НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

СПОРИШЕВ Костянтин Олександрович

УДК 351.74:355/359:004

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

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

Подається на здобуття наукового ступеня доктора наук
з державного управління

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ К.О. Споришев

Харків – 2024

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. Узагальненні фактори системи кіберзахисту, які включають підсистеми шифрування, обмеження доступу, програмно-технічні модулі захисту інформації, наявність засобів автоматизації управління, наявність геопросторового аналізу та їх вплив на ефективність системи інформаційно-аналітичного забезпечення сил безпеки. Досліджена залежність навченості персоналу, що забезпечує роботу ІАС на ефективність виконання службово-бойових завдань силами безпеки. Визначена 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 на ефективність системи інформаційно-аналітичного забезпечення сил безпеки.

Досліджено засади функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України. Визначена роль та місце математичних методів, інформаційних технологій та моделювання процесів та

явищ, що характерні для систем державного управління. Визначеннішляхи покращення системи підтримки прийняття рішень у державному управлінні силами безпеки України за рахунок підвищення компетентності та професіоналізму персоналу, застосування сучасних інформаційних технологій таких як штучний інтелект, обробки великих масивів даних та покращення якості прийнятих рішень.Удосконалені механізми державного управління системою підтримки прийняття рішень за рахунок покращення кадрових, організаційних, правових, технічних механізмів державного управління.

Визначені аспекти функціонування підсистеми захисту інформації в суб'єктах сил безпеки України.Вдосконаленні механізми державного управління системами захисту інформації сил безпеки України з урахуванням викликів з якими зіткнулась наша держава. Обґрунтовані вимоги до підсистеми захисту інформації та вимоги до захищеностіінформації, що циркулює в системахдержавного управління силами безпеки України. Визначенні фактори що впливають на ефективність державного управління підсистемами захисту інформації. Визначений механізм впливу на державну безпеку станупідсистеми захисту інформації в суб'єктах сил безпеки України. Вдосконалення підсистеми захисту інформації в системі державного управління силами безпеки України проведено за рахунок комплексного поєднання організаційних, правових, кадрових механізмів державного управління.

Досліджено організаційний механізм державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Покращення організаційно-штатної структури системи інформаційно-аналітичного забезпечення суб'єктів сил безпеки шляхом оптимізації інформаційних потреб органів управління. Удосконалення організаційних механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України за рахунок 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.

Нормативно-правова база функціонування системи інформаційно-аналітичного забезпечення сил безпеки України удосконалена шляхом 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, що дозволило надати пропозиції з визначення інформаційних потреб органів управління силами безпеки, узгодження вітчизняних стандартів зі стандартами НАТО, а також адаптації нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України до стандартів НАТО.

Визначеніймеханізмзастосуваннягеоінформаційних систем в державному управлінні силами безпеки Українидозволив підвищити ефективність прийняття рішень та планування в сферідержавного управлінні силами безпеки України. Визначений вплив механізмузастосуваннягеоінформаційних систем у державному управлінні силами безпеки України надержавну безпеку. Досліджений вплив геоінформаційних систем на ефективність управління в секторі безпеки та оборони України, які на відміну від існуючих ураховують особливості завдань, що вирішуються в суб’єктах сил безпеки України.

Удосконалений механізм державного управління кадровими ресурсами в системі інформаційно-аналітичного забезпечення сил безпеки України, який базується 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 прийняття обґрунтованих рішень. Надані пропозиції для впровадження механізму 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, розробки та імплементації програм управління компетенціями, використанні інструментів на основі штучного інтелекту, впровадженні аналітичних інструментів для збору та аналізу даних про персонал.Створені практичні рекомендаціїдозволилипідвищити ефективність та адаптивність кадрової політикиза рахунок впровадження сучасних ІТ-рішень, розвитку компетенцій та професійного навчання, використання зворотного зв’язку з роботодавцями.

Сформульовані 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 методологічні засади розвитку системи інформаційно-аналітичного забезпечення сил безпеки щодо забезпечення обороноздатності держави, а також розробленні механізми державного управління системою інтеграції технологій в систему інформаційно-аналітичного забезпечення сил безпеки України та запропоновані інформаційні механізми державного управління інформаційно-аналітичного забезпечення сил безпеки України. Підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України проведено за рахунок удосконалення 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 та технологій; створення механізмів для забезпечення ефективної міжвідомчої координації та обміну інформацією; інтеграція та модернізація технологічної інфраструктури; інвестиції в оновлення та розвиток єдиної інтегрованої технологічної платформи для обробки та аналізу даних; розробка та впровадження єдиної інформаційно-аналітичної платформи для збору, обробки, аналізу та розподілу інформації між усіма зацікавленими структурами безпеки; уніфікація форматів даних; стимулювання розробки вітчизняних інноваційних рішень в області інформаційної безпеки та аналітики.

Обґрунтована загальнодержавна модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, яка базується на механізмах: формування організаційної структури кожного суб'єкту в залежності від його виду діяльності, завдань та призначення; правового забезпечення системи інформаційно-аналітичного забезпечення; підготовки та перепідготовки персоналу в сфері інформаційно-аналітичного забезпечення; фінансового забезпечення і дозволила визначити впливи державного управління на систему інформаційно-аналітичного забезпечення сил безпеки для подальшого удосконалення системи інформаційно-аналітичного забезпечення та механізмів державної безпеки.

Розроблено стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України на основі SWOT-аналізу, 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», та дозволили визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

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

ANNOTATION

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

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 the theoretical and methodological substantiation and 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.

The factors of the state of the system of information and analytical support of the security forces of Ukraine, which affect state security, are determined using the Ishikawa diagram. Generalized factors of the cyber defense system, which include encryption subsystems, access restrictions, software and technical modules for information protection, the availability of control automation tools, the presence of geospatial analysis and their impact on the effectiveness of the information and analytical support system of the security forces. The dependence of the training of the personnel that ensures the operation of the IAS on the effectiveness of the performance of official and combat tasks by the security forces has been investigated. The dependence of the factors of material and technical support of the IAS was determined, which include: financial support of the IAS, provision of computing equipment and software and technical means, technical support of software and mathematical support of the IAS on the effectiveness of the system of information and analytical support of the security forces.

The principles of the functioning of the decision-making support system in the state management of the security forces of Ukraine have been studied. The role and place of mathematical methods, information technologies and modeling of processes and phenomena characteristic of public administration systems is defined. Identified

ways to improve the decision-making support system in the state management of the security forces of Ukraine by increasing the competence and professionalism of personnel, using modern information technologies such as artificial intelligence, processing large data sets and improving the quality of decisions made. Improved mechanisms of state management of the decision-making support system by improvement of personnel, organizational, legal, and technical mechanisms of state administration.

Identified aspects of the functioning of the subsystem of information protection in the entities of the security forces of Ukraine. Improved mechanisms of state management of information protection systems of the security forces of Ukraine, taking into account the challenges faced by our state. Reasoned requirements for the subsystem of information protection and requirements for the security of information circulating in the state management systems of the security forces of Ukraine. Determined factors affecting the effectiveness of state management of information protection subsystems. The mechanism of influence on state security of the state of the subsystem of information protection in the entities of the security forces of Ukraine is determined. The improvement of the information protection subsystem in the system of state management of the security forces of Ukraine was carried out at the expense of a complex combination of organizational, legal, and personnel mechanisms of state management. The organizational mechanism of state management of the system of information and analytical support of the security forces of Ukraine has been studied. Improvement of the organizational and staff structure of the system of information and analytical support of subjects of the security forces by optimizing the information needs of management bodies. Improvement of the organizational mechanisms of state management of the system of information and analytical support of the security forces of Ukraine due to the creation of information coordination between units and subjects of the security forces, adaptation of the mechanisms of state management of the system of information and analytical support 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 the functioning of the system of information and analytical support of the security forces of Ukraine has been improved by substantiating state-wide approaches to the prospects for the development of information and analytical support, based on the systematization of normative and legal acts of the information and analytical support of the security forces of Ukraine, as well as departmental guidance documents of the security forces of Ukraine. which specify the use of information and analytical methods during the performance of service and combat tasks, which made it possible to provide proposals for determining the information needs of security forces management bodies, harmonizing domestic standards with NATO standards, as well as adapting the legal framework for information and analytical support of the security forces of Ukraine to NATO standards. The defined mechanism of application of geoinformation systems in the state management of the security forces of Ukraine allowed to increase the efficiency of decision-making and planning in the field of state management of the security forces of Ukraine. The influence of the mechanism of application of geoinformation systems in the state management of the security forces of Ukraine on state security is determined. The influence of geoinformation systems on the effectiveness of management in the security and defense sector of Ukraine, which, unlike the existing ones, take into account the peculiarities of the tasks solved by the entities of the security forces of Ukraine, is studied.

The improved mechanism of state management of personnel resources in the system of information and analytical support of the security forces of Ukraine, which is based on the use of information technologies for 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. Proposals for the implementation of the mechanism of state management of personnel resources in the system of information and analytical support of the security forces of Ukraine, which consist in the transition to complex human resources management systems, the use of training management systems, the development and implementation of

competence management programs, the use of tools based on artificial intelligence, the implementation of analytical tools for collecting and analyzing personnel data. The created practical recommendations made it possible to increase the efficiency and adaptability of the personnel policy due to the implementation of modern IT solutions, the development of competencies and professional training, and the use of feedback from employers.

Formulated key directions for increasing the efficiency of planning information and analytical activities in the security forces of Ukraine, which consist in the formation of the theoretical foundations of the functioning of the system of information and analytical support of the security forces, the outline of the methodological principles of the development of the system of information and analytical support of the security forces to ensure the state's defense capability, as well as the development mechanisms of state management of the system of integration of technologies into the system of information and analytical support of the security forces of Ukraine and proposed information mechanisms of state management of information and analytical support of the security forces of Ukraine. 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; creation of mechanisms to ensure effective interdepartmental coordination and information exchange; integration and modernization of technological infrastructure; investment in updating and developing a single integrated technological platform for data processing and analysis; 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 substantiated nationwide model of the functioning and development of state

management mechanisms of the system of information and analytical support of the security forces of Ukraine, which is based on the mechanisms: formation of the organizational structure of each subject depending on its type of activity, tasks and purpose; legal support of the information and analytical support system; training and retraining of personnel in the field of information and analytical support; financial support and allowed to determine the influence of state administration on the system of information and analytical support of security forces for further improvement of the system of information and analytical support and state security mechanisms.

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 developed on the basis of a SWOT analysis, the matrix of which describes strategic definitions that can be implemented by finding the optimal combination between strengths and weaknesses as internal factors, as well as opportunities and threats as external factors , namely: "Strengths: Qualified personnel, international partnership, adaptability to threats"; "Weaknesses: Technological lag, limited budgetary resources, lack of effective coordination and interaction between various security structures"; "Opportunities: Implementation of the latest technologies and innovative solutions in the field of analytics and cyber security, international financing and assistance, regulatory and legal reforms"; "Threats: Cyberthreats, political instability, technological dependence", and allowed 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: state 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.

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/ijsdp.190126
URL: https://www.iieta.org/journals/ijsdp/paper/10.18280/ijsdp.190126 *(Scopus).*

Особистий внесок: визначено підхід до формування інформаційної основи для прийняття та реалізації управлінських рішень.

4. Kryshtanovych 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/fcaptp.2.55.2024.4298
URL: https://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/papers/A_34.pdf. *(Web of Sience).* DOI: https://doi.org/10.33543/j.140140.209214

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

Наукові статті у фахових виданнях

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

Особистий внесок: визначений вплив на ефективність державного управління у сфері державній безпеці України інформаційних загроз.

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

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

9. Бєлай С.В., Споришев 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: визначений вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку.

10. Єманов В.В., Споришев 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: проведений аналіз функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу.

11. Споришев 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: визначена 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://nayka.com.ua/index.php/dy/article/view/2998/3034

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

16. Споришев К.О. Аналіз нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки Україні. *Честь 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 адмініструванн.* 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. 30–309.

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.nayka.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: визначені 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 XLI-ої 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 XLII-ої 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 XLIII-ої 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 XLIV-ої 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 XXI століття*: зб. тез до. 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 JCATS. *Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів:* зб. тез доп. XII 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. XI Міжнар. наук.-практ. конф., м. Харків, 28 жовт. 2022 р. Харків: НА НГУ, 2022. С. 287.

32. Бєлай 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: визначений 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 робото технічні комплекси (ІІРТК-2020)*: зб. тез Тринадцятої міжнар. наук.-практ. конф., м. Київ, 19-20 трав. 2020 р. Київ: НАУ, 2020. С.293–295.

