

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ТОРІЧНИЙ ВАДИМ ОЛЕКСАНДРОВИЧ

УДК 351:342.57

**ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ
В УМОВАХ ТРАНСФОРМАЦІЙНИХ ВИКЛИКІВ І ЗАГРОЗ**

25.00.05 – державне управління у сфері державної безпеки
та охорони громадського порядку

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
доктора наук з державного управління

Харків – 2020

Дисертацією є рукопис.

Робота виконана в Національному університеті цивільного захисту України.

Науковий консультант: доктор наук з державного управління, професор **Шведун Вікторія Олександрівна**, Національний університет цивільного захисту України, завідувач кафедри менеджменту навчально-науково-виробничого центру.

Офіційні опоненти: доктор наук з державного управління, професор **ОРЛОВ Олександр Валентинович**, Харківський регіональний інститут державного управління Національної академії державного управління при Президентові України, завідувач кафедри інформаційних технологій і систем управління;

доктор наук з державного управління, доцент **ОРТІНА Ганна Володимирівна**, Таврійський державний агротехнологічний університет імені Дмитра Моторного, в.о. декана факультету економіки та бізнесу;

доктор наук з державного управління, доцент **ГОРНИК Володимир Гнатович** Інститут управління, економіки та природокористування Таврійського національного університету імені В.І. Вернадського, директор.

Захист відбудеться «10» вересня 2020 р. об 11.00 годині на засіданні спеціалізованої вченої ради Д 64.707.03 Національного університету цивільного захисту України за адресою: 61024, м. Харків, вул. Лермонтовська, 28, ауд. 3 (1-й поверх).

З дисертацією можна ознайомитись у бібліотеці Національного університету цивільного захисту України за адресою: 61023, м. Харків, вул. Чернишевська, 94.

Автореферат розісланий «10» серпня 2020 р.

**Учений секретар
спеціалізованої вченої ради**

Н. С. Грабар

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасному світі інформаційний обмін досяг найвищого рівня інтенсифікації, а обсяг одержуваної інформації, такої, що зберігається, переробляється і передається, на даному етапі розвитку людства знаходиться вже у своєму максимумі. Найбільш розвинені країни світу вступають в якісно новий етап цивілізаційного розвитку – інформаційне суспільство. При цьому кожна держава неминуче має враховувати, що не існує універсальних способів для переходу в інформаційне суспільство, для кожної з них існує «свій» самобутній і конкретний спосіб.

Реалізація даного проекту потребує насамперед наявності державної концепції побудови інформаційного суспільства, де чітко й однозначно мають бути позначені ролі його основних акторів, які забезпечують національну безпеку держави в інформаційному просторі.

До факторів, що визначають актуальність державно-управлінського аналізу інформаційної політики держави, слід віднести такі:

По-перше, багато країн у своєму розвитку цілком закономірно йдуть до інформаційного суспільства, і перешкоди, з якими вони стикаються на цьому шляху, вимагають наукового осмислення й ретельного аналізу. У свою чергу вдосконалення інформаційно-комунікаційних технологій призвело до виникнення глобального інформаційного простору, і всі країни мають інтегруватися в цей процес. Останній носить об'єктивний характер, однак при цьому існують серйозні відмінності у підходах. Так, Західна Європа і США підійшли до нього більш підготовленими й відповідно знаходяться найближче до побудови цілісного інформаційного суспільства. Глобальна інформатизація суспільства об'єктивно й безумовно поступово стає своєрідним базисом усього державно-управлінського, соціально-політичного, економічного і науково-технічного розвитку. Водночас процес інформатизації тісно пов'язаний з процесом демократизації, розвитком громадянського суспільства, здатного впливати на прийняття тих чи інших державних рішень. В інформаційному суспільстві має переважати інтерактивний тип комунікації, що обумовлює активне ставлення до інформації та організації інформаційного обміну між суб'єктами інформаційного процесу.

По-друге, інформаційна політика, її розробка та реалізація глобально й перманентно виходять сьогодні на передній план всієї державної політики, оскільки від грамотно розробленої концепції інформаційного забезпечення державної політики та її успішної реалізації багато в чому залежить ефективність роботи всіх державних і громадських структур, і зрештою – їх інформаційна безпека. Інформаційна політика виступає тут як найважливіший

засіб підтримки публічного діалогу державної влади і громадянського суспільства. Державна влада, на наш погляд, може користуватися довірою громадян тільки в тому випадку, якщо одержувач повідомлення є таким же повноправним учасником комунікації, як і ініціатор повідомлення (в даному випадку – держава), а державні інформаційні служби відмовляться у своїй діяльності від технологій односпрямованого впливу на суспільну свідомість. Державне управління інформаційними процесами перш за все необхідне в питаннях, які зачіпають національні інтереси, і в даному аспекті пряме чи непряме втручання держави є закономірним у діалозі перципієнт – реципієнт.

По-третє, не викликає сумніву, що проблема реалізації інформаційної політики, в силу цілої низки причин, нерозривно пов'язана із забезпеченням державної, а відтак і національної безпеки, тому на сучасному етапі розвитку України необхідний комплексний підхід до їх дослідження.

По-четверте, поряд з цим очевидна необхідність власне державно-управлінського аналізу інформаційної політики та механізму її реалізації, тому що саме в цьому конкретному контексті ціла низка проблем не отримали глибокого відображення, оскільки зазначена тематика є досить новою в науці державного управління.

Сьогодні одним із нагальних завдань державного управління в Україні є вироблення ефективної державної інформаційної політики. Це пов'язано в тому числі з тим, що події останнього часу засвідчили, що інформаційна політика держави ще не повною мірою враховує ті досить серйозні зміни, які відбулися й відбуваються в нашій державно-управлінській і політичній реальності.

Проблеми, пов'язані з інформаційною політикою та її реалізацією, в тому числі в умовах перехідного суспільства, були предметом дослідження багатьох науковців, проте деякі з них залишилися маловивченими. Зокрема, наразі недостатньо розробленими є критерії систематизації видів і форм реалізації інформаційної політики та забезпечення державної й національної безпеки, специфіка функціонування інформаційної політики в умовах відносно слабо розвиненої системи комунікацій і можливості інститутів громадянського суспільства впливати на інформаційну політику держави.

Значний внесок у розвиток знань у сфері інформаційного суспільства зробили такі вчені, як Д. Белл, А. Берг, З. Бжезинський, Д. Блюменау, Е. Брандман, П. Браун, Н. Вінер, М. Кастельс, Б. Ківі, Е. Масуда, Д. Тапскотт, Е. Тоффлер, Ф. Уебстер, Г. Хакен, Ю. Харари, К. Шеннон та ін.

Різним аспектам проблеми інформаційного суспільства та забезпечення національної безпеки присвятили свої праці українські автори, серед яких можна виділити А. Барінова, Е. Буравльова, О. Валецьку, О. Власюка, В. Голобуцького, В. Горбуліна, А. Гуза, О. Данільяна, Ю. Древалю, Б. Кормич,

В. Костюка, О. Кохановського, О. Крюкова, В. Ліпкана, С. Луценка, Є. Макаренко, А. Марущака, П. Маслянка, Й. Масляну, Г. Почепцова, О. Радченко, Я. Романовського, О. Сенченко, В. Степанова, В. Тертічку та ін.

Питанням інформаційного забезпечення національної безпеки держави присвятили свої дослідження багато авторів на пострадянському просторі, серед яких можна виділити О. Андрінова, Є. Горелова, І. Дмитрачкова, Д. Іванова, Г. Іващенко, Н. Лапіна, В. Легасова, А. Манойло, О. Музику, Г. Мухіна, Ю. Нісневіча, І. Панаріна, Б. Порфирьєва, Л. Сморгунова, В. Халіпова, А. Федорова та ін.

Також окремі аспекти забезпечення національної безпеки розглядали у своїх роботах такі вітчизняні вчені, як: У. Бережницька, З. Варналій, А. Возженіков, А. Васильєв, В. Геєць, Р. Дацків, А. Качинський, В. Коврегін, В. Мамонова, Р. Науменко, В. Пономаренко, С. Степашин, О. Судакова, С. Тоцький, Ю. Холтунцов, Т. Шуберт, А. Фоміна, І. Яремко та ін.

Питанням державного управління національною безпекою присвячені численні праці вітчизняних і зарубіжних науковців, зокрема, таких, як: О. Береза, Д. Венцковський, В. Колокольцев, М. Криштанович, Я. Малік, В. Манілов, С. Павленко, С. Пирожков, І. Проценко, І. Руснак, Ш. Султанов, О. Соснін, М. Сунгуровський, та ін.

Проте ступінь дослідження проблеми державного управління національною безпекою наразі залишається недостатньо розкритим, наукові праці з цієї проблематики розрізнені, методологічно необ'єднані, у них відсутня єдина цілісна наукова державно-управлінська теорія.

Науково-теоретичним підґрунтям дисертаційної роботи стали праці вітчизняних і зарубіжних учених, присвячені концептуальним засадам державного управління (В. Авер'янов, В. Бакуменко, О. Бойко-Бойчук, В. Голуб, В. Дзюндзюк, А. Дегтяр, С. Домбровська, О. Іваницька, О. Кілієвич, В. Князєв, А. Мерзляк, О. Мордвінов, Н. Нижник, В. Олуйко, Ю. Сурмін та ін.), проблематиці інформаційного забезпечення (П. Бакут, О. Дубас, М. Кастельс), державним інформаційним ресурсам (О. Нестеренко, О. Рубанець, О. Сенченко, Г. Сілкова, В. Яковенко), державній інформаційній політиці (І. Арістова, В. Гусєв, О. Карпенко, В. Конах, О. Манойло), загальним питанням інформаційної безпеки (Ю. Борсуковський, А. Гуз, Б. Кормич, Н. Кунанець, С. Ленков, І. Маракова, А. Момот), правовим аспектам інформаційного забезпечення державної безпеки (С. Бондаренко, К. Беляков, В. Бутузов, А. Венгеров, С. Головань, В. Дурдинець, Л. Харченко) та ін.

У той же час категорії, закономірності, принципи, методи, концепції, моделі, системи, класифікація у сфері інформаційного забезпечення державної безпеки практично не розроблені. Сучасні дослідники зосереджують увагу переважно на окремих проблемах, а питання перетворення України на ефективну державу з точки зору інформаційної безпеки ще не стало предметом всебічного науково-практичного вивчення, що, у свою чергу, потребує системного аналізу ролі та місця інформаційного забезпечення державної

безпеки України в державному управлінні інформаційною безпекою як частини забезпечення національної безпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у Національному університеті цивільного захисту України відповідно до тематики науково-дослідних робіт «Розробка наукових основ державного управління в сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (державний реєстраційний номер 0115U002035), у межах якої дисертантом запропоновано шляхи вдосконалення єдиної державної політики у сфері забезпечення інформаційної безпеки та «Розробка механізмів державного управління соціально-економічною сферою та її галузями в контексті забезпечення безпеки українського суспільства» (ДР № 0118U001007), у межах якої автором вдосконалено систему інформаційного забезпечення державної безпеки в Україні.

Мета і завдання дослідження. *Метою* дисертаційної роботи є розробка теоретико-методологічних засад державно-управлінського аналізу сутності та особливостей реалізації інформаційного забезпечення як фактора національної безпеки сучасної України

Відповідно до поставленої мети визначено такі основні *завдання*:

- розкрити сутність інформаційної політики як феномена інформаційного суспільства та забезпечення його безпеки, визначити основні ознаки інформаційного суспільства за допомогою виявлення критеріїв систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки;

- дослідити методологічні основи інформаційного забезпечення державної політики безпеки держави, структуру національної безпеки, класифікувати інформаційні зв'язки суб'єктів національної безпеки, а також чинники отримання і подачі інформації у забезпеченні інформаційної безпеки України;

- розкрити значення інформаційної безпеки в державно-управлінських відносинах через організацію та здійснення певних принципів інформаційного забезпечення національної безпеки, показати комунікативну взаємодію органів влади та суспільства як ключових суб'єктів реалізації інформаційної політики забезпечення національної безпеки сучасної України;

- проаналізувати процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства;

- здійснити порівняльний аналіз вітчизняного та закордонного досвіду розробки та впровадження інформаційного забезпечення державної безпеки;

- охарактеризувати особливості функціонування організаційно-правового механізму інформаційного забезпечення державної безпеки;

- визначити напрями модернізації єдиної державної політики у сфері інформаційної безпеки;

- запропонувати шляхи вдосконалення державної системи інформаційної безпеки;

- сформулювати концептуальні положення інформаційного забезпечення

державної безпеки;

– окреслити стратегічні орієнтири інформаційного забезпечення державної безпеки України.

