

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ



СПОРИШЕВ Костянтин Олександрович

УДК 351.74:355/359:004

**МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ
ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ
СИЛ БЕЗПЕКИ УКРАЇНИ**

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

РЕФЕРАТ

дисертації на здобуття наукового ступеня
доктора наук з державного управління

Харків
2024

Дисертацією є рукопис.

Роботу виконано в Національній академії Національної гвардії України.

Науковий консультант – **БЄЛАЙ Сергій Вікторович**,

доктор наук з державного управління, професор,
Національна академія Національної гвардії України,
заступник начальника навчально-наукового центру
організації освітнього процесу – начальник науково-
методичного відділу.

Офіційні опоненти:

ГРИЦИШЕН Дмитрій Олександрович,

доктор наук з державного управління, професор,
Державний університет «Житомирська політехніка»,
проректор з науково-педагогічної роботи
та інноваційного розвитку;

КРАВЧУК Олег Вікторович,

доктор наук з державного управління, професор,
Хмельницький університет управління та права імені
Леоніда Юзькова, професор кафедри
кримінального права та процесу;

ПОМАЗА-ПОНОМАРЕНКО Аліна Леонідівна

доктор наук з державного управління,
старший дослідник,
Національний університет цивільного захисту України,
начальник наукового відділу з дослідження проблем
державної безпеки науково-дослідного центру.

Захист відбудеться «27» вересня 2024 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. вул. Майка Йогансена, 28, ауд. 4 (1-й поверх).

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

Вчений секретар
спеціалізованої вченої ради



Світлана МОРОЗ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Розвиток інформаційних технологій впливає на всі сфери людської діяльності. Не є виключенням й державна політика у сфері забезпечення національної безпеки. Інформаційно-аналітична підтримка дій сил безпеки дає змогу виконувати їх з достатньою ефективністю та як результат – забезпечити державну безпеку на потрібному рівні. Розвиток інформаційно-аналітичного забезпечення складових сектору безпеки і оборони України має відповідати сучасним і прогнозованим геостратегічним, соціально-політичним, економічним і військово-технічним загрозам та забезпечувати максимальну ефективність і здатність давати адекватну відповідь реальним і потенційним викликам державній безпеці України.

Загрози національним інтересам та національній безпеці України в інформаційній сфері визначено у Стратегіях національної безпеки та інформаційної безпеки України, затверджених, відповідно, Указами Президента України від 14.09.2020 № 392/2020 та від 28.12.2021 № 685/2021. Одним з основних завдань політики держави у сфері захисту суверенітету і територіальної цілісності України є підтримка в боєздатному стані складових сектору безпеки і оборони через організацію раціональних управлінських впливів. Відсіч збройній агресії російської федерації проти України залежить від ефективного управління силами безпеки і оборони. Характерною особливістю ведення сучасних службово-бойових дій є інтенсивне використання інформаційних технологій та автоматизованих систем управління силами і підрозділами, що значно змінює підходи до стратегії та тактики їх застосування.

До основних тенденцій державного управління у сфері державної безпеки можна віднести: а) модернізацію сил безпеки і оборони за допомогою цифрових технологій, що дає їм змогу швидко обмінюватися інформацією; координувати дії та підвищувати ефективність дій за призначенням; унеможливити негативні кібернетичні впливи, які здатні впливати на роботу критично важливих інфраструктур, та вести інформаційні операції; б) використання штучного інтелекту для аналізу великих обсягів даних, управління системами зброї та моделювання службово-бойових дій; в) стрімкий розвиток інформаційних технологій, що дає змогу збирати точнішу і актуальнішу інформацію про стан сил безпеки, їх службово-бойову діяльність, підвищуючи оперативну обізнаність і реактивність сил; г) використання інтелектуальних систем високоточного озброєння, що дає змогу ефективно вражати цілі з мінімальними колатеральними втратами.

До основних проблемних питань державної політики щодо інформаційно-аналітичного забезпечення органів управління сил безпеки станом на сьогодні належать: а) недостатній рівень розроблення нормативно-правової бази в силах безпеки України щодо створення інформаційних ресурсів і продуктів, надання інформаційних послуг та функціонування системи інформаційно-аналітичного забезпечення органів управління в цілому; б) відсутність системи інформаційно-аналітичних органів сил безпеки, пов'язаних між собою функціонально, технологічно та технічно; в) відсутність єдиної системи державної класифікації і

кодування інформації в силах безпеки України; г) недостатній рівень розвитку загальних інформаційних ресурсів та відсутність інтегрованого банку даних, який має стати елементом загальнодержавної інформаційної структури; д) необхідність використання системного сертифікованого програмно-математичного забезпечення, що вже зарекомендувало себе в практичній діяльності; е) відсутність сертифікованих засобів закриття інформації; ж) відсутність чітко визначеного комплексу спеціального програмно-математичного забезпечення інформаційної діяльності; и) необхідність підготовки фахівців для роботи в сучасних інформаційно-аналітичних системах; к) відсутність комплексного підходу в організації досліджень щодо вирішення проблем створення системи інформаційного забезпечення сил безпеки України. На цей час недостатньо проводяться дослідження за такими напрямками, як удосконалення нормативно-правової бази, удосконалення системи інформаційно-аналітичних підрозділів, створення комплексної системи захисту інформації, розроблення системних вимог щодо сертифікації засобів інформатизації та інформаційно-телекомунікаційних систем у силах безпеки України.

Беручи до уваги зазначене, нинішні механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України потребують подальшого розвитку, а в деяких напрямках – реформування.

Розглядаючи наукові та методичні засади, слід зазначити, що інформаційно-аналітичне забезпечення сил безпеки України як система являє собою сукупність засобів, технологій, особового складу підрозділів і частин, які експлуатують бойову та іншу техніку, персоналу, який проводить аналітичну діяльність, а також органів управління. За таких умов актуальність дослідження обраної теми визначається необхідністю розроблення та вдосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Теоретичним та прикладним аспектам функціонування, формування й розвитку державного управління у сфері реагування сил безпеки України на виклики сьогодення приділено увагу досить широкого кола досліджень вітчизняних науковців, зокрема С. В. Белая, С. М. Домбровської, В. І. Довганя, Д. О. Грицишина, І. В. Євтушенка, В. О. Копанчука, О. В. Кравчука, С. О. Кузніченка, О. В. Мейка, С. Т. Полторака, А. Л. Помази-Пономаренко, А. І. Семенченка, Л. В. Сергієнко, Г. П. Ситника, Т. С. Ярового та ін.

Питання забезпечення інформаційної безпеки держави розглянуто в працях таких вчених, як: Г. В. Андрусів, В. В. Гафнер, П. І. Гаранюк, В. В. Демиденко, І. В. Діордіца, В. Б. Дудикевич, І. М. Забара, В. С. Зачепило, Є. В. Іванченко, І. С. Іванченко, Н. В. Камінська, Б. А. Кормич, І. В. Костюк, О. О. Климчук, М. І. Лібікі, В. А. Ліпкан, С. В. Любарський, Р. Е. Моландер, Т. М. Мужанова, І. Р. Опірський, А. В. Пазюк, А. І. Партика, Г. Г. Почепцов, В. М. Петрик, М. М. Присяжнюк, Г. В. Сасин, О. І. Сивак, П. П. Ткачук, В. О. Хорошко, Ю. Є. Хохлачова, П. І. Шевчук, О. В. Цуканова, О. М. Щурко. Крім того, серед закордонних науковців слід виокремити розробки D. Alberts, J. Garstka, R. Hayes, A. David, J. McKittrick, J. Nye, J. Fountain, M. Schönberger, E. Anderson.

Дослідження проблемних питань державного управління в частині інформаційних ресурсів України висвітлено в доробку таких вчених, як Ю. Г. Даник, В. М. Варенко, Н. Є. Лелюк, Ю. О. Саричев, Є. Б. Смірнов, О. Ю. Пермяков, С. В. Пеньков, В. В. Шендрик, Н. Ф. Чечетова тощо.

Науковцями зроблено значний внесок у дослідження елементів державної політики щодо розвитку інформаційно-аналітичного забезпечення в різних сферах життєдіяльності суспільства. Проте слід зазначити, що вони розглядали лише окремі питання державного управління системою інформаційно-аналітичного забезпечення сил безпеки. Водночас комплексного дослідження щодо опрацювання механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України не проводилося, що зумовило вибір теми та її актуальність. Наведені вище питання потребують проведення окремого дослідження та розроблення відповідних теоретичних і практичних рекомендацій.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота пов'язана з планами наукових досліджень Національної академії Національної гвардії України за темами: «Методи та способи оцінювання можливостей бригади оперативного призначення Національної гвардії України» (держ. реєстр. № 0217U000719), особистий внесок – обґрунтування шляхів розвитку нормативно-правової бази функціонування системи інформаційно-аналітичного забезпечення сил безпеки України, генезису дій сил безпеки України в парадигмі державної безпеки, розроблення показників можливостей та ефективності дій бригади, підходів щодо розрахунку їх значень, методів та способів оцінювання значень показників можливостей бригади оперативного призначення; «Обґрунтування нових тактичних прийомів і способів дій підрозділів Національної гвардії України при забезпеченні громадської безпеки та охороні громадського порядку під час масових заходів та з припинення масових заворушень» (держ. реєстр. № 0115U002858), особистий внесок – дослідження організаційного механізму державного управління системою інформаційно-аналітичного забезпечення сил безпеки України; «Угруповання Національної гвардії України під час участі в ліквідації катастрофи техногенного характеру (на гідроелектростанції)» (держ. реєстр. № 0116U005048), особистий внесок – визначення механізму застосування геоінформаційних систем у державному управлінні силами безпеки України.

Мета і завдання дослідження. *Мета* роботи полягає в теоретико-методологічному обґрунтуванні й розробленні практичних рекомендацій щодо формування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Для досягнення мети дослідження визначено такі *завдання*:

- оцінити вплив системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку;
- розвинути засади функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України;
- визначити аспекти функціонування підсистеми захисту інформації в суб'єктах сил безпеки України;

- удосконалити організаційний механізм державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;
- запропонувати шляхи розвитку правового механізму функціонування системи інформаційно-аналітичного забезпечення сил безпеки України;
- обґрунтувати підходи до застосування геоінформаційних систем у державному управлінні силами безпеки України;
- надати пропозиції з удосконалення підготовки кадрових ресурсів у системі інформаційно-аналітичного забезпечення сил безпеки України;
- обґрунтувати ключові напрямки для підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України;
- сформувати загальнодержавну модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;
- розробити стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Об'єкт дослідження – державне управління у сфері інформаційно-аналітичного забезпечення сил безпеки.

Предмет дослідження – механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Методи дослідження. Для досягнення зазначеної мети дослідження і вирішення відповідних завдань широко використовувалися загальні та спеціальні методи наукового пізнання.

Дисертаційне дослідження побудовано на системному, синергетичному та програмно-цільовому підходах, а також сукупності методів, які забезпечують їхню реалізацію, а саме:

- історичної аналогії, системного та морфологічного аналізу – для дослідження теоретичних засад функціонування системи інформаційно-аналітичного забезпечення сил безпеки;
- моделювання, абстрагування, діалектичного аналізу – для обґрунтування теоретико-методологічних засад дослідження проблем державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;
- логіко-семантичного аналізу, індукції та дедукції – для дослідження ефективності планування інформаційно-аналітичної діяльності в силах безпеки України;
- правового, порівняльного та структурно-функціонального аналізу – для обґрунтування підходів до розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;
- структурно-логічного аналізу, SWOT-аналізу, синтезу та узагальнення – для формування шляхів удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Нормативно-правовою та емпіричною базою дисертаційного дослідження є Конституція України, міжнародно-правові конвенційні документи, закони, що регулюють систему державного управління силами безпеки України, а також відповідні укази Президента України, постанови та розпорядження Уряду України, відомчі нормативні акти щодо окремих аспектів інформаційно-

аналітичного забезпечення сил безпеки України.