Особистий внесок: визначені 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., Бєлай 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:проведено 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: визначенні шляхи зменшення впливу негативних факторів втрат озброєння і військової техніки на ефективність інформатизації процесів управління.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АСУ – автоматизована система управління
БД – база даних
ВВНЗ – вищий військовий навчальний заклад
ВВП – валовий внутрішній продукт
ВМС – Військово-морські сили
ВПС – Військово-повітряні сили
ГІС – Географічні інформаційні системи
ДАЕ – Державне агентство з питань електронного урядування
ДК – державнийкордон
ДПСУ – Державна прикордонна служба України
ДРГ – диверсійно-розвідувальні групи
ДСНС – Державна служба України з надзвичайних ситуацій
ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації
ЄАСУ – єдина автоматизована система управління
ЄІС – єдина інформаційна система
ЄС – Європейський Союз
ЗМІ – засоби масової інформації
ЗСУ – Збройні Сили України
ІАЗ – інформаційно-аналітичне забезпечення
ІАСПУ – інформаційно-аналітична система забезпечення процесів управління
ІПНП – інформаційний портал Національної поліції України
ІТ – інформаційні технології
КМУ – Кабінет Міністрів України
МВС – Міністерство внутрішніх справ
МН – машинне навчання
МОУ – Міністерство оборони України
МС – місцеве самоврядування

МТЗ – матеріально-технічне забезпечення
МЦТ – Міністерство цифрової трансформації України
НАДС – Національне агентство з питань державної служби України
НАТО – Організація Північноатлантичного договору
НГУ – Національна гвардія України
НЗФ – незаконні збройні формування
НПУ – Національна поліція України
ОБСЄ – Організація Безпеки Ради Європи
ОВТ – озброєння та військова техніка
ОГП – охорона громадського порядку
ОДВ – органи державної влади
ООН – Організація Об'єднаних Націй
ОПР – особа що приймає рішення
ПР – прийняття рішення
ПТКАПК – програмно-технічний комплекс для автоматизації прикордонного контролю
СБ – сили безпеки
СБД – службово-бойова діяльність
СБО – сили безпеки і оборони
СБУ – Служба безпеки України
СЗІБ – суб'єкти забезпечення інформаційної безпеки України
СО – сили оборони
СОІС – складні організаційні ієрархічні системи
СППР –системи підтримки прийняття рішень
ССЗІ – Спеціальна служба зв'язку та захисту інформації
ТЦК – територіальний центр комплектування
ШІ – штучний інтелект
BIG DATA – набор інформації великих розмірів
BEREC – орган європейських регуляторів електронних комунікацій
CEPOL – Європейське агентство з питань правоохоронної підготовки

CSIS – Центр стратегічних і міжнародних досліджень

eu-LISA – Європейське агентство оперативного управління ІТ-системами у сферах свободи, безпеки та юстиції

ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки

FIEP – Організація співдружності сил жандармерії (правоохоронних структур з військовим статусом)

JTLS – військова комп’ютерна симуляційна система

JCATS – система імітаційного моделювання

MDMP – процедури прийняття військових рішень

NSA – Агентство національної безпеки

ВСТУП

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 інформаційноаналітичного 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 функціювання 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 програмноматематичного 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 функціювання, 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. Бєлая, 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. McKitrick, 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 інформаційноаналітичного забезпечення сил безпеки. Водночас комплексного дослідження щодо опрацювання механізмів державного управління системою інформаційноаналітичного 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 функціювання 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 функціювання системи підтримки прийняття рішень у державному управлінні силами безпеки України;

– визначити аспекти функціювання 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 функціювання 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 функціювання 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 інформаційноаналітичного 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 функціювання системи інформаційноаналітичного 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 функціювання 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 функціювання 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 інформаційноаналітичного 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 функціювання системи інформаційноаналітичного 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 інформаційноаналітичного 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 інформаційноаналітичного забезпечення сил безпеки України, здійснюючи таким чином дієвий державний контроль у сфері інформаційно-аналітичного забезпечення сил безпеки України;

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

дістали подальшого розвитку:

– теоретико-методологічні засади функціювання 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 службовобойових завдань на забезпечення державної безпеки;

– теоретико-методологічні аспекти функціювання 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 функціювання 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 Сєвєродонецького 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 інформаційно-аналітичного забезпечення сил безпеки України 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. Антоновою, О. В. Батюком, С. В. Бєлаєм, В. В. Бурнатним, Г. П. Власовою, С. М. Гололобовим, І. В. Євтушенком, В. В. Єрмановим, 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 науковокомунікативних 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 службовобойової 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 науковопрактична інтернет-конференція «Публічне управління у сфері цивільного захисту: освіта, наука, практика»(м. Харків, 2024); XLI Міжнародна науковопрактична 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.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ

1.1 Аналіз та моніторинг інформаційних загроздержавній безпеці України

З метою аналізу сучасного стану інформаційних загроз державній безпеці України потрібно розглянути перелік існуючих загроз та нормативно-правову базу, яка ці загрози визначає.

Існує два основних підходи, щодо трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо [75].

Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Зокрема, проблему відображено у працях Петрика В.М., Ліпкана В.А., Кормича Б.А., Почепцова Г.Г. та інших фахівців.Так, слід згадати тих вітчизняних і зарубіжних учених, які зробили значний внесок у вивчення інформаційних впливів та небезпек, інформаційних війн і т.д.: Андрусів Г.В., Гафнер В.В., Демиденко В.В., Діордіца І.В., Забара І.М., Пазюк А.В., Почепцов Г.Г., Камінська Н.В., Кормич Б.А., Костюк І.В., Лібікі М.І., Ліпкан В.А., Любарський С.В., Моландер Р.Е., Най Дж., Сасин Г.В., Сивак О.І., Ткачук П.В., Шевчук П.І., Цуканова О.В., Хорошко В.О., Щурко О.М. та ін.

Інформаційна безпека є невід’ємною частиною національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпека, з одного боку, забезпечує всебічне інформування громадян та доступ до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння

єдності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційним впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій [4, 75]. Інформаційна безпека є складним, багаторівневим явищем, на яке впливають зовнішні та внутрішні фактори, найважливішими з яких є: політична ситуація у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан та рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична ситуація в державі [249].

Сучасний стан проблеми забезпечення інформаційної безпеки, зокрема в Україні, характеризується активними спробами розвитку відповідних теоретичних засад, про що свідчать численні публікації в наукових виданнях. Серед вітчизняних учених і фахівців цій проблемі приділено увагу в роботах Юдіна О., Богуша В., Горбуліна В., Остроухова В., Присяжнюка М., Толубка В., Почепцова Г., Петрика В., Левченка О. [60, 77, 78, 79, 144, 145, 167, 173, 197] та ін..

Основні напрями забезпечення інформаційної безпеки держави включають значний комплекс заходів, до яких належать:

- розвиток наукових і практичних основ інформаційної безпеки;
- удосконалення законодавчої та нормативно-правової бази для забезпечення інформаційної безпеки;
- створення концептуальних, нормативно-правових та організаційно-методичних документів для збереження і розвитку інформаційних ресурсів;
- визначення правового статусу суб’єктів системи інформаційної безпеки;
- розробка законодавчих і нормативних актів для регулювання порядку ліквідації наслідків загроз інформаційній безпеці;
- вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці;
- розвиток сучасних методів забезпечення інформаційної безпеки [50].

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 [171] та від 28.12.2021 № 685/2021 [172].

Варто відзначити, що Стратегією інформаційної безпеки України вперше введено в офіційний обіг термін «інформаційна безпека України» – невід'ємна частина національної безпеки України. Це стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших важливих інтересів людини, суспільства і держави. Він забезпечує конституційні права і свободи людини щодо збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації. Також існує ефективна система захисту і протидії негативним інформаційним впливам, у тому числі поширенню недостовірної інформації, деструктивної пропаганди, несанкціонованому розповсюдженню, використанню й порушенню цілісності інформації з обмеженим доступом [172].

Зокрема, у Стратегії визначено такі загрози, що є актуальними в сучасних У Стратегії визначено актуальні загрози для інформаційної безпеки:

Глобальні виклики:

- збільшення кількості дезінформаційних кампаній;
- інформаційна політика російської федерації як загроза для України та інших демократичних країн;
- вплив соціальних мереж в інформаційному просторі;
- низький рівень медіа-грамотності на фоні швидкого розвитку цифрових технологій.

Національні виклики:

- вплив російської федерації на населення України;
- домінування російської федерації на тимчасово окупованих територіях;
- обмежені можливості реагування на дезінформаційні кампанії;
- недосконала система стратегічних комунікацій;
- недосконале регулювання інформаційної діяльності та захисту журналістів;

– маніпуляції свідомістю громадян щодо європейської та євроатлантичної інтеграції України;

– обмежений доступ до інформації на місцевому рівні;

– низький рівень інформаційної культури та медіа-грамотності в суспільстві [171].

Поряд із цим, Стратегія національної безпеки України сучасними загрозами для національної безпеки України в інформаційній сфері визначила:

– стрімкі технологічні зміни та зростання ролі інформаційних технологій у всіх сферах суспільного життя;

– використання рф інформаційної «зброї» у поєднанні з енергетичною для зміцнення позицій у Європі, її спроби впливати на внутрішню ситуацію у європейських державах, підтримка триваючих конфліктів, збільшення військової присутності у Східній Європі;

– продовження російською федерацією гібридної війни проти України через системне застосування інформаційно-психологічних, кібернетичних, політичних, економічних та військових засобів для відновлення свого впливу на неї;

– внутрішню і зовнішню деструктивну пропаганду, яка розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи суспільні суперечності в умовах відсутності цілісної інформаційної політики держави та слабкості системи стратегічних комунікацій;

– недостатню ефективність державних органів, що ускладнює вироблення і реалізацію ефективної державної політики (зокрема в інформаційній сфері), створюючи загрози незалежності України, її суверенітету та демократії;

– посилення загроз для критичної інформаційної інфраструктури, зумовлених погіршенням її технічного стану, відсутністю інвестицій у її оновлення та розвиток, несанкціонованим втручанням у її функціонування, включаючи фізичні та кібернетичні атаки, триваючими бойовими діями, а також тимчасовою окупацією частини території України [172].

На сьогоднішній день національні інтереси та національна безпека України в інформаційній сфері стикаються з такими актуальними загрозами:

– проведення спеціальних інформаційних операцій, що підривають обороноздатність, деморалізують особовий склад Збройних Сил України та інших військових формувань, провокують екстремістські дії, сприяють панічним настроям, загострюють і дестабілізують суспільно-політичну та соціально-економічну ситуацію, розпалюють міжетнічні та міжконфесійні конфлікти;

– організація державою-агресором спеціальних інформаційних операцій у інших країнах для створення негативного іміджу України на міжнародній арені;

– інформаційна експансія держави-агресора та її контрольованих структур шляхом розширення власної інформаційної інфраструктури на території України та за її межами;

– недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та активно діяти в інформаційному полі для захисту національних інтересів;

– неефективність державної інформаційної політики, недосконале законодавство щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, низький рівень медіа-культури населення;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [153].

У загальному випадку загрози інформаційній безпеці можна поділити на зовнішні та внутрішні. Серед зовнішніх загроз найбільшу небезпеку становлять:

– вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію зовнішньої політики України;

– поширення дезінформації про зовнішню політику України за кордоном;

– порушення прав громадян України та юридичних осіб в інформаційній сфері за межами країни;

– несанкціоновані спроби доступу до інформації та вплив на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, що реалізують зовнішню політику України, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях.

Основні загрози національній безпеці України в інформаційній сфері [136, 158]:

– поширення ідей, що провокують конфлікти на національному, релігійному і соціальному ґрунті, масові заворушення, а також розпалювання ідей сепаратизму серед українського населення;

– заклики до посягання на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал держави з боку окремих груп та осіб;

– проведення інформаційних операцій та актів зовнішньої інформаційної агресії на шкоду інтересам України;

– комп’ютерна злочинність;

– інформаційний тероризм;

– розвідувально-підривна діяльність іноземних спецслужб;

– розголошення інформації, що становить державну таємницю або конфіденційної інформації, яка належить державі або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– дискредитація державної політики та авторитету окремих державних діячів;

– обмеження свободи слова і доступу громадян до інформації та інших їхніх прав і свобод;

– поширення ЗМІ культу насильства, жорстокості, порнографії та інших проявів аморальності;

– маніпуляції громадською думкою через поширення недостовірної, неповної або упередженої інформації;

– значна іноземна присутність в інформаційному просторі України;

– небезпечне зростання частки іноземного капіталу у стратегічних галузях економіки, пов’язаних з інформаційною сферою, що загрожує економічній незалежності України;

– науково-технологічне відставання України від розвинутих країн;

– низька конкурентоспроможність продукції для обслуговування інформаційної сфери;

– нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії;

– зниження внутрішнього попиту на підготовку науково-технічних кадрів, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності;

– відтік учених, фахівців, кваліфікованої робочої сили за межі України;

– інспірування інших деструктивних процесів в інформаційній сфері держави.

Основні функції системи забезпечення інформаційної безпеки України охоплюють створення та підтримку діяльності державних органів, які є елементами цієї системи. Це включає створення правових основ для формування, розвитку та функціонування системи, організацію її структури та окремих елементів, а також визначення та оптимальний розподіл їх функцій. Комплексне забезпечення діяльності елементів системи включає кадрове, фінансове, матеріальне, технічне та інформаційне забезпечення, а також підготовку цих елементів до виконання їх завдань.

Управління діяльністю системи інформаційної безпеки передбачає розробку стратегій та планування конкретних заходів, організацію та безпосереднє керівництво системою та її структурними елементами, оцінку ефективності дій, витрат на проведення заходів та їх наслідків. Планова та оперативна діяльність щодо забезпечення інформаційної безпеки включає визначення національних інтересів та їх пріоритетів в інформаційній сфері,

прогнозування, виявлення та оцінку можливих загроз, дестабілізуючих чинників та конфліктів, а також запобігання та усунення впливу цих загроз на національні інтереси.

Міжнародне співробітництво в сфері інформаційної безпеки передбачає розробку нормативно-правової бази, що регулює інформаційні відносини між державами, участь у існуючих та створення нових двосторонніх і багатосторонніх структур, спрямованих на спільне вирішення проблем інформаційної безпеки, а також участь у роботі керівних, виконавчих та забезпечувальних підрозділів цих структур.

Виконання повного переліку цих функцій є необхідною умовою для ефективного функціонування системи забезпечення інформаційної безпеки України. Для сил безпеки України інформаційна безпека в контексті національної безпеки розглядається як інтегральний показник, що складається з показників інформаційно-технічної безпеки, протидії кіберзлочинності та інформаційного протиборства.