Об'єктом дослідження державна безпека в умовах трансформаційних викликів і загроз.

Предмет дослідження – інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз.

Методи дослідження. Для досягнення поставленої мети й вирішення зумовлених нею завдань, забезпечення наукової обґрунтованості дослідження і його результатів було використано комплекс загальнонаукових і спеціальних методів, що ґрунтуються на сучасних наукових засадах державно-управлінської та споріднених із нею наук.

За допомогою методів індукції та дедукції сформовано методологію дисертаційної роботи, що дозволило сформулювати гіпотезу дослідження, а також побудувати евристичні моделі інформаційного забезпечення державної безпеки. Основою для визначення рівня розробленості в науковій літературі процесів інформаційного забезпечення державної безпеки стали методи наукового узагальнення та логічного аналізу. Для вдосконалення системи інформаційного забезпечення державної безпеки у роботі застосовано системний підхід. Присутність у дослідженні порівняльного методу зумовлено необхідністю порівняння вітчизняного та закордонного досвіду розробки й упровадження інформаційного забезпечення державної безпеки.

Нормативно-ціннісний підхід використано для оцінки й аналізу державної інформаційної політики з точки зору її аксіологічної сутності, відповідності функціонуючим та ідеальним нормам і цінностям. У роботі також застосовано метод структурного моделювання для побудови моделі Стратегії інформаційного забезпечення державної безпеки.

В основу методології дослідження покладено системний підхід, методологічна специфіка якого визначається тим, що він орієнтує дослідження на розкриття цілісності об'єкта і механізмів, які її забезпечують, виділення різноманітних типів зв'язків складного об'єкта і зведення їх в єдину теоретичну картину. Зокрема, для більш точного вимірювання й оцінювання процесів формування та взаємного впливу систем інформаційної безпеки й розвитку державної політики України у сфері інформаційної політики застосовано соціологічний метод. З використанням статистичного методу визначено реальний стан досліджуваного об'єкта, а прогностичного – складові функціонально-цільової моделі державного управління інформаційною безпекою країни. Теоретико-концептуальний метод визначив напрям дослідження, втілений в аналізі функцій, структури та параметрів об'єкта, дав змогу запропонувати стратегічні напрями вдосконалення механізмів державного управління інформаційною політикою як важливої складової національної безпеки України. Нормативно-інформаційну базу дисертації склали закони України, укази Президента України, постанови Кабінету Міністрів України, нормативні документи органів державної влади України, Міністерства освіти і науки України, матеріали анкетування,

результати особистих напрацювань автора, а також зарубіжні й вітчизняні наукові джерела з досліджуваної проблематики.

Наукова новизна отриманих результатів полягає в розв'язанні актуальної наукової проблеми в галузі науки державного управління з теоретико-методологічного обґрунтування та розробки практичних рекомендацій щодо розвитку процесів інформаційного забезпечення безпеки держави.

При цьому наукова новизна конкретизується в таких положеннях:

уперше:

– сформульовано наукову концепцію інформаційного забезпечення державної безпеки, суть якої полягає, з одного боку, у необхідності глобальної інформатизації сучасного українського суспільства з точки зору інформаційного забезпечення державної безпеки, а також її аналізу як державно-управлінської складової національної безпеки, а з іншого боку – як феномена інформаційного забезпечення державної безпеки, який функціонує в умовах глобального переходу більшості держав світу до управління інформаційним суспільством в умовах швидко мінливого світу з точки зору нових загроз і викликів сучасній політиці державної безпеки;

– визначено критерії систематизації і відповідні форми, види і напрями інформаційної політики сучасних держав щодо забезпечення інформаційної безпеки, де в якості основ класифікації методологічного апарату дослідження інформаційної політики інформаційна безпека розглядається як з позиції її пізнання, так і з позиції впливу на формування ефективної державної політики з урахуванням специфіки функціонування даних методів на перехідному етапі розвитку українського суспільства;

удосконалено:

– методологічний апарат, адаптований до проблеми управління інформаційним забезпеченням безпеки держави, що включає елементи інституційного підходу, а також теорії організації й управління через системно-діалектичну модель проблеми забезпечення безпеки глобального управління, яка розкриває основні суперечності між фактичним станом системи й її цільовим інформаційним станом, якого необхідно досягти за певний час і з найменшими ресурсними витратами;

– положення про те, що проблема забезпечення інформаційної безпеки є проблемою розвитку інформаційного суспільства та докорінно відрізняється від проблеми функціонування держави в постіндустріальний період, маючи на увазі мотиваційну модель поведінки людини через потреби згідно основних циклів управління;

– положення про сутнісний взаємозв'язок світового глобального процесу і процесу забезпечення інформаційної безпеки у вигляді теоретичних аспектів щодо шляхів підвищення цільової ефективності державного управління інформаційним забезпеченням державної безпеки за допомогою розробки і реалізації державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою в системі інформаційної безпеки, стосовно її формалізації на відповідній нормативно-правовій базі;

– формалізація теоретико-методологічних розробок та концептуально-конструктивних рішень щодо проблем державного управління інформаційною безпекою на рівні основних моделей управління через використання у сфері національної безпеки найрізноманітніших інформаційних потоків, а також вивчення та оптимізацію цих потоків в контексті удосконалення інформаційного забезпечення національної безпеки;

дістали подальшого розвитку:

– теоретичний підхід до формування стратегії інформаційного забезпечення державної безпеки, який орієнтований на передбачення умов для створення можливостей максимального впровадження інтелектуальних систем в основні галузі економіки з метою побудови більш відкритої, доступної та конкурентоспроможної економіки через створення єдиного інформаційно-аналітичного середовища державних органів як основного інструменту узгодженого проведення всіх видів реформ державного управління у сфері інформаційної безпеки;

– методологічний підхід до розробки концепції інформаційного забезпечення державної безпеки, яка покликана забезпечити єдність підходів до формування та реалізації єдиної державної політики забезпечення інформаційної безпеки, складає методологічну основу для вдосконалення нормативно-правових актів, що регулюють дану сферу, а також є базисом для створення державної системи забезпечення інформаційної безпеки, яка гарантує захист національних інтересів України в інформаційній сфері яка уможлиблює ї рівноправну участь у світових інформаційних відносинах, забезпечення надійності та стійкості функціонування критично важливих інформаційних систем, стабільне функціонування й надійний захист єдиного національного інформаційного простору;

– практичний підхід до підвищення ефективності роботи державних органів через автоматизацію їх діяльності, який, на відміну від існуючих, передбачає створення інформаційно-комунікаційної архітектури для кожного державного органу у сфері забезпечення інформаційної безпеки та являє собою сукупність документів і моделей, що містять детальний опис поточного й перспективного стану державного органу, а також плану заходів з оптимізації взаємозалежностей і взаємозв'язків між функціями, бізнес-процесами, даними, інформаційними системами та компонентами технічної інфраструктури у межах плану інформатизації для забезпечення реалізації стратегічних цілей і завдань державного органу;

– уточнення сутності дефініцій: «інформаційне забезпечення державної безпеки України» як здійснення взаємопов'язаних заходів правового, організаційного, оперативного-розшукового, розвідувального, контррозвідувального, науково-технічного, інформаційно-аналітичного, кадрового, економічного та іншого характеру з виявлення, прогнозування, запобігання, стримування і нейтралізації інформаційних загроз та ліквідації наслідків їх прояву для державної безпеки України; «єдина державна політика інформаційного забезпечення державної безпеки України» як механізм узгодження інтересів суб'єктів інформаційних відносин і знаходження

компромісних рішень щодо забезпечення державної безпеки через розробку та реалізацію єдиних стандартів у сфері забезпечення вимог інформаційної безпеки до державних і недержавних інформаційних систем, ресурсів та підтримуючої інфраструктури; «механізм реалізації політики інформаційного забезпечення державної безпеки» як єдиний алгоритм міжвідомчої взаємодії, що виключає дублювання функцій і бере до уваги інформаційну роботу держави в період значущих подій у житті країни через пряму взаємодію державних органів з аудиторією ЗМІ, включаючи технології краудсорсингу, з метою захисту національних інтересів.

Практичне значення отриманих результатів дослідження полягає в можливості й доцільності застосування ключових положень і висновків дисертації в навчальному процесі для розробки та підготовки навчально-методичної літератури, а також у практичній діяльності органів державної влади та органів місцевого самоврядування з метою формування та впровадження державно-управлінських рішень з інформаційного забезпечення державної безпеки.

Пропозиції дисертаційного дослідження використано в роботі Головного управління Державної служби України з надзвичайних ситуацій у Хмельницькій області стосовно створення можливостей максимального впровадження інтелектуальних систем в у процесі забезпечення державної безпеки (довідка № 01-1985/02 від 19.12.2019), виконавчого комітету Хмельницької міської ради щодо формування інформаційно-комунікаційної архітектури органів місцевого самоврядування (довідка № 02-21-598 від 13.05.2020) та департаменту освіти і науки Хмельницької обласної державної адміністрації відносно впровадження елементів запропонованої національної Стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку (довідка № 1189-41/2020 від 13.05.2020).

Крім того, теоретичні положення та наукові результати дисертаційної роботи використано в навчальному процесі Національної академії Державної прикордонної служби України імені Богдана Хмельницького відносно поглиблення змістовно-понятійної бази щодо інформаційного забезпечення державної безпеки, удосконалення його механізмів, виокремлення принципів функціонування державної системи інформаційної безпеки, а також розвитку єдиної державної політики у сфері інформаційної безпеки в Україні (Акт № 186/20-354 від 17.01.2020).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Всі сформульовані в ній висновки, наукові положення та пропозиції ґрунтуються на особистих дослідженнях здобувача.

Апробація матеріалів дисертації. Основні теоретичні й практичні положення, висновки, пропозиції та рекомендації, сформульовані в дисертації, оприлюднені на таких регіональних і міжнародних науково-практичних конференціях, конгресах і семінарах: «Актуальні проблеми економіки, управління та фінансів» (м. Дніпро, 19 квітня 2019 р.); «Актуальні

проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 16 травня 2019 р.); «Державне управління у сфері цивільного захисту: наука, освіта, практика» (м. Харків, 17–18 травня 2019 р., 18–19 березня 2020 р.); «XXVII науково-практичної конференції MicroCAD-2019» (м. Харків, 15–17 травня 2019 р.), «Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти» (м. Суми, 23 травня 2019 р.); «Формування громадянської культури в новій українській школі: традиційні та інноваційні практики» (м. Суми, 6–7 червня 2019 р.); «Забезпечення діяльності складових сектору безпеки і оборони України» (м. Хмельницький, 22 листопада 2019 р.); «XXVIII науково-практичної конференції MicroCAD-2020» (м. Харків, травень, 2020 р.).

Публікації. Основні положення та отримані наукові результати дисертаційного дослідження відображено в 31 наукових працях, з яких: 1 – одноосібна монографія, 16 статей у вітчизняних наукових фахових виданнях, 4 статті у зарубіжних спеціалізованих виданнях та 10 тез доповідей. Загальний обсяг публікацій за темою дослідження становить 34,6 авт. арк.

