозами реалізуються лише через інформаційну сферу.

вперше:

виявлено та обґрунтовано, що людина та її права, інформація та інформаційні системи та права на них – є основними об'єктами не лише національної безпеки в інформаційній сфері, але й головними елементами усіх об'єктів безпеки у всіх галузях;

удосконалено:

доведено, що інформаційна складова – притаманна будь-якій сфері життєдіяльності суспільства;

набули подальшого розвитку:

інтенсивне впровадження інформаційних технологій у всі сфери життя й діяльності сучасного суспільства, ріст питомої ваги інформаційної безпеки щодо забезпечення цілісності держави призвели до того, що інформаційні ресурси почали вважатися таким же багатством країни, як і її корисні копалини, виробничі потужності та інтелектуальний потенціал.

Теоретичне значення роботи полягає в розробленні питань, пов'язаних з вивченням особливостей державної політики у сфері інформаційної безпеки.

Практичне значення отриманих результатів полягає у тому, що наукові узагальнення доведені до рівня конкретних пропозицій. Висновки, отримані у результаті дослідження, мають важливе значення для подальшої теоретичної розробки питання публічно-управлінської взаємодії в умовах модернізації й інформатизації українського суспільства. Рекомендації та пропозиції, викладені в роботі, можуть використовуватися в діяльності органів державної влади як такі, що стосуються, по-перше, оптимізації організаційно-функціональної структури органів виконавчої влади загальної та спеціальної

компетенції, а по-друге, активного залучення громадськості до державного управління у сфері інформаційної безпеки.

Крім того, положення та висновки магістерської роботи можуть бути використані для подальшого науково-теоретичного дослідження особливостей забезпечення належного рівня інформаційної безпеки в державі, а також у навчальному процесі – під час розроблення та викладання курсів та спецкурсів з державного управління, політології, інформаційних технологій, публічного управління та адміністрування, тощо у вищих навчальних закладах, що здійснюють підготовку, перепідготовку та підвищення кваліфікації державних службовців та осіб місцевого самоврядування.

Структура дослідження. Структура та обсяг магістерської роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків. Повний обсяг роботи становить 112 сторінок, з них 93 – основного тексту.

ОСНОВНИЙ ЗМІСТ МАГІСТЕРСЬКОЇ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовано мету та основні завдання, об'єкт і предмет, методи дослідження, висвітлено наукову новизну і практичне значення виконаної роботи. Наведено результати апробації основних положень та особистий внесок автора дослідження.

У першому розділі «*Теоретичні основи дослідження інформаційної безпеки в системі державного управління»* висвітлено історію поняття «інформаційна безпека» у вітчизняній та зарубіжній науковій думці, охарактеризовано особливості інформаційної безпеки в зарубіжних країнах.

Підрозділ 1.1. «Теоретичні підходи щодо поняття та змісту «інформаційної безпеки» в державному управлінні» присвячений аналізу історичних етапів розвитку поняття «інформаційна безпека».

Наголошено, що розуміння та сприйняття сутності змісту поняття «інформаційна безпека» – це важливе завдання наукового аналізу. Будь-яке вчення лише тоді досягає необхідного рівня зрілості та досконалості, коли відбувається розкриття сутності досліджуваного явища, наявна можливість передбачити майбутні зміни не лише у сфері досліджуваних явищ, а й у сфері сутностей.

Зроблено висновок, що пізнання сутності інформаційної безпеки є можливим лише на основі абстрактного мислення, створення теорій досліджуваного предмету, усвідомлення внутрішнього змісту, виявлення характерних ознак, розкриття сутнісних характеристик поняття, що піддається вивченню.

Встановлено, що інформаційна безпека – це складовий компонент загальної проблеми інформаційного забезпечення людини, держави та суспільства. Вона орієнтується на здійснення захисту значимих чи вже згадуваних суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається за допомогою практичної діяльності, здійснення наукових досліджень, а також нормативно-правових документів.