Зокрема, створення правових основ для функціонування системи є фундаментом для її розвитку. Формування організаційної структури забезпечує оптимальний розподіл функцій між різними елементами системи. Комплексне забезпечення діяльності елементів системи гарантує їхню здатність ефективно виконувати свої завдання.

Управління діяльністю системи інформаційної безпеки включає стратегічне планування та оцінку ефективності дій. Планова та оперативна діяльність зосереджена на виявленні та нейтралізації загроз, які можуть вплинути на національні інтереси в інформаційній сфері. Міжнародне співробітництво дозволяє узгоджувати зусилля з іншими державами у забезпеченні інформаційної безпеки, що є важливим елементом національної безпеки.

Таким чином, система забезпечення інформаційної безпеки України є комплексним механізмом, який вимагає узгоджених дій на всіх рівнях управління та ефективного використання ресурсів.

Суб’єктами забезпечення інформаційної безпеки України (СЗІБ) є державні та недержавні інституції, а також громадяни України, об'єднані спільною метою захисту національних інтересів в інформаційній сфері. Таким чином, суб’єкти забезпечення інформаційної безпеки України утворюють багаторівневу систему з єдиною метою – забезпечення інформаційної безпеки країни, але мають різні повноваження, можливості та засоби для її реалізації [4].

До таких суб’єктів належать:

– держава, яка виконує свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки;

– громадяни, суспільні або інші організації та об'єднання, що мають повноваження забезпечувати інформаційну безпеку відповідно до законодавства України.

Це свідчить про те, що СЗІБ взаємодіє із системою суб’єктів, які здійснюють інформаційний вплив. Важливим для функціонування цих систем є саме перетин їхніх інтересів. Перевага в інформаційному протистоянні залежить від того, на чий бік схиляться ваги приватного сектору.

Моніторинг інформаційних загроз державній безпеці є ключовим елементом сучасного управління безпекою країни, особливо в умовах швидкого розвитку технологій та інформаційного простору. Відстеження інформаційних загроз включає аналіз і контроль за різними джерелами інформації, такими як мас-медіа, соціальні мережі, веб-сайти, електронна пошта та інші.

Розглянемо деякі аспекти, які можуть бути включені в систему моніторингу інформаційних загроз для державної безпеки України [13, 15]:

Спостереження за ЗМІ та соціальними мережами. Відслідковування та аналіз новин, коментарів та інших висловлювань в ЗМІ та соціальних мережах, що стосуються політичної ситуації в країні та закордоном.

Аналіз інтернет-ресурсів. Моніторинг форумів, блогів, веб-сайтів, де може з’являтися інформація, що загрожує державній безпеці.

Кібербезпека. Слідкування за кіберзагрозами, включаючи атаки на

інформаційні системи, критичну інфраструктуру та комп’ютерні мережі.

Моніторинг дезінформації. Виявлення та відслідковування спроб дезінформації або інформаційної війни.

Співпраця з розвідувальними структурами. Обмін інформацією з розвідувальними службами для забезпечення комплексного аналізу потенційних загроз.

Реагування та протидія. Розробка та впровадження стратегій та заходів для ефективного реагування на інформаційні загрози.

Навчання та розвиток. Забезпечення навчання персоналу та розвитку експертизи в галузі моніторингу інформаційних загроз.

Це лише загальний підхід, і конкретний моніторинг буде залежати від конкретних викликів та потреб держави в конкретний період часу. Важливо, щоб система моніторингу була гнучкою та адаптивною до змін у суспільстві та технологіях [15].

Система суб'єктів, відповідальних за забезпечення інформаційної безпеки, має діяти незалежно від внутрішньополітичної ситуації в Україні та стану окремих її елементів. Основним об'єднуючим фактором є спільна мета цих суб'єктів – забезпечення національного інформаційного суверенітету.

Для кращого розуміння питання виявлення ознак загроз національній безпеці в інформаційній сфері необхідно виокремити суб’єктів, що займаються процесами виявлення та оцінки інформаційних загроз і організовують заходи щодо їх протидії. До таких суб’єктів належать:

1. Президент України, який очолює Раду Національної безпеки і оборони (РНБО) України. Президенту також підпорядковується Національний інститут стратегічних досліджень. Апарат РНБО координує діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України та інших стратегічних науково-дослідних установ.

2. Кабінет Міністрів України, у складі якого діє Управління стратегії розвитку інформаційних ресурсів та технологій. Основні органи Кабінету Міністрів, відповідальні за інформаційну сферу, включають:

- Державний комітет телебачення та радіомовлення;
- Державний департамент інформатизації;
- Національну комісію з питань регулювання зв’язку.

Кабінет Міністрів також координує діяльність:

- Державного департаменту інтелектуальної власності Міністерства освіти та науки України;
- Державної адміністрації зв’язку Міністерства транспорту та зв’язку України;
- Департаменту Державної служби боротьби з економічною злочинністю Міністерства внутрішніх справ України, в якому діє Управління боротьби з правопорушеннями у сфері інтелектуальної власності та високих технологій;
- Дипломатичних представництв, консульських установ та інших структурних підрозділів Міністерства закордонних справ України;
- Спеціальних підрозділів Міністерства оборони і Збройних Сил України.

3. Служба безпеки України.

4. Державна служба спеціального зв’язку та захисту інформації України.

5. Розвідувальні органи України.

6. Національна поліція України.

Ці суб’єкти повинні діяти злагоджено та ефективно, забезпечуючи інформаційну безпеку країни на всіх рівнях управління. Важливим елементом цієї системи є моніторинг інформаційних загроз, який включає аналіз і контроль за різноманітними джерелами інформації, такими як мас-медіа, соціальні мережі, веб-сайти, електронна пошта та інші, що сприяє забезпеченню національної безпеки України в інформаційній сфері.

Забезпечення інформаційної безпеки України включає в себе ряд суб’єктів, які спільно приймають участь у захисті інформації та кіберпростору країни. Основні суб’єкти забезпечення інформаційної безпеки в Україні включають:

Державні органи та владні структури:

Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ): Здійснює управління системою захисту інформації та забезпечує імплементацію заходів інформаційної безпеки на державному рівні.

Міністерство цифрової трансформації України: Відповідає за розвиток та реалізацію державної політики у сфері інформаційних технологій та кібербезпеки.

Спеціальна служба зв’язку та захисту інформації (ССЗІ) Міністерства оборони України: Забезпечує захист інформації у військовому секторі.

Інші владні органи та служби: Виконують різноманітні функції у сфері інформаційної безпеки, включаючи правоохоронні органи та розвідувальні служби.

Кіберполіція та правоохоронні органи. Займаються розслідуванням кіберзлочинів та вживають заходів для протидії кіберзагрозам.

Спеціалізовані одиниці Служби безпеки України (СБУ). Відповідають за контррозвідувальні заходи в кіберпросторі та захист критичної інфраструктури.

Регулюючі та стандартизаційні органи. Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації (НКРЗІ): Регулює діяльність у сфері зв’язку та інформаційних технологій.

Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ). Розробляє стандарти та нормативні акти з питань інформаційної безпеки.

Приватний сектор та громадські організації:

Компанії та підприємства. Забезпечують кібербезпеку своїх інформаційних систем та взаємодіють з владними структурами для обміну інформацією про загрози.

Громадські організації та експертні групи. Відіграють роль у розвитку стратегій інформаційної безпеки та вивченні нових загроз.

Громадяни та користувачі:

Інтернет-спільнота та активісти: Можуть виявляти та повідомляти про інформаційні загрози, а також вживати заходів для своєї власної кібербезпеки.

Взаємодія між цими суб'єктами є важливим аспектом забезпечення інформаційної безпеки в Україні. Тільки спільні зусилля державних, приватних та громадських секторів можуть ефективно протистояти сучасним інформаційним загрозам.

Центральні органи державного управління при виконанні завдань щодо виявлення загроз інформаційній безпеці можуть залучати органи державної влади (ОДВ) та місцевого самоврядування (МС), засоби масової інформації, політичні партії та рухи, громадські організації та професійні спілки, неурядові дослідницькі організації та інші суб'єкти, що працюють в інформаційній сфері [4].

У Законі України «Про основи національної безпеки України» визначено основні функції суб'єктів, що забезпечують національну безпеку. Ці функції часто дублюються в положеннях про державні органи, що забезпечують інформаційну безпеку [4]. Це особливо актуально для органів, які входять до функціональної групи оперативного виявлення інформаційних загроз та організації протидії. Основна функція цих ОДВ полягає в моніторингу засобів масової інформації у власних інтересах, проте не передбачено завдання з виявлення загроз та ознак інформаційних небезпек, а також відстеження їх динаміки, спрямованості, характеру та розвитку у загрозу інформаційній безпеці держави.

Інформаційна безпека визначається як стан захищеності життєво важливих інтересів особистості, суспільства та держави, за якого мінімізуються збитки через неповноту, невчасність та недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [164]. Це визначення є оптимальним і відображає всі аспекти взаємодії суб'єктів інформаційних відносин.

Увага до проблем інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі, намагаються зруйнувати національну ідентичність,

міжнаціональну злагоду, порушити конституційний лад та територіальну цілісність держави. Проблема забезпечення інформаційної безпеки України актуалізується під час війни на Сході, коли російська федерація здійснює інформаційну експансію, упереджено висвітлює факти та події, використовуючи технології інформаційно-психологічних операцій для домінування в українському та глобальному інформаційному просторі, утримуючи медійну перевагу.

Російські пропагандистські кампанії та медіазаходи впливають не лише на суспільну свідомість громадян України, але й на світову громадськість. Внаслідок цього національний інформаційний простір України зазнає значних загроз, що створюють небезпеку для функціонування держави, її політичного та економічного розвитку, а також інтеграції до європейських та євроатлантичних структур.

Загрози національній безпеці України в інформаційній сфері – це сукупність умов та чинників, які становлять небезпеку для життєво важливих інтересів держави, суспільства та особи через можливий негативний інформаційний вплив на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [114]. Як зазначено у Законі України «Про основи національної безпеки» однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [164]. У Доктрині інформаційної безпеки України вказані такі загрози: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що шкодить національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ та Інтернет; деструктивні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ та Інтернеті за етнічними, мовними, релігійними та іншими ознаками [153]. Марутян Р.Р. вказує, що найсуттєвішою загрозою національній безпеці України в інформаційній сфері є

негативний інформаційно-психологічний вплив іноземних держав на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси в країні. Такі дії впливають на зовнішню та внутрішню політику держави, знижують її міжнародний імідж та мають політичне й економічне підґрунтя. Метою таких інформаційних операцій є забезпечення національних інтересів інших держав [111].

До загроз національній безпеці України в інформаційній сфері також відносяться: обмеження свободи слова та доступу громадян до інформації; викривлення, спотворення, блокування, замовчування та упереджене висвітлення інформації; несанкціоноване поширення інформації; відкрита дезінформація; інформаційна експансія з боку інших держав та руйнівне вторгнення у національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом отримують можливість розширити свій вплив через ЗМІ на населення менш потужної держави; функціонування у національному інформаційному просторі неконтрольованих інформаційних потоків; поширення ЗМІ культу насильства та жорстокості; повільність інтеграції України у світовий інформаційний простір; невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення дезінформації в Інтернеті.

Враховуючи відсутність єдиного загальноприйнятого підходу до розкриття розуміння понять «інформаційна безпека»; «загрози інформаційній безпеці», а також їх активне поширення у суспільно-державному житті та на міжнародній арені з непередбачуваними переважно негативними наслідками, доцільно детальніше розглянути дану проблематику. Насамперед, потребують розмежування однорідні та споріднені поняття «загроза», «ризик», «небезпека», «виклик» і т.д., а також «інформаційна загроза», інформаційний конфлікт», інформаційна війна», «інформаційне протистояння», «інформаційне

протиборство», «інформаційний тероризм» тощо [58, 251]. Звісно, першочергово слід звернутись до існуючих нормативно-правових актів у даній сфері. І протягом тривалого часу у полі зору законодавців перебували ці питання. Ще Законом України «Про основи національної безпеки України» у ст. 7 (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018) до загроз національним інтересам і національній безпеці в інформаційній сфері було віднесено наступні:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [161]. У даному законі відсутнє трактування загроз інформаційній безпеці, але було визначено поняття «загрози національній безпеці» як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України (ст. 1); З огляду на врегулювання завдань забезпечення свободи слова та інформаційної безпеки, кібербезпеки та кіберзахисту, можна зробити висновок, що це одно порядкові і відмінні категорії, як і відповідні їм загрози. У свою чергу, у Законі України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. Закріплено визначення «загрози національній безпеці України» – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. Вони згідно п. 5. ст. 3, як і відповідні пріоритети державної політики у сферах національної безпеки і оборони, визначаються у Стратегії

національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [165]. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII більше уваги приділяє питаню гагроз у даній сфері. Зокрема, індикатори кіберзагроз визначаються як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози. Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Тут розкриваються поняття кіберінцидентів та кібератак, кіберзлочинів (комп'ютерних злочинів), кібертероризму і-кібершпигунства тощо [165]. У Доктрині інформаційної безпеки України», затвердженій Указом Президента України №47/2017 від 25 лютого 2017 року перелічено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

– здійснення спеціальних інформаційних операцій, що мають на меті підрив обороноздатності, деморалізацію особового складу сил безпеки та оборони, а також провокування екстремістських дій;

– підживлення панічних настроїв, загострення та дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших країнах з метою створення негативного іміджу України на міжнародній арені;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема через розширення власної інформаційної інфраструктури на території України та за її межами;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України у протидії інформаційній агресії та реалізації національних інтересів в інформаційній сфері;

– неефективність державної інформаційної політики, недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, низький рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [153].