Структура та обсяг дисертації обумовлені предметом, метою та завданнями дослідження. Робота складається зі вступу, п'яти розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 375 сторінок, з яких основного тексту – 330 сторінок, кількість використаних джерел – 370 найменувань на 45 сторінках, 6 рисунків і 9 таблиць, 1 додаток – на 5 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано вибір теми дослідження та її актуальність, розкрито зв'язок з науковими програмами, планами й темами, визначено мету, завдання, об'єкт, предмет і методи дослідження, розкрито наукову новизну отриманих результатів, наведено дані про апробацію основних положень дисертації, а також структуру та обсяг роботи.

У **першому розділі** *«Теоретико-методологічний аналіз проблем інформаційного забезпечення державної безпеки в умовах сучасних викликів та загроз»* визначено концептуальні засади інформаційної складової в системі забезпечення державної безпеки на основі системного й концептуально-порівняльного підходів, охарактеризовано стан та особливості механізмів державного управління інформаційним забезпеченням державної політики як важливого чиннику безпеки держави, окреслено й розкрито змістовні характеристики методології та системи державного управління функціонуванням сучасного інформаційного суспільства в умовах викликів і загроз глобального світу.

Визначено, що актуальність даної проблематики визначається всезростаючою роллю інформаційної сфери, яка є сукупністю інформації, інформаційної інфраструктури та суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання суспільних відносин, що виникають при цьому. Інформаційна сфера виступає

системоутворюючим фактором життя суспільства, активно впливає на стан політичної, економічної, державно-управлінської та інших складових безпеки сучасних держав, істотно залежить від інформаційного забезпечення безпеки і в ході технічного прогресу ця залежність постійно зростає.

Зроблено висновок, що інформація без перебільшення є одним із найважливіших ресурсів розвитку цивілізації. Вона активно впливає на всі сфери життя як окремих суспільств і держав, так і всієї світової спільноти. Водночас, як показав досвід, інформація може використовуватись не тільки на благо, але й на шкоду інтересам особистості, суспільства і держави.

Розвиток і поширення інформаційно-комунікаційних технологій, їх проникнення практично в усі сфери життєдіяльності людини, з одного боку, є важливим чинником світової інтеграції, соціального розвитку та економічного зростання. З іншого боку, будучи найсильнішим каталізатором інформаційного обміну, ці технології несуть у собі й безліч як явних, так і прихованих загроз. У зв'язку з цим надзвичайної актуальності набувають питання забезпечення інформаційної безпеки, які, на наш погляд, є однією з найважливіших складових національної безпеки. Більш того, існує думка, що інформаційна безпека в сучасному постіндустріальному світі, де основним продуктом є саме інформація, яка і впливає на прийняття державою тактичних і стратегічних рішень у сфері державного управління, виступає основою національної безпеки.

Доведено, що зміст поняття «інформаційна безпека» як у науковій літературі, так і в державних нормативних документах, трактується не зовсім чітко. На нашу думку, на сьогоднішній день воно є результатом інтеграції змісту понять «національна безпека» та «безпека інформації».

Так, під інформаційною безпекою, як правило, розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної збитку суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та інфраструктурі, що її підтримує.

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На нашу думку, адекватний з методологічної точки зору підхід до проблем інформаційної безпеки має починатися з виявлення суб'єктів інформаційних відносин та їх інтересів, пов'язаних з використанням інформаційно-комунікаційних технологій. Загрози інформаційній безпеці – це зворотний бік використання інформаційно-комунікаційних технологій.

Трактування проблем, пов'язаних з інформаційною безпекою різних категорій суб'єктів державного управління, може мати суттєві відмінності. Весь спектр інтересів суб'єктів, пов'язаних з використанням інформаційно-комунікаційних технологій, можна поділити на такі категорії: забезпечення доступності, цілісності й конфіденційності інформації та підтримуючої інфраструктури. Мета заходів у сфері інформаційної безпеки – захистити інтереси суб'єктів інформаційних відносин.

Державна політика забезпечення інформаційної безпеки визначається за основними сферами прояву, системне вираження якої локалізується: а) у сфері

функціонування органів державного управління (державна інформаційна безпека); б) у сфері громадянського суспільства (інформаційна безпека суспільства); в) у сфері інтересів особистості.

Інформаційне забезпечення – це особливий вид забезпечення, зумовлений специфікою самого продукту забезпечення – інформацією. В останні десятиліття інформаційні ресурси набувають все більшого значення у функціонуванні сучасних держав. Тому не випадково ще на зорі свого існування у розвитку людської цивілізації виділялися два напрямки діяльності: матеріальне виробництво та інтенсифікація інформаційних процесів.

Наголошено, що специфіка і відмінна риса інформаційного забезпечення від інших видів забезпечення національної безпеки полягає в самому продукті забезпечення – інформації, в силу того, що остання лежить в основі будь-якої діяльності людини й тому виступає необхідною умовою її раціонального життєзабезпечення.

Таким чином, національна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки – держави, особистості та суспільства. Саме взаємопов'язана, системна єдність останніх становить якісну визначеність, покликану захисти життєво важливі інтереси держави, особистості та суспільства, забезпечити їх конкурентоспроможний, прогресивний розвиток.

Доведено, що специфіка інформаційного забезпечення полягає в тому, що в ході його здійснення не створюється нова інформація, а збирається, обробляється й подається вже наявна у зручній для споживача формі. А весь процес підготовки інформації спрямований на створення інформаційних ресурсів, під якими у сфері національної безпеки в найвужчому сенсі слід розуміти сукупність документів і їх масивів, баз даних, що знаходяться в інформаційних системах (архівах, фондах, банках даних і т. ін.). Саме інформаційні ресурси є тим необхідним компонентом, з якого за допомогою інформаційних засобів споживач може отримувати необхідну інформацію. Тому формування інформаційних ресурсів у сфері національної безпеки є завданням загальнонаціонального плану, оскільки вони багато в чому визначають ефективність інформаційного забезпечення споживачів інформації в даній сфері.

Проведене дослідження дозволило дійти висновку, що організація і здійснення інформаційного забезпечення національної безпеки, його раціональне функціонування та ефективне використання можуть бути досягнуті за умови дотримання певних принципів. Видається, що найбільш важливими з них є такі:

1. Повнота інформаційного забезпечення. Результати пошуку повинні містити інформацію в повному обсязі, водночас звести до мінімуму «шум» і виключити дезінформацію. Основне – вибрати таку пошукову стратегію, щоб споживач отримав інформацію, що відповідає не лише заданій тематиці, а й його інформаційним потребам.

2. Актуальність інформаційного забезпечення, завдання якого полягає в поданні споживачеві пріоритетної інформації, що відповідає умовам і в

установлені терміни.

3. Точність і надійність інформаційного забезпечення, які полягають у наданні споживачеві всієї необхідної інформації з урахуванням потрібних видів і мовного оформлення, хронологічної глибини і т. ін.

4. Інформація повинна подаватись у зручній для споживача формі (машинопис, мікрофільм, екран дисплея і т. ін.).

5. Диференційованість інформаційного забезпечення з урахуванням функцій споживача, його статусу та оперативності розв'язуваних ним завдань.

6. Системність інформаційного забезпечення, що проявляється в систематичному задоволенні інформаційних потреб на всіх етапах забезпечення національної безпеки і комплексності видів інформаційного забезпечення з урахуванням категорій споживачів, характеру їх інформаційних потреб, специфіки завдань, що вирішуються.

У ХХІ ст. в Україні спостерігається бурхливий розвиток телекомунікаційних мереж, Інтернету, мобільного зв'язку. Впроваджуються нові інформаційні технології, розвивається комп'ютерна преса, відкриваються нові сайти, численні компанії пропонують послуги IP-телефонії, реалізують стільникові телефони, комп'ютери, модеми та ін. Однак усі зазначені процеси розвиваються досить стихійно, з незрозумілим поки знаком для суспільства, з неясними й невизначеними наслідками.

В Україні, на наш погляд, наразі не існує сформованої загальнонаціональної стратегії входження у глобальний інформаційний простір, не вироблені пріоритети, не сформульовані цілі, не усвідомлені альтернативи. При цьому цілком очевидно, що багато пострадянських країн, і в тому числі Україна, відстають у розвитку інформаційно-комунікаційних технологій і, відповідно, характеризуються певним «запізненням» у процесі інтеграції в структури інформаційного суспільства.

Сучасне інформаційне суспільство, на наш погляд, повинно являти собою єдину комп'ютеризовану інформаційну спільноту людей, діяльність яких головним чином зосереджена на обробці інформації, де матеріальне виробництво і виробництво енергії автоматизовано, а інформаційні технології набувають глобального характеру, охоплюють усі сфери діяльності людини.

У **другому розділі** *«Концептуальні підходи щодо особливості формування безпеки держави в інформаційній сфері»* викладено методологію дослідження, охарактеризовано процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства проаналізовано особливості забезпечення комунікації державного управління та суспільства як чинника формування та реалізації політики інформаційної безпеки держави, розглянуто інформаційну безпеку в державно-управлінських відносинах в контексті процесів демократизації суспільства.

За результатами проведеного дослідження визначено, що в умовах постійно мінливого світу стає очевидним, що використання сучасних інформаційних технологій безпосередньо впливає і на інформаційну безпеку держави. Як справедливо зазначав відомий американський футуролог

О. Тоффлер, на сучасному етапі знання та інформація стали найважливішими ресурсами влади.

Сьогодні у світі відбувається інтенсивне нарощування інформаційно-комунікаційного потенціалу, все активніше фахівці у сфері інформаційних комунікацій сучасний етап називають інформаційною глобалізацією. На наш погляд, не менш точною характеристикою змін, що відбуваються у ХХІ ст. у розвитку держав, є формування глобального інформаційного суспільства, в якому інформаційні ресурси державного управління набувають найбільш важливого значення поряд з ресурсами сили і багатства.

Обґрунтовано положення про те, що основними характерними рисами інформаційного суспільства є інформаційна економіка та інформаційне управління, високий рівень інформаційних потреб усіх членів суспільства й фактичне їх задоволення для основної маси населення, висока інформаційна культура, вільний доступ кожного члена суспільства до інформації, обмежений тільки інформаційною безпекою особистості, суспільних груп і держави.

Якщо говорити більш конкретно, то інформаційному суспільству притаманні такі ознаки:

- наявність єдиного інформаційного простору;
- домінування в економіці й публічному управлінні нових технологічних укладів, що базуються на масовому використанні інформаційно-комунікаційних технологій;
- підвищення ролі інфраструктури (телекомунікаційної, транспортної, організаційної) в системі суспільного виробництва, державного управління, а також посилення тенденцій до спільного функціонування в економіці та управлінні інформаційних і грошових потоків;
- зростання значущості проблем забезпечення інформаційної безпеки особистості, суспільства і держави, наявність ефективної системи забезпечення прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації;
- високий рівень освіти, зумовлений розширенням інформаційного обміну на міжнародному, національному та регіональному рівнях, і відповідно підвищена роль кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик праці;
- провідна роль інформаційних ресурсів у забезпеченні сталого поступального розвитку суспільства і забезпечення інформаційної безпеки держави;
- фактичне задоволення потреб суспільства в інформаційних продуктах і послугах.

Як результат – відбуваються неочікувані нелінійні процеси, які зумовлюють зміну системи та спричиняють її еволюційний розвиток чи загибель. Принцип самоорганізації та збалансованості розвитку не лише не заперечує, але й передбачає можливі біфуркації.

Наголошено, що найважливішою особливістю інформаційного суспільства є перенесення акценту у виробництві з використання сировини,

матеріалів та енергії на продукування інформації й надання інформаційних послуг. Як зазначав відомий японський вчений І. Масуда, саме «продукування інформаційного продукту, а не продукту матеріального, буде рушійною силою освіти і розвитку суспільства».

За результатами дослідження визначено, що серед питань, які найбільш гостро стоять у зв'язку з розвитком інформаційних процесів і відносин, слід виділити проблему нерівномірності розвитку останніх у різних регіонах і країнах, що, у свою чергу, впливає на систему інформаційної безпеки держави.