Наукова новизна дисертаційної роботи й отриманих результатів полягає у вирішенні актуальної наукової проблеми теоретико-методологічного обґрунтування та розроблення практичних рекомендацій щодо вдосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Водночас наукова новизна конкретизується в таких положеннях:

уперше:

– обґрунтовано загальнодержавну модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, яка базується на: формуванні організаційної структури інформаційно-аналітичного забезпечення; оптимізації контролю у сфері функціонування системи інформаційно-аналітичного забезпечення; удосконаленні нормативно-правової бази; підготовці й перепідготовці персоналу у сфері інформаційно-аналітичного і фінансового забезпечення та дає змогу визначити впливи державного управління на систему інформаційно-аналітичного забезпечення сил безпеки для подальшого удосконалення інформаційно-аналітичної діяльності сил безпеки України;

– проведено системне і комплексне дослідження стратегічних засад розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, які охоплюють комплекс стратегій, що розроблені на базі інструментарію SWOT-аналізу, та дають можливість визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;

– сформовано ключові напрямки для підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України, які полягають в обґрунтуванні теоретичних засад функціонування системи інформаційно-аналітичного забезпечення сил безпеки, визначенні методологічних засад розвитку системи інформаційно-аналітичного забезпечення сил безпеки щодо зміцнення обороноздатності держави, а також розробленні механізму державного управління системою інтеграції технологій у систему інформаційно-аналітичного забезпечення сил безпеки України та створенні інформаційного механізму державного управління інформаційно-аналітичного забезпечення сил безпеки України;

удосконалено:

– організаційний механізм державного управління системою інформаційно-аналітичного забезпечення сил безпеки України за допомогою створення інформаційної координації між підрозділами та суб'єктами сил безпеки, адаптації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України до потреб економіки, а також забезпечення високого рівня захисту даних та приватності;

– методи оцінювання впливу системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку внаслідок комплексної дії факторів, що спрямовані на забезпечення службово-бойової діяльності сил безпеки та охоплюють матеріально-технічну, інформаційну, фінансову та

кадрову складові механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, здійснюючи таким чином дієвий державний контроль у сфері інформаційно-аналітичного забезпечення сил безпеки України;

– правовий механізм функціонування системи інформаційно-аналітичного забезпечення сил безпеки України через обґрунтування загальнодержавних підходів до перспектив розвитку інформаційно-аналітичного забезпечення, базуючись на систематизації нормативно-правових актів інформаційно-аналітичного забезпечення сил безпеки України;

дістали подальшого розвитку:

– теоретико-методологічні засади функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України на основі дослідження сутності безперервності управління силами безпеки, визначення ролі та місця інформаційно-аналітичного забезпечення в циклі управління силами безпеки, а також визначення впливу стану системи інформаційно-аналітичного забезпечення сил безпеки України під час виконання службово-бойових завдань на забезпечення державної безпеки;

– теоретико-методологічні аспекти функціонування підсистеми захисту інформації в суб'єктах сил безпеки України на основі комплексного підходу до кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури;

– концепція підготовки кадрових ресурсів у системі інформаційно-аналітичного забезпечення сил безпеки України, яка базується на використанні інформаційних технологій автоматизації управління персоналом, управлінні компетенціями та плануванням потреб у навчанні, використанні аналітичних інструментів для прогнозування потреб у персоналі, аналізові тенденцій на ринку праці, оцінюванні ефективності персоналу та прийнятті обґрунтованих рішень;

– підходи до застосування геоінформаційних систем у державному управлінні силами безпеки України через розвиток стратегічного планування та оперативного реагування, що сприяє посиленню обороноздатності країни та захисту національних інтересів, дослідження впливу геоінформаційних систем на ефективність управління в секторі безпеки і оборони України з огляду на особливості завдань, що вирішуються в суб'єктах сил безпеки України.

Практичне значення одержаних результатів полягає в можливості й доцільності використання основних положень і висновків дисертації для розроблення наукової та навчальної літератури, а також у практичній діяльності органів державної влади і місцевого самоврядування щодо процесів розроблення ними державно-управлінських рішень для формування та реалізації державної політики у сфері функціонування і розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Основні теоретичні положення і висновки дисертаційної роботи були взяті до уваги та використовуються у практичній діяльності Департаменту з питань оборонної роботи, цивільного захисту та взаємодії з правоохоронними органами Харківської обласної військової адміністрації (довідка про впровадження від 12.03.2024), Східного територіального управління Національної гвардії України (військова частина 3001) (довідка від 29.03.2024), ОУВ «Харків» тактичної групи «СЛОБОДА» (довідка від 15.04.2023), Рубіжанської міської військової адміністрації Сєверодонецького району Луганської області (довідка від 15.04.2023).

Крім того, теоретичні положення і наукові результати дослідження впроваджено у навчальний процес Національної академії Національної гвардії України на кафедрі забезпечення державної безпеки, кафедрі військового зв'язку та інформатизації командно-штабного факультету під час підготовки за навчальними дисциплінами «Тактико-спеціальна підготовка», «Інформаційні технології та електронні комунікаційні системи», а також у процесі проведення наукових досліджень за напрямом розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення складових сектору безпеки і оборони України (акт впровадження результатів дисертаційного дослідження від 17.05.2024).

Особистий внесок здобувача. Дисертаційна робота є завершеним самостійним науковим дослідженням, що містить авторське розуміння і визначення державного управління системою технічного забезпечення сил безпеки України в умовах кризових ситуацій та шляхів їх подальшого вдосконалення. Наукові результати і висновки, обґрунтовані та викладені в дисертації, одержані автором особисто. Конкретний внесок здобувача у восьми наукових працях, підготовлених у співавторстві з Л. В. Антоною, О. В. Батюком, С. В. Белаєм, В. В. Бурнатним, Г. П. Власовою, С. М. Гололобовим, І. В. Євтушенком, В. В. Ємановим, М. Ф. Криштановичем, О. С. Онопрієнко, Т. О. Панфіловою, М. С. Пузиревим, О. І. Шаповаловим, зазначено у списку опублікованих праць за темою дисертації.

Апробація результатів дослідження. Основні положення та результати дисертаційного дослідження були оприлюднені на таких науково-комунікативних заходах, як: V Всеукраїнська науково-практична конференція кафедри тактики командно-штабного факультету Національної академії Національної гвардії України «Участь правоохоронних органів та військових формувань держави у забезпеченні безпеки України» (м. Харків, 2020); Тринадцята міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси» (м. Київ, 2020); Всеукраїнська науково-практична конференція «Проблеми бойового та логістичного забезпечення складових сектору безпеки і оборони України» (м. Харків, 2021); XI Міжнародна науково-практична конференція «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів» (м. Харків, 2022); Всеукраїнська науково-практична конференція «Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття» (м. Житомир, 2023); XII Міжнародна

науково-практична конференція «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів» (м. Харків, 2023); міжвідомчий круглий стіл співробітників підрозділів СБУ, науково-педагогічних працівників Національної академії СБУ «Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони в умовах воєнного стану» (м. Київ, 2023); Міжнародна науково-практична інтернет-конференція «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (м. Харків, 2024); XLI Міжнародна науково-практична конференція «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (м. Анкара, 2024); III Міжнародна науково-практична конференція «Публічне управління в Україні: виклики сьогодення та глобальні імперативи» (м. Хмельницький, 2024); XLII Міжнародна науково-практична конференція «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (м. Мілан, 2024); XLIII Міжнародна науково-практична конференція «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (м. Пештера, 2024); XLIV Міжнародна науково-практична конференція «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (м. Умео, 2024).

Публікації. Матеріали дисертаційної роботи викладено у 38 публікаціях, зокрема це: 2 монографії (з яких – одна колективна), 22 наукові статті у фахових виданнях (з яких 3 – у наукометричних базах Scopus та Web of Science), 11 тез доповідей у збірниках матеріалів наукових форумів та 3 наукових статтях, що додатково відображають наукові результати дисертації.

Дисертація складається зі вступу, п'яти розділів та додатків. Загальний обсяг дисертації становить 444 сторінки. Обсяг основного тексту складає 395 сторінок і містить 5 рисунків, 6 таблиць, 2 додатки на 14 сторінках та список використаних джерел у кількості 300 найменувань на 34 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність вибраної теми; з'ясовано зв'язок дослідження з науковими програмами, планами, темами, визначено мету і завдання, об'єкт і предмет, методи дослідження. Розкрито наукову новизну та практичне значення одержаних результатів. Наведено відомості про апробацію і впровадження результатів, структуру дисертації.

У **першому розділі** «*Теоретичні основи державного управління системою інформаційно-аналітичного забезпечення сил безпеки*» досліджено теоретичні основи державного управління системою інформаційно-аналітичного забезпечення сил безпеки. Проведено аналіз інформаційних загроз державній безпеці України, розглянуто стан інформаційно-аналітичних технологій у сучасному державному управлінні, представлено генезис інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки України.

Розкрито основні підходи щодо трактування інформаційної безпеки в контексті національної безпеки. Інформаційна безпека є, з одного боку, самостійним елементом національної безпеки будь-якої країни, а з іншого боку – інтегрованою складовою будь-якої іншої безпеки: військової, економічної,

політичної тощо.

Для сил безпеки України інформаційну безпеку в контексті національної безпеки фахівці розглядають як інтегральний показник, який складається з показників інформаційно-технічної безпеки, протидії кіберзлочинності, інформаційного протиборства.

Суб'єктами забезпечення інформаційної безпеки України слід вважати систему державних і недержавних інституцій, а також громадян України, об'єднаних спільною метою щодо захисту національних інтересів в інформаційній сфері. Отже, коло суб'єктів забезпечення інформаційної безпеки України являє собою багаторівневу систему, що має спільну мету – забезпечення інформаційної безпеки України, але різні повноваження, можливості, засоби тощо.

Проведений аналіз дав змогу визначити такі напрями застосування інформаційних технологій у службово-бойовій діяльності сил безпеки, а саме: а) у системах управління суб'єктами сил безпеки; б) у системах управління озброєнням та військовою технікою; в) як засіб протидії (зброї); г) як підґрунтя для структурно-функціональної трансформації сил безпеки та розроблення нових концепцій службово-бойової діяльності сил безпеки.

Завоювання та утримання інформаційної переваги передбачає проведення заходів, спрямованих проти системи управління та прийняття рішення, а також проти комп'ютерних та інформаційних мереж і систем противника.

Таким чином, новітні інформаційні технології перетворюються нині в системоутворювальний фактор сучасних службово-бойових дій. Світова практика показує, що інформаційне навантаження на органи управління значно збільшується. Об'єм інформації, що створюється і використовується у світовому суспільстві, постійно зростає в середньому на 57 % щороку. У цій же пропорції відбувається й зростання інформаційного навантаження на органи військового управління. Прийняття рішень через декілька років без сучасного інформаційно-аналітичного забезпечення буде для органів управління проблематичним.

Увага до двостороннього характеру протистояння є найбільш важливою методологічною особливістю моделювання. Складними є процеси протистояння двох антагоністичних систем, які вступають між собою не тільки в бойовий, але і в інтелектуальний конфлікт, що передбачається задумами дій сторін. З огляду на це, протистояння (операція, бій) розглядаються сьогодні не тільки як протиборство двох антагоністичних систем, але і як системи, що одночасно реалізують увесь свій інформаційний, морально-бойовий, психологічний та морально-технічний потенціал, який відбивається у двох рішеннях конфлікувальних сторін, тобто інтелектуальному протиборстві двох супротивників, що реалізують свої рішення крізь призму дій підпорядкованих сил та засобів.

Такий підхід дає змогу створити біполярну модель, яка має у своєму складі два конкурувальних центри управління, що представлені відповідними моделями на декількох рівнях (рис. 1). У цій моделі на перший план висунуто не матеріальну складову протиборства, а прийняте командиром рішення та покладені на сили (підрозділи) завдання.