Автори Доктрини, виділяючи загрози інформаційній безпеці держави, застосували той самий підхід, що й до визначення національних інтересів в інформаційній сфері, що призвело до повторень, неповноти переліку, термінологічної невизначеності та донесення однієї думки різними формулюваннями. Наприклад, поняття «спеціальні інформаційні операції» використовується кілька разів, хоча в національному законодавстві це поняття не розкривається. Незрозуміло, чому загрозою визнаються саме спеціальні інформаційні операції. Крім того, при характеристиці першої загрози не вказано, від кого вона походить. Можна припустити, що йдеться про російську федерацію, але у доктринальному документі бажано чітко вказувати джерело загрози. Також формулювання загрози «поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій» не уточнює, від кого походить ця загроза. В цілому ж закріплені у Доктрині положення щодо спеціальних інформаційних операції описують одну і ту саму загрозу – перманентну інформаційну війну рф проти України, що здійснюється різними засобами як в українському національному інформаційному просторі так і в глобальному. Що стосується термінологічної невизначеності, то розробники Доктрини інформаційної безпеки України дуже вільно оперують поняттями, зміст яких у законодавчих актах не розкривається. Зокрема використовуються

поняття інформаційної експансії та інформаційного домінування без врахування особливостей їх співвідношення, яке наявне у науковій літературі. Так, інформаційна експансія – це діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою:

- поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

- витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;

- збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;

- нарощування присутності власних ЗМІ в інформаційній сфері об’єкта проникнення і тому подібне [106].

За критеріями масштабності, інтенсивності та характеру засобів, інформаційна експансія займає найнижчий рівень інформаційного протиборства, тоді як до найвищого рівня відносять інформаційну війну. Водночас, як випливає з наведеного визначення інформаційної експансії, саме інформаційне домінування є однією з її цілей, і, відповідно, наслідком такої експансії. Таким чином, інформаційне домінування е складовою інформаційної експансії, тому є невірним виділення інформаційної експансії та інформаційного домінування як окремих загроз. Певні питання викликає і віднесення авторами Доктрини до загроз таких проблем, як недосконалі законодавство та інформаційна інфраструктура, неефективність державної інформаційної політики та недостатній рівень медіа-культури суспільства. Враховуючи те, що мова йде про загрози інформаційній безпеці держави, яка є складовою національної безпеки, то в умовах гібридної війни з рф, особи, які відповідальні за виникнення вказаних загроз, вочевидь, мають нести і кримінальну відповідальність. Однак, на практиці закріплення вказаних загроз у Доктрині інформаційної безпеки України не викликало належної реакції ані з

боку громадянського суспільства, ані з боку державних органів. На наш погляд, недоліки аналізу загроз інформаційної безпеки, що викладені у Доктрині, також зумовлені відсутністю відповідного переліку загроз у профільному законі. На сьогодні, більш детальний перелік загроз в інформаційній сфері, представлений у Стратегії національної безпеки України, яка була введена у дію Указом Президента № 287/2015 від 26.05.2015 р. Відповідно до п. 3.6. Стратегії загрозами інформаційній безпеці є [227]: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Згідно з п. 3.7. Стратегії загрозами кібербезпеці і безпеці інформаційних ресурсів виступають: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Пунктом 3.8. Стратегії визначені загрози безпеці критичної інфраструктури, а саме: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення [227]. Отже, п.п. 3.6., 3.7, та 3.8. Стратегії присвячені загрозам інформаційній безпеці, загрозам кібербезпеці і безпеці інформаційних ресурсів та загрозам безпеці критичної інфраструктури. На наш погляд, поділ загроз на вказані групи не є вдалим, оскільки не враховано структуру механізму забезпечення інформаційної безпеки держави та місце елементів у ньому. Зокрема, загрози інформаційній безпеці є широким поняттям, яке включає загрози кібербезпеки, інформаційної інфраструктури тощо. Водночас складовою інформаційної інфраструктури є критично важлива інформаційна інфраструктура. Разом з тим, аналіз загроз в інформаційній сфері, закріплений у Стратегії, є більш ґрунтовним. На наш погляд, доцільно було б його врахувати при розробці Доктрини інформаційної безпеки України. Адже, враховуючи принцип загального і спеціального нормативного акту, спеціальний, доктринальний документ повинен містити

всебічний та повний аналіз стану інформаційної безпеки, в тому числі і в аспекті існуючих загроз. Таким чином, на підставі вивчення положень Доктрини інформаційної безпеки України, закріплені у ній загрози інформаційної сфери можна класифікувати за джерелом походження на зовнішні та внутрішні.

Зовнішні загрози:

- проведення державою-агресором спеціальних інформаційних операції проти України, як на її території, так і поза її межами;

- інформаційна експансія та інформаційне домінування держави-агресора.

Внутрішні загрози включають:

- недостатню розвиненість національної інформаційної інфраструктури;

- неефективність державної інформаційної політики;

- недосконалість законодавства;

- невизначеність стратегічного наративу;

- недостатній рівень медіа-культури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Представлена класифікація загроз демонструє помилковий аналіз ситуації в сфері інформаційної безпеки, проведений авторами Доктрини інформаційної безпеки України. В умовах гібридної війни неправильно в профільному доктринальному документі акцентувати увагу лише на двох загрозах з боку держави-агресора і шести внутрішніх загрозах, створених органами державної влади та суспільством. Така оцінка ситуації знижує ефективність механізму забезпечення інформаційної безпеки.

Важливо згадати суб’єкти механізму забезпечення інформаційної безпеки: особа, суспільство (його певні групи чи об’єднання) та держава (в цілому, окремі державні органи та органи місцевого самоврядування). У Доктрині інформаційної безпеки України суб’єкти прямо не визначені, але аналіз розділу про механізм реалізації дозволяє виділити такі суб’єкти

забезпечення інформаційної безпеки держави: Рада національної безпеки і оборони України, Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, розвідувальні органи України, Державна служба спеціального зв'язку та захисту інформації України, Національний інститут стратегічних досліджень.

Зокрема, на Міністерство інформаційної політики України покладено завдання з організації та забезпечення моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері [106]. Перелік суб'єктів у Доктрині включає лише державні органи, а суб'єкти на рівні суспільства та особи не згадуються. Це підтверджує думку В.О. Демиденко і Н.В. Камінської про важливість покладання відповідних повноважень і відповідальності на органи публічної влади всіх рівнів, зокрема органи місцевого самоврядування [46, 83]. Чим чіткіше встановлено коло суб'єктів забезпечення інформаційної безпеки, тим краще вони розуміють механізм її забезпечення, що підвищує його ефективність.

Аналіз нормативно-правових актів показує, що на законодавчому рівні відсутнє чітке поняття загроз інформаційній безпеці держави. Тому варто звернутись до доктринальних джерел, енциклопедичних та інших наукових видань. Загрози інформаційним ресурсам розглядаються як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть вплинути на інформаційну систему та інформацію, що в ній зберігається. Виникнення загрози пов'язане з уразливістю системи. Самі загрози є невичерпними за своєю суттю, тому їх не можна повністю описати в жодному дослідженні [138].

Загроза (threat) – це будь-які обставини або події, що можуть призвести до порушення політики безпеки інформації або нанесення збитків

автоматизованій системі. Спробу реалізації загрози називають «атакою». Загроза безпеці інформації (security threat) – це загрози викрадення, зміни або знищення інформації, які можуть бути випадковими або навмисними [80].

Загрози інформаційній безпеці системи управління національною безпекою включають:

- розкриття інформаційних ресурсів;
- порушення їх цілісності;
- збої в роботі обладнання.

Відповідно до загальної класифікації загроз національній безпеці, загрози інформаційній безпеці поділяються за різними критеріями. За джерелами походження:

- природного походження (масове руйнування каналів зв'язку через природні катаклізми);
- техногенного походження (аварії на інженерних мережах або головних серверах системи управління національною безпекою);
- антропогенного походження (помилковий запуск програми, недотримання правил безпеки в Інтернеті).

За характером реалізації:

- реальні (неминуча активізація шляхів дестабілізації);
- потенційні (можливі шляхи дестабілізації за певних умов);
- здійснені (загрози, що вже реалізовані);
- уявні (умовні або схожі з існуючими).

За ступенем гіпотетичної шкоди:

- загроза (дії, що ускладнюють реалізацію національних інтересів у інформаційній сфері);
- небезпека (безпосередня дестабілізація функціонування системи управління національною безпекою).

За ймовірністю реалізації:

- вірогідні (які обов'язково настануть за певних умов);
- неможливі (які ніколи не настануть за певних умов);

- випадкові (які аналізують за допомогою теорії ймовірностей та теорії ігор).

За рівнем детермінізму:

- випадкові (які можуть трапитися або ні);
- закономірні (стійкі загрози, що повторюються) [21, 80, 123].

Цей перелік можна продовжувати, але важливо зазначити, що поняття загрози розглядаються переважно абстрактно або спрощено, що ускладнює розуміння повного контексту поняття «інформаційна безпека». Загрози інформаційній безпеці України розглядаються як фактори, що зумовлюють негативні явища, які посягають на національні інтереси в інформаційній сфері та функціонування національного інформаційного простору. Вони можуть мати широкомасштабні наслідки, пов’язані з ризиками в інших сферах.

У законодавстві України регламентовані загрози національній безпеці в зовнішньополітичній, державній, воєнній, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, цивільній та екологічній сферах, а також у сфері державного кордону України та інформаційній сфері. Вони безпосередньо детермінують посягання на інформаційну безпеку та державний суверенітет України. Загрози інформаційній безпеці виходять за межі географічних кордонів держав, але можуть мати транскордонні або глобальні наслідки [123].

Необхідність подальшого вивчення та розроблення чіткого поняття «загроза» є нагальною для формування ефективної системи моніторингу та управління загрозами і ризиками для інформаційної безпеки держави. З метою попередження та протидії загрозам інформаційній безпеці стратегічне завдання держави полягає у створенні механізму забезпечення інформаційної безпеки, що включає системну діяльність, заходи та державно-правові інституції, які покликані гарантувати реалізацію національних інтересів в інформаційній сфері та попереджувати інформаційні конфлікти. Враховуючи глобалізацію інформаційно-комунікаційних мереж, важливо залучати до співпраці міжнародні організації для протидії інформаційній агресії [100, 244, 251].

1.2 Інформаційно-аналітичні технології у сучасному державному управлінні

Сьогодні світ переживає стрімкий розвиток інформаційних технологій (ІТ), які проникають у всі сфери людської діяльності: соціальну, економічну, політичну, воєнну тощо. Ключовими рисами сучасної інформаційної та комунікаційної революції у військовій справі є [72, 117, 233]:

- глобалізація інформаційних процесів у збройних силах провідних країн світу;
- мініатюризація елементної бази обчислювальної техніки та її легка інтеграція зі зразками озброєння;
- підвищення надійності та мобільності обчислювальних мереж, які стають матеріальною основою для створення різноманітних інформаційних систем воєнного призначення.

Основні стратегічні цілі розвитку інформаційного суспільства в Україні включають [72]:

- прискорення розробки та впровадження новітніх конкурентоспроможних ІТ в усі сфери суспільного життя, зокрема в економіку України і діяльність органів державної влади та місцевого самоврядування;
- розвиток національної інформаційної інфраструктури та її інтеграція зі світовою мережею;
- створення загальнодержавних інформаційних систем у сферах охорони здоров’я, освіти, науки, культури та охорони довкілля;
- покращення стану інформаційної безпеки з використанням сучасних ІТ.

Ці тенденції викликають значні зміни у військовій сфері:

- розробляються нові концепції ведення воєнних конфліктів, особливо концепції «неконтактних бойових дій»;
- удосконалюються форми та методи застосування військ.

Сучасні воєнні конфлікти характеризуються рішучістю у досягненні політичних цілей, спрямованістю на параліч систем державного військового

управління і критичної інфраструктури противника, динамічністю, швидкоплинністю та високою технологічністю застосованих засобів. Також відбувається вдосконалення автоматизованих систем управління військами та зброєю, зокрема перехід до розробки автоматичних систем управління озброєнням. Засоби високоточної зброї, інтегровані в інформаційне середовище «бойового простору», можуть отримувати коригування навіть після запуску. Засоби розвідки розвиваються, включаючи використання космічної та безпілотної розвідки, а також автономних датчиків і сенсорів, здатних діяти на великих відстанях [57].

Сучасна збройна боротьба тепер ведеться не лише у традиційних вимірах «простір-час», але й в «інформаційному вимірі» [233].

Проведений аналіз дозволяє виокремити такі напрями застосування ІТ у сучасній збройній боротьбі:

- використання ІТ у системах управління військами;
- застосування ІТ у системах управління зброєю;
- використання ІТ як зброї;

застосування ІТ для структурно-функціональної трансформації збройних сил та розробки нових концепцій ведення конфліктів і форм застосування військ [72].

Сучасна стратегія досягнення інформаційної переваги над противником, що базується на впровадженні новітніх ІТ у системи управління, стала ключовим фактором, що визначає ефективність державного та військового керівництва. Відтепер надійне функціонування інформаційних систем стало критично важливим для забезпечення стійкості цих органів. Інформаційна перевага виступає як невід'ємний інструмент, що дозволяє командуванню максимально ефективно використовувати розосереджені групи різнорідних сил у вирішальних операціях, підвищувати рівень захисту військових підрозділів, вводити в дію угруповання, склад яких найбільш точно відповідає поставленим задачам, а також здійснювати гнучке і цілеспрямоване матеріально-технічне забезпечення (МТЗ).