Яка б не була економічна вигода від впровадження інформаційних і комунікаційних технологій, розподіл ІКТ-ресурсів (інформаційно-комунікативних) у світі носить вкрай нерівномірний характер. Існують значні відмінності не лише між багатими і бідними країнами, а й між різними соціальними групами населення в кожній країні.

Доведено, що в рамках комунікативного підходу державна влада інтерпретується як обмежена в часі і просторі субстанція впливу, підпорядкування, сили або відносин.

На нашу думку, це особливий різновид соціальної взаємодії державно-управлінських суб'єктів, специфічна форма соціальної комунікації між суб'єктами і об'єктами державно-управлінської діяльності з приводу отримання, зберігання, відтворення і трансформації державно-управлінської інформації з метою вироблення адекватних або неадекватних політичних цінностей суспільства рішень.

У сучасних умовах, на нашу думку, внаслідок протиріч влади і суспільства комунікативна діяльність органів влади характеризується такими ознаками, як недостатня відкритість, фрагментарність, маніпулятивність технік. Це підтверджується урядовими стратегіями інформування, тактиками комунікативної поведінки представників влади, соціальними практиками професійних PR-агентств, які виконують державні замовлення.

У зв'язку з цим, як видається, недостатня соціальна відповідальність влади й особливості її комунікації детерміновані інструментальним підходом. Публічні служби використовуються як інструмент збереження владних інтересів, конструювання одностороннього бачення смислів державно-управлінських рішень. У цілому комунікативна модель формування та підтримки відносин із суспільством характеризується як одностороння, в результаті чого утворюється розрив між реальною політикою та інформаційним продуктом, що негативно позначається на легітимності влади.

Отже, процеси збору, накопичення, переробки та поширення інформації стають необхідною умовою ефективного функціонування існуючих структур державного управління, здійснення державно-політичних впливів на все суспільство, вирішення масштабних економічних завдань. При цьому слід мати на увазі, що інформація – це не лише сила творити. На жаль, вона володіє дестабілізуючими факторами, які можуть впливати на суспільство і систему державного управління.

Можна припустити, що в сучасних умовах використання інформаційних ресурсів створює практично необмежені можливості впливу на людину, суспільство та державне управління й далеко не завжди це відбувається в інтересах суспільства і держави.

Доведено, що інформаційна безпека у сфері державно-управлінських відносин у політичному процесі може розглядатись як сукупність взаємодіючих і взаємопов'язаних компонентів, а саме:

- загрози життєво важливим інтересам суспільства у сфері інформаційної безпеки, а також небезпеки, виклики та ризики;
- самі життєво важливі інтереси суспільства, держави та особистості, що підлягають інформаційному захисті;
- основні заходи, що проводяться суб'єктами держави і громадянського суспільства, з нейтралізації загроз, небезпек і ризиків у сфері інформаційної безпеки.

З процесуальної точки зору інформаційна безпека в державно-управлінських відносинах може бути представлена такими основними напрямками:

- інформаційна безпека у сфері державно-політичних інтересів;
- інформаційна безпека в системі державного управління;
- інформаційна безпека в процесі партійного будівництва;
- інформаційна безпека зовнішньополітичного процесу і т. п.

За основними сферами прояву системне вираження інформаційної безпеки локалізується в трьох напрямках:

- інформаційна безпека у сфері функціонування державних органів політичної влади (державна інформаційна безпека);
- інформаційна безпека, здійснювана у сфері громадянського суспільства (громадська інформаційна безпека);
- інформаційна безпека особистості, а також особиста інформаційна безпека.

Нарешті, за рівнями соціальної організації й геополітичним змістом інформаційна безпека виступає у вигляді таких компонентів:

- інформаційна безпека, яку забезпечують на міждержавному рівні;
- інформаційна безпека на національно державному рівні;
- інформаційна безпека окремих регіонів на внутрішньодержавному рівні;
- інформаційна безпека, яку забезпечують на рівні органів місцевого самоврядування.

У **третьому розділі** «Оцінка сучасного стану та перспектив розвитку інформаційного забезпечення державної безпеки» проаналізовано закордонний досвід розробки та впровадження інформаційного забезпечення державної безпеки, виокремлено особливості функціонування організаційно-правових механізмів інформаційного забезпечення державної безпеки, а також охарактеризовано поточний стан і тенденції розвитку державної інформаційної політики в Україні.

Відповідно до Європейської конвенції про кіберзлочинність

(інформаційну безпеку) забезпечення інформаційної безпеки передбачало недопущення чи усунення таких суспільно-небезпечних діянь проти конфіденційності даних: протиправний доступ; перехоплення; порушення цілісності; втручання в роботу; виробництво, обіг та використання спеціальних засобів для комп'ютерних злочинів з використанням комп'ютерів; підроблення; інформаційне шахрайство.

Нині діючі міжнародні стандарти державного регулювання інформаційної безпеки висвітлюють його окремі аспекти. Дійсно, стандарт ISO 17799 згадує про важливість аудиту інформаційної безпеки, але не містить жодної інформації про те, як його здійснювати. Тут можуть використовуватися керівні принципи аудиту COBIT, особливо в тих умовах, коли COBIT активно порівнюється з ISO 17799. Процес стратегічного управління інформаційною безпекою описаний в BS 7799, а оперативна складова управління безпекою інформаційних технологій розкрита в Security Management ITIL.

Однак в умовах існування великої кількості стандартів інформаційного забезпечення державної безпеки необхідно встановлювати зв'язки між ними, що, у свою чергу, зумовлює необхідність розробки та впровадження мега-стандарту інформаційного забезпечення державної безпеки.

Вже сьогодні всю систему діючих нормативно-правових актів, що є базовими для реалізації інформаційно-комунікативної функції держави, умовно можна розглядати, з одного боку, як трирівневу (по вертикалі), що включає:

- рівень міжнародного права;
- конституційний рівень;
- рівень поточного, внутрішньодержавного законодавства.

З іншого боку, зазначена нормативно-правова база може розглядатися й у функціональному аспекті (по горизонталі), наприклад, як підсистема нормативно-правових актів, що забезпечують реалізацію прав та інтересів особистості, суспільства і держави за такими напрямками:

- вільний доступ до масової інформації та вільний інформаційний обмін нею;
- захист визначених законом видів інформації від несанкціонованого доступу;
- захист особи та суспільства від деструктивного інформаційного впливу.

Так, відносно декларативності слід зазначити, що, наприклад, в різних нормативних актах перераховується велика кількість таємниць, проте за розголошення не всіх з них передбачена відповідальність.

Необхідно зазначити, що сучасне законодавство, яке регулює питання забезпечення інформаційної безпеки України, не розглядає її у форматі захисту інформаційної свободи. Крім того, недосконалість правової бази є природною в період, коли суспільні відносини випереджають законодавчу базу і громадяни, суспільство, підприємства та організації змушені самі захищати свої права, нерідко порушуючи задекларовані норми.

Аналіз нормативно-правової бази реалізації інформаційно-комунікативної функції держави дозволяє дійти висновку про те, що, незважаючи на існуючі прогресивні зрушення, законодавство, що розглядається, не можна назвати

розвиненим, тому що воно суперечливе, здебільшого носить декларативний характер, має суттєві прогалини. Все це створює юридичні бар'єри на шляху реалізації державою інформаційно-комунікативної функції.

Крім того, сьогодні слід визнати відсутність єдиного правового поля стосовно регулювання інформаційного забезпечення державної безпеки. Зокрема, в різних нормативних актах перераховується велика кількість таємниць, проте за розголошення не всіх з них передбачена відповідальність. Водночас сучасне законодавство, яке регулює питання забезпечення інформаційної безпеки України, не розглядає інформаційну безпеку у форматі захисту інформаційної свободи.

З огляду на поточний стан нормативно-правового забезпечення, у дисертаційній роботі здійснено поділ органів державної влади спеціальної компетенції, що регулюють інформаційну безпеку, залежно від визначеного виду інформаційних відносин, які підлягають інформаційному впливу, та виокремлено такі їх групи:

- органи, які регулюють сферу інформаційних відносин у загальному контексті та впроваджують державну інформаційну політику (Державний комітет телебачення і радіомовлення України);

- органи, що розробляють і впроваджують державну мовну політику та державну політику стосовно захисту суспільної моралі (Міністерство культури та інформаційної політики України);

- органи, які регулюють функціонування сфери отримання і зберігання інформації (Державний служба статистики України та Державна архівна служба);

- органи, що проводять аналіз і моніторинг визначених типів інформації (Державна служба фінансового моніторингу України).

Однак такий підхід не дозволяє повноцінно здійснювати забезпечення інформаційної безпеки в державі, відтак необхідно чітко визначити частку і межі участі держави у забезпеченні інформаційної безпеки, в тому числі через законодавче встановлення заборон і обмежень в інформаційній сфері. При цьому слід взяти до уваги, що інформаційна політика держави включає в себе дві складові, а саме техніко-технологічну та гуманітарну. Зокрема, зазначено, що техніко-технологічна складова пов'язана з вирішенням завдань інформатизації суспільства, розвитком і впровадженням інформаційно-комунікаційних технологій, створенням конкурентоспроможної інформаційно-технологічної інфраструктури. Гуманітарна складова державної інформаційної політики, у свою чергу, включає в себе поняття, зміст, якість інформації та вплив інформаційної політики держави на політичні, духовні й соціальні процеси в суспільстві. При цьому правомірно виділити гуманітарну складову інформаційної політики як визначальну (рис. 1).

Крім того, у роботі запропоновано виокремити низку напрямів забезпечення державою своєї інформаційної політики, найважливішими з яких є фінансово-економічний, організаційно-технічний і правовий. Зокрема, фінансово-економічний напрям передбачає: удосконалення системи фінансування робіт з розробки програм забезпечення інформаційної безпеки та створення системи страхування інформаційних ризиків фізичних і юридичних осіб.



Рис. 1. Модель вдосконалення державної інформаційної політики
Джерело: авторська розробка.

Організаційно-технічні, відповідно, передбачають:

- створення і впровадження засобів несанкціонованого доступу до інформації, що оброблюється;
- розробку програм, які перешкоджають руйнуванню та спотворенню інформації;
- підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем;
- постійне спостереження за діями обслуговуючого персоналу в захищених інформаційних системах.

Правова або законодавча діяльність держави щодо забезпечення інформаційної безпеки передбачає такі заходи:

- розробку законодавчих актів, що встановлюють відповідальність фізичних і юридичних осіб за несанкціонований доступ до інформації; розголошення інформації, яка містить державну або комерційну таємницю; спотворення, протизаконне використання або протиправне копіювання інформації; використання в злочинних цілях службової інформації та навмисне поширення недостовірної інформації;
- розробку законодавчих актів, що обмежують частку іноземної участі у володінні загальнодержавними засобами масової інформації;
- встановлення законодавчого розмежування повноважень у галузі інформаційної безпеки між органами влади;
- розробку нормативних актів, що регламентують взаємовідносини держави зі своїми контрагентами (як поза, так і всередині держави) в інформаційній сфері.

У четвертому розділі *«Розвиток інформаційного забезпечення державної безпеки України в умовах функціонування цифрового суспільства»* розроблено комплекс заходів щодо інвентаризації та категорювання інформаційних ресурсів в державному та регіональному інформаційному просторі, запропоновано напрями модернізації єдиної державної політики у сфері інформаційної безпеки, а також сформульовано пропозиції щодо удосконалення державної системи інформаційної безпеки.

Підкреслено необхідність вироблення ефективної комплексної внутрішньої і зовнішньої державної інформаційної політики як інструменту регулювання взаємодій всіх компонентів суспільно-політичної системи, виходячи з національних інтересів держави та з орієнтацією на збереження територіальної цілісності і суверенітету України.