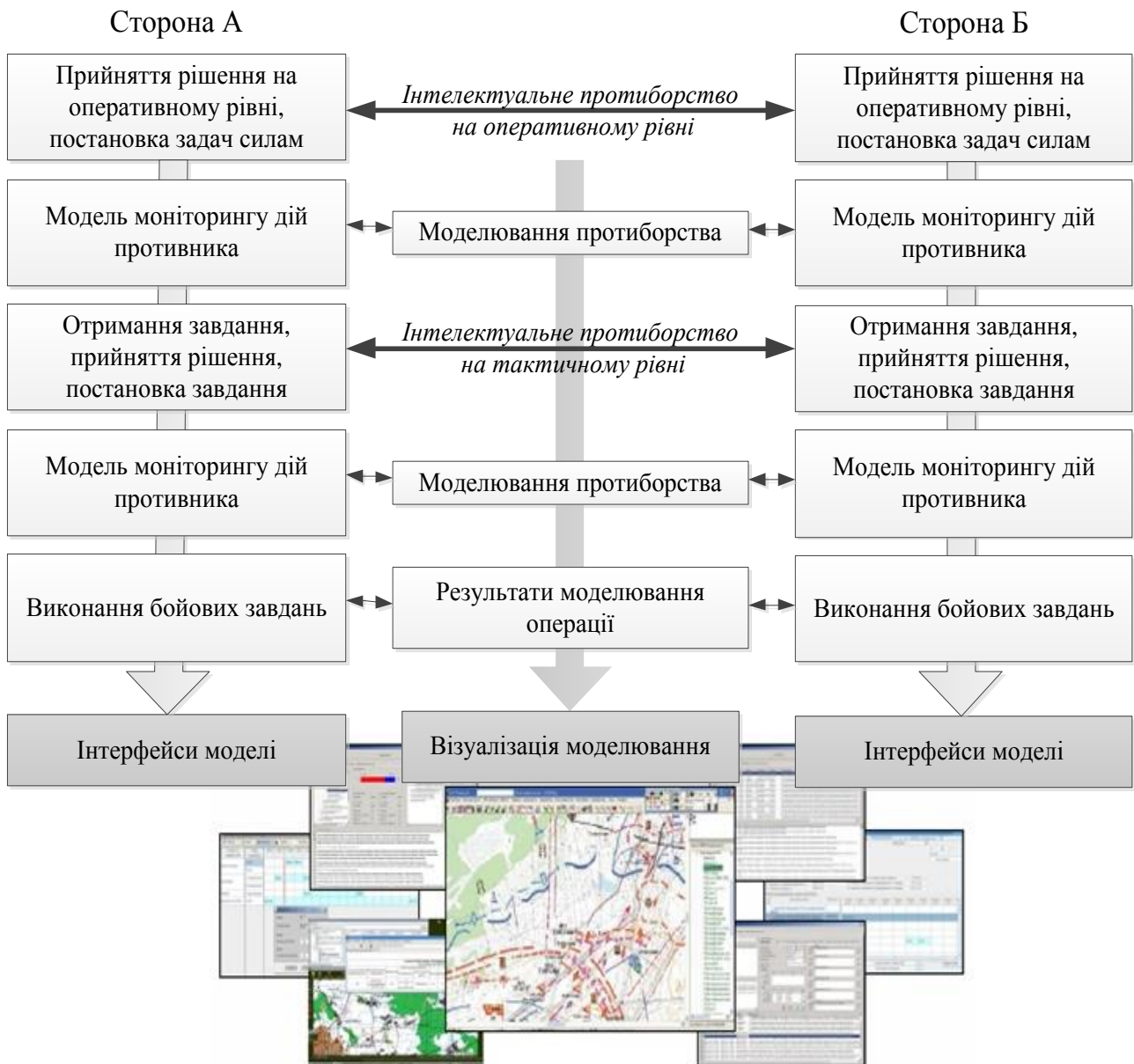


Рис.1. Структура моделі службово-бойових дій з огляду на інтелектуальне протиборство сторін

Інформаційні технології охоплюють широкий спектр технологій та систем, які використовуються для створення, зберігання, обміну та обробки інформації. До ключових властивостей, які характеризують інформаційні технології, належать: швидкість обробки інформації; зберігання та доступ до даних; комунікація; автоматизація; масштабованість; складні заходи безпеки; інтегрованість різних систем і програм, поліпшуючи взаємодію між різними відділами та оптимізуючи робочі процеси; підтримка прийняття рішень.

На рис. 2 показано класифікацію інформаційних технологій.

Для реалізації властивостей системи управління доцільно навести показники ефективності функціонування інформаційно-аналітичної системи забезпечення процесів управління силами безпеки, які характеризують здатність (приспосовність) системи виконувати покладені на неї функції. З реалізованими значеннями цих показників безпосередньо пов'язані значення основних

показників, проте їхньою перевагою є те, що вони порівняно легко вимірюються або визначаються за відомих характеристик окремих елементів конкретної інформаційної (інформаційно-керівної) системи.

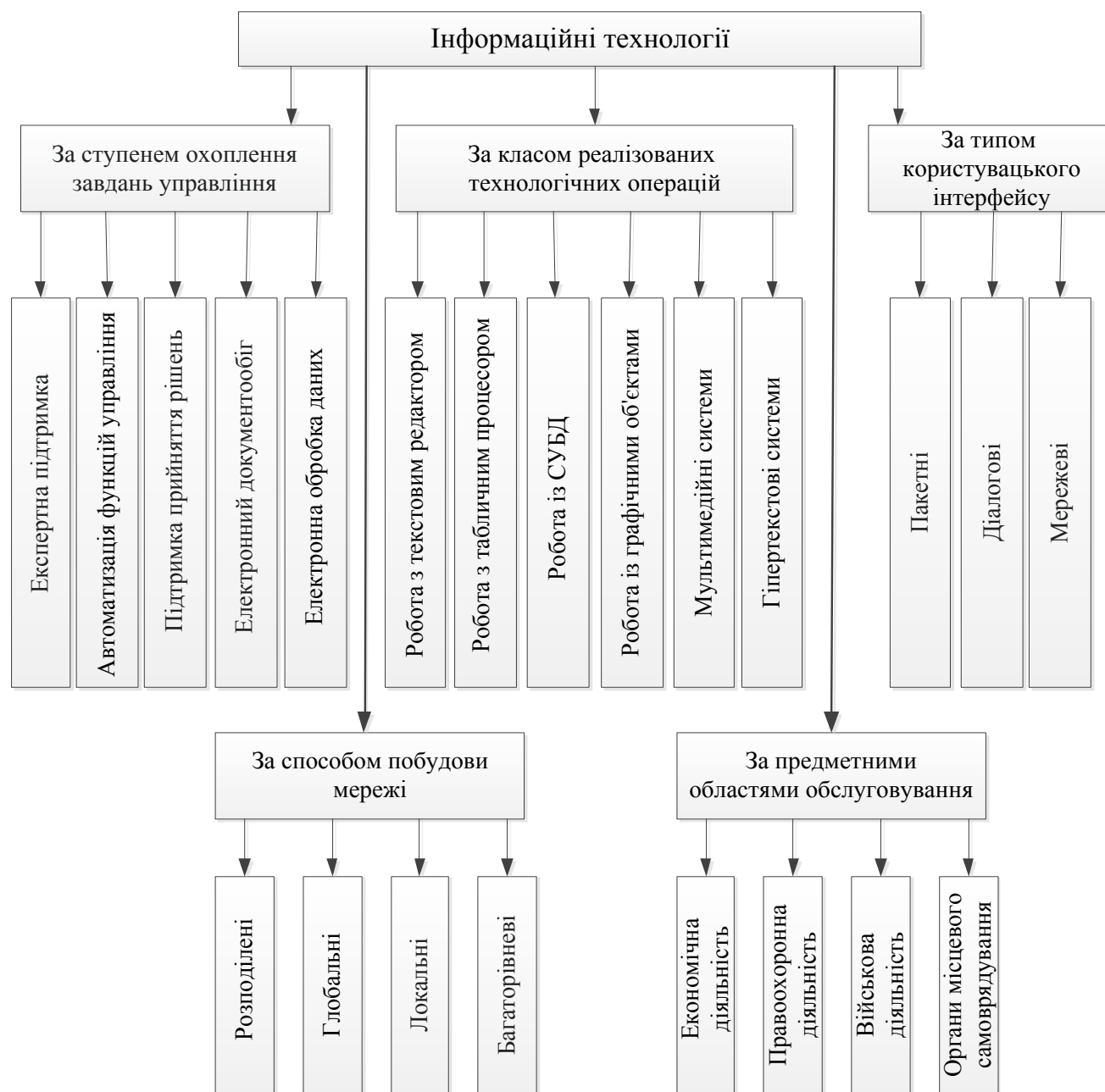


Рис. 2. Класифікація інформаційних технологій у сфері забезпечення державної безпеки

До цих показників відносять такі.

1. Показники якості структури інформаційно-аналітичної системи забезпечення, що характеризують її кількісний і якісний склад. До них належать: кількість елементів за типами, характеристики технічних засобів, що використовуються, можливості та порівняльна ефективність завдань і моделей, що реалізуються, тощо.

2. Показники, які характеризують взаємозв'язки між джерелами та споживачами інформації. До них належать: складність організації структури

інформаційної мережі; взаємозв'язок вузлів інформаційної мережі; нерівномірність інформаційного навантаження вузлів інформаційної мережі; ізолюваність вузлів інформаційної мережі).

2. Показники, які характеризують можливості системи щодо обробки та передачі інформації відповідного обсягу за заданий інтервал часу. До них належать: пропускна здатність напрямку (каналу, зв'язку) передачі даних та зведень; продуктивність вузла обробки інформації; завантаженість вузла обробки інформації (або напрямку інформаційного зв'язку).

3. Показники, які характеризують окремі складові інформаційно-аналітичної системи забезпечення процесів управління сил безпеки. До них належать: а) показники якості інформаційних складових (сукупності даних та зведень, згрупованих за ознаками їх використання джерелами, споживачами, за їхніми характеристиками та ін.); б) показники, що характеризують можливості технічних засобів обробки та передачі інформації; в) показники, що характеризують можливості та ефективність інформаційно-розрахункового та інформаційно-командного забезпечення (у тому числі за складовими інформаційного, математичного, лінгвістичного та програмного забезпечення систем управління).

Реалізація властивостей інформаційно-аналітичної системи забезпечення процесів управління сил безпеки дає змогу додати потрібних якостей управлінській інформації. Отриманий ефект безпосередньо характеризується відповідними показниками інформаційних складових, що використовуються у ході інформаційно-аналітичного забезпечення процесів управління військами (силами).

До кількісних показників інформаційних складових належать: обсяг інформації; повнота інформації; цінність (важливість) інформації; достовірність інформації; повнота урахування значущих факторів, що характеризують об'єкти управління та процеси; своєчасність надходження (надання) інформації; оперативність обробки інформації, її добування, збору, передачі, пошуку, відображення; глибина прогнозу інформації; частота (темп, інтенсивність) оновлення інформації, її надходження, обробки, використання; інтервал надходження інформації; інтенсивність потоку інформації; час старіння (тривалість «корисності») інформації; безперервність надання (отримання) інформації; стійкість інформації; ступінь захищеності інформації; доступність інформації; ступінь деталізації інформації.

У **другому розділі** *«Методологічні основи механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки»* визначено вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку, проведено аналіз досвіду функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу, наведено методологічні основи функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки.

Дослідження питання впливу стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку в цій роботі

пропонується за допомогою діаграми Ісікави. Діаграма дає змогу виявити ключові взаємозв'язки між різними факторами й більш точно зрозуміти досліджуваний процес. Діаграма сприяє визначенню головних факторів, що здійснюють найбільш значний вплив на розвиток розглянутої проблеми, а також попередженню або усуненню дії цих факторів. На рис. 3 представлено розроблену діаграму Ісікави, яка дає змогу оцінити вплив факторів на інформаційно-аналітичну систему (ІАС) сил безпеки.



Рис. 3. Метод оцінювання впливу системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку

Основною групою, що об'єднує фактори, є така, що описує наявність інформаційних технологій у системі інформаційно-аналітичного забезпечення діяльності сил безпеки. До її складу входять такі фактори, як наявність системи кіберзахисту, яка може охоплювати підсистеми шифрування, обмеження доступу, програмно-технічні модулі захисту інформації, наявність засобів автоматизованих систем управління (АСУ), наявність геоінформаційних систем (ГІС). Також значущим фактором є темп розвитку інформаційних технологій, який залежить від загальних досягнень науки в галузях фізики, хімії тощо. Цей фактор у зазначеній групі виступає як позитивний, тобто він працює на розвиток ІАС.

Навченість персоналу, що забезпечує роботу ІАС, віднесена до іншої групи факторів. Складовими в ній є заклади вищої освіти, курси підвищення кваліфікації. Темп розвитку інформаційних технологій виступає в цій групі

фактором, що знижує ефективність навчання. Це пов'язане із швидкоплинними змінами в галузі інформаційних технологій, появою нових технологій, виникнення яких потребує постійного підвищення рівня кваліфікації персоналу ІАС.