Для досягнення та утримання інформаційної переваги необхідно впроваджувати заходи, спрямовані на підрив систем управління, процесів прийняття рішень, а також на руйнування комп'ютерних та інформаційних мереж і систем противника. Отже, новітні ІТ перетворюються на фундаментальний елемент сучасного збройного протистояння. Завдяки їхньому впровадженню значно розширюється кількість можливих сценаріїв для розв'язання і ведення збройних конфліктів, зокрема з використанням детального планування і прогнозування їх наслідків у всіх сферах – політичній, економічній, військовій та інших.

Використання ІТ створює можливості для розробки нових систем і форм збройної боротьби, які володіють принципово новими властивостями. Іншими словами, ІТ дозволяють не лише якісніше збирати, аналізувати, обробляти та інтерпретувати дані, а й завдяки їх системоутворюючій ролі, відкривають нові перспективи для розробки та вдосконалення як теоретичних, так і експериментальних методів наукових досліджень у сфері автоматизації військового управління, створення перспективних зразків озброєння та військової техніки (ОВТ), а також удосконалення існуючих.

Для глибшого розуміння цього системоутворюючого процесу, що сприяє створенню нової якості, майбутнім науковцям необхідно детальніше досліджувати зміст поняття «система» з діалектичних позицій та ознайомитися з основними положеннями теорії складних систем. Це дозволить повніше використовувати потенціал ІТ для підвищення ефективності ОВТ, систем управління військами та зброєю як складних систем військового призначення. Окрім того, з'являються нові можливості для відкриття якісно нового етапу розвитку військового мистецтва – переходу від управління військами в ході збройного конфлікту до управління конфліктом у цілому [72, 295].

На думку багатьох військових експертів, інформаційно-аналітичне забезпечення (ІАЗ) є не менш важливою складовою підтримки сил безпеки та оборони, ніж такі традиційні види забезпечення, як матеріально-технічне, бойове, медичне та інші. ІАЗ розглядається як невід'ємний елемент сучасних

військових операцій, що забезпечує ефективне управління та прийняття рішень на всіх рівнях.

Зародження ІАЗ тісно пов’язане з розвитком обчислювальної техніки, яка здійснила значний вплив на формування та вдосконалення цієї системи. Розвиток комп’ютерних технологій кардинально змінив підходи до обробки інформації, що дозволило значно підвищити якість аналітичної роботи, яка раніше виконувалася вручну в штабах. Зараз важливо розглянути ІАЗ у контексті загальної системи військового управління, яка еволюціонувала разом із технологічним прогресом.

Хронологічний розвиток теорії управління організаційними системами відображено на рисунку 1.1. Інформаційно-аналітична система забезпечення процесів управління (ІАСПУ) є основною складовою автоматизованих систем управління (АСУ). Вона включає дві ключові підсистеми: підсистему інформаційного забезпечення та підсистему підтримки прийняття рішень. Залежно від типу інформації, яка обробляється в ІАСПУ, в системі підтримки прийняття рішень використовуються відповідні алгоритми обробки даних.

Перша категорія інформації охоплює ті дані, які описують ймовірнісні події, параметри та показники яких можуть бути описані за допомогою відомих законів розподілу випадкових величин. Друга категорія включає інформацію, що має нестохастичний характер, тобто коли параметри подій і показники не підлягають стандартним законам і описуються за допомогою методів теорії нечітких множин. Третя категорія інформації є детермінованою і обробляється за допомогою звичайних математичних методів, що застосовуються у дослідженні операцій.

Таким чином, ІАЗ відіграє ключову роль у сучасних системах військового управління, забезпечуючи не тільки ефективну обробку інформації, але й підтримуючи процеси прийняття рішень на стратегічному рівні. Урахування специфіки оброблюваної інформації дозволяє значно підвищити точність і надійність військового планування та управління, що, в кінцевому підсумку, підвищує ефективність усієї військової операції [233, 295].

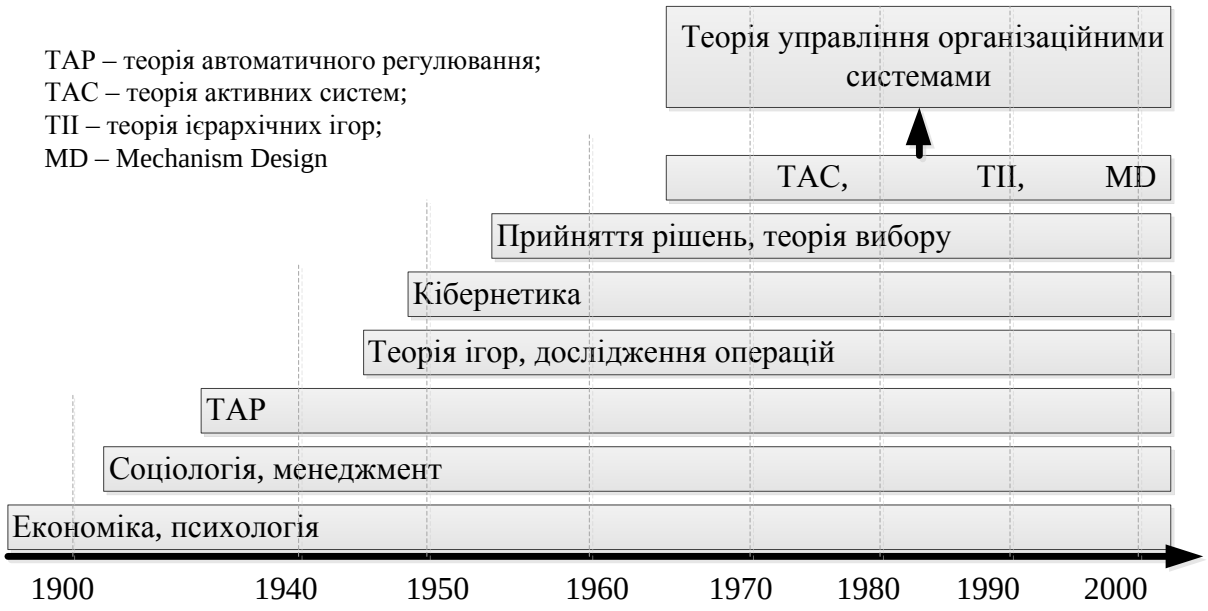

Рисунок 1.1 – Основи виникнення теорії управління [233]

Однією з найважливіших складових, що визначають ефективність та можливості системи управління, є її ресурси. Ці ресурси складаються з елементів ієрархічного пошуку та розподілу інформації, що включає в себе всі джерела, з яких система отримує інформацію. Окрім цього, на потенціал системи управління суттєво впливають ресурси, які забезпечують активний вплив на противника під час виконання рішень. До таких ресурсів відносяться інформаційні потоки, що відображають можливості сил безпеки.

Ці інформаційні ресурси стають невід'ємною частиною системи управління тоді, коли вони розгортаються і інтегруються в загальну структуру управління. Така система управління, оснащена відповідною інформаційно-аналітичною підсистемою, виявляє високу адаптивність до типу вхідної інформації, до стану поточної обстановки та бойових сил, що постійно відстежується. Це дозволяє системі приймати оперативні рішення в ритмі роботи штабів, що є головною метою такої системи управління [233, 295].

Світова практика доводить, що інформаційне навантаження на органи управління неухильно зростає. Наприклад, компанія EMC-Corporation оприлюднила результати досліджень, що демонструють вибухове збільшення

обсягу інформації, яка створюється і використовується у світовому співтоваристві. За їхніми даними, у 2006 році було створено та скопійовано 161 екзабайт цифрової інформації, що є приблизно в 3 мільйони разів більшим обсягом, ніж міститься у всіх написаних людством книгах. Це лише початок безпрецедентного зростання обсягу інформації: згідно з даними IDC (International Data Corporation), до 2010 року цей обсяг зріс більш ніж у шість разів і досяг 988 екзабайт, при цьому щорічний приріст становив 57% [190].

У зв'язку з цим спостерігається й значне збільшення інформаційного навантаження на органи військового управління. Через декілька років, без сучасних інформаційно-аналітичних систем забезпечення, процес прийняття рішень може стати проблематичним для керівництва. Це призводить до першого суттєвого протиріччя в системах управління – протиріччя між об'єктивним зростанням обсягів інформації та неможливістю органів управління своєчасно обробляти надану інформацію для прийняття оптимальних рішень.

Сьогодні головним завданням для науковців та військово-промислового комплексу кожної країни є пошук шляхів автоматизації творчих процесів у діяльності військових органів управління, особливо у контексті прийняття рішень у реальному часі під час оперативного управління службово-бойовими діями.

Це, в свою чергу, породжує друге протиріччя в системі військового управління – між зростаючою роллю організаційних задач і функцій органів управління та недостатнім розвитком наукових методів, що забезпечують підготовку та прийняття рішень в умовах невизначеності.

З цієї причини виникає нагальна потреба у розвитку теоретичних основ прийняття рішень для військових органів управління. Це дозволить науковцям у галузі військової кібернетики розробляти системні алгоритми, що охоплюють процеси управління та прийняття рішень.

Поняття інформаційно-аналітичного забезпечення є однією з категорій теорії управління, і до функцій інформаційно-аналітичної системи забезпечення

процесів управління (ІАСПУ) необхідно включати забезпечення процесів управління зброєю на тактичному рівні. Однією з найважливіших задач ІАСПУ є підтримка процесів підготовки та прийняття рішень органами управління сил безпеки України, що є критично важливим для ефективного функціонування системи національної безпеки [233, 295].

Варто зазначити, що технологія підготовки та прийняття рішень у військовій сфері протягом багатьох десятиліть, починаючи з часів Другої світової війни, практично не зазнавала суттєвих змін. Це має серйозні наслідки для якості управління бойовими діями в режимі реального часу, всебічного забезпечення цих процесів, а також для ефективності повсякденної діяльності військових організацій. На тлі швидкого впровадження нових технологій в інших сферах державного управління, застарілі методи підготовки та прийняття рішень у складних умовах негативно позначаються на узгодженості співпраці військових структур із органами державного управління, які вже застосовують сучасні технології та пред’являють нові вимоги до рішень, що приймаються в оборонній галузі [233, 295].

Виникає і третє протиріччя, яке полягає у необхідності застосування новітніх методів прийняття рішень, спрямованих на зниження впливу невизначеності на їх ефективність, при водночас існуючому дефіциті відповідних технологій для обґрунтування та формулювання пропозицій до цих рішень.

Завдяки формалізації процесів врахування нечітко визначених факторів, що впливають на зміст планів і задумів, недостатня достовірність взаємно незалежних альтернатив може бути компенсована їх кількісною перевагою. Це дозволяє вважати, що підсумкова достовірність отриманого результату буде вищою, ніж достовірність кожної окремо взятої альтернативи. Цей підхід підкріплюється також врахуванням фізичної суті самих факторів, які впливають на рішення.

Якщо під час прийняття рішень розглядати невизначеність обстановки як брак або недостатність необхідної інформації, то з використанням теорії

інформації можна визначити рівень цієї невизначеності через функцію належності нечітких множин. Це дозволяє розрахувати інформаційну ентропію і встановити шуканий поріг достовірності, який вважається достатнім для прийняття рішення. Такий підхід сприяє підвищенню ефективності рішень у ході бойових операцій [233, 295].

Окрім технологій підготовки та прийняття рішень, на якість управління військовими силами у сучасних умовах значний вплив мають структура інформаційно-аналітичної системи, її інтегрованість, а також якість забезпечення процесів управління силами безпеки. Важливу роль відіграють змістовність і повнота аналізованих даних. Оскільки основою процесів управління є рішення, що приймаються органами управління, інформаційно-аналітична система повинна насамперед забезпечувати ефективну підготовку та ухвалення цих рішень. Якість прийнятих рішень визначатиме не тільки ефективність самої системи управління, але й результати інших процесів службово-бойової діяльності, від яких залежить загальний успіх військових операцій та забезпечення безпеки.

До основних проблемних аспектів інформаційно-аналітичного забезпечення органів управління силами безпеки на сучасному етапі розвитку належать такі питання [124]: недостатня розробка нормативно-правової бази у силових структурах України, що стосується створення інформаційних ресурсів та продуктів, надання інформаційних послуг, а також функціонування системи інформаційно-аналітичного забезпечення органів управління в цілому; відсутність інтегрованої системи інформаційно-аналітичних підрозділів сил безпеки, які б були функціонально, технологічно та технічно взаємопов’язані між собою; брак єдиної системи класифікації та кодування інформації в силових структурах України; низький рівень розвитку загальних інформаційних ресурсів у силових структурах та відсутність інтегрованого банку даних, що міг би стати важливим елементом загальнодержавної інформаційної структури.

Особливо важливою є потреба у використанні сертифікованого системного програмно-математичного забезпечення, що вже довело свою

ефективність у практичній діяльності. До цього додається проблема відсутності сертифікованих засобів захисту інформації, що створює ризики для безпеки даних. Також відсутній чітко визначений комплекс спеціального програмно-математичного забезпечення для інформаційної діяльності. Наявність цієї проблеми вимагає термінової підготовки фахівців, здатних працювати з сучасними інформаційно-аналітичними системами.