При цьому принциповими особливостями процесу формування та реалізації єдиної державної політики у сфері інформаційної безпеки мають бути такі: вона формується в рамках державної системи забезпечення інформаційної безпеки; як основні методи управління у зазначеному контексті використовується координація та функціональне регулювання діяльності із забезпечення інформаційної безпеки; найважливішим завданням формування та реалізації єдиної державної політики у сфері інформаційної безпеки є створення і вдосконалення механізмів забезпечення інформаційної безпеки у сфері компетенції органів державної влади та місцевого самоврядування.

У зазначеному контексті всі протиріччя інформаційної безпеки соціуму умовно розділити на три групи, кожна з яких має чіткі межі та специфічні шляхи розв'язання.

Так, до першої групи слід включити протиріччя інформаційної безпеки соціуму як самостійного автономного явища, що має свої особливості та специфічну логіку розвитку. У цьому контексті найбільш чітко виступають протиріччя структурно-змістовного плану, які утворюють протиріччя між рівнями, видами і формами інформаційної безпеки. При цьому протиріччя видового порядку, представлені в розбіжностях комп'ютерної, культурно-когнітивної та інформаційно-психологічної безпеки, з розвитком утворюють свій комплекс протиріч.

Другу групу утворюють протиріччя інформаційної безпеки як умови існування і прогресивного розвитку інформаційної сфери соціуму. В даному випадку виділяються зв'язки інформаційної безпеки з інформаційними відносинами й інформаційною практикою соціальних суб'єктів, а також іншими елементами інформаційної сфери соціуму.

Третю групу складають протиріччя, що сформувалися в результаті взаємин інформаційної безпеки з іншими видами безпеки, а також загальною безпекою соціуму. Досліджуючи цю групу протиріч, необхідно зрозуміти причини їх розвитку, а також враховувати як внутрішні протиріччя, властиві даному явищу, так і внутрішні протиріччя більш великої системи, які по відношенню до досліджуваного явища виступають як зовнішні та є складною частиною умов виникнення протиріч.

Враховуючи зазначені протиріччя, доцільною видається побудова дієвої державної системи інформаційної безпеки, якій притаманні такі властивості, як багаторівневність і багатофункціональність (рис. 2).

Структура державної системи інформаційної безпеки включає державні органи управління, а також територіальні органи державних органів виконавчої влади, які вирішують загальносистемні завдання інформаційної безпеки, об'єктні (цільові) й функціональні підсистеми державної системи інформаційної безпеки.

В основу формування державної системи інформаційної безпеки мають бути покладені такі принципи: законність; розмежування повноважень щодо забезпечення інформаційної безпеки між державними органами державної системи захисту інформації та органами місцевого самоврядування; добровільність входження до складу державної системи інформаційної безпеки підприємств, установ і організацій; колегіальність керівництва державної системи інформаційної безпеки; стабільність ядра державної системи інформаційної безпеки, що забезпечує виконання функцій інформаційної безпеки; адаптивність оболонки державної системи інформаційної безпеки до зовнішніх умов і завдань; раціональне поєднання універсальності та диференціації механізмів забезпечення інформаційної безпеки; облік досвіду забезпечення інформаційної безпеки в Україні й її регіонах; поетапність формування і розвитку державної системи інформаційної безпеки. Існує можливість застосування таких методів державного управління регіональними системами інформаційної безпеки:

– директивне управління органами регіональних систем інформаційної безпеки з використанням організаційно-розпорядчих актів органів виконавчої влади, спрямованих на виконання прийнятих рішень у сфері інформаційної

безпеки;

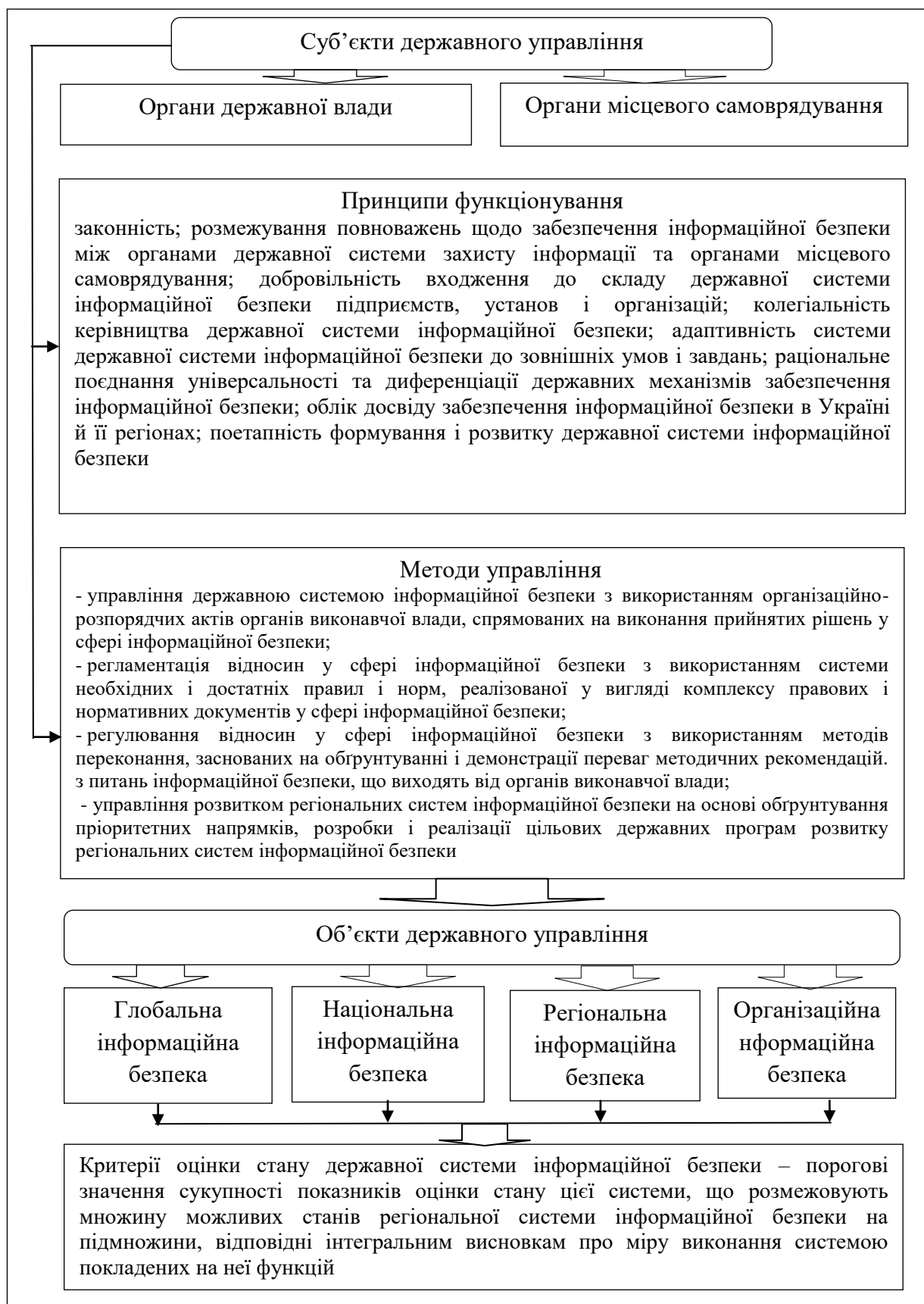


Рис. 2. Складові державної системи інформаційної безпеки
Джерело: авторська розробка.

– регламентація відносин у сфері інформаційної безпеки на рівні регіону і використання системи необхідних і достатніх правил і норм, реалізованої у вигляді системи правових і нормативних документів у сфері інформаційної безпеки;

– регулювання відносин у сфері інформаційної безпеки з використанням методів переконання, заснованих на обґрунтуванні та демонстрації переваг методичних рекомендацій з питань інформаційної безпеки, що виходять від органів виконавчої влади;

– управління розвитком регіональних систем інформаційної безпеки на основі обґрунтування пріоритетних напрямків, розробки та реалізації цільових державних програм розвитку регіональних систем інформаційної безпеки.

При цьому під критеріями оцінки стану регіональної системи інформаційної безпеки рекомендовано розуміти порогові значення сукупності показників оцінки стану цієї системи, що розмежовують множину можливих станів регіональної системи інформаційної безпеки на підмножини, відповідні інтегральним висновкам про міру виконання системою покладених на неї функцій.

У п'ятому розділі *«Напрями вдосконалення інформаційного забезпечення державної безпеки в умовах сучасних викликів та загроз»* сформульовано концептуальні положення інформаційного забезпечення державної безпеки, виокремлено стратегічні орієнтири інформаційного забезпечення державної безпеки України, а також запропоновано напрями трансформації системи інформаційного забезпечення державної безпеки України.

Зокрема, запропоновано Концепцію інформаційного забезпечення державної безпеки, яка покликана забезпечити єдність підходів до формування та реалізації державної політики забезпечення інформаційної безпеки, а також методологічну основу для вдосконалення нормативно-правових актів, що регулюють дану сферу. Метою Концепції є створення державної системи забезпечення інформаційної безпеки, яка гарантує захист національних інтересів України в інформаційній сфері.

Запровадження Концепції інформаційного забезпечення державної безпеки вимагає розвитку трьох напрямів: законодавчого й нормативно-методичного, організаційно-розпорядчого та організаційно-технічного, а також кадрового, що в кінцевому підсумку сприятиме:

- реалізації конституційних прав громадян на отримання, зберігання і поширення повної, достовірної та своєчасної інформації;
- рівноправній участі України у світових інформаційних відносинах;
- ефективному інформаційному забезпеченню державної політики;
- забезпеченню надійності та стійкості функціонування критично важливих інформаційних систем;
- безперебійному функціонуванню й надійному захисту єдиного національного інформаційного простору.

В межах напрямів організаційно-розпорядчого та організаційно-технічного забезпечення інформаційного забезпечення державної безпеки потрібна реалізація комплексу заходів щодо забезпечення інформаційної

безпеки критично важливих об'єктів інформатизації, а також запровадження єдиної державної політики у даній сфері, в тому числі захисту інформації. Для цього необхідно створити єдину державну систему моніторингу інформаційного простору, а також інформаційної системи та інфраструктури Оперативного центру забезпечення інформаційної безпеки. При цьому єдина державна політика у даній сфері має забезпечити розробку та реалізацію єдиних стандартів у сфері забезпечення вимог інформаційної безпеки державних і недержавних інформаційних систем, ресурсів та підтримуючої інфраструктури.

Підвищення ефективності роботи державних органів доцільно здійснювати через застосування архітектурного підходу, який передбачає автоматизацію їх діяльності за допомогою створення інформаційно-комунікаційної архітектури для кожного з них, погодженої уповноваженим органом. Зокрема, інформаційно-комунікаційна архітектура державного органу являтиме собою сукупність документів, моделей, матриць і діаграм, які містять детальний опис поточного й планованого стану державного органу, а також плану заходів з оптимізації взаємозалежностей і взаємозв'язків між функціями, бізнес-процесами, даними, інформаційними системами та компонентами технічної інфраструктури в межах плану інформатизації для забезпечення реалізації стратегічних цілей і завдань державного органу. Інформаційно-комунікаційна архітектура створюватиметься на основі моделі, яка складається з таких взаємопов'язаних компонентів: архітектура діяльності; архітектура даних; архітектура додатків; технологічна архітектура; архітектура інформаційної безпеки.

Створення інформаційно-комунікаційної архітектури органів місцевого самоврядування у регіонах дозволить уніфікувати діяльність державних органів за рахунок використання єдиних бізнес-процесів, шаблонів документів, стандартів і типових рішень у межах інформаційно-комунікаційних технологій.

З метою консолідації всіх верств суспільства для досягнення цілей інформаційного та інноваційного розвитку, координації бізнесу, всіх суспільних інститутів і громадян визнано необхідним формування національної Стратегії інформаційного забезпечення державної безпеки. Враховуючи міжнародний досвід побудови інформаційного суспільства, в межах Стратегії слід визначити чотири ключові напрями:

- забезпечення ефективності системи державного управління;
- забезпечення доступності інформаційно-комунікаційної інфраструктури;
- створення інформаційного середовища для соціально-економічного і культурного розвитку суспільства;
- розвиток вітчизняного інформаційного простору (рис. 3).