У підрозділі 1.2. «Зарубіжний досвід інформаційної безпеки в публічному управлінні» розкрито основні напрями формування, становлення та забезпечення інформаційної безпеки в зарубіжних країнах.

Встановлено, що зміни, котрі пов'язані з особливостями розвитку інформаційного суспільства, стосуються всіх без виключення соціокультурних інститутів та стверджують принципово новий спосіб життя людини.

Наголошено, що за умов формування глобального інформаційного суспільства людині необхідно вирішувати завдання щодо освоєння принципово нового простору.

Зроблено висновок, що досвід останніх десятиліть є підтвердженням того, що на роль лідерів у сучасному соціально-економічному розвитку претендують саме ті країни, які вже мають високий рівень освіти, науки, охорони здоров'я, культури та духовності. Власну інформаційну політику ведуть більшість сучасних держав світу, однак обсяги їхньої

діяльності у вказаній сфері є залежними від поставлених завдань й рівня зацікавленості певної країни в інтеграції щодо глобальної системи комунікації, від особливостей історичних чинників, політичного та економічного розвитку, фінансових та матеріальних ресурсів.

У другому розділі «Аналіз механізмів державної політики у сфері інформаційної безпеки» визначені основні види, форми та особливості функціонування механізмів державної політики щодо сфери інформаційної безпеки.

У підрозділі 2.1. «Аналіз стану дії організаційно-правових механізмів державної політики у сфері інформаційної безпеки» визначено, що державна інформаційна політика має відбивати нагальні питання, що склалися у міжнародній сфері й сфері інформаційної безпеки тощо.

Необхідним є забезпечення законодавчого захисту прав й інтересів всіх суб'єктів інформаційних взаємовідносин.

Встановлено, що найскладнішими тут є такі завдання, котрі передбачають гармонійне забезпечення інформаційної безпеки держави, особи та суспільства з одночасним виокремленням нагальних пріоритетів, до яких варто віднести створення/відновлення основних точок захисту системи національної безпеки щодо інформаційної сфери, практичну реалізацію наведеної вище схеми формування ефективної системи інформаційної безпеки держави, перегляду списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків й рівнів їх інтенсивності.

Зроблено висновок, що основні акценти державної інформаційної політики мають базуватись на забезпеченні права на достовірну, повну й своєчасну інформацію, свободу слова й інформаційної діяльності в національному інформаційному просторі, недопущенні втручання в зміст й внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до положень Основного закону; збереженні й вдосконаленні вітчизняного національного інформаційного продукту й технологій, вітчизняних національно-духовних і культурних цінностей; забезпеченні інформаційної й національно-культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки й розвитку ресурсів науково-технічної продукції й інформаційних технологій.

У підрозділі 2.2. «Сучасні механізми міжсекторної взаємодії у сфері інформаційної безпеки» показано, що ситуація, що склалася в Україні з кінця 2013 року вказала на низьку ефективність державного управління інформаційною безпекою в умовах інформаційно-психологічного протиборства та ще раз довела, що забезпечення національної безпеки держави це справа не лише органів державної влади, а й усього суспільства і кожного громадянина.

Наголошено, що в сучасних умовах стрімкого зростання рівня загроз національній безпеці України, висока активність інститутів громадянського суспільства слугує найкращим доказом того, що сьогодні громадськість не бажає лишатися пасивним спостерігачем в такий надскладний час для Української держави.

Зроблено висновок, що між секторальна взаємодія та недержавний сектор своїми діями реально довів, що він спроможний ефективно та оперативно вирішувати нагальні питання забезпечення національної безпеки України. Такий безпрецедентний досвід дає підстави розглядати неурядові організації як суб'єкти забезпечення інформаційної безпеки, а налагодження взаємодії державних інститутів з неурядовими організаціями може слугувати одним з чинників підвищення ефективності державного управління інформаційною безпекою.

У третьому розділі «Напрями вдосконалення організаційно-правових механізмів державної політики у сфері інформаційної безпеки» обґрунтовані правові основи і напрямки діяльності у сфері інформаційної політики та безпеки в Україні; визначено основні проблеми та шляхи їх вдосконалення, що впливають на формування публічної

політики в Україні.