Недостатнє фінансування залишається однією з ключових перешкод на шляху до вирішення зазначених проблем. Важливо також зауважити, що бракує комплексного підходу в організації досліджень, спрямованих на вирішення проблеми створення ефективної системи інформаційного забезпечення сил безпеки України. На сьогоднішній день недостатньо проводяться дослідження у таких важливих напрямках, як удосконалення нормативно-правової бази, розвиток системи інформаційно-аналітичних підрозділів, створення комплексної системи захисту інформації, а також розробка системних вимог щодо сертифікації засобів інформатизації та інформаційно-телекомунікаційних систем в структурах сил безпеки України [294, 295].

Таким чином, вирішення цих проблем потребує не лише значних ресурсів, але й стратегічного підходу до впровадження інноваційних технологій та управлінських рішень. Лише таким чином можна створити ефективну систему інформаційно-аналітичного забезпечення, яка відповідатиме сучасним викликам і забезпечить надійну підтримку органів управління силами безпеки України.

Імітаційні моделі та симуляції військових або бойових дій використовуються для аналізу та моделювання різних аспектів військових операцій. Ці інструменти дозволяють проводити віртуальні тренування, вивчення стратегій, оцінку та аналіз варіантів, а також вдосконалення тактичних та стратегічних рішень. Ось кілька типових імітаційних моделей і симуляцій в цьому контексті [212]:

JTLS (Joint Theater Level Simulation) є прикладом великомасштабної симуляційної системи для аналізу та тренувань на рівні театру військових дій.

VBS3 (Virtual Battlespace 3) є симулятором, розробленим для моделювання різних аспектів бойових дій та військових операцій. Використовується для тренувань, аналізу та вивчення тактичних рішень.

CMANO (Command: Modern Air/Naval Operations) це симуляційна гра, спрямована на моделювання сучасних повітряно-морських операцій. Вона дозволяє аналізувати тактичні сценарії та стратегії.

SIMDIS (Simulation Display System) – використовується для візуалізації імітаційних даних і може використовуватися для аналізу руху військових одиниць, моделювання атмосферних та теренопереshкодових умов тощо.

ACE (Advanced Computerized Environment) це платформа для створення імітаційних моделей та симуляцій військових операцій. Забезпечує можливості для тренувань та досліджень.

DI-Guy використовується для моделювання вигляду та руху військових персоналу в різних сценаріях.

Ці інструменти допомагають військовим фахівцям аналізувати різні сценарії, вдосконалювати стратегії, тренувати військовий персонал та вивчати вплив різних факторів на результати військових операцій. Окрім того, вони можуть використовуватися для вивчення нових технологій та тактик у військовій сфері.

Прийняття стратегічних і тактичних військових рішень вимагає ретельного планування, аналізу та ефективного управління ресурсами. Існують різні підходи до цього процесу, і вони можуть відрізнятися в залежності від конкретної ситуації, методології та області військових операцій. Ось деякі загальні підходи до прийняття стратегічних і тактичних військових рішень:

Прийняття стратегічних рішень:

- використання системного підходу для розгляду всієї картини військових операцій, враховуючи різні взаємозв'язки та вплив різних чинників;

- оцінка внутрішніх сил та слабкостей власних військ та сил супротивника для розробки стратегій, які максимально використовують переваги та компенсують недоліки;

- врахування геополітичних факторів, таких як географічне положення, ресурси та геостратегічне значення регіонів;

- оцінка потенційних загроз та можливостей, що випливають з зовнішнього середовища, для формулювання стратегій безпеки та оборони.

Прийняття тактичних рішень:

- SWOT-аналіз (Strengths, Weaknesses, Opportunities, Threats) використання SWOT-аналізу для визначення стратегічних переваг, недоліків та можливостей, а також для виявлення потенційних загроз;

- розробка різних курсів дій, враховуючи різні можливі варіанти розвитку подій та визначення найбільш оптимального;

- здатність швидко адаптуватися до змін у військовому середовищі та реагувати на непередбачені обставини;

- лідерство та спільна робота в команді для ефективної координації дій на полі бою;

- використання сучасних технологій для підвищення ефективності та забезпечення переваги в противоборстві.

Прийняття військових рішень вимагає багатофакторного підходу та глибокого розуміння власних можливостей, стратегічних цілей та тактичних обставин. Кожен етап військових операцій вимагає уважного аналізу та розробки ефективних стратегій для досягнення поставлених цілей.

MDMP – це скорочення від «Military Decision-Making Process» (процес військового прийняття рішень). Це стандартний підхід до прийняття стратегічних і тактичних військових рішень, який використовується в арміях численних країн. Основна мета MDMP – це систематизація та стандартизація процесу військового планування та прийняття рішень. Він враховує численні аспекти, щоб забезпечити ефективність та успішність виконання військових операцій.

Основні етапи MDMP включають:

Оцінка ситуації (Mission Analysis) – це перший етап, на якому командир аналізує завдання (місію), збирає інформацію про ситуацію та робить оцінку

вихідних умов;

Розробка курсів дій (Course of Action Development). На цьому етапі генеруються можливі курси дій для виконання місії. Кожен курс дій ретельно розробляється та оцінюється з урахуванням різних факторів, таких як ворожі сили, рельєф, час і ресурси.

Оцінка курсів дій (Course of Action Analysis). Командир та його штаб проводять оцінку кожного курсу дій, порівнюючи їх за різними критеріями, такими як ефективність, ризики та вартість.

Вибір курсу дій (Course of Action Selection). Командир обирає найбільш оптимальний курс дій, з урахуванням оцінок та аналізу, проведеного на попередніх етапах.

Розробка розпорядження (Orders Production). На цьому етапі генерується розпорядження, яке включає в себе всі необхідні деталі для реалізації обраного курсу дій, включаючи завдання для підрозділів, визначення ресурсів та комунікацій.

Виконання (Execution). В цьому етапі розпочинається виконання розпорядження, а командир спостерігає за розвитком ситуації, вносячи необхідні зміни у виконання завдань.

MDMP визначається структурою, дисципліною та орієнтацією на прийняття рішень у військовому контексті. Його основна мета – забезпечити штабам та командирам ефективні інструменти для планування та керування військовими операціями.

JTLS (Joint Theater Level Simulation) – це великомасштабна військова комп’ютерна симуляційна система, яка використовується для навчання та тренувань зі спільних операцій на театральному рівні. Ця система призначена для моделювання та аналізу військових операцій в реальному часі на великих територіях з врахуванням різноманітних аспектів, таких як логістика, комунікації, вогнева підтримка, розвідка, інженерія та інші.

Основні характеристики та функції JTLS можуть включати:

Моделювання різних аспектів бойових дій. Врахування різних складових

сучасного бойового середовища, включаючи сухопутні, повітряні та морські сили.

Моделювання логістичних аспектів, таких як постачання, транспорт, обслуговування, амуніція тощо.

Урахування можливостей вогневої підтримки, артилерії, авіації та інших вогневих систем.

Моделювання систем зв’язку та командно-керівницької структури в реальному часі.

Врахування дій розвідувальних засобів та збору інформації.

Надання військового персоналу можливості використовувати систему для тренування та підготовки до реальних ситуацій.

Здатність моделювати різні типи конфліктів, включаючи симетричні та асиметричні загрози.

JTLS дозволяє військовим командам та аналітикам виконувати аналіз та планування в реальному часі, вдосконалюючи їх рішення та стратегії в умовах віртуального військового середовища.

Розвиток військової справи в більшості, базується на аналізі досвіду минулих війн та збройних конфліктів, однак у сучасних умовах все більше розповсюдження набувають обчислювальні експерименти з використанням різного роду та масштабу математичних моделей та моделюючих комплексів, за допомогою яких можна спрогнозувати характер, форми та види збройних конфліктів, апробувати нове озброєння, нові технології організації і ведення військових дій.

На сьогодні існують різні тенденції застосування математичного опису збройного протистояння, зокрема математичний опис заснований на порівнянні бойових потенціалів, логіко-аналітичні методи, що характеризуються представленням реальних процесів і систем у вигляді явних функціональних залежностей (сценаріїв, етапів вирішальних правил), імітаційні, де описується апарат прийняття більш частих рішень з елементом ймовірності (ціль вражена/не уражена, виявлена/не виявлена та інш.). В свою чергу, для процесів

і систем, що мають складний характер поведінки, якими є процеси збройної боротьби, при відсутності можливості математичної формалізації, яка забезпечує аналітичне рішення задачі, єдиними підходом до дослідження є використання методів імітаційного моделювання.

При проектуванні моделей збройного протистояння, підготовки системотехнічних та програмних рішень в першу чергу беруться до уваги цільова настанова моделювання, її функціональне призначення та місце моделі у системі прийняття рішення. При цьому, треба розуміти, що модель є лише інструментом діяльності посадових осіб штабу та командирів та не може забезпечувати відпрацювання єдиного вірного та всебічно обґрунтованого рішення за умови конкретної обстановки. Модель є допоміжним інструментом підтримки процесу прийняття рішення та оцінки можливих альтернатив. Це пов’язано із тим, що її математичний апарат і алгоритми охоплюють собою множину складних процесів, факторів і умов, які безпосередньо впливають результати моделювання. Частина з них задається кількісно, наприклад бойовий та чисельний склад конфліктуючих угрупувань, види та характеристики озброєння та військової техніки, ресурси, що виділяються фізико-географічні та метеорологічні умови та інші.

Інша частина вихідних даних за об’єктивними причинами неможливо представити у кількісному вимірюванні у наслідок того, що вони відносяться до когнітивної сфери людини. Саме тому, сьогодні при моделюванні бойових дій враховуються тільки формальні дані.

Врахування двостороннього характеру збройного протистояння є найбільш важливою методологічною особливістю моделювання. В цьому випадку мова йде про складні процеси протистояння двох антагоністичних систем, які вступають між собою не тільки в бойовий, але й в інтелектуальний конфлікт, що передбачається задумами дій сторін. Виходячи з цього, сьогодні збройне протистояння (операція, бій) розглядаються не тільки як збройне протиборство двох антагоністичних систем, але і як систем, що одночасно реалізують увесь свій інформаційний, морально-бойовий, психологічний та

морально-технічний потенціал, який враховується у двох рішеннях конфліктуючих сторін. Тобто інтелектуальному протиборству двох супротивників, які реалізують свої рішень крізь призму дії підлеглих військ.

Таким чином, цей підхід дозволяє створити біполярну модель, яка має у своєму складі два конкуруючих центра управління, що представляються відповідними моделями на декількох рівнях (рисунок 1.2) . Як можна побачити, тут на перший план виходить не матеріальна складова війни, а прийняте рішення командиром та поставлені задачі військам [11].

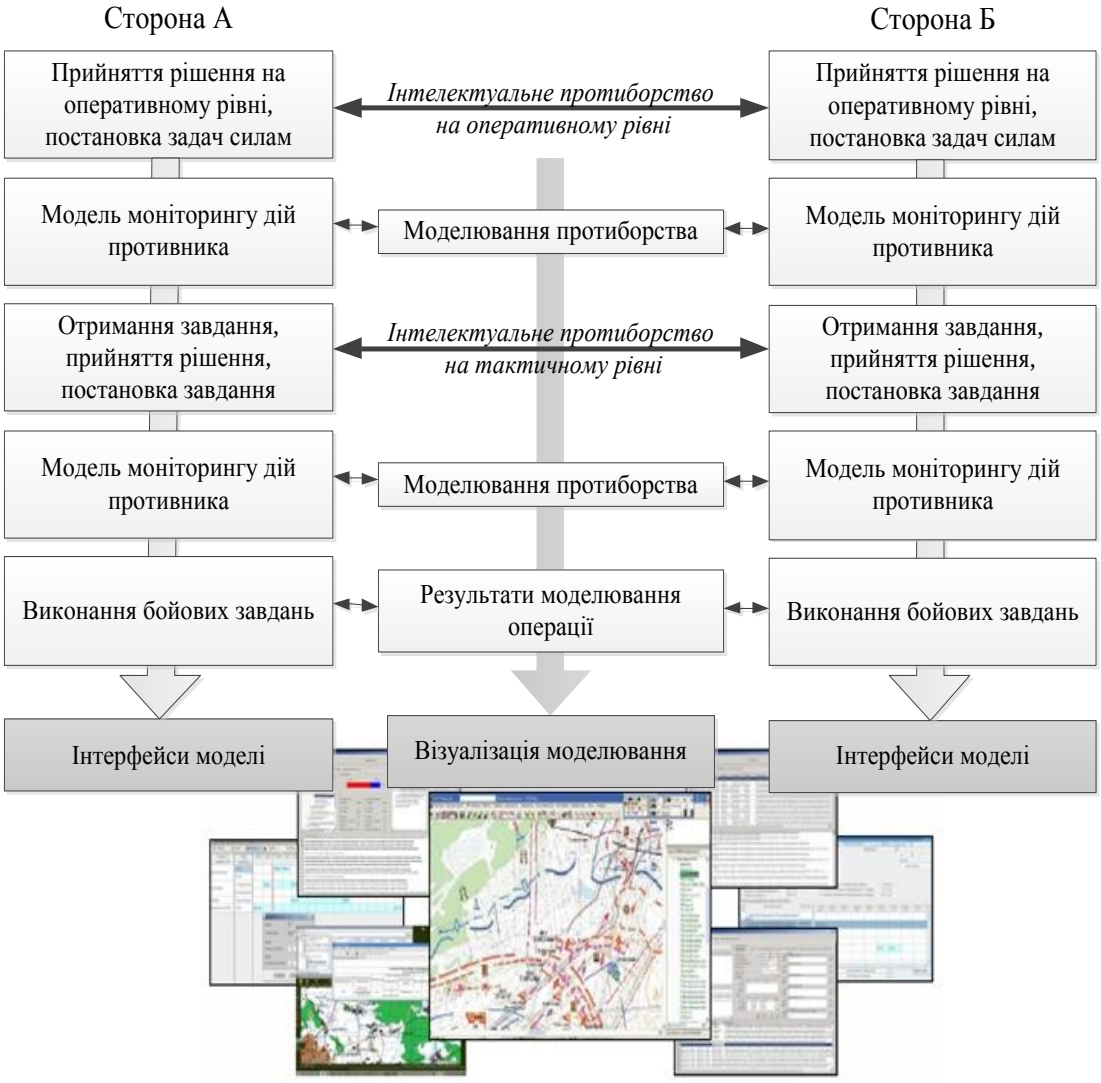

Рисунок 1.2 – Структура моделі службово-бойових дій з врахуванням інтелектуального протиборства сторін

У цьому підході необхідно враховувати те, що підсумки бойових дій необхідно розглядати крізь призму досягнення цілі та виконання поставлених бойових завдань своїми військами, незважаючи на те, що у даній структурі відтворена симетрія дій сторін, а противник розглядається як зовнішнє джерело випадкових та невигідних дій, що примушують до пошуку нових рішень, у відповідності до швидкоплинної обстановки.