У Стратегії інформаційного забезпечення державної безпеки необхідно також передбачити умови для створення можливостей громадянам освоїти й отримати навички роботи з інформаційними технологіями за допомогою електронної освіти, довічного навчання і підготовки, дистанційної роботи, а також отримання послуг доступної електронної охорони здоров'я.



Рис. 3. Узагальнена модель формування Стратегії інформаційного забезпечення державної безпеки

Джерело: авторська розробка.

З метою побудови більш відкритої, доступної та конкурентоспроможної економіки нашої країни у Стратегії інформаційного забезпечення державної безпеки слід передбачити максимальне впровадження інтелектуальних систем в основні галузі економіки. У цьому контексті з метою систематизації збору даних та структурування інформації державних органів визнано доцільним реалізувати такі заходи:

- розширити перелік публічної інформації, що подається Урядом України та державними органами громадянам і бізнесу;
- внести зміни до чинного законодавства з метою своєчасності подання, об'єктивності, повноти та достовірності електронних інформаційних ресурсів, відносно яких відповідними нормативно-правовими

актами України встановлено обов'язковий характер їх публічного розповсюдження або подання державними органами;

- розвивати портал «електронного уряду», який, зокрема, буде служити майданчиком для діалогу з населенням, обговорення якості державних послуг, що надаються, а також консолідації даних з планування і фактичного освоєння бюджетних коштів державними органами;

- залучати громадян, неурядові та інші недержавні організації до процесу постійного громадського моніторингу якості надання державних послуг;

- використовувати соціальні майданчики в мережі Інтернет для широкого обговорення державними органами і населенням соціальних проблем;

- формувати й впроваджувати механізм залучення громадян до процесу реформування й поліпшення іміджу держави;

- уніфікувати сайти державних установ та перевести їх на єдину платформу;

- реалізувати механізми електронної оцінки громадянами ефективності роботи органів державної влади та місцевого самоврядування.

Система інформаційного забезпечення державної безпеки базується на розмежуванні повноважень органів законодавчої, виконавчої та судової влади у даній сфері з урахуванням предметів ведення органів державної влади та місцевого самоврядування, що визначаються відповідним законодавством України. При цьому дана система и має забезпечувати гнучке управління процесами інформаційної безпеки на державному, регіональному, галузевому, виробничому та користувальницькому рівнях.

При цьому передбачається, що сучасна телекомунікаційна мережа доступу і «електронний уряд» України слугуватимуть інфраструктурою створення нового інформаційного суспільства. Зокрема, в числі значущих нових напрямів розвитку «електронного уряду» будуть вирішені наступні завдання:

- перегляд життєвого циклу проектів інформаційно-комп'ютерних технологій у бік впровадження модульного підходу, орієнтованого на короткі кроки і швидке досягнення конкретних результатів;

- проведення заходів з метою усунення «вхідних порогів» для участі в державних інформаційно-комп'ютерних проектах невеликих ІТ-компаній;

- розробка Єдиного інформаційно-аналітичного середовища державних органів, яке стане основним інструментом узгодженого проведення всіх видів реформ державного управління;

- здійснення ревізії і паспортизації всієї соціально значущої інфраструктури держави (інженерні мережі, житловий фонд, дороги тощо), створення нових державних баз даних;

- забезпечення єдиного національного геоінформаційного середовища, яке надасть державним органам доступ до сучасного, якісного та повного геоінформаційного матеріалу, інтегрованого з об'єктами обліку державних баз даних;

- системне вирішення завдання збору і переведення в електронний вигляд історичних відомостей для державних баз даних, архівів та відомчих інформаційних систем на державному рівні;
- визначення переліку типових інформаційних систем та їх впровадження в державних і місцевих виконавчих органах в рамках нової моделі інформатизації у вигляді «хмарних сервісів» на основі аналізу процесів органів державної влади та місцевого самоврядування;
- продовження процесу скорочення і спрощення бізнес-процесів із надання державних послуг та їх автоматизація;
- автоматизація функцій місцевих органів виконавчої влади;
- розробка єдиної системи нумерації та кодування адміністративних документів;
- інтенсивний розвиток «мобільного уряду» – одного з напрямів «електронного уряду», призначеного для оперативного представлення результатів державних послуг для громадян і бізнесу за допомогою мобільних пристроїв;
- продовження роботи по значному скороченню документообігу між державними органами шляхом удосконалення регламентів їх роботи з електронними документами, засвідчених електронним цифровим підписом, та впровадження Єдиної системи електронного документообігу на основі «хмарних сервісів» і роботи на мобільних пристроях з використанням засобів криптографічного захисту інформації;
- ужиття заходів щодо інтеграції комерційних і державних систем і сервісів;
- регламентація питань використання ліцензійного та вільного програмного забезпечення.

Поряд з цим в Україні доцільно розробити державну цільову програму «Електронна Україна–2030», спрямовану на налагодження діалогу між державними структурами та громадянським суспільством. У рамках цієї програми з використанням сучасних методів інформаційного обміну між органами державної влади і суспільством будуть створені принципово нові можливості для забезпечення інформаційної відкритості та гласності прийняття рішень, підвищення рівня довіри й взаємодії між суспільством та органами державної влади. При цьому рівень інформованості населення про діяльність держави також буде забезпечуватися через пряму взаємодію державних органів з аудиторією ЗМІ з використанням технології краудсорсингу. Крім того, доцільною є розробка Єдиного інформаційно-аналітичного середовища державних органів, що має стати основним інструментом узгодженого проведення всіх видів реформ державного управління.

ВИСНОВКИ

У дисертації на доктринальному рівні вирішено важливу й актуальну для науки державного управління проблему, яка полягає в системному аналізі стану

та перспектив національної безпеки держави в інформаційній сфері, розробленні нових підходів до вирішення проблемних питань і підготовці науково-прикладних рекомендацій щодо формування та реалізації державної інформаційної політики держави в контексті національної безпеки.

Абсолютно очевидно, що відсутність чіткої стратегії з реалізації державної інформаційної політики призводить не лише до погіршення загальної ситуації, але й серйозних загроз у сфері інформаційної безпеки держави. Саме тому все більшої актуальності набуває вироблення державної концепції інформаційної безпеки саме в сучасних умовах. У зв'язку з цим інформаційну безпеку можна розглядати як одну з обов'язкових умов функціонування сучасної держави.

Аналіз проблем у сфері інформаційної безпеки сучасних держав у цілому та України зокрема засвідчив, що їх державна політика спрямована на формування ефективної політики у сфері інформації і має розглядатися тільки в комплексі з урахуванням системного підходу, що працює в парадигмі функціонування теорії соціальних мереж. З огляду на це забезпечення ефективної системи державного управління національною безпекою України, де інформаційна безпека розглядається як її найважливіша ланка, можливо з урахуванням реалізації наступних основних висновків дисертації, які конкретизуються в таких положеннях:

1. Розкрито сутність інформаційної політики як феномена інформаційного суспільства та забезпечення його безпеки. Узагальнено сучасні теоретико-методологічні та державно-управлінські підходи у сфері розвитку інформаційної політики як невід'ємної частини функціонування інформаційного суспільства через виявлення критеріїв систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки, яка являє собою процес задоволення інформаційних потреб суб'єктів управління у сфері державної безпеки та виконує важливу багатопланову роль стосовно:

- визначення національних інтересів і пріоритетів національної безпеки;
- пошуку нових форм і способів забезпечення державної безпеки;
- впливу на діяльність суб'єктів управління безпекою, з урахуванням формування їх думки і поведінки відповідно до визначених пріоритетів і цінностей державної безпеки;
- розвитку всього механізму прийняття і реалізації державно-управлінських рішень у сфері державної безпеки.

Доведено, що інформаційному суспільству притаманні такі ознаки як:

- наявність єдиного інформаційного простору;
- домінування в економіці та управлінні нових технологічних укладів, що базуються на масовому використанні інформаційно-комунікаційних технологій;
- зростання ролі інфраструктури (телекомунікаційної, транспортної, організаційної) в системі суспільного виробництва і посилення тенденцій до спільного функціонування в економіці інформаційних і грошових потоків;
- зростання значущості проблем забезпечення інформаційної безпеки особистості, суспільства і держави, наявність ефективної системи забезпечення

прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації;

– високий рівень освіти, обумовлений розширенням інформаційного обміну на міжнародному, національному та регіональному рівнях, і відповідно підвищена роль кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик праці;

– провідна роль інформаційних ресурсів у забезпеченні сталого поступального розвитку суспільства;

– фактичне задоволення потреб суспільства в інформаційних продуктах і послугах.

2. Доведено, що методологічні основи інформаційного забезпечення державної політики безпеки держави забезпечуються якісною і високоефективною політикою органів державної влади, яка визначається наступними сутнісними характеристиками: по-перше, вибором форм, методів і способів її здійснення; по-друге, структурою національної безпеки і специфікою реалізації державної інформаційної політики в конкретних умовах. Крім того, показано, що зміст інформаційного забезпечення національної безпеки визначається також і характером інформаційних зв'язків суб'єктів національної безпеки, які пов'язані: з обміном інформацією між суб'єктами забезпечення національної безпеки, що забезпечують створення цілісної організаційної системи; інформаційними зв'язками між людьми, безпосередньо і опосередковано пов'язаними із забезпеченням функціонування системи національної безпеки; інформаційними зв'язками між технічними компонентами системи державної безпеки, оскільки частина інформаційних функцій надмірні для людини, проте є необхідними для забезпечення національної безпеки в сучасних умовах.

Крім того, інформаційні зв'язки можна поділити на дві групи. Першу групу складають змістовні інформаційні зв'язки, які характеризуються структурною (пов'язаною) інформацією. Це зв'язки між елементами видів безпеки; між внутрішніми елементами кожного виду безпеки; між кожним видом безпеки і зовнішнім середовищем (під зовнішнім середовищем тут розуміються національні інтереси інших країн) і т. ін.

Другу групу представляють функціональні інформаційні зв'язки, які характеризуються оперативною інформацією. До них можна віднести суб'єктно-об'єктні зв'язки (між суб'єктами, об'єктами, між суб'єктами і об'єктами, а також усередині них); зв'язки між суб'єктами, об'єктами та джерелами загроз, а також із зовнішнім середовищем. Разом з тим усю сукупність інформаційних зв'язків відносно національної безпеки можна поділити на зовнішні та внутрішні інформаційні зв'язки.

3. Розкрито значення інформаційної безпеки в державно-управлінських відносинах через організацію та здійснення певних принципів інформаційного забезпечення національної безпеки. Показано, що ефективна інформаційна безпека в державно-управлінських відносинах можлива з урахуванням впровадження інформаційного забезпечення національної безпеки за умови дотримання певних принципів. Видається, що найбільш важливими з них є такі:

– повнота інформаційного забезпечення. Результати пошуку повинні містити інформацію в повному обсязі, в той же час звести до мінімуму «шум» і виключити дезінформацію. Основне – вибрати таку пошукову стратегію, щоб споживач отримав інформацію, що відповідає не лише заданій тематиці, а й його інформаційним потребам;

– актуальність інформаційного забезпечення, завдання якого полягає в поданні споживачеві пріоритетної інформації, що відповідає умовам і в установлені терміни;

– точність і надійність інформаційного забезпечення, які полягають у наданні споживачеві всієї необхідної інформації з урахуванням потрібних видів і мовного оформлення, хронологічної глибини тощо;

– інформація повинна подаватись у зручній для споживача формі (машинопис, мікрофільм, екран дисплея тощо);

– диференційованість інформаційного забезпечення з урахуванням функцій споживача, його статусу та оперативності розв'язуваних ним завдань;

– системність інформаційного забезпечення, що проявляється в систематичному задоволенні інформаційних потреб на всіх етапах забезпечення національної безпеки і комплексності видів інформаційного забезпечення з урахуванням категорій споживачів, характеру їх інформаційних потреб, специфіки завдань, що вирішуються.