У підрозділі 3.1. «Шляхи вдосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки» визначено, що вплив інформаційно-комунікаційних технологій на свідомість людини, процеси формування громадської думки дозволяють втручатися у розвиток політичних процесів, формування державної політики, вироблення й прийняття державних і управлінських рішень.

Виявлено основні проблеми державного управління забезпеченням інформаційної безпеки України, до яких належать такі: забезпечення життєво значущих потреб об'єктів інформаційної безпеки України в сучасних умовах інформаційно-психологічного протиборства, що зумовлені браком систематизованих знань про сучасні методи та форми інформаційно-психологічного протиборства, аналітичної інформації та відповідних ресурсів, необхідних для ефективного реагування на загрози інформаційній безпеці; концептуально-доктринального визначення інформаційно-психологічної безпеки; швидка адаптація нормативно-правової бази у сфері інформаційної безпеки з урахуванням появи нових викликів, загроз, небезпек інформаційно-психологічного характеру, а також наявних розривів в організації діяльності суб'єктів забезпечення інформаційної безпеки України; оптимізація структури і функцій системи забезпечення інформаційної безпеки; удосконалення механізмів забезпечення інформаційної безпеки.

Зроблено висновок, що в Україні система державного управління забезпеченням інформаційної безпеки залишається остаточно не сформованою й не готовою діяти як єдина функціональна структура. На сьогодні уповноважені відомства здійснюють лише окремі види забезпечення інформаційної безпеки, що знижує можливу інтегральну ефективність дій. Це може також призвести до небезпечної різноспрямованості зусиль державного апарату у сфері забезпечення інформаційної безпеки.

У підрозділі 3.2. «Обґрунтування новітніх функціоналів системи державного управління у сфері інформаційної безпеки» показано, що інформаційний простір має ґрунтуватися на засадах відкритості, об'єктивності інформації щодо внутрішнього та зовнішнього становища, на законодавчому рівні повинна проводитися систематична робота щодо вдосконалення законодавствав інформаційній сфері, лише такими методами впливів державна влада виявиться спроможною сформувати демократично-орієнтованого громадянина, котрий буде сприяти розвитку духовності, культури, піднесенню самосвідомості, соціальної та політичної ідентичності так і досягнення соціального ефекту – формуванню довіри до влади, громадянської активності та відповідальності.

Встановлено, що державне регулювання політико-правовими аспектів інформаційної безпеки залишається найбільш неврегульованою сферою державної управлінської діяльності й потребує суттєвого вдосконалення взаємодії, координованості та узгодженості дій і рішень всіх гілок влади з питань забезпечення інформаційної безпеки України. В гібридній війні проти України основні зусилля перенесені на сектор інформаційної безпеки, саме цей сектор найбільше потерпає від інформаційних атак і потребує ефективних державно управлінських підходів для організації її забезпечення. Тому Україні вкрай необхідна система забезпечення інформаційної безпеки. В умовах єдиного інформаційного простору питання формування су спільної думки, суспільно-психологічного настрою не може бути віддано на відкуп інформаційним джерелам зарубіжних країн. Україна в своїй державній політиці в умовах зовнішнього та внутрішнього агресивного ІПВ повинна широко застосовувати світовий досвід захисту національної інформаційно-психологічної сфер.

Зроблено висновок, що діяльність органів державної влади із забезпечення інформаційної безпеки повинна ґрунтуватись перш за все на перспективних напрямах, що відповідають вимогам сьогодення: Концепції державної інформаційної політики в умовах зовнішнього та внутрішнього агресивного ІПВ; розгортанні широкої та багатопрофільної підготовки фахівців з інформаційної та інформаційно-психологічної боротьби; наповнення вітчизняного та світового інформаційного простору своїм інформаційним продуктом.