В даній структурі бойові дії моделюються на трьох рівнях управління.

Перший рівень, забезпечує моделювання в інтересах прийняття рішення командуючим оперативного об'єднання (HICON).

Другий, охоплює процеси прийняття рішення і постановку завдань у тактичної ланці управління (РТА).

Третій рівень – це рівень виконавців поставлених завдань, тобто безпосередньо підпорядкованих підрозділів (LOWCON), де моделюється практична реалізація рішень двох вищих рівнів. За своєю суттю третій рівень представляє собою сукупність окремих моделей бойових дій різних видів і родів військ та є «фізичним» середовищем моделі, де відтворюється не просто збройний конфлікт, а сукупність усіх протиборств у всіх сферах їх прояву.

Для забезпечення гнучкості моделі, врахування проміжних результатів оперативно-тактичних розрахунків та вплив умов розвитку бойової обстановки передбачається втручання людини в процес моделювання за допомогою специфічних процедур. Завдяки цьому можливо враховувати нові данні, що виникають з розвитком обстановки, отримувати проміжні та кінцеві показники, змінювати умови моделювання, уточняти та оцінювати вплив різних факторів на попередній план. За цих умов процес моделювання програмується дискретно, по етапам та покроковою фіксацією стану та положення сили і засобів сторін. На кожному з етапів забезпечується можливість уточнення даних та отримання різних варіантів дій.

Необхідно відмітити, що на сьогодні практично всі існуючі моделі:

- не враховують зміни у сутності та змісті сучасного збройного протиборства;

- не «відчувають» усю різноманітність форм і способів оперативного і службово-бойового застосування військ;
- не враховують неформальні вихідні дані, якими є військове мистецтво командирів, їх тактична «грамотність», бойовий дух та морально-психологічна підготовка особового складу;
- не відповідають на питання, що зробити, щоб отримати бажаний результат.

Застосування сучасних моделей для складання найбільш раціонального плану потребує розгляду великої кількості альтернатив та підходить тільки для етапу завчасної підготовки до бойових дій.

Розробка моделей збройного протистояння передбачає реалізацію принципу послідовного просування по етапам побудови моделі. Цей принцип дозволяє системно забезпечити найбільш раціональний і цілісний порядок розробки моделі. Для цього процес її побудови розбивається на низку відокремлених етапів, які дозволяють з використанням принципу цілісності проводити корекцію кожного з них.

При розробці математичних моделей необхідно визначитися із системою основних принципів, що дозволяють досягнути необхідної якості комплексу, що розробляється [233].

1. Принцип декомпозиції системи, що моделюється, який передбачає визначення підсистем, які в свою чергу можуть поділятися на елементи. Такий підхід дозволить створити математичну модель бойових дій, спираючись на моделюючі алгоритми окремих об’єктів та алгоритми їх функціональної взаємодії.
2. Принцип раціонального компромісу між рівнем деталізації моделей та складністю комплексу, який пов’язаний із аналізом можливих спрощень як похідних алгоритмів функціонування окремих елементів, так і алгоритмів їх взаємодії. Критерієм такого компромісу є досягнення мети моделювання, при цьому повинна бути передбачена можливість введення додаткових спрощень або навпаки, можливість деталізації опису деяких підсистем та їх елементів.

3. Побудова комплексу у вигляді ієрархічної агрегативної системи, де процеси перетворення вхідної інформації здійснюються із врахуванням поточного стану кожного агрегату. Формування сигналів здійснюється у відповідності із заданим алгоритмом який враховує особливості функціонування кожного агрегату та існуючі зв'язки.

Підхід до реалізації вказаних принципів та відповідний аналіз даних в імітаційній системі моделювання бойових дій розглянемо на прикладі ієрархічної системи управління ланки відділення – рота сухопутних військ.

Для цього потрібно ввести поняття типового бойового об'єкту, під яким розуміється неподільну вогневу одиницю, яка здатна виконувати чотири основні задачі: рух (маневр на основі цифрової карти місцевості), спостереження (розвідка), стрільба (ураження цілі) та прийняття рішення по виконанню вищевказаних дій за різних умов обстановки.

За цих умов математична модель типового об'єкта типового бойового об'єкту повинна реалізовувати чотири основні функції: прийняття рішень (управління бойовим об'єктом), маневрування, розвідка, ураження.

В цьому випадку структура моделі типового об'єкту має вигляд у відповідності до рисунку 1.3.

Рисунок 1.3 – Структура моделі типового об'єкту управління

Модель управління повинна забезпечувати реалізацію функцій командира по управлінню підрозділом, а саме функцій прийняття рішення на усіх

виділених підетапах: маневрування, розвідки, ураження, а також функцій коректування прийнятого рішення.

Процес маневрування є переміщення об’єктів у напрямках, що визначені завданням від командира та швидкостями, що відповідають характеру місцевості, часу доби, а також характеру дій за умов завдання, що вирішується. При цьому на основі цифрової карти місцевості на кожен з моментів модельного часу потрібно оцінювати місцеположення (розраховувати поточні координати) об’єкта, що моделюється та параметри його руху.

Моделювання процесу розвідки полягає в отриманні низки оцінок, які характеризують можливість виявлення об’єктів супротивника за умов обстановки, що склалася. На основі цих оцінок приймається рішення про виявлення та розпізнавання об’єкту (цілі для ураження).

Модель досягнення мети операції включає:

- визначення ймовірності влучення у ціль обраним озброєнням та визначення ймовірності ураження, виходячи з характеристик засобу ураження, властивостей цілі та умов обстановки, що склалася;

- визначення збитку, що наноситься об’єктам противника при застосуванні по ньому зазначених засобів ураження.

Основною частиною моделі типового бойового об’єкту є підмодель управління цим об’єктом, яка повинна забезпечити не тільки прийняття рішення про поведінку підрозділу в залежності від параметрів маневрування, розвідки та ураження цілі але й «пояснити», чому в даній системі обрано саме це рішення, показати його раціональність серед усіх можливих.

Математичні моделі системи імітаційного моделювання JCATS.

Моделі бойових дій агрегованих військ широко використовуються у оборонних відомствах провідних країн світу для моделювання військових операцій в ході підготовки військ та у дослідницьких цілях для підвищення обґрунтованості планів та програм створення, розвитку та застосування збройних сил та підтримки прийняття рішень.

Теоретичною основою таких моделей є системи детермінованих диференціальних рівнянь. Такими загальновідомими диференціальними рівняннями є так звані ланчестеровськи моделі.

Імітаційна система JCATS з точки зору використання математичного апарату для формалізованого опису процесів ведення збройної боротьби представляє собою ієрархічну модель [265, 298], яка складається з двох рівнів:

1 рівень – деталізований опис взаємодії на рівні окремих об’єктів з використанням методу статистичних випробувань (Монте-Карло).

При цьому враховуються: склад та тактико-технічні характеристики озброєння, засобів спостереження, тип боєприпасів та їх здатність до ураження, габарити об’єкту, діапазон можливих швидкостей руху об’єктів; вплив на процеси руху об’єктів, виявлення і ураження цілей характеристик місцевості, погодних умов, пори року,часу доби, а також впливу інших факторів (дим, шум, швидкість течії рік, глибина водних перешкод та характер дна, поповнення запасів, відновлення сил і засобів, втома особового складу, рівень його підготовки, застосування зброї масового ураження, вплив наслідків стрільби, стихійного лиха та інше)

2 рівень – опис взаємодії на рівні організаційних одиниць (Unit Level), які визначаються як агрегативні системи, з використанням диференційних рівнянь Ланчестера. Агрегативні системи створюються від ланки відділення та вище.

Таким чином, в системі JCATS використовується ієрархічний підхід, де на нижньому рівні методом Монте-Карло імітується взаємодія окремих бойових одиниць, на середньому рівні взаємодія описується марковськими моделями, а на верхньому (агрегованому, детермінованому) рівні використовуються відповідно диференціальні рівняння Ланчестера. Над цими моделями, вводячи до них управляючі параметри, можна добудовувати задачі управління в термінах керованих динамічних систем, диференціальних ігор або ігор, що повторюються.

Інформація про внутрішні деталі та математичні аспекти таких систем часто є об’єктом класифікації та не розголошується з міркувань безпеки.

Однак імітаційне моделювання, включаючи JCATS, зазвичай використовує різноманітні математичні моделі для опису руху, взаємодії та прийняття рішень у військових сценаріях. Деякі загальні аспекти, які можуть включати математичні моделі, визначені нижче [213]:

Кінематика та динаміка: Математичні моделі, які описують рух і взаємодію об’єктів в просторі, такі як транспортні засоби, військові одиниці тощо.

Озброєння та вогнева підтримка: Моделі для визначення результативності та впливу різних видів озброєння, а також алгоритми для моделювання вогневої підтримки.

Логістика та забезпечення: Математичні моделі для опису логістичних операцій, таких як постачання, транспортування, обслуговування тощо.

Розвідка та визначення позицій: Моделі для розвідувальних операцій та визначення позицій ворожих та власних сил.

Алгоритми прийняття рішень: Математичні моделі для алгоритмів, які визначають дії та реакції сил у різних сценаріях.

Комунікації та керівництво: Моделі для опису систем зв’язку та керівництва в реальному часі.

Ці математичні моделі і алгоритми дозволяють системі імітаційного моделювання створювати віртуальне військове середовище, в якому можна вивчати та тренувати різні військові сценарії.

Інформаційні технології (ІТ) включають широкий спектр технологій та систем, які використовуються для створення, зберігання, обміну та обробки інформації. Розглянемо деякі з ключових властивостей, які характеризують інформаційні технології:

- швидкість обробки інформації. Сучасні ІТ-системи можуть обробляти величезні обсяги даних за дуже короткий час, що значно підвищує продуктивність та ефективність робочих процесів;

- зберігання та доступ до даних. Інформаційні технології дозволяють зберігати великі обсяги даних у компактному, легко доступному форматі. Це спрощує управління інформацією і підвищує її доступність;

- комунікація. ІТ значно поліпшили здатність до комунікації, дозволяючи миттєвий обмін інформацією через електронну пошту, інтернет, соціальні медіа та інші цифрові платформи;

- автоматизація за допомогою ІТ дозволяє зменшити кількість рутинної ручної роботи, звільняючи співробітників для вирішення більш складних завдань та підвищуючи загальну продуктивність;

- масштабованість. ІТ-системи легко масштабуються, що дозволяє організаціям збільшувати або зменшувати їхні ресурси залежно від потреб без необхідності значних змін у інфраструктурі;

- сучасні ІТ-системи включають складні заходи безпеки, щоб захистити дані від несанкціонованого доступу, зловмисного втручання та інших загроз;

- ІТ дозволяють інтегрувати різні системи і програми, поліпшуючи взаємодію між різними відділами та оптимізуючи робочі процеси;

- підтримка прийняття рішень. ІТ надають потужні інструменти для аналізу даних, які можуть допомогти керівникам у прийнятті обґрунтованих управлінських рішень, заснованих на детальному аналізі доступної інформації.

На рисунку 1.4 наведена класифікація інформаційних технологій.

Мережі інформаційно-аналітичного забезпечення органів управління сил безпеки можуть бути визначені як складні організаційно-технічні системи. Це обумовлено їхньою структурою, яка інтегрує декілька комп’ютерних мереж різних підрозділів і відділів у єдину інформаційно-телекомунікаційну мережу. На сучасному етапі така мережа представляє собою високоскладну програмно-технічну конструкцію, яка має наступні характеристики:

- ієрархічність структури та взаємодій між підсистемами та елементами;
- складність взаємозв’язків усередині системи;
- наявність об’єднаної цільової функції, що пронизує різні рівні ієрархії;

- емерджентність, яка дозволяє системі демонструвати нову функціональність або рівень продуктивності, який перевищує сукупні можливості її окремих компонентів.