У сучасних умовах, внаслідок протиріч влади і суспільства комунікативна діяльність органів влади характеризується такими ознаками, як недостатня відкритість, фрагментарність, маніпулятивність технік. У зв'язку з цим, недостатня соціальна відповідальність влади й особливості її комунікації детерміновані інструментальним підходом. Публічні служби використовуються як інструмент збереження владних інтересів, конструювання одностороннього бачення смислів державно-управлінських рішень. В цілому комунікативна модель формування та підтримки відносин з суспільством характеризується як одностороння, в результаті чого утворюється розрив між реальною політикою і інформаційним продуктом, що створює негативні наслідки для легітимності влади.

4. Проаналізовано процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства. Доведено, що процеси інформатизації мають чіткий зв'язок з безпечним стійким розвитком суспільства і держави, що основа глобального інформаційного суспільства та державного управління – знання або інтелектуально-інформаційний ресурс. Оцінюючи результати перспектив забезпечення інформаційної безпеки в умовах становлення глобального інформаційного суспільства, можна зробити такі висновки.

Сучасний етап розвитку інформаційного суспільства характеризується нерівномірністю розвитку й розподілу інформаційно-комунікаційних технологій у різних регіонах світу. Це явище отримало офіційну назву «цифровий розрив» або «інформаційне нерівність». На сучасному етапі існують значні відмінності не тільки між розвиненими країнами та країнами, що розвиваються, а й між різними соціальними групами населення в кожній країні.

В рамках розвитку інформаційного суспільства формується також глобальна система інформаційної безпеки. Для еволюційного, поступального переходу України на новий етап розвитку необхідно забезпечити умову, за якої її національні інтереси будуть природною, невід'ємною складовою частиною інтересів глобального інформаційного співтовариства. Отже, інформаційна безпека України буде одним із складових елементів системи глобальної інформаційної безпеки.

Інформаційне суспільство несе з собою не тільки нові рішення та можливості, а й нові загрози і ризики. Як і будь-яке інше, інформаційне суспільство недосконале, а інформаційно-комунікаційні технології – нейтральні. Наслідки їх застосування залежать від ціннісних настанов і державно-політичних рішень. Реалізація можливостей інформаційного суспільства – питання адекватної політики й своєчасних державно-управлінських рішень.

5. Здійснено порівняльний аналіз вітчизняного та закордонного досвіду розробки й впровадження інформаційного забезпечення державної безпеки. Зазначено, що відповідно до Європейської конвенції про кіберзлочинність (інформаційну безпеку), забезпечення інформаційної безпеки передбачало недопущення чи усунення таких суспільно-небезпечних діянь проти конфіденційності даних: протиправний доступ; перехоплення; порушення цілісності; втручання в роботу; виробництво, обіг та використання спеціальних засобів для комп'ютерних злочинів з використанням комп'ютерів; підроблення; інформаційне шахрайство.

Показано, що в Україні поточне інформаційне забезпечення державної безпеки характеризується наявністю таких проблем:

- малоефективна система державного регулювання національного медіапростору;
- низький рівень присутності у глобальному медіапросторі, високий рівень інформаційної залежності від іноземних держав і структур;
- ринкова стихійність впровадження засобів комп'ютеризації та телекомунікаційних мереж;
- відсутність довгострокової державної стратегії щодо розвитку інформаційної сфери;
- недосконалість законодавства про інформацію;
- недостатній рівень державної підтримки виробництва та розповсюдження інформаційної продукції.

6. Охарактеризовано особливості функціонування організаційно-правового механізму інформаційного забезпечення державної безпеки. Обґрунтовано, що сьогодні слід визнати відсутність єдиного правового поля стосовно регулювання інформаційного забезпечення державної безпеки. Зокрема зазначено, що в різних нормативних актах перераховується велика кількість таємниць, проте за розголошення не всіх з них передбачена відповідальність. Крім того, наголошено, що сучасне законодавство, яке регулює питання забезпечення інформаційної безпеки України, не розглядає інформаційну безпеку у форматі захисту інформаційної свободи.

Здійснено поділ органів державної влади спеціальної компетенції, що регулюють інформаційну безпеку, залежно від певного виду інформаційних відносин, які підлягають інформаційному впливу, та виокремлено такі їх групи:

- органи, які регулюють сферу інформаційних відносин у загальному контексті та впроваджують державну інформаційну політику (Державний комітет телебачення і радіомовлення України);

- органи, що розробляють і впроваджують державну мовну політику та державну політику стосовно захисту суспільної моралі (Міністерство культури та інформаційної політики України);

- органи, які регулюють функціонування сфери отримання і зберігання інформації (Державний служба статистики України та Державна архівна служба);

- органи, що проводять аналіз і моніторинг визначених типів інформації (Державна служба фінансового моніторингу України).

Наголошено, що такий підхід не дозволяє повноцінно здійснювати забезпечення інформаційної безпеки в державі, відтак необхідно чітко визначити частку і межі участі держави у забезпеченні інформаційної безпеки, в тому числі через законодавче встановлення заборон і обмежень в інформаційній сфері.

7. Визначено напрями модернізації єдиної державної політики у сфері інформаційної безпеки:

- збір, систематизація й узагальнення інформації щодо стану процесів інформаційної безпеки на об'єктах управління, оцінка стану інформаційної безпеки в регіоні, виявлення невирішених проблем у забезпеченні інформаційної безпеки, надання необхідної інформації щодо стану інформаційної безпеки органам державної влади та місцевого самоврядування;

- контроль стану інформаційної безпеки на об'єктах управління;

- визначення пріоритетних напрямків забезпечення інформаційної безпеки в державі та регіонах;

- розробка і контроль виконання цільових програм із забезпечення інформаційної безпеки;

- організація науково-технічних досліджень і розробок у сфері забезпечення інформаційної безпеки в державі та регіонах, виконання вимог нормативних документів щодо забезпечення інформаційної безпеки;

- розробка та затвердження регіональних нормативних і методичних документів із забезпечення інформаційної безпеки (концепції, положення, вимоги, норми, моделі, методики, рекомендації, інструкції та інші документи);

- надання методичної допомоги підприємствам, установам та організаціям в підготовці до ліцензування, а також у діяльності, пов'язаній з наданням послуг у сфері інформаційної безпеки, створенням засобів інформаційної безпеки, а також впровадження засобів контролю їх ефективності;

- методичне керівництво підготовкою, професійною перепідготовкою та підвищенням кваліфікації фахівців у сфері інформаційної безпеки;

- координація діяльності органів місцевого самоврядування зі створення

муниципальних систем інформаційної безпеки.

8. Запропоновано шляхи вдосконалення державної системи інформаційної безпеки. Показано, що цілі державної системи інформаційної безпеки досягаються шляхом створення та реалізації механізму забезпечення інформаційної безпеки, що включає:

- органи державної системи інформаційної безпеки, які забезпечують виконання всієї повноти завдань і функцій у сфері інформаційної безпеки та наділені відповідними повноваженнями;

- систему планових законодавчих, організаційно-розпорядчих, нормативних та інформаційних документів, що регламентують і забезпечують діяльність органів державної системи інформаційної безпеки;

- технології, системи і засоби, що знаходяться у віданні органів державної системи інформаційної безпеки.

9. Сформульовано концептуальні положення інформаційного забезпечення державної безпеки. Обґрунтовано, що реалізація Концепції інформаційного забезпечення державної безпеки в кінцевому підсумку сприятиме:

- реалізації конституційних прав громадян на отримання, зберігання і поширення повної, достовірної та своєчасної інформації;

- рівноправній участі України у світових інформаційних відносинах;

- ефективному інформаційному забезпеченню державної політики;

- забезпеченню надійності та стійкості функціонування критично важливих інформаційних систем;

- безперебійному функціонуванню й надійному захисту єдиного національного інформаційного простору.

10. Окреслено стратегічні орієнтири інформаційного забезпечення державної безпеки України. Доведено необхідність формування національної Стратегії інформаційного забезпечення державної безпеки в контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян щодо реалізації цієї Стратегії.

Зроблено висновок, що у Стратегії інформаційного забезпечення державної безпеки необхідно передбачити умови для створення можливостей громадянам освоїти й отримати навички роботи з інформаційними технологіями за допомогою електронної освіти, довічного навчання і підготовки, дистанційної роботи, а також отримання послуг доступної електронної охорони здоров'я. Крім того, з метою побудови більш відкритої, доступної та конкурентоспроможної економіки нашої країни у Стратегії інформаційного забезпечення державної безпеки слід передбачити максимальне впровадження інтелектуальних систем в основні галузі економіки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Монографія

1. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.

Статті у фахових виданнях:

2. Торічний В. О. Основні функції та принципи інформаційного забезпечення держави. *Державно-управлінські студії*. 2018. № 8 (10). URL: <http://studio.ipk.edu.ua/wp-content/uploads/2019/11/Torichnyy-O.V.-Inform.-zabezpr..pdf>

3. Торічний В. О. Проблема інформаційної безпеки в умовах розвитку інформаційного суспільства. *Теорія та практика державного управління*. 2019. № 2 (65). С. 256–262.

4. Торічний В. О. Процеси інформатизації державно-управлінських відносин та їх вплив на безпеку держави. *Теорія та практика державного управління*. 2019. № 4 (67). С. 179–187.

5. Торічний В. О. Формування та впровадження державної інформаційної політики як запорука забезпечення державної безпеки. *Вісник Національного університету цивільного захисту України*. 2019. Вип. 1 (10). С. 64–69. (Серія «Державне управління»).

6. Торічний В. О. Особливості державного управління регіональними системами інформаційної безпеки. *Публічне управління і адміністрування в Україні*. 2019. № 11. С. 183–185.

7. Торічний В. О. Особливості побудови державної системи інформаційної безпеки. *Вчені записки Таврійського національного університету ім. В. І. Вернадського*. 2019. Т. 30 (69). № 3. С. 180–182.

8. Торічний В. О. Інформаційне забезпечення державної політики як найважливіший фактор безпеки держави. *Актуальні проблеми державного управління*. 2019. № 1 (55). С. 77–85.

9. Торічний В. О. Технології формування та реалізації інформаційної політики держави. *Вісник Національного університету цивільного захисту України*. 2019. Вип. 2 (11). С. 201–207. (Серія «Державне управління»).

10. Торічний В. О. Дослідження пропаганди як інструменту інформаційного забезпечення державної безпеки. *Право та державне управління*. 2019. № 3 (36). Т. 2. С. 183–186.

11. Торічний В. О. Дослідження методів оцінки результативності державної інформаційної політики у контексті забезпечення державної безпеки. *Держава та регіони*. 2019. № 3 (67). С. 200–203. (Серія «Державне управління»).

12. Торічний В. О. Інформаційне забезпечення безпеки держави в контексті використання комп'ютерних технологій: державно-управлінський аспект. *Актуальні проблеми державного управління*. 2019. № 2 (56). С. 39–46.

13. Торічний В. О. Стратегічні орієнтири інформаційного забезпечення державної безпеки України *Державне управління: удосконалення та розвиток*. 2019. № 11. URL: <http://www.dy.nauka.com.ua/?op=1&z=1711>

14. Торічний В. О., Шведун В. О. Державний функціональний комплекс

забезпечення інформаційної безпеки на прикладі ветеринарного нагляду і контролю. *Публічне управління і адміністрування в Україні*. 2020. Вип. 15. С. 118–121.

Особистий внесок здобувача: розробка методичного підходу щодо застосування заходів щодо забезпечення інформаційної безпеки у спеціалізованих галузях.

15. Торічний В. О., Шведун В. О. Державні механізми забезпечення корпоративної інформаційної культури. *Державно-управлінські студії*. 2019. №1(12). URL: <http://studio.ipk.edu.ua/wp-content/uploads/2020/02/Borovs-ka-7.pdf>

Особистий внесок здобувача: пропозиція комплексу заходів щодо вдосконалення державних механізмів забезпечення інформаційної культури.