Третьою групою факторів впливу є матеріально-технічне забезпечення ІАС. До них віднесено: фінансове забезпечення ІАС, забезпеченість обчислювальною технікою та програмно-технічними засобами, наявність технічного супроводження програмного і математичного забезпечення ІАС.

Характеристики ІАС віднесені до четвертої групи. Ці фактори більше належать до технічних характеристик, а саме: пропускна спроможність ІАС (кількість одночасно оброблювальних завдань, кількість інформації, що спроможна обробляти ІАС); архітектура ІАС (способи та методи побудови ІАС); наявність вітчизняних розробників програмного забезпечення; наявність у державі розвинутої системи мережі зв'язку.

Проведено аналіз функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу. Технологічні й організаційні питання управління силами безпеки базуються на концепції петлі OODA. Петля Бойда (OODA) є занадто грубим спрощенням, у якому військова організація ототожнюється з деяким єдиним замислом і єдиним скоординованим рішенням, що проходить через всі функції й рівні організації. OODA є застарілою конструкцією, що не дає змогу формалізувати потрібний аналіз процесів у автоматизованих системах управління (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – C4ISR), без яких немислиме управління військами в сучасних умовах. На відміну від логіки, у більш простій петлі OODA, у якій вихід розумових (пізнавальних) процесів вбачається як рішення або вибір альтернатив, процеси в C4ISR мають більш складну характеристику й передбачають більш складний результат – замисел особи, що приймає рішення.

Розглянуто практичні кроки закордонних держав з розроблення стратегій та методик для протидії інформаційним загрозам, залежно від їхніх політичних, економічних і технологічних можливостей. Одним з найпоширеніших підходів є створення спеціалізованих установ. Багато країн мають відомства або органи, які спеціалізуються на кібербезпеці та інформаційній безпеці. Наприклад, у США є Агентство національної безпеки (NSA) та Кіберкомандування, в Європі – Європейське агентство з кібербезпеки (ENISA). Створення спеціалізованих установ є одним із ключових кроків, який допомагає країнам ефективно протидіяти кіберзагрозам і забезпечувати національну безпеку у сфері інформації. Ці органи не тільки опікуються моніторингом і виявленням кібератак, але й розробляють національні стратегії кібербезпеки, проводять навчання і координують заходи між різними державними та приватними структурами.

Методологічні засади функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України охоплюють комплексний підхід до забезпечення ефективної роботи інформаційних систем, аналітичних засобів та процесів прийняття рішень у

сфері національної безпеки. Цей підхід передбачає розроблення та впровадження стандартів, методів та процедур, які забезпечують збір, аналіз, зберігання та передачу інформації, необхідної для підтримки діяльності сил безпеки. Ключовими аспектами механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України є такі:

– інтеграція інформаційних систем вимагає узгодження технічних та програмних компонентів, щоб забезпечити безперебійний обмін даними між різними платформами й базами даних. Забезпечення сумісності та інтеграції різних інформаційних систем і баз даних, які використовуються в силових структурах, для забезпечення безперервного доступу до актуальної інформації. Стандартизація процесів обробки даних;

– розвиток аналітичних засобів та створення ефективних систем підтримки прийняття рішень є вирішальними для підвищення ефективності управлінських процесів у контексті національної безпеки і оборони. Особливо це стосується сил безпеки України, де швидкі й обґрунтовані рішення можуть мати стратегічне значення. Використання сучасних методів аналітики, включно з машинним навчанням і штучним інтелектом, для обробки великих обсягів даних та виявлення потенційних загроз. Прогнозування та виявлення загроз. Розроблення ІАС, які надають оперативну інформацію та рекомендації для прийняття рішень на різних рівнях управління. Системи підтримки прийняття рішень відіграють ключову роль у покращенні процесу управління, надаючи керівництву сил безпеки актуальну інформацію та аналітичні рекомендації;

– впровадження комплексних заходів щодо захисту інформаційних систем та даних від несанкціонованого доступу, зловмисного втручання або витоку інформації. Використання сучасних криптографічних методів для шифрування інформації, що передається або зберігається в інформаційних системах сил безпеки. Забезпечення інформаційної безпеки вимагає комплексного підходу, який охоплює заходи адміністративного, технічного і фізичного характеру для захисту інформаційних систем та даних. Розроблення та впровадження політик безпеки, що визначають правила поведінки з інформаційними системами. Криптографічний захист інформації, що передається через мережі або зберігається в інформаційних системах. Використання «сильних» алгоритмів шифрування для захисту конфіденційності даних під час їхнього зберігання та передачі. Застосування цифрових підписів для забезпечення цілісності й автентичності електронних документів і повідомлень;

– створення та постійне оновлення нормативно-правових актів, які регулюють діяльність системи інформаційно-аналітичного забезпечення, для забезпечення її законності та ефективності. Розроблення законодавчої та нормативної бази є фундаментальним для забезпечення законності, прозорості й ефективності функціонування систем інформаційно-аналітичного забезпечення, особливо у сфері національної безпеки і оборони. Визначення правових, технічних та оперативних вимог, які необхідні для ефективного функціонування системи інформаційно-аналітичного забезпечення. Моніторинг впливу нового законодавства на діяльність ІАС та їхню ефективність. Оцінка потреби в подальших змінах або доповненнях. Гармонізація національного законодавства з

міжнародними стандартами та нормами;

– програми підготовки та навчання персоналу, залученого до роботи з ІАС, відіграють критично важливу роль у забезпеченні ефективності й безпеки діяльності організацій. Розроблення та впровадження цілеспрямованих програм навчання сприяють не тільки підвищенню кваліфікації співробітників, але й зміцненню загальної інформаційної безпеки та оперативності реагування на загрози. Навчальні програми мають бути гнучкими й адаптованими до конкретних потреб суб'єкта сил безпеки. Технології та загрози інформаційній безпеці швидко змінюються, тому навчальні програми потребують регулярного перегляду й оновлення. Також важливо проводити оцінку ефективності навчання, збираючи зворотний зв'язок від учасників та аналізуючи результати їхньої роботи після завершення курсів.

Розвиток інформаційно-аналітичного забезпечення доцільно здійснювати за такими напрямками: впровадження новітніх інформаційних технологій для прийняття рішень під час виконання службово-бойових завдань; створення нових технічних рішень під час розроблення (модернізації) ІАС; розроблення і вдосконалення інформаційної інфраструктури сил безпеки з огляду на національні та міжнародні стандарти; створення ІАС з огляду на вимоги щодо забезпечення взаємодії між наявними та створюваними у силах безпеки інформаційними системами; використання гнучких технологічних платформ під час впровадження розроблених ІАС; урахування вимог до відмово- та катастрофостійкості ІАС, що розробляються; впровадження автоматичної ідентифікації та автентифікації користувачів ІАС, регламентованого доступу і обміну даними, забезпечення необхідного рівня захисту інформації від зовнішніх та внутрішніх загроз; удосконалення організаційної структури ІАС, що розробляються.

У **третьому розділі** *«Сучасний стан та результативність механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки»* досліджено системи підтримки прийняття рішень у державному управлінні силами безпеки України та підсистеми захисту інформації в системі державного управління силами безпеки України, визначено засади автоматизації інформаційних систем управлінського призначення сил безпеки передових країн ЄС та НАТО.

Процес управління безперервно пов'язують із процесом підготовки і прийняття рішень. Цикл управління містить у собі: збір інформації (безперервно), формування ситуацій та їхній аналіз, оцінку обстановки (безперервно), підготовку і прийняття рішення, постановку та доведення завдань, контроль їх виконання і знову збір інформації та оцінку обстановки для прийняття подальших рішень (рис. 4).

Більшість визначених на цьому рис. функцій (1...9) входять до складу процесу підготовки прийняття рішення, акт прийняття рішення (10) передбачає постановку завдань та контроль їх виконання (11, 12). Не можна розділити формально процеси управління та підготовки й прийняття рішення, бо всі зазначені функції органів управління є складовими саме процесу управління. Таким чином, процес управління формально можна розділити на складові: збір

інформації; підготовка пропозицій до рішення; прийняття рішення; постановка завдань; контроль їх виконання. Слід підкреслити, що будь-яке рішення має охоплювати формування завдань підлеглим для подальшої реалізації рішення. Щоб завдання було зрозумілим, воно повинно мати відповідну форму, містити необхідну інформацію щодо узгодженого порядку виконання завдання, часу виконання, застосовуваних ресурсів, напряду подальшої діяльності та ін.



Рис. 4. Безперервний цикл державного управління та процеси підготовки прийняття рішень у сфері забезпечення державної безпеки

Метод підготовки і прийняття рішення складається із сукупності прийомів та операцій практичного (організаційна робота органів управління) і теоретичного (принципи і методи дослідження) засвоювання покладених завдань, проблем і обстановки, що дає змогу для організації ефективної службово-бойової діяльності вирішити багатокритерійну задачу за відповідною кількістю цільових функцій.

Побудова моделі інформаційного механізму прийняття рішень є важливою складовою для оптимізації процесу управління національною безпекою. Цей механізм спрямований на ефективне регулювання інформаційного обміну між суб'єктами державного управління та об'єктами, над якими ведеться управління, в контексті наявних владних відносин і суспільних цінностей.

Основні аспекти моделі інформаційного механізму є такі:

Інституціонально-правовий аспект. Модель містить компоненти, що відображають правові норми та інституційні рамки, які регулюють процеси в межах політичної системи. Це забезпечує легітимність і формальну коректність прийнятих рішень.

Системна інтеграція зусиль. Модель узгоджує зусилля всіх зацікавлених сторін відповідно до принципів поліцентризму, ієрархії, оптимальності,

адекватності та багатоваріантності, що дає змогу комплексно підходити до вирішення питань національної безпеки.

Використання математичних методів. Аналіз та моделювання використовують кількісні методи для визначення оптимальних рішень і стратегій. Це охоплює статистичний аналіз, теорію ігор, оптимізаційні моделі тощо, що дає змогу об'єктивно оцінювати різні сценарії та їхні можливі наслідки.

Теоретична підготовка та концептуальна розробка. Перед застосуванням формальних методів необхідно ретельно розробити теоретичні засади та концептуальні підходи, щоб забезпечити їхню коректність та адекватність до контексту національної безпеки.

Важливість моделі. Модель інформаційного механізму прийняття рішень дає нагоду раціоналізувати процеси управління, підвищити їх прозорість та відповідність до актуальних викликів і загроз. Вона також сприяє кращому розумінню та адекватному реагуванню на зовнішні та внутрішні зміни, що має велике значення для ефективної політики національної безпеки.

Системний аналіз розглядає процес прийняття управлінських рішень у державному апараті як активну взаємодію між інформаційними потоками. Дослідження цих потоків має відбуватися з огляду на їхні зв'язки з внутрішнім та зовнішнім середовищами, які є основними джерелами даних про об'єкти та суб'єкти управління. Через суперечливий та непевний характер цієї інформації її оцінка може бути ускладнена. Процес управління поділяється на низку етапів, де кожен містить специфічні операції з обробки інформації. Ці операції визначають дії, необхідні на кожному етапі, а також критерії переходу до наступного. Модель прийняття управлінських рішень у сфері національної безпеки здійснюється відповідно до чітко визначеного алгоритму. У разі необхідності весь процес може бути повторено, що робить його ітеративним. Процес триває до моменту знаходження оптимального рішення, яке відповідає встановленим критеріям, з огляду на час, доступний для суб'єктів управління.

Формалізація процесу прийняття управлінських рішень у контексті національної безпеки через модель пропонує такі переваги: розгляд процесу як системи з певними входами та виходами, що сприяє структуруванню підходів; мінімізація суб'єктивізму у виборі рішень завдяки заміні неоднозначних формулювань на точніші дає змогу чітко визначати критерії та процедури оцінювання; використання математичних методів для визначення оптимальних рішень залежно від складності та специфіки проблем, що дає змогу ефективніше розв'язувати задачі на кожному етапі.

Діяльність суб'єктів державного управління інтегрована в єдину систему, що вміщує: аналіз стану об'єкта управління; розроблення та порівняння альтернатив, узгодження з цілями управління; оцінку ефективності досягнення цілей; вибір оптимальної альтернативи.