ВИСНОВКИ

Під час переходу від індустріального до інформаційного суспільства з традиційними ресурсами – матеріальними, енергетичними, технічними тощо – відбувається різке зростання ролі ресурсів інформаційних та інтелектуальних. Знання та інформація набувають значення стратегічного ресурсу суспільства, який визначає перспективи його економічного, соціального, культурного тощо розвитку в новому тисячолітті. Крім того, інформаційні ресурси – є об'єктом власності конкретних юридичних та фізичних осіб, вони мають потреби щодо захисту, забезпечення правового режиму їхнього володіння, розпорядження й користування. Отже, у цей час життя суспільства характеризується всезростаючою роллю інформаційної сери, яка виступає сукупністю інформації, інформаційної інфраструктури, суб'єктів, що здійснюють процеси збирання, формування, поширення та використання інформації, а також системи регулювання суспільних взаємовідносин, що виникають при цьому.

У результаті проведеного дослідження стало можливим дійти нижчевикладених висновків.

1. Аналіз зарубіжних і вітчизняних джерел щодо проблем інформаційної політики та безпеки дає можливість стверджувати про наявність різних підходів щодо визначення поняття та змісту політики інформаційної безпеки. Наявність суттєвої різниці пояснюється існуючими відмінностями щодо розвитку інформаційної сфери та різними визначеннями пріоритетів національної безпеки, складовою якої на сьогодні є й інформаційна безпека (кібербезпека). Крім того такі відмінності знаходять прояв на і рівні мовних систем (наявність різної термінології), так і в концептуальному плані. Зарубіжна наука робить акцент на захисті інформації та даних у віртуальних мережах, в той час як основна характеристика інформаційної безпеки в більшості наукових шкіл – це захист суспільної свідомості населення від шкідливих інформаційних впливів держави. Відмінності в існуючих підходах знаходять свій прояв також і на рівні виокремлення об'єктів інформаційної безпеки. Якщо вітчизняна наука відносить до таких державу, суспільство та людину, то західна наука веде мову про комп'ютерні мережі та інформацію, що міститься в них.

2. З'ясовано зміст інформаційної безпеки, який правомірно розглядати в межах дихотомічності інформаційної сфери, елементами якої визнано сукупність інформації, засобів її виробництва, обробка та зберігання, інформаційний простір й інфраструктура, суб'єктів, що здійснюють збір, формування, розповсюдження і використання інформації, а також системи державного управління, виникаючих при цьому державно-владних відносин. Така система передбачає здійснення цілеспрямованого й організуючого впливу керованої підсистеми (держави) на сферу інформаційної безпеки шляхом застосування правового й організаційного інструментарію, який становить підґрунтя для класифікації механізмів державної політики в означеній сфері.

3. Узагальнення та систематизація зарубіжного досвіду державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства дозволяє констатувати, що державне управління забезпеченням інформаційної безпеки України повинно ґрунтуватися на врахуванні відповідних концептуальних засадах захисту і наступу в цій галузі, а також необхідно мати для цього відповідні політичні, економічні й технічні можливості. При цьому слід враховувати культурно-цивілізаційні особливості суб'єктів інформаційно-психологічного протиборства, адже релігія і культура, а також підсвідоме архе, яке лежить в їхній основі, не менш важливі для сучасних стратегій взаємодії та впливу, ніж досить очевидні промислові та фінансові реалії життя.

4. Під час аналізу дії правового й організаційного механізмів державної політики у сфері інформаційної безпеки в Україні встановлено таке:

1) відсутня єдина інфраструктура зв'язку й інформації державних органів влади,

побудована на єдиних стандартах і платформах, ускладнюючи тим самим процес своєчасного впровадження сучасних технологій;

2) діючі інформаційні системи органів державної влади були розроблені і введені в експлуатацію в різний час, що й зумовило несумісність програмно-технічних рішень сьогодні;

3) вітчизняна правова база відзначається розпорошенням і дублюванням напрямків діяльності органів виконавчої влади загальної та спеціальної компетенції щодо забезпечення інформаційної безпеки тощо.