16. Торічний В. О. Система інформаційного забезпечення державної безпеки України. *Державне будівництво*. 2020. № 1. URL: www.kbuara.kharkov.ua/e-book/db/2020-1/index.html

17. Торічний В. О. Умови ефективної розробки та впровадження державної інформаційної політики. *Публічне управління та митне адміністрування*. 2020. № 2 (25). С. 50–62.

Статті у зарубіжних спеціалізованих виданнях:

18. Торичный, В. А. (2018). Научные основы формирования и реализации государственной политики украины в сфере информационной безопасности. *East Journal of Security Studies*. 3 (1). Retrieved from: <http://repositsc.nuczu.edu.ua/bitstream/123456789/10661/1/torichnyiEJSS.pdf>.

19. Torichnyi, V. (2019). Information support of the national security of the state in the context of globalization. *East Journal of Security Studies*. 4 (1), 56–66. Retrieved from: <https://ejss.nuczu.edu.ua/index.php/ejss/article/view/9>.

20. Торичный В. А. Концептуальные основы формирования и реализации государственной политики в сфере информационной безопасности. *Authority and society*. 2019. № 4 (52). С. 343–349.

21. Торичный В. А. Субъектно-объектная составляющая механизма государственного управления в сфере информационной безопасности / В. А. Торичный. *Virtus*. 2020. № 42. С. 193–196.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

22. Торічний В. О. Необхідність створення і розвитку державної системи інформаційної безпеки: впровадження європейського досвіду дослідження впливових факторів. *Актуальні проблеми європейської та євроатлантичної інтеграції України* : матеріали 16-ої регіон. наук.-практ. конф. Дніпро : ДРІДУ НАДУ, 2019. С. 229–230.

23. Торічний В. О. Дослідження суперечностей у системі інформаційного забезпечення державної безпеки соціуму в умовах функціонування цифрового суспільства. *Актуальні проблеми економіки, управління та фінансів* : матеріали міжнар. наук.-практ. конф. Дніпро : Університет митної справи та фінансів, 2019. С. 141–143.

24. Торічний В. О. Формування та реалізація єдиної державної політики у сфері інформаційної безпеки. *Державне управління у сфері цивільного захисту: наука, освіта, практика* : матеріали міжнар. наук.-практ. конф. Харків : Вид-во НУЦЗУ, 2019. С. 112–113.

25. Торічний В. О. Процеси управління інформаційним забезпеченням соціальної безпеки в державі: особливості та вимоги. *Інформаційні технології: наука, техніка, технологія, здоров'я* : тези доповідей XXVII наук.-практ. конф. MicroCAD-2019. Ч. IV. Харків : НТУ «ХП», 2019. С. 122.

26. Торічний В. О. Застосування інформаційно-комунікаційних технологій при реалізації освіти протягом життя. *Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти* : матеріали III Всеукр. наук.-практ. інтернет-конф. Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. URL: <https://drive.google.com/file/d/1kyurQfLDyMbzXusWvuzpKw5Nnanog2Hc/view>.

27. Торічний В. О. Інформаційна безпека як чинник функціонування сучасної держави в контексті формування суспільства знань. *Формування громадянської культури в новій українській школі: традиційні та інноваційні практики* : матеріали II Всеукр. наук.-практ. конф. Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. С. 254–256.

28. Торічний В. Державне управління у сфері боротьби з комп'ютерними злочинами як напрям забезпечення національної безпеки й охорони громадського порядку. *Забезпечення діяльності складових сектору безпеки і оборони України* : тези міжнар. наук.-практ. конф. Хмельницький : Вид-во НАДПСУ, 2019. С. 574–575.

29. Торічний В.О. Розробка інноваційних методів державного захисту територіального інформаційного простору. Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад : матеріали науково-практичної конференції за міжнародною участю. Дніпро : ДРІДУ НАДУ, 2019. С. 301–302.

30. Торічний В. О. Критерії та умови ефективності впровадження механізму реалізації державної інформаційної політики. *Державне управління у сфері цивільного захисту: наука, освіта, практика* : матеріали міжнар. наук.-практ. конф. інтернет-конф. Харків : Вид-во НУЦЗУ, 2020. С. 80–81.

31. Торічний В. О. Шляхи підвищення інформаційної безпеки на державному рівні. *Інформаційні технології: наука, техніка, технологія, здоров'я* : тези доп. XXVIII наук.-практ. конф. MicroCAD-2020. Ч. V. Харків : НТУ «ХП», 2020. С. 128–129.

АНОТАЦІЯ

Торічний В. О. Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної

безпеки та охорони громадського порядку. Національний університет цивільного захисту України, Харків, 2020.

У дисертації визначено сутність інформаційної політики як феномена інформаційного суспільства і забезпечення його безпеки за допомогою критеріїв систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки. Досліджено методологічні основи інформаційного забезпечення державної політики безпеки держави, класифіковано методи оцінки, отримання, подачі інформації при здійсненні інформаційної безпеки, розкрито значення інформаційної безпеки в державно-управлінських відносинах у контексті процесів демократизації суспільства, охарактеризовано роль державно-управлінських інститутів як ключових суб'єктів реалізації інформаційної політики забезпечення національної безпеки сучасної України. Проаналізовано процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства, здійснено порівняльний аналіз вітчизняного й закордонного досвіду розробки та впровадження інформаційного забезпечення державної безпеки, визначено особливості функціонування організаційно-правових механізмів інформаційного забезпечення державної безпеки, а також охарактеризовано поточний стан і тенденції розвитку державної інформаційної політики в Україні.

Розроблено комплекс заходів з інвентаризації та категорювання інформаційних ресурсів у державному та регіональному інформаційному просторі, запропоновано напрями модернізації єдиної державної політики у сфері інформаційної безпеки, а також сформульовано пропозиції щодо вдосконалення державної системи інформаційної безпеки.

Сформульовано концептуальні положення інформаційного забезпечення державної безпеки, виокремлено стратегічні орієнтири та розроблено пропозиції щодо напрямів трансформації системи інформаційного забезпечення державної безпеки України.

Ключові слова: державне управління, інформаційне забезпечення, національна безпека, державна інформаційна політика, державна система інформаційної безпеки, стратегія державного забезпечення інформаційної безпеки.

АННОТАЦІЯ

Торичный В. А. Информационное обеспечение государственной безопасности Украины в условиях трансформационных вызовов и угроз. – Квалификационный научный труд на правах рукописи.

Диссертация на соискание ученой степени доктора наук по государственному управлению по специальности 25.00.05 – государственное управление в сфере государственной безопасности и охраны общественного порядка. Национальный университет гражданской защиты Украины, Харьков,

2020.

В диссертации определена сущность информационной политики как феномена информационного общества и обеспечения его безопасности с помощью критериев систематизации и соответствующих им форм и видов информационного обеспечения национальной безопасности. Исследованы методологические основы информационного обеспечения государственной политики безопасности государства, классифицированы методы оценки, получения, подачи информации при реализации информационной безопасности, раскрыто значение информационной безопасности в государственно-управленческих отношениях в контексте процессов демократизации общества, охарактеризована роль государственно-управленческих институтов как ключевых субъектов реализации информационной политики обеспечения национальной безопасности современной Украины. Проанализирован процесс информатизации государственно-управленческих отношений в формировании государственной безопасности в условиях глобального информационного общества, осуществлен сравнительный анализ отечественного и зарубежного опыта разработки и внедрения информационного обеспечения государственной безопасности, определены особенности функционирования организационно-правовых механизмов информационного обеспечения государственной безопасности, а также охарактеризованы текущее состояние и тенденции развития государственной информационной политики в Украине.

Разработан комплекс мероприятий по инвентаризации и категорированию информационных ресурсов в государственном и региональном информационном пространстве, предложены направления модернизации единой государственной политики в сфере информационной безопасности, а также сформулированы предложения по совершенствованию государственной системы информационной безопасности.

Сформулированы концептуальные положения информационного обеспечения государственной безопасности, выделены стратегические ориентиры и разработаны предложения по направлениям трансформации системы информационного обеспечения государственной безопасности Украины.

Для достижения поставленной цели и решения обусловленных ею задач, обеспечения научной обоснованности исследования и его результатов был использован комплекс общенаучных и специальных методов, основанных на современных научных принципах государственно-управленческой и родственных с ней наук.

Так, с помощью методов индукции и дедукции сформирована методология диссертационной работы, что позволило сформулировать гипотезу исследования и построить эвристические модели информационного обеспечения государственной безопасности. Основой для определения уровня разработанности в научной литературе процессов информационного обеспечения государственной безопасности стали методы научного обобщения

и логического анализа. В работе также применен системный подход – для совершенствования системы информационного обеспечения государственной безопасности. Использование сравнительного метода обусловлено необходимостью сравнения отечественного и зарубежного опыта разработки и внедрения информационного обеспечения государственной безопасности.

Нормативно-ценностный подход применен для оценки и анализа государственной информационной политики с точки зрения ее аксиологической сущности, соответствия функционирующим и идеальным нормам и ценностям. В работе также использовался метод структурного моделирования – для построения модели Стратегии информационного обеспечения государственной безопасности.

Ключевые слова: государственное управление, информационное обеспечение, национальная безопасность, государственная информационная политика, государственная система информационной безопасности, стратегия государственного обеспечения информационной безопасности.

ANNOTATION

Torichniy V. O. Information support of state security of Ukraine in conditions of transformational challenges and threats. – *The qualified scientific work on the right of manuscript.*

Dissertation on competition of Doctor of Sciences degree in Public Administration by specialty 25.00.05 – Public Administration of State Security and Enforcement of Public Order. National University of Civil Defence of Ukraine, Kharkiv, 2020.

The thesis reveals: the essence of information policy as a phenomenon of the information society and ensuring of its security by identifying the systematization criteria and appropriate forms, types, information support of national security. Also the methodological basis of information support of the state security policy is studied, the methods of assessment, receipt and submission of information within implementation of information security of Ukraine are classified, the importance of information security of public-management processes in the context of democratization of society is revealed, the role of state-management institutions as key factors in the implementation of information policy to ensure the national security of modern Ukraine is shown, the process of informatization of public-management relations in formation of state security in conditions of global information society is analyzed.

In addition, the foreign experience concerning development and implementation of the state security information support are analyzed, the peculiarities of the functioning of organizational and legal mechanisms of the state security information support are highlighted, the current state and trends of development of state information policy in Ukraine were described.

A set of measures to inventory and categorize the information resources in the state and regional information space is carried out in the work, the directions of

modernization of the unified state policy in the field of information security are proposed, the proposals for improvement of the state information security system are formulated.

The conceptual bases of information support of state security are formulated in the work. Besides, the strategic guidelines of information support of state security of Ukraine are identified, the directions of transformation of the system of information support of state security of Ukraine are proposed.

A set of popular scientific and special methods based on modern scientific principles of state-management and related sciences is used in the work in order to achieve the stated goal, to solve the tasks caused by it, and to ensure scientific validity of research and its results.

The methodology of dissertation work is formed with the help of induction and derivation methods, which allowed formulating a hypothesis of the study, as well as building of the heuristic models of information support of state security. The methods of scientific generalization and logical analysis are the basis for determining of the level of development of processes of information support of state security in the scientific literature. The systematic approach is also used in the work - to improve the system of information support of state security. The presence of a comparative method in the study is due to the need to compare domestic and foreign experience concerning development and implementation of state security information support.

The use of a normative and value approach is caused by the need to evaluate and analyze public information policy in terms of its axiological nature and its compliance with functioning and ideal norms and values. The dissertation work also uses the method of structural modeling - to build a model of the State Security Information Support Strategy.

Keywords: public administration, information support, national security, state information policy, state information security system, state information security strategy.

Відповідальна за випуск *Шведун Вікторія Олександрівна*

Підписано до друку 03.07.2020 р.
Формат 60x84 ¹/₁₆. Обл.-вид. арк. 2,5.
Гарнітура Таймс. Тираж 100 прим.

Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80.