Особливістю зазначеної моделі є взаємозалежність етапів обробки інформації, де кожен наступний етап розвивається з результатів попереднього. Можна виділити ключові функції та завдання для кожного з етапів, починаючи з аналізу стану об'єкта управління і закінчуючи вибором найкращого рішення з

доступних варіантів. Ці етапи складають як ситуативну, так і концептуальну частини моделі управлінських рішень у сфері національної безпеки.

Ситуативна частина моделі фокусується на прийомі та аналізові надходження інформації, що дає нагоду суб'єктам управління адекватно оцінити стан об'єкта управління. Концептуальна частина моделі аналізує потенційні методи та інструменти для досягнення національних цілей, визначає стратегії їхнього досягнення та формує критерії для вибору оптимального рішення. Таким чином, модель інформаційного механізму процесу прийняття рішень є всеохопним алгоритмом обробки інформації у сфері державного управління.

Система державного управління силами безпеки України має у складі різноманітні підсистеми захисту інформації, оскільки забезпечення безпеки інформації є однією з найважливіших складових сучасної національної безпеки. До основних підсистем захисту інформації в системі державного управління силами безпеки України належить ІАС, яка відповідає за збір, обробку, аналіз та використання інформації для прийняття рішень у сфері національної безпеки. Інформаційно-технічна підсистема охоплює різноманітні технічні засоби захисту інформації, такі як системи шифрування, мережеві заходи безпеки, антивірусні програми та ін. Інформаційно-правова підсистема забезпечує розвиток та впровадження правових актів, які регулюють сферу захисту інформації в державі. Організаційно-методична підсистема містить розроблення та впровадження методик, стандартів, інструкцій та інших документів, які регулюють організаційні аспекти захисту інформації, включно з процедурами аудиту безпеки, навчання персоналу тощо. Технологічна підсистема захисту інформації відповідає за впровадження сучасних технологій захисту інформації, таких як системи ідентифікації та аутентифікації, системи контролю доступу, механізми виявлення та реагування на кіберзагрози. Перелічені підсистеми захисту інформації в системі державного управління силами безпеки України частково наявні в підсистемах захисту інформації в кожному із суб'єктів сил безпеки.

Кіберзагрози для сил безпеки розглянуто з двох основних позицій. По-перше, сили безпеки мають активно працювати над запобіганням та протидією кіберзагрозам, розробляючи і впроваджуючи заходи кібербезпеки. Це охоплює створення спеціалізованих підрозділів, розроблення і виконання стратегій захисту інфраструктури та даних, а також навчання персоналу ефективним методам протидії кіберзлочинності. По-друге, сили безпеки самі можуть стати об'єктами кіберзагроз, що вимагає від них розроблення особливих механізмів захисту, зокрема впровадження сучасних технологій шифрування, використання захищених каналів зв'язку та застосування надійних систем ідентифікації та аутентифікації. Така двоїстість впливу інформаційних технологій на сили безпеки актуалізує необхідність комплексного підходу до забезпечення кібербезпеки. Розроблення державної політики в цій сфері має бути спрямовано не тільки на формування ефективної системи захисту державних інформаційних ресурсів, але й на створення умов для сталого розвитку інформаційних технологій у секторі безпеки.

Завданнями та функціями оперативних АСУ є: підтримка управління

операціями сил безпеки на оперативному рівні, об'єднуючи підрозділи та з'єднання в рамках великих операцій або кампаній. Забезпечують планування, координацію та контроль за виконанням оперативних завдань і місій. Аналізують оперативну обстановку, ресурси та можливості для розроблення оптимальних планів дій. До основних їхніх характеристик належать: інтеграція з ширшими інформаційними системами для обміну даними з тактичним та стратегічним рівнями, спроможність до довготривалого планування та управління ресурсами.

Завданнями та функціями стратегічних АСУ є: підтримка прийняття рішень на найвищому рівні військового та політичного керівництва. Забезпечують аналіз загальної обстановки, стратегічне планування, розроблення довгострокових стратегій та моніторинг виконання стратегічних завдань. Зважають на політичні, економічні, соціальні і міжнародні фактори, що впливають на оборонну політику. Кожен тип АСУ має свої унікальні технологічні рішення, інтерфейси, засоби зв'язку та обчислювальні можливості, які оптимізовані для виконання специфічних завдань відповідного рівня управління. Розроблення та впровадження таких систем вимагає комплексного підходу, що містить аналіз потреб, вибір технологій, розроблення програмного забезпечення, інтеграцію з наявними системами та навчання персоналу. На цей час у силах безпеки та оборони України використовується декілька абсолютно різних АСУ – «Дзвін» (управління та контроль стратегічного рівня), «Дельта» – (спостереження та рекогносцювання), «Віраж-планшет» (відстеження повітряного простору), «Кропива» (управління тактичного рівня), «Гермес-2» (управління тактичного рівня) та низка інших перспективних розробок.

У **четвертому розділі** *«Удосконалення державного управління системою інформаційно-аналітичного забезпечення сил безпеки України»* розглянуто організаційні механізми управління інформаційними ресурсами, удосконалено нормативно-правові механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, визначено підходи до застосування ГІС в управлінській діяльності сил безпеки України. Визначено шляхи вирішення суперечностей реалізації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Поліпшення засобів інтелектуалізації інформаційної діяльності є одним із ключових аспектів сучасної стратегії розвитку інформаційних систем та технологій. Цей процес передбачає інтеграцію сучасних методів штучного інтелекту, машинного навчання, а також вдосконалення алгоритмічної бази для ефективнішого аналізу, обробки та використання даних. Розвиток інтелектуалізації інформаційної діяльності відіграє важливу роль у підвищенні оперативності прийняття рішень, точності даних та забезпеченні безпеки інформаційних процесів. Викликами сучасності є потреби державних органів управління до адаптації до швидких технологічних змін. Організаційні структури державних органів управління та їхня роль в інформаційно-аналітичному забезпеченні мають бути гнучкими, щоб адаптуватися до нових технологій та методів обробки даних. Також підвищення кваліфікації та розвиток компетенцій співробітників у сфері інформаційно-аналітичного

забезпечення є ключовими для підвищення ефективності управління інформаційними ресурсами.

Управління інформаційними ресурсами державного управління в Україні пройшло значний шлях розвитку, особливо в контексті цифрової трансформації та спрямування на підвищення прозорості, ефективності й доступності державних послуг. Успішне управління інформаційними ресурсами ілюструється такими кейсами. У галузі електронного урядування – проєкт «Дія». У системі державних закупівель – проєкт «Prozorro». Проєкт цифровізації земельного кадастру та реєстру нерухомості.

Україна продемонструвала значний прогрес у сфері управління інформаційно-аналітичним забезпеченням, зокрема через реалізацію цифрових ініціатив, які спрямовані на покращення державного управління та надання послуг. Ці кейси свідчать про важливість інтеграції новітніх технологій у сферу інформаційно-аналітичного забезпечення для підвищення ефективності, прозорості й доступності державних послуг для громадян. Основним викликом залишається подальше розширення й адаптація цифрових сервісів до змінюваних потреб громадян і економіки, а також забезпечення високого рівня захисту даних та приватності. Організаційні структури та ролі в управлінні інформаційними ресурсами державного управління мають вирішальне значення для ефективної реалізації стратегій інформаційно-аналітичного забезпечення. Вони сприяють забезпеченню координації, ефективності та безпеки в обробці й використанні інформаційних ресурсів, що є важливим для досягнення цілей державного управління. Розроблення і впровадження законодавчих ініціатив для удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є критично важливим кроком у забезпеченні національної безпеки й обороноздатності країни. Нормативно-правова база інформаційно-аналітичного забезпечення впливає на ефективність службово-бойових дій сил безпеки через такі аспекти: юридична визначеність та прозорість; адаптація до сучасних викликів; міжвідомча координація; міжнародна співпраця; інновації та технології; гармонізація з міжнародними стандартами; посилення міжвідомчої координації.

Україна має низку законів та нормативних актів, які регулюють діяльність сил безпеки, у тому числі закони «Про національну безпеку України», «Про державну таємницю», «Про боротьбу з тероризмом» та ін. Проте динаміка сучасних загроз вимагає постійного оновлення й доповнення чинної нормативної бази. Багато чинних нормативних актів було розроблено та прийнято ще до масового розвитку цифрових технологій, що робить їх не повністю адаптованими до викликів сучасної інформаційної безпеки. Це стосується, зокрема, захисту інформаційної інфраструктури, кібербезпеки та обігу інформації в цифровому середовищі. У деяких випадках чинне законодавство містить прогалини або невизначеності, які ускладнюють ефективне застосування законів на практиці. Це може стосуватися питань юрисдикції, відповідальності, а також координації між різними відомствами. Україна активно співпрацює з міжнародними організаціями та інтегрується в міжнародні стандарти у сфері безпеки, потрібною є додаткова робота для

гармонізації внутрішнього законодавства з міжнародними нормами, особливо в контексті кібербезпеки та захисту інформаційного простору.

Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є ключовим для підвищення ефективності національної безпеки і оборони. Це, відповідно, потребує комплексного підходу, що містить законодавчі, технічні й організаційні заходи, а також урахування багатьох факторів, що впливають на безпекову складову.

До основних сфер застосування ГІС у державному управлінні можна віднести: міське планування і управління; розроблення генеральних планів розвитку міст та інших населених пунктів; планування інфраструктури і комунальних послуг; моніторинг забудови та використання земель; екологічний моніторинг і управління; оцінку впливу на довкілля, моніторинг екосистем і біорізноманіття; контроль за забрудненням повітря, води та ґрунтів; планування зон охорони природи і національних парків; управління надзвичайними ситуаціями; аналіз ризиків і вразливостей територій до природних та техногенних катастроф; планування заходів цивільного захисту та евакуації; координацію дій рятувальних служб під час надзвичайних ситуацій; транспортне планування; аналіз трафіку, планування транспортних мереж і маршрутів; управління дорожнім рухом та планування громадського транспорту; земельний кадастр і управління земельними ресурсами; громадську безпеку та правопорядок; моніторинг громадського порядку і превенцію злочинності; планування розміщення органів правопорядку та інфраструктури безпеки; аналіз даних про злочинність для розроблення стратегій профілактики.

Перевагами використання ГІС є підвищення ефективності управління завдяки точному аналізу геопросторових даних. Оптимізація ресурсів через планування і координацію на основі актуальних даних. Покращення прийняття рішень завдяки візуалізації та моделюванню різних сценаріїв. Забезпечення прозорості та доступності інформації для громадськості й зацікавлених сторін.

Розвиток та інтеграція ГІС у силові структури України супроводжуються низкою викликів, зокрема потребою в оновленні технічної бази, підготовкою кваліфікованих фахівців, забезпеченням кібербезпеки інформаційних систем. Водночас активний розвиток цифрових технологій та штучного інтелекту відкриває нові можливості для підвищення ефективності використання ГІС в оборонній сфері, зокрема через автоматизацію процесів аналізу даних та прийняття.

Суперечності в реалізації механізмів державного управління можуть бути ідентифіковані в таких аспектах: є значний розрив між розробленими науковими підходами та їх реальним упровадженням у діяльність сил безпеки. Це призводить до неефективності використання ресурсів і втрати потенційних переваг; різні органи безпеки можуть мати відмінні цілі та задачі, що ускладнює єдину політику управління інформацією й аналітикою; відсутність єдиної інтегрованої системи обробки та аналізу даних. Брак єдиної системи призводить до фрагментації даних, ускладнюючи аналіз та швидке реагування на загрози; проблеми з оновленням технологічної бази. Швидкий розвиток технологій вимагає постійного оновлення обладнання та програмного забезпечення, що

часто сповільнюється через бюрократичні процеси й обмеження бюджету; необхідність у забезпеченні високого рівня інформаційної безпеки, з одного боку, та обмеження бюджету та технологічних можливостей, з іншого; наявність різноманітних баз даних і систем ускладнює інтеграцію та єдине використання інформації; розбіжності між довгостроковими стратегічними цілями держави в секторі безпеки та поточними оперативними завданнями і потребами.