5. Визначено шляхи вдосконалення організаційно-правових механізмів державної політики у сфері інформаційної безпеки України, які передбачають адаптацію в Україні світового досвіду (зокрема, США) щодо створення єдиної державної інформаційно-комунікаційної інфраструктури. Вона, з одного боку, передбачає формування стійкої організаційно-інформаційної мережі та системи, а з другого – покликана забезпечити системне «виробництво – споживання – захист» інформаційних і комунікаційних засобів, продуктів і послуг. При цьому уточнено модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки.

6. На підставі аналізу стану організаційно-функціонального та правового забезпечення державної політики у сфері інформаційної безпеки обґрунтовано новітні функціонали системи державного управління, покликані забезпечити комплексне дотримання основоположних державноуправлінських принципів. Їх урахування дозволило запропонувати напрямки вдосконалення основної та допоміжно-функціональної організаційної будови інформаційної політики України. Це можливо шляхом формування його представництв на регіональному рівні, як установ з узгодженим розподілом повноважень і сфер відповідальності, а також створення регіональних громадських рад при них.

Розбудова системи забезпечення інформаційної безпеки сучасної держави в умовах інформаційно-психологічного протиборства має здійснюватися на основі синтезу положень сучасних теорій, а саме: теорії національної безпеки – парадигм захищеності та самореалізації, синергетичного та діяльнісного підходів до розуміння безпеки; теорії інформаційної безпеки, що обґрунтовує підходи до захисту національного інформаційного простору; теорії глобалістики, що обґрунтовує перехід від державного управління до глобального та публічного управління; теорії інформаційної війни, яка розглядає адаптивні механізми й архетипи інформаційної війни; теорії спеціальних інформаційних операцій, яка розглядає об’єкти та етапи здійснення вказаних операцій; інституціоналізму, який підкреслює роль держави і громадянського суспільства в розробленні інформаційної політики; індустріальної теорії, які в сукупності змінюють бачення ролі інформаційних чинників безпеки.

Визначено, що система державного управління інформаційною безпекою як складова системи забезпечення інформаційної безпеки виконує основні функції: планування, організації, координації і контролю. Водночас функції управління та адаптації системи забезпечення інформаційної безпеки реалізовуються системою державного управління забезпеченням інформаційної безпеки, яка, у свою чергу, є структурним елементом системи державного управління інформаційною безпекою.

Наголошено на пропозиціях щодо вдосконалення механізмів державної політики інформаційної безпеки України в умовах інформаційно-психологічного протиборства, зокрема на сучасному етапі необхідно:

– надати інформаційно-психологічній безпеці статусу пріоритетного напряму в роботі органів законодавчої та виконавчої влади;

– упровадити в державно-управлінську практику рефлексивну модель організації системи державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства, що дасть змогу системно впливати на інформаційну безпеку Української держави та забезпечити нестандартність системно-

інституційної поведінки суб'єктів інформаційної безпеки для запобігання негативним зовнішнім інформаційно-психологічним впливам;

– у рамках реалізації функції адаптації системи забезпечення інформаційної безпеки до нових викликів і загроз:

а) розширити перелік викликів і загроз інформаційно-психологічного характеру та конкретизувати положення нормативно-правових актів щодо до протидії інформаційно-психологічним впливам;

б) оптимізувати структуру та функції системи забезпечення інформаційної безпеки України з урахуванням сучасних викликів і загроз національним інтересам України в інформаційній сфері та вимог до систем забезпечення безпеки креативного типу, а саме: до структури системи забезпечення інформаційної безпеки включити: механізм інформаційно-аналітичного забезпечення інформаційно-психологічної безпеки, що охоплює мережу аналітичних інститутів (державних і недержавних); механізми взаємодії держави з інститутами громадянського суспільства, з міжнародними організаціями та структурами регіональної безпеки; до переліку завдань щодо реалізації основоположної функції додати завдання вжиття заходів випереджального впливу на причини, що породжують загрози національним інтересам в інформаційній сфері;

в) удосконалити механізм інформаційно-аналітичного забезпечення шляхом розробки та впровадження в державно-управлінську практику паспортів загроз інформаційно-психологічній безпеці;

г) удосконалити механізм державного реагування шляхом розробки та впровадження в державно-управлінську практику технологій державного реагування на загрози інформаційно-психологічній безпеці;

д) удосконалити механізм кадрового забезпечення шляхом упровадження інноваційних підходів до формування практико орієнтованого навчання фахівців-управлінців у сфері інформаційної безпеки України.