Для ефективного вирішення ідентифікованих суперечностей можуть бути запропоновані такі заходи: удосконалення законодавчої та нормативної бази для забезпечення чіткого розмежування повноважень між різними структурами безпеки. Адаптація законодавчої та нормативної бази до сучасних викликів у сфері інформаційної безпеки і технологій. Встановлення чітких процедур використання даних, у тому числі з питань конфіденційності та захисту особистих даних; створення механізмів для забезпечення ефективної міжвідомчої координації й обміну інформацією; інтеграція та модернізація технологічної інфраструктури. Інвестиції в оновлення та розвиток єдиної інтегрованої технологічної платформи для обробки та аналізу даних; розроблення і впровадження єдиної інформаційно-аналітичної платформи для збору, обробки, аналізу та розподілу інформації між усіма зацікавленими структурами безпеки; уніфікація форматів даних. Забезпечення сумісності різноманітних джерел інформації через уніфікацію форматів даних та протоколів обміну; організація регулярних навчальних програм і тренінгів для підвищення професійних навичок аналітиків, інженерів і керівників у галузі обробки та аналізу даних; формування крос-функціональних команд для обміну досвідом та найкращими практиками у сфері інформаційної безпеки; залучення інвестицій для придбання і впровадження передових технологій обробки великих даних, штучного інтелекту та машинного навчання; стимулювання розроблення вітчизняних інноваційних рішень в галузі інформаційної безпеки й аналітики.

Цей аналіз виявляє комплексність проблематики і необхідність інтегрованого підходу для її вирішення. Імплементация відповідних механізмів дасть змогу не тільки оптимізувати та удосконалити систему інформаційно-аналітичного забезпечення сил безпеки України, а й значно підвищити загальну ефективність державного управління в цій сфері. Ефективне впровадження запропонованих заходів вимагає комплексного підходу, забезпечення міжвідомчої координації та неперервного моніторингу реалізації заходів.

У **п'ятому розділі** *«Концептуальні напрями розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України»* визначено шляхи планування інформаційно-аналітичної діяльності в силах безпеки України, обґрунтовано напрями розвитку менеджменту кадрових ресурсів у системі інформаційно-аналітичного забезпечення сил безпеки України, обґрунтовано загальнодержавну модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, сформовано стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Особливість сил безпеки полягає в необхідності поєднання високого рівня професіоналізму, стресостійкості та адаптивності до швидко змінюваних умов. Впровадження компетентнісного підходу, укупі з акцентом на стратегічне планування і розвиток, може забезпечити підвищення ефективності інформаційно-аналітичного забезпечення та загальної готовності сил безпеки. Стратегії розвитку кадрових ресурсів відіграють ключову роль у підвищенні ефективності службово-бойової діяльності сил безпеки України. Розвиток кадрових ресурсів вимагає від сил безпеки України впровадження комплексного підходу, що охоплює набір, мотивацію, навчання, розвиток та утримання працівників.

На рис.5 наведено розроблену загальнодержавну модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

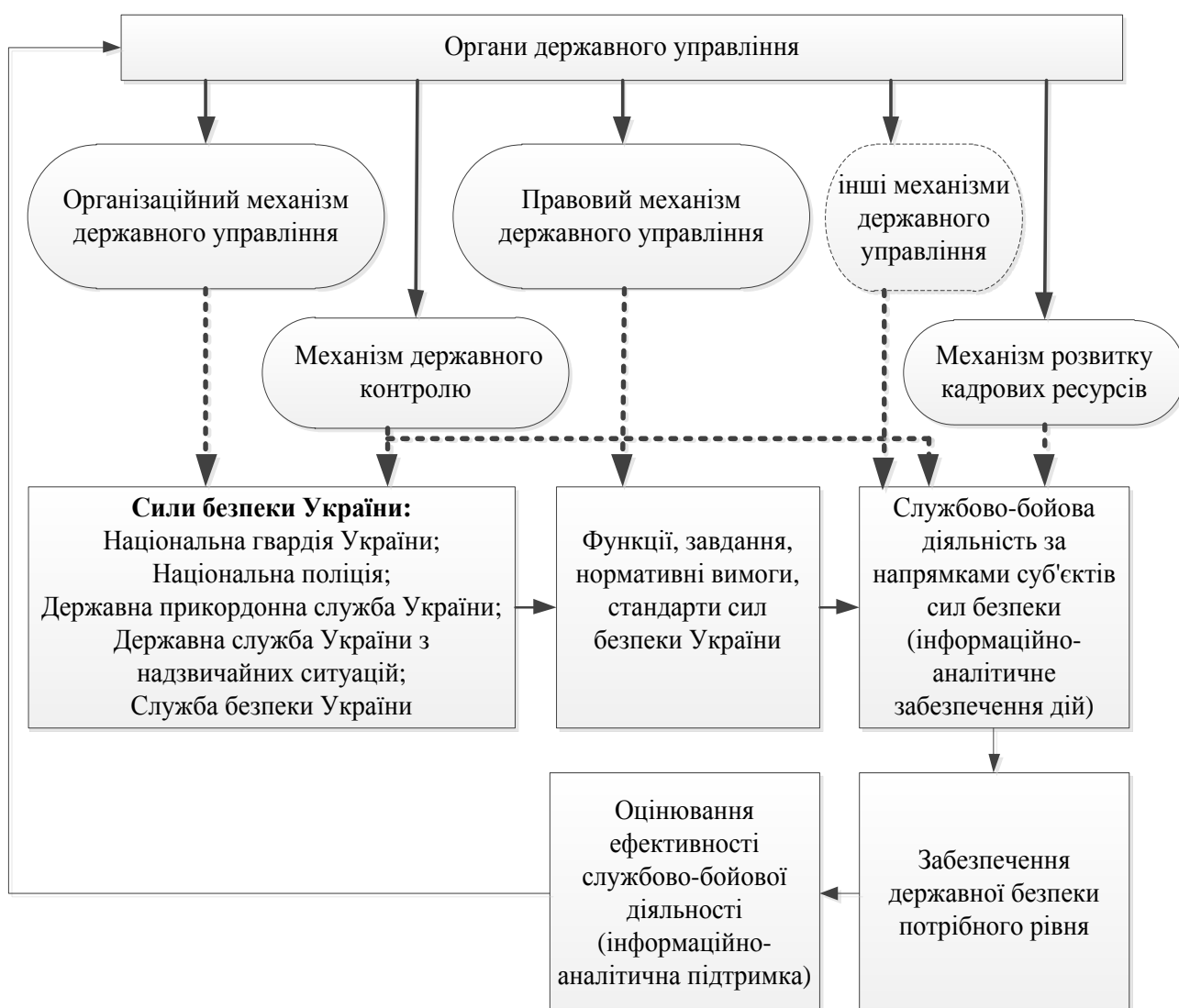


Рис.5. Схема моделі функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

Розроблена модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки

України базується на механізмах: формування організаційної структури кожного суб'єкта в залежності від його виду діяльності, завдань та призначення; контролю у сфері функціонування системи інформаційно-аналітичного забезпечення; правового забезпечення, яке формує функції та завдання системи інформаційно-аналітичного забезпечення; підготовки та перепідготовки персоналу у сфері інформаційно-аналітичного забезпечення; фінансового забезпечення та дає змогу визначити впливи державного управління на систему інформаційно-аналітичного забезпечення сил безпеки для подальшого удосконалення як самої системи, так і механізмів державної безпеки. Це дасть змогу в подальшому визначити напрями удосконалення системи інформаційно-аналітичного забезпечення і механізми державної безпеки.

У табл. 1 наведено приклад SWOT-аналізу системи інформаційно-аналітичного забезпечення сил безпеки України.

Таблиця 1 – Приклад SWOT-аналізу системи інформаційно-аналітичного забезпечення сил безпеки України

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)
1. Кваліфікований персонал. Наявність досвідчених та висококваліфікованих фахівців у сфері безпеки й аналітики. 2. Міжнародне партнерство. Співпраця з міжнародними організаціями і союзниками у сфері обміну інформацією та технологічної підтримки. 3. Адаптивність. Здатність швидко реагувати на зміни в безпековому середовищі	1. Технологічне відставання. Застаріле обладнання і програмне забезпечення. 2. Обмежені бюджетні ресурси. Недостатнє фінансування для модернізації технологій та навчання персоналу. 3. Координація між відомствами. Відсутність ефективної координації та взаємодії між різними структурами безпеки
Можливості (Opportunities)	Загрози (Threats)
1. Технологічний прогрес. Впровадження новітніх технологій та інноваційних рішень у сфері аналітики та кібербезпеки. 2. Міжнародне фінансування і допомога. Залучення додаткових ресурсів та інвестицій від міжнародних партнерів. 3. Нормативно-правові реформи. Удосконалення законодавчої бази для підтримки сучасних потреб інформаційно-аналітичного забезпечення	1. Кіберзагрози. Зростаюча небезпека кібератак та витоку інформації. 2. Політична нестабільність. Вплив міжнародних конфліктів та внутрішніх політичних змін на безпекову політику. 3. Технологічна залежність. Залежність від іноземних технологій та виробників, які можуть бути обмежені в умовах кризи або конфлікту

На основі SWOT-аналізу сформовано стратегічні засади розвитку механізмів державного управління системою інформаційно-аналітичного

забезпечення сил безпеки України, які охоплюють комплекс стратегій, а саме: «Сильні сторони: Кваліфікований персонал, міжнародне партнерство, адаптивність до загроз»; «Слабкі сторони: Технологічне відставання, обмежені бюджетні ресурси, відсутність ефективної координації та взаємодії між різними структурами безпеки»; «Можливості: Впровадження новітніх технологій та інноваційних рішень у сфері аналітики та кібербезпеки, міжнародне фінансування та допомога, нормативно-правові реформи»; «Загрози: Кіберзагрози, політична нестабільність, технологічна залежність», та дають змогу визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

На основі цього SWOT-аналізу стратегія розвитку механізмів державного управління може бути сфокусована на зміцненні сильних сторін, усуненні слабкостей, використанні можливостей для зростання та мінімізації загроз.

Сформовано стратегічні засади розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, що дають змогу визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

ВИСНОВКИ

У дисертаційному дослідженні вирішено актуальну наукову проблему, що полягає в теоретико-методологічному обґрунтуванні й розробленні практичних рекомендацій щодо розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Реалізована мета і визначені завдання дають підстави сформулювати такі висновки та практичні рекомендації.

1. Оцінено вплив системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку. З цією метою визначено фактори стану системи інформаційно-аналітичного забезпечення сил безпеки України, що впливають на державну безпеку. Досліджено вплив факторів системи кіберзахисту, які охоплюють підсистеми шифрування, обмеження доступу, програмно-технічні модулі захисту інформації, наявність засобів автоматизації управління, наявність геопросторового аналізу, на ефективність системи інформаційно-аналітичного забезпечення сил безпеки. Отримано залежність фактора темпу розвитку інформаційних технологій від загальних досягнень науки. Встановлено вплив навченості персоналу, що забезпечує роботу ІАС, на ефективність виконання службово-бойових завдань силами безпеки. Обґрунтовано залежність факторів матеріально-технічного забезпечення ІАС, до яких віднесено: фінансове забезпечення ІАС, забезпеченість обчислювальною технікою та програмно-технічними засобами, технічне супроводження програмного та математичного забезпечення ІАС, та їхній вплив на ефективність системи інформаційно-аналітичного забезпечення сил безпеки.

2. Досліджено засади функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України. Для цього визначено роль і місце математичних методів, інформаційних технологій і моделювання процесів та явищ, що характерні для систем державного управління. Встановлено шляхи покращення системи підтримки прийняття рішень у державному управлінні силами безпеки України через підвищення компетентності та професіоналізму

персоналу, застосування сучасних інформаційних технологій, таких як штучний інтелект, обробка великих масивів даних та покращення якості прийнятих рішень. Удосконалено механізми державного управління системою підтримки прийняття рішень через покращення кадрових, організаційних, правових, технічних механізмів державного управління.

3. Визначено аспекти функціонування підсистеми захисту інформації в суб'єктах сил безпеки України. З огляду на виклики, з якими зіткнулася наша держава, були вдосконалені механізми державного управління системами захисту інформації сил безпеки України. Обґрунтовано вимоги до підсистеми захисту інформації та вимоги до захищеності інформації, що циркулює в системах державного управління силами безпеки України. Встановлено фактори, що впливають на ефективність державного управління підсистемами захисту інформації. Комплексне поєднання організаційних, правових, кадрових механізмів державного управління дало змогу сформулювати пропозиції з удосконалення підсистеми захисту інформації в системі державного управління силами безпеки України.

4. Удосконалено організаційний механізм державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Встановлено, що покращення організаційно-штатної структури системи інформаційно-аналітичного забезпечення суб'єктів сил безпеки доречно проводити через оптимізацію інформаційних потреб органів управління. Удосконалення організаційних механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України здійснено завдяки створенню інформаційної координації між підрозділами та суб'єктами сил безпеки, адаптації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України до потреб економіки, а також забезпеченню високого рівня захисту даних та приватності.

5. Встановлено шляхи розвитку правового механізму функціонування системи інформаційно-аналітичного забезпечення сил безпеки України за допомогою комплексного підходу, що містить законодавчі, технічні та організаційні заходи. З цією метою досліджено міжнародний досвід у сфері нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки, який дає змогу визначити передові практики та інноваційні підходи, які можуть бути адаптовані та впроваджені в Україні. Через обґрунтування загальнодержавних підходів до перспектив розвитку інформаційно-аналітичного забезпечення, базуючись на систематизації нормативно-правових актів інформаційно-аналітичного забезпечення сил безпеки України, а також відомчих керівних документів сил безпеки України, які конкретизують використання інформаційно-аналітичних методів під час виконання службово-бойових завдань, удосконалено нормативно-правову базу функціонування системи інформаційно-аналітичного забезпечення сил безпеки України, що дало змогу надати пропозиції з визначення інформаційних потреб органів управління силами безпеки, узгодження вітчизняних стандартів зі стандартами НАТО, а також здійснити адаптацію нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України до стандартів НАТО.

6. Обґрунтовано підходи до застосування ГІС у державному управлінні силами безпеки України, які дають змогу підвищити ефективність прийняття

рішень та планування у сфері державного управління силами безпеки України. Обґрунтування зазначених підходів отримано через подальший розвиток механізмів стратегічного планування та оперативного реагування, що сприяє підвищенню обороноздатності країни та захисту національних інтересів. Також визначено вплив механізму застосування ГІС у державному управлінні силами безпеки України задля забезпечення державної безпеки. Встановлено вплив ГІС на ефективність управління в секторі безпеки і оборони України.

7. Надано пропозиції з удосконалення підготовки кадрових ресурсів у системі інформаційно-аналітичного забезпечення сил безпеки України, які базуються на використанні інформаційних технологій автоматизації управління персоналом, управлінні компетенціями та плануванням потреб у навчанні, використанні аналітичних інструментів для прогнозування потреб у персоналі, аналізу тенденцій на ринку праці, оцінки ефективності персоналу та прийнятті обґрунтованих рішень. Надано концептуальні пропозиції для удосконалення державного управління кадровими ресурсами в системі інформаційно-аналітичного забезпечення сил безпеки України, які полягають у переході на комплексні системи управління людськими ресурсами, використанні систем управління навчанням, розробленні та імплементації програм управління компетенціями, використанні інструментів на основі штучного інтелекту, впровадженні аналітичних інструментів для збору та аналізу даних про персонал. Створено практичні рекомендації, покликані підвищити ефективність та адаптивність кадрової політики завдяки впровадженню сучасних ІТ-рішень, розвитку компетенцій та професійного навчання, використанню зворотного зв'язку з роботодавцями.

8. Сформульовано ключові напрямки для підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України, які полягають у формуванні теоретичних засад функціонування системи інформаційно-аналітичного забезпечення сил безпеки, окресленні методологічних засад розвитку цієї системи в частині забезпечення обороноздатності держави, а також розробленні механізмів державного управління системою інтеграції технологій у систему інформаційно-аналітичного забезпечення сил безпеки України, та запропоновано інформаційні механізми державного управління інформаційно-аналітичного забезпечення сил безпеки України. Підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України проведено завдяки удосконаленню законодавчої та нормативної бази для забезпечення чіткого розмежування повноважень між різними структурами безпеки; адаптації законодавчої та нормативної бази до сучасних викликів у сфері інформаційної безпеки і технологій; створенню механізмів для забезпечення ефективної міжвідомчої координації та обміну інформацією; інтеграції та модернізації технологічної інфраструктури; інвестиціям в оновлення і розвиток єдиної інтегрованої технологічної платформи для обробки та аналізу даних; розробленню і впровадженню єдиної інформаційно-аналітичної платформи для збору, обробки, аналізу та розподілу інформації між усіма зацікавленими структурами безпеки; уніфікації форматів даних; стимулюванню розроблення вітчизняних інноваційних рішень в галузі інформаційної безпеки й аналітики.

9. Обґрунтовано загальнодержавну модель функціонування та розвитку

механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Модель базується на механізмах: формування організаційної структури кожного суб'єкта в залежності від його виду діяльності, завдань та призначення; контролю у сфері функціонування системи інформаційно-аналітичного забезпечення; правового забезпечення системи інформаційно-аналітичного забезпечення; підготовки та перепідготовки персоналу у сфері інформаційно-аналітичного забезпечення; фінансового забезпечення. Зазначена модель дала змогу визначити впливи державного управління на систему інформаційно-аналітичного забезпечення сил безпеки для подальшого удосконалення системи інформаційно-аналітичного забезпечення та механізмів державної безпеки.

10. Розроблено стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Стратегія базується на SWOT-аналізі, матриця якого описує стратегічні визначення, що можна реалізувати, знаходячи оптимальне поєднання між сильними і слабкими сторонами як внутрішніми чинниками, а також можливостями і загрозами як зовнішніми факторами, а саме: «Сильні сторони: Кваліфікований персонал, міжнародне партнерство, адаптивність до загроз»; «Слабкі сторони: Технологічне відставання, обмежені бюджетні ресурси, відсутність ефективної координації та взаємодії між різними структурами безпеки»; «Можливості: Впровадження новітніх технологій та інноваційних рішень у сфері аналітики та кібербезпеки, міжнародне фінансування та допомога, нормативно-правові реформи»; «Загрози: Кіберзагрози, політична нестабільність, технологічна залежність», відповідно, це дало змогу визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Споришев К. О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України: теорія, методологія, практика : монографія. Одеса : Олді+, 2024. 314 с.

2. Sporyshev K. Theoretical basis of the information and analytical support development of the security forces of Ukraine: aspects of state governance. *International security studios: managerial, technical, legal, environmental, informative and psychological aspects : international collective monograph*. Oslo, Kingdom of Norway, 2024. Vol. I. Pp. 379–407.

Наукові статті у виданнях, що включені до наукометричних баз Scopus, Web of Science

3. Bielai S., Antonova L., Hololobov S., Yevtushenko I., Sporyshev K. The Impact of a Practice-Oriented Paradigm on Public Administration and National Security. *International Journal of Sustainable Development and Planning*. 2024. Vol. 19, No. 1. Pp. 277–288. DOI: <https://doi.org/10.18280/ijstdp.190126>
URL: <https://www.iieta.org/journals/ijstdp/paper/10.18280/ijstdp.190126> (*Scopus*).

Особистий внесок: визначено підхід до формування інформаційної основи

для прийняття та реалізації управлінських рішень.

4. Kryshchanovych M., Batiuk O., Panfilova T., Burnatnyi V., Sporyshev K. Mechanism for information supporting the financial and economic security of information and telecommunication enterprises under the influence of modern cyber threats. *Financial and credit activity: problems of theory and practice*. 2024. Vol. 2 (55). Pp. 461-473. DOI: <https://doi.org/10.55643/fcaptop.2.55.2024.4298>
URL: <https://www.fkd.net.ua/index.php/fkd/article/view/4298/4088> (*Scopus*).

Особистий внесок: обґрунтовано підхід до механізмів захисту інформації системи державного управління.

5. Batiuk O., Puzyrov M., Sporyshev K., Yevtushenko I., Vlasova G. Overcoming threats to national security in conditions of war. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14, Issue 1, Special issue XL. Pp. 209–214. URL: <https://www.magnanimitas.cz/ADALTA/140140/PDF/140140.pdf> (*Web of Science*). DOI: <https://doi.org/10.33543/j.140140.209214>

Особистий внесок: визначено проблеми національної безпеки в умовах воєнного стану.

Наукові статті у фахових виданнях

6. Бєлай С. В., Спорішев К. О. Ефективність державного управління у сфері моніторингу та аналізу сучасних викликів державній безпеці України від інформаційних загроз. *Наукові перспективи. Державне управління*. 2023. Вип. 12 (42). С. 71–79.

Особистий внесок: визначено вплив інформаційних загроз на ефективність державного управління у сфері безпеки України.

7. Спорішев К. О. Інформаційно-аналітичні технології сил безпеки у парадигмі державного управління. *Наукові інновації та передові технології. Управління та адміністрування*. 2024. № 1 (29). С. 128–136.

8. Бєлай С. В., Спорішев К. О., Онопрієнко О. С. Генезис інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки України: сучасні виклики державного управління. *Актуальні питання у сучасній науці. Державне управління*. 2024. № 1 (19). С. 105–113.

Особистий внесок: визначено проблеми інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки України.

9. Бєлай С. В., Спорішев К. О. Вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку. *Наукові інновації та передові технології. Управління та адміністрування*. 2024. № 2 (30). С. 29–37.

Особистий внесок: визначено вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку.

10. Єманов В. В., Спорішев К. О. Досвід функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу. *Наукові перспективи. Державне управління*. 2024. № 1 (43). С. 132–142.

Особистий внесок: проведено аналіз функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу.

11. Спорішев К. О. Методологічні засади функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Інвестиції: практика та досвід*. 2024. Вип. 6. С. 251–255.

12. Бєлай С. В., Споришев К. О. Системи підтримки прийняття рішень у державному управлінні силами безпеки України. *Актуальні питання у сучасній науці. Державне управління*. 2024. № 2 (20). С. 320–329.

Особистий внесок: визначено роль та місце інформаційно-аналітичного забезпечення в циклі управління силами безпеки.

13. Споришев К. О. Підсистеми захисту інформації в системі державного управління силами безпеки України. *Інвестиції: практика та досвід*. 2024. № 4. С. 224–228.

14. Споришев К. О. Засади автоматизації інформаційних систем управлінського призначення сил безпеки передових країн ЄС та НАТО. *Державне управління: удосконалення та розвиток*. 2024. Вип. 2. URL: <https://nauka.com.ua/index.php/dy/article/view/2998/3034>.

15. Споришев К. О. Організаційні аспекти управління інформаційними ресурсами. *Наукові перспективи. Державне управління*. 2024. Вип. 2 (44). С. 466–475.

16. Споришев К. О. Аналіз нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України. *Чесць і закон*. 2024. № 1 (88). С. 142–149.

17. Споришев К. О. Підходи до застосування геоінформаційних систем в управлінській діяльності сил безпеки України. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Публічне управління та адміністрування*. 2024. Т. 35 (74), № 1. С. 196–200. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/1_2024/36.pdf.

18. Споришев К. О. Проблеми формування і суперечності реалізації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Наукові інновації та передові технології. Управління та адміністрування*. 2024. № 3 (31). С. 301–309.

19. Споришев К. О. Перспективні шляхи планування інформаційно-аналітичної діяльності в силах безпеки України. *Державне управління: удосконалення та розвиток*. 2024. Вип. 3. URL: <https://www.nauka.com.ua/index.php/dy/issue/view/135>.

20. Споришев К. О. Розвиток менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України. *Актуальні питання у сучасній науці. Державне управління*. 2024. № 3 (21). С. 410–421.

21. Споришев К. О. Загальнодержавна концептуальна модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Наукові перспективи. Державне управління*. 2024. № 3 (45). С. 390–398.

22. Споришев К. О. Стратегія розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Наукові інновації та передові технології. Управління та адміністрування*. 2024. № 4 (32). С. 165–175.

Наукові праці, які засвідчують апробацію матеріалів дисертації

23. Бєлай С. В., Споришев К. О. Аналіз протиріч системи військового управління силами безпеки України. *Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони в умовах воєнного*

стану : матеріали міжвідомчого круглого столу співробітників підрозділів СБУ, науково-педагогічних працівників Національної академії СБУ, м. Київ, 16 листоп. 2023 р. Київ, 2023. Вип. 2. С. 36.