Анотація

У межах дослідження окреслено історичні особливості виникнення й становлення поняття «інформаційна безпека», обґрунтовано світовий досвід функціонування державної політики у сфері інформаційної безпеки й можливості його використання у вітчизняних умовах, а також перспективи вдосконалення механізмів державної політики інформаційної безпеки. Результатом дослідження став розвиток теоретичних і практичних аспектів функціонування механізмів державної політики інформаційної безпеки України. Доведено особливості інформаційної безпеки в процесах формування вітчизняної державної політики. Обґрунтована необхідність підвищення ефективності механізмів інформаційної безпеки в сучасному українському суспільстві.

Охарактеризовано проблематику та джерельну базу дослідження інформаційної безпеки у формування публічної політки України. Встановлено, що незважаючи на наявність низки наукових праць та досліджень щодо розвитку інформаційної безпеки у формуванні публічної політики існує нагальна потреба здійснити ґрунтовне дослідження особливостей такого формування та розвитку.

Визначено основні приклади кращих зарубіжних практик щодо формування та функціонування інформаційної безпеки у публічній політиці та можливі шляхи оптимального використання у вітчизняних умовах. З'ясовано, в більшості розвинутих держав світу існують власні традиції щодо проведення реформ у сфері публічної політики, а зарубіжний досвід для нашої країни є вкрай важливим та актуальним. Наголошено на наявності ряду проблем з якими стикаються під час формування та функціонування механізмів державної політики інформаційної безпеки.

Встановлено, що довгий шлях розвитку, становлення та функціонування призвели до того, що інформаційна безпека посіли вагоме місце в процесах розвитку державної політики більшості зарубіжних країн. Визначено, що незважаючи на існування й

застосування власних методів та засобів забезпечення відкритості й доступності механізмів державної політики інформаційної безпеки, така безпека займає основне місце і являється запорукою ефективного розвитку державної політики та держави в цілому, що є запорукою розбудови демократичного суспільства.

Ключові слова: інформація; безпека; інформаційна безпека; державна політика; публічна політика; механізми державної політики; інформаційний простір; інформаційна небезпека; інформаційна загроза.

Summary

The study outlines the historical peculiarities of the emergence and formation of the notion of «information security», grounded the world experience in the functioning of the state policy in the field of information security and the possibility of its use in domestic conditions, as well as prospects for improving the mechanisms of state information security policy. The result of the study was the development of theoretical and practical aspects of the functioning of the mechanisms of state policy of information security of Ukraine. The peculiarities of information security in the processes of formation of the national state policy are proved. The necessity of increasing the effectiveness of information security mechanisms in the modern Ukrainian society is substantiated.

The problem and source of research on information security in the formation of public policy of Ukraine are described. It has been established that in spite of the existence of a number of scientific works and studies on the development of information security in the formation of public policy, there is an urgent need to thoroughly study the peculiarities of such formation and development.

The basic examples of the best foreign practices concerning formation and functioning of information security in public policy are determined and possible ways of optimal use in domestic conditions. It has been found that in most developed countries of the world there are their own traditions in carrying out reforms in the field of public policy, and foreign experience for our country is extremely important and relevant. It is emphasized that there are a number of problems faced during the formation and functioning of mechanisms of state policy of information security.

It has been established that the long path of development, formation and functioning led to the fact that information security took an important place in the processes of development of state policy of the majority of foreign countries. It has been determined that, despite the existence and application of their own methods and means of ensuring the openness and accessibility of state policy information security tools, such security occupies a central place and is the key to the effective development of state policy and the state as a whole, which is the key to building a democratic society.

Keywords: information; security; informational security; state policy; public policy; mechanisms of state policy; information space; information danger; information threat.