Особистий внесок: визначено аспекти протиріч системи військового управління силами безпеки України.

24. Споришев К. О. Аналіз стану системи інформаційно-аналітичного забезпечення сил безпеки України. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* : матеріали ХLI Міжнар. наук.-практ. конф., м. Анкара, 07 лют. 2024 р. Київ : ГО «ВАДНД», 2024. С. 64–68.

25. Споришев К. О. Вплив невизначеності обстановки на якість прийняття управлінських рішень в системі державного управління силами безпеки України. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* : матеріали ХLII Міжнар. наук.-практ. конф., м. Мілан, 07 берез. 2024 р. Київ : ГО «ВАДНД», 2024. С. 39–41.

26. Споришев К. О. Інформаційні механізми державного управління інформаційно-аналітичним забезпеченням сил безпеки України. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку*: матеріали ХLIII Міжнар. наук.-практ. конф., м. Пештера, 07 квіт. 2024 р. Київ : ГО «ВАДНД», 2024. С. 41–44.

27. Споришев К. О. Аспекти стратегії розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* : матеріали ХLIV Міжнар. наук.-практ. конф., м. Умео, 07 трав. 2024 р. Київ : ГО «ВАДНД», 2024. С. 20–23.

28. Споришев К. О. Проблемні аспекти функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. *Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів ХХI століття* : зб. тез доп. Всеукр. наук.-практ. конф., м. Житомир, 7-8 груд. 2023 р. Житомир : Житомирська політехніка, 2023. С. 340–344.

29. Споришев К. О. Економічна складова механізмів державного управління інформаційно-аналітичним забезпеченням. *Публічне управління у сфері цивільного захисту: освіта, наука, практика* : зб. матеріалів міжнар. наук.-практ. інтернет-конф., м. Харків, 29 берез. 2024 р. Харків : НУЦЗУ, 2024. С. 245–247.

30. Споришев К. О. Математичні моделі системи імітаційного моделювання JSATS. *Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів* : зб. тез доп. ХII Міжнар. наук.-практ. конф., м. Харків, 27 жовт. 2023 р. Харків : НА НГУ, 2023. С. 314.

31. Споришев К. О. Інформаційно-аналітичне забезпечення діяльності військових формувань України. *Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів* : зб. тез доп. ХI Міжнар. наук.-практ. конф., м. Харків, 28 жовт. 2022 р. Харків : НА НГУ, 2022. С. 287.

32. Белай С. В., Споришев К. О. Стан інформаційно-аналітичного

забезпечення в суб'єктах сил безпеки. *Публічне управління в Україні: виклики сьогодення та глобальні імперативи* : зб. тез III Міжнар. наук.-практ. конф., м. Хмельницький, 8 лют. 2024 р. Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2024. С. 149–151.

Особистий внесок: визначено стан інформаційно-аналітичного забезпечення в окремих суб'єктах сил безпеки.

33. Споришев К. О., Семенко Є. Ю., Майборода І. М. Тенденції застосування систем управління силами відомств охорони правопорядку провідних країн світу. *Інтегровані інтелектуальні робототехнічні комплекси (ІРТК-2020)* : зб. тез Тринадцятої міжнар. наук.-практ. конф., м. Київ, 19-20 трав. 2020 р. Київ : НАУ, 2020. С. 293–295.

Особистий внесок: визначено тенденції розвитку систем управління силами відомств охорони правопорядку провідних країн світу.

34. Споришев К. О. Теорія ігор як інструментарій теорії прийняття рішень під час виконання службово-бойових завдань підрозділами Національної гвардії України. *Проблеми бойового та логістичного забезпечення складових сектору безпеки і оборони України* : зб. тез доп. Всеукр. наук.-практ. конф., м. Харків, 09 лют. 2021 р. Харків : НА НГУ, 2021. С. 322–323.

35. Споришев К. О. Проблемні питання розвитку інформаційно-аналітичного забезпечення Національної гвардії України. *Участь правоохоронних органів та військових формувань держави у забезпеченні безпеки України* : зб. тез доп. V Всеукр. наук.-практ. конф., м. Харків, 26 листоп. 2020 р. Харків : НА НГУ, 2020. С. 134.

Наукові статті, які додатково відображають наукові результати дисертації

36. Єманов В. В., Белай С. В., Споришев К. О. Інформаційно-аналітичний метод підвищення ефективності технічної розвідки підрозділів технічного забезпечення Національної гвардії України. *Збірник наукових праць Національної академії Національної гвардії України*. Харків, 2022. Вип. 1 (39). С. 104–110.

Особистий внесок: запропоновано інформаційно-аналітичний метод підвищення ефективності технічної розвідки підрозділів технічного забезпечення.

37. Єманов В. В., Споришев К. О., Онопрієнко О. С. Метод багатофакторного вибору експертів за максимумом коефіцієнта компетентності. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Технічні науки*. 2022. № 5 (72). С. 73–80.

Особистий внесок: виконано аналіз методів вибору групи експертів для проведення експертного оцінювання та розроблено метод вибору експертів.

38. Єманов В. В., Споришев К. О., Шаповалов О. І. Проблеми інформатизації процесів управління системою технічного обслуговування та ремонту автобронетанкової техніки. *Честь і закон*. Харків, 2022. Вип. 3 (82). С. 108–116.

Особистий внесок: визначено шляхи зменшення впливу негативних факторів втрат озброєння і військової техніки на ефективність інформатизації процесів управління.

АНОТАЦІЯ

Споришев К. О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. – 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. Національна академія Національної гвардії України, Харків, 2024.

У дисертаційному дослідженні вирішено актуальну наукову проблему, що полягає в теоретико-методологічному обґрунтуванні й розробленні практичних рекомендацій щодо розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Визначено фактори стану системи інформаційно-аналітичного забезпечення сил безпеки України, що впливають на державну безпеку, за допомогою діаграми Ісікави. Досліджено системи підтримки прийняття рішень у державному управлінні силами безпеки України. Визначено шляхи покращення системи підтримки прийняття рішень у державному управлінні силами безпеки України через підвищення компетентності та професіоналізму персоналу, застосування сучасних інформаційних технологій, таких як штучний інтелект, обробка великих масивів даних та розвиток технологій. Удосконалено механізми державного управління системою підтримки прийняття рішень через покращення кадрових, організаційних, правових, технічних механізмів державного управління.

Удосконалення підсистеми захисту інформації в системі державного управління силами безпеки України проводиться через реформування організаційних, правових, кадрових механізмів державного управління. Покращено організаційно-штатну структуру системи інформаційно-аналітичного забезпечення суб'єктів сил безпеки завдяки оптимізації інформаційних потреб органів управління за допомогою створення інформаційної координації між підрозділами та суб'єктами сил безпеки, адаптації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України до потреб економіки, а також забезпечення високого рівня захисту даних та приватності.

Удосконалено нормативно-правову базу інформаційно-аналітичного забезпечення сил безпеки України завдяки комплексному підходу, що охоплює законодавчі, технічні та організаційні заходи. Дослідження міжнародного досвіду у сфері нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки дає змогу визначити передові практики та інноваційні підходи, які можуть бути адаптовані та впроваджені в Україні.

Удосконалення механізму застосування геоінформаційних систем у державному управлінні силами безпеки України отримано через розвиток механізмів стратегічного планування й оперативного реагування, що сприяє підвищенню обороноздатності країни та захисту національних інтересів, а також дослідження впливу геоінформаційних систем на ефективність управління в секторі безпеки та оборони України, які, на відміну від нинішніх, зважають на особливості завдань, що вирішуються в суб'єктах сил безпеки України.

Удосконалено механізми державного управління кадровими ресурсами в системі інформаційно-аналітичного забезпечення сил безпеки України, які базуються на використанні інформаційних технологій автоматизації управління персоналом, управлінні компетенціями та плануванням потреб у навчанні, використанні аналітичних інструментів для прогнозування потреб у персоналі, аналізу тенденцій на ринку праці, оцінки ефективності персоналу та прийнятті обґрунтованих рішень.

Підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України проведено завдяки удосконаленню законодавчої та нормативної бази для забезпечення чіткого розмежування повноважень між різними структурами безпеки; адаптації законодавчої та нормативної бази до сучасних викликів у сфері інформаційної безпеки і технологій; розробленню та впровадженню єдиної інформаційно-аналітичної платформи для збору, обробки, аналізу та розподілу інформації між усіма зацікавленими структурами безпеки; уніфікації форматів даних; стимулюванню розроблення вітчизняних інноваційних рішень у сфері інформаційної безпеки та аналітики.

Сформовано стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Розроблені стратегії дадуть змогу визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Ключові слова: державне управління, механізми державного управління, державна безпека, інформаційно-аналітичне забезпечення, сили безпеки, сектор безпеки і оборони України, службово-бойова діяльність, забезпечення громадської безпеки.

SUMMARY

Sporyshev K. Mechanisms of state management of the system of information and analytical support of the security forces of Ukraine. – Qualifying scientific work as a manuscript.

Dissertation for obtaining the scientific degree of Doctor of Sciences in public administration, specialty 25.00.05 – public administration in the field of state security and protection of public order. National Academy of the National Guard of Ukraine, Kharkiv, 2024.

The dissertation study solved an actual scientific problem, which consists in theoretical and methodological substantiation and the development of practical recommendations for the development of mechanisms of state management of the system of information and analytical support of the security forces of Ukraine. Ways to improve the decision-making support system in the state management of the security forces of Ukraine due to increasing the competence and professionalism of personnel, the use of modern information technologies such as artificial intelligence, processing of large data sets and the development of technologies are identified. Improved state management mechanisms and decision-making support system due to improvement of personnel, organizational, legal, and technical mechanisms of state management.

The improvement of the information protection subsystem in the system of state

management of the security forces of Ukraine is carried out at the expense of the improvement of organizational, legal, personnel mechanisms of state management. Improvement of the organizational and staff structure of the system of information and analytical provision of the security forces by optimizing the information needs of management bodies due to the creation of information coordination between units and entities of the security forces, adaptation of state management mechanisms of the system of information and analytical provision of the security forces of Ukraine to the needs of the economy, as well as ensuring a high level of data protection and privacy.

The regulatory and legal basis of information and analytical support of the security forces of Ukraine has been improved due to a comprehensive approach, which includes legislative, technical, and organizational measures. The researched international experience in the field of regulatory and legal framework of information and analytical provision of security forces allows to determine best practices and innovative approaches that can be adapted and implemented in Ukraine.

The improvement of the mechanism of the application of geoinformation systems in the state management of the security forces of Ukraine was obtained through the development of mechanisms for strategic planning and operational response, which contributes to the increase of the country's defense capabilities and the protection of national interests, the study of the influence of geoinformation systems on the effectiveness of management in the security and defense sector of Ukraine, which, unlike the existing take into account the peculiarities of the tasks solved in the subjects of the security forces of Ukraine.

Improved mechanisms of state management of personnel resources in the system of information and analytical support of the security forces of Ukraine, which are based on the use of information technologies for the automation of personnel management, management of competencies and planning of training needs, use of analytical tools for forecasting personnel needs, analysis of trends in the labor market, evaluation personnel efficiency and informed decision-making.

Increasing the effectiveness of planning information and analytical activities in the security forces of Ukraine was carried out due to the improvement of the legislative and regulatory framework to ensure a clear separation of powers between various security structures; adaptation of the legislative and regulatory framework to modern challenges in the field of information security and technologies; development and implementation of a single information and analytical platform for the collection, processing, analysis and distribution of information among all interested security structures; unification of data formats; stimulating the development of domestic innovative solutions in the field of information security and analytics.

A strategy for the development of mechanisms of state management of the system of information and analytical support of the security forces of Ukraine has been formed. The developed strategies will allow to determine the ways of improving the state management mechanisms of the system of information and analytical support of the security forces of Ukraine.

Keywords: public administration, mechanism of state administration, state security, information and analytical support, security forces, security and defense sector of Ukraine, service and combat activity, security support.

Відповідальний за випуск *Споришев Костянтин Олександрович*

Підписано до друку 18.08.2024 р.
Формат 60x84/16. Ум.-друк. арк. 2,27.
Гарнітура Таймс. Наклад 100 прим.

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