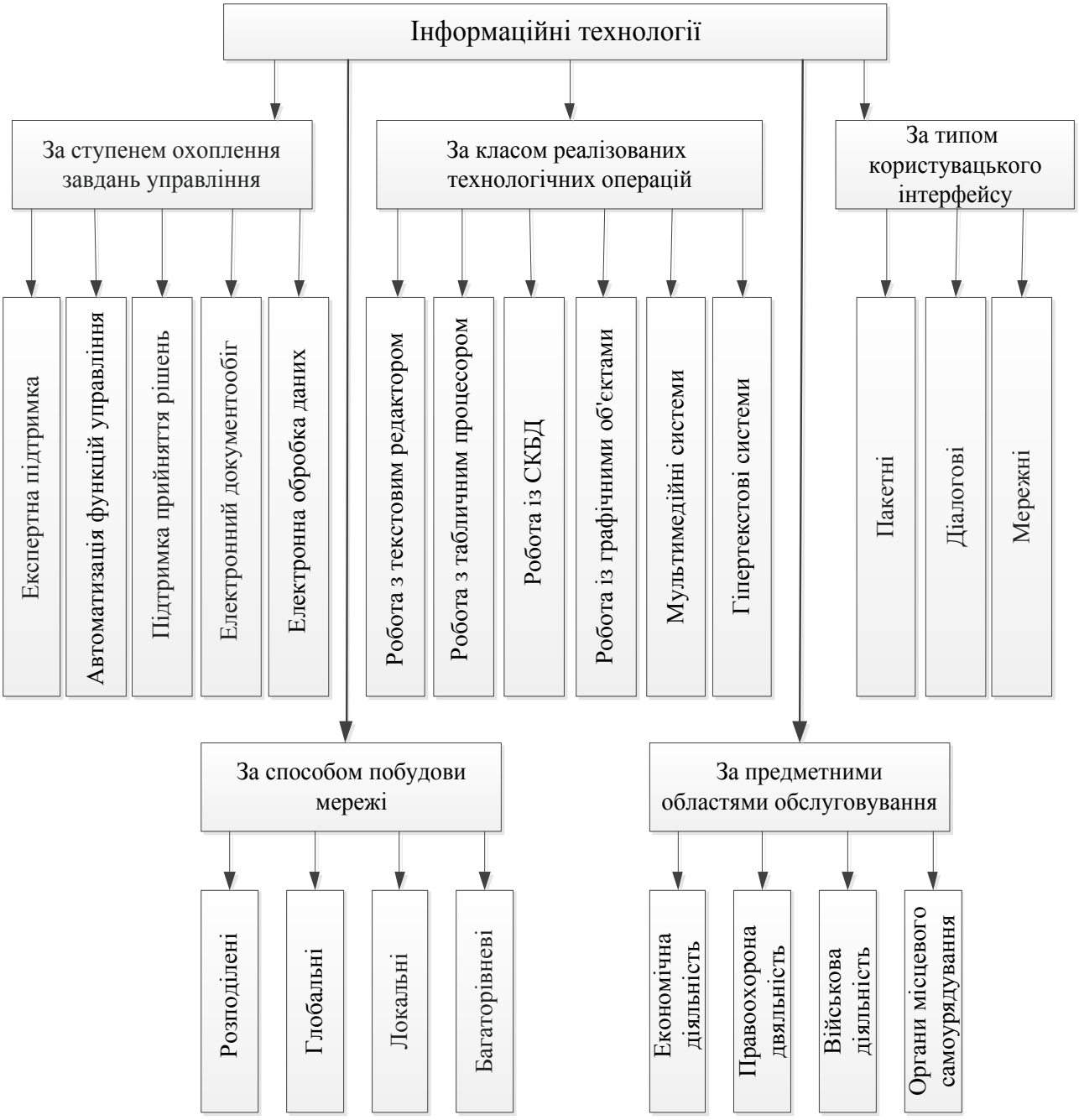

Рисунок 1.4 – Класифікація інформаційних технологій

Ознаки складних систем включають ряд структурних і функціональних характеристик, наявність яких дозволяє високою імовірністю класифікувати

систему як складну. Основні ознаки таких систем охоплюють ієрархічність структури, емерджентність властивостей, інтеграцію та складність взаємодій між різними рівнями системи, складні взаємодії з зовнішнім середовищем, здатність адаптуватися до змін у середовищі і системі, а також присутність спільної цільової функції на всіх рівнях ієрархії.

Специфічні ознаки складних систем включають значущість і складність цільових функцій, наявність операторів у системах на всіх рівнях ієрархії, складність життєвого циклу та багатофазові стани, різноманітність завдань, що вирішуються різними підсистемами, високий рівень ергономічності, а також складність науково-технічних принципів, фізичних процесів та використовуваних елементів.

Так на думку таких вчених, як Мацько О. Й., Микусь С. А., Солонніков В.Г., характерними ознаками функціонування складних систем є: мета системи, стан системи, поведінка системи, якість системи, цільова функція, показник якості, ефективність, швидкість тощо [73 с.19].

Вони розглядають цільову функцію як узагальнений функціональний критерій оцінювання (пошуку) оптимальної якості системи через її параметри. Ця функція віддзеркалює необхідний речовинний, енергетичний та інформаційний обмін, необхідний для досягнення системою цілі. Кількісне значення цільової функції, визначене для конкретних значень параметрів системи, називають показником якості системи. Під час вирішення воєнних задач досить часто як цільову функцію приймають ефективність системи. Поняття ефективності системи є більш вузьке ніж поняття цільової функції.

До характеристик функціонування також належать: надійність, швидкодія, перешкодозахищеність, завадостійкість, пропускна спроможність та інші. Однак визначення цих характеристик мало відрізняється від загальновизнаних і вони, як правило, є складовими елементами сформованого показника якості досліджуваної системи.

Дослідник у галузі теорії систем М. Месарович вважає обов'язковими атрибутами великої системи ієрархічність структури, масштабність, складність, різноманітність, широкий спектр функціональної координації тощо [73 с.18].

Складні системи за їх масштабністю прийнято поділяти на чотири групи: малі (10–10^3 елементів), складні (10^3 –10^7 елементів), ультраскладні (10^7– 10^{30} елементів), суперсистеми (10^{30}–10^{200} елементів).

У складних системах процес існує на багатьох рівнях, при чому діє принцип підлеглості нижчих рівнів вищим. Це означає, що кожна система стосовно свого складу є частиною більш складної системи (системи вищого рівня) і цілі кожної системи підлеглі цілям систем більш високого рівня і є засобом їх досягнення. Ієрархія систем є відображенням ієрархії цілей.

До основних характеристик системи інформаційно-аналітичного забезпечення процесів управління, на думку таких вчених, як Городнов В.П., Дробаха Г.А., Єрмошин М.О. відносяться [117]:

- склад системи, тобто перелік джерел та споживачів інформації з вказівкою їх задач, функцій та взаємозв'язків між ними, програмно-технічних комплексів та інших засобів, що забезпечують реалізацію функцій управління;

- структура (як характеристика) системи інформаційного забезпечення процесів управління як взаємне розташування її елементів та сукупність стійких зв'язків між ними, що забезпечують реалізацію функцій добування, збору, передачі, обробки, зберігання, пошуку, відображення та безпосереднього використання інформації для вирішення управлінських задач у будь-яких умовах обстановки;

- перелік інформаційних складових, кожна з яких являє собою сукупність корисних (потрібних) органу управління зведень, згрупованих за значущим змістом, та таких, що характеризують одну з істотних сторін об'єкта управління, умов обстановки або процесу бойових дій (дані про противника, про умови обстановки, про свої і взаємодіючі війська та ін.) з деталізацією, необхідною для кожного конкретного випадку;

- склад, зміст та перелік функції розрахункових та інформаційно-

розрахункових задач, моделей, які забезпечують вирішення управлінських завдань, параметри розподілу і передачі інформації між джерелами та споживачами, її обробки, подання та відображення на робочих місцях посадових осіб на різних етапах підготовки і ведення службово-бойових дій;

- склад та характеристики локальних та розподілених баз даних, перелік документів та форм, у яких міститься інформація, потрібна органам управління для реалізації своїх функцій;

- показники інформаційних властивостей та можливостей системи інформаційного забезпечення процесів управління;

- критерії, що визначають вимоги до технології обробки та захисту інформації, до реалізації технічного, інформаційно-розрахункового та інформаційно-командного забезпечення процесів управління, до інформаційного, математичного, лінгвістичного та програмного забезпечення системи управління [117].

Пам’ятаючи про те, що система військового управління є спланованим, узгодженим й організованим розміщенням за єдиним замислом і планом функціонально пов’язаних органів управління, командних пунктів (центрів, пунктів управління), засобів зв’язку й АСУ сил безпеки для централізованого (а при необхідності у поєднанні з децентралізацією) управління всіма силами і засобами, вона, як система, характеризується емерджентними властивостями. Ці властивості утворилися в системі завдяки привнесеним елементам структури управління у ЗСУ. Наприклад, система управління зенітними ракетними військами характеризується оперативністю реагування вогнем ЗРК на широкому фронті дій повітряного противника і по ешелонах у глибину його проникнення, системі управління авіацією додатково притаманна властивість безперервності процесів вибору зброї для вогневого ураження противника на великому просторі ведення бойових дій як у повітрі, так і на землі.

За результатами досліджень управління [117] до основних властивостей системи управління сил безпеки, реалізація яких є принциповою з точки зору вирішення покладених на неї завдань та показників, що характеризують ці

властивості, відносяться такі:

1. Оперативна готовність системи до здійснення управління – властивість, що характеризує здатність цієї системи приступити до виконання покладених на неї функцій із заданого вихідного стану. Оперативна готовність характеризується часовими показниками (витратою та затримкою часу на підготовку системи до використання) та імовірнісними показниками (імовірність того, що на заданий момент часу система буде здатною виконувати свої функції за призначенням). У практичному плані доцільним є введення ступенів оперативної готовності системи та визначення відповідних заходів, що забезпечують підтримку системи управління у заданому ступені оперативної готовності [117].

2. Оперативність функціонування системи управління – властивість системи виконувати свої функції за час, що дозволяє органам управління своєчасно виконувати завдання. Наявність цієї властивості (тобто здатність системи виконувати свої функції за заданий час) характеризується часом, потрібним на виконання відповідної задачі (функції) управління або на вирішення комплексу функціонально закінчених задач при відомому часі, що є у розпорядженні органів управління, або показником оперативності – тобто ймовірністю того, що завдання управління будуть виконані у зазначений термін, коли органи управління залишаються здатними приймати й реалізовувати прийняті рішення та здійснювати управляючі впливи на дії підлеглих [117].

3. Повнота інформаційного забезпечення – властивість системи своєчасно надавати органам управління інформацію у такому обсязі та з такою достовірністю, які є достатніми для вирішення відповідних управлінських завдань. Показник повноти інформаційного забезпечення характеризує здатність системи забезпечувати органи управління необхідною інформацією з урахуванням значущих факторів та достовірності інформації [117].

4. Обґрунтованість прийнятих рішень органами управління характеризується достовірністю даних, що отримують та використовують

органи управління, точністю розрахунків та результатів моделювання, які здатні забезпечувати прогноз (передбачення) розвитку ситуацій на потрібний період. Обґрунтованість також характеризується якістю (ефективністю) методик розрахунків, використаних задач та моделей, повнотою урахування факторів щодо прийняття рішення та ін. [117].

5. Адаптивність системи управління до умов обстановки – властивість системи змінювати параметри власної структури, її інформаційно-аналітичної підсистеми для зберігання своїх якостей в умовах зміни дій протилежної сторони, стану своїх сил, непередбаченого розвитку обстановки та змін рівня завантаженості органів управління під час вирішення відповідних управлінських задач та виконання функцій. У свою чергу ця властивість залежить від гнучкості, багатоваріантності і здатності до нарощування відповідних елементів, з яких складається структура системи управління [117].

6. Безперервність визначених процесів в системі управління – така її властивість, за якої протягом заданого часу вирішення управлінських задач система управління здатна своєчасно переробляти необхідні об‘єми інформації, формувати раціональні управлінські впливи та здійснювати контроль за об‘єктами управління. Як показники безперервності управління доцільно використовувати часові показники (тривалість часу, протягом якого не відбуваються порушення безперервності процесів управління) та імовірнісні показники (ймовірність того, що на заданому інтервалі часу не відбудеться таких порушень процесів управління, які призводять до неможливості вирішувати завдання управління або виконувати відповідні функції) [117].

7. Стійкість системи управління – властивість системи зберігати свої якості та функції при впливі деструктивних факторів на елементи системи управління з метою виведення її з ладу, порушення функціонування технічних пристроїв добування, обробки та передачі інформації, викривлення та обмеження даних і зведень, які потрібні для вирішення завдань управління та ін. Стійкість системи управління характеризується показниками надійності, живучості, завадостійкості, захищеності структури, її елементів та імовірністю

того, що при визначеному впливі противника на елементи система управління не втрачатиме своїх якостей.

8. Прихованість процесів управління – властивість, за якої забезпечується прихованість даних, що використовуються органами управління, порядку та результатів прийняття рішень, доведення їх до підлеглих та контроль виконання. Прихованість процесів управління характеризується показниками захищеності інформації від початку її добування різноманітними засобами розвідки, прихованістю елементів системи управління та її структури, захищеністю каналів передачі даних та ін.

9. Рефлексивність процесів управління – властивість системи, що дає змогу випереджувати противника в діях на необхідний час, з достатнім ступенем достовірності прогнозувати його дії та вводити його в оману з метою створення вигідної для себе ситуації. Як показник рефлексивності прийнято використовувати ранг рефлексії [117] або час, на який створена можливість випереджувати противника в діях хоча б на один ранг.

10. Раціональність (оптимальність) процесів управління – така їх організація та побудова, за яких передбачається максимальний ефект у діях об‘єктів управління при витратах, менших за потрібні на здійснення всебічного їх забезпечення. Раціональність процесів управління залежить від ступеня відповідності прийнятих рішень (впливів управління) меті, задачам, які необхідно виконати органам управління на різних етапах їх роботи.

11. Комунікативність процесів управління військами – властивість, за якої досягається такий взаємозв’язок між елементами структури системи управління, що дозволяє кожному органу управління своєчасно отримати будь-яку необхідну інформацію, у тому числі і ту, яка є у розпорядженні інших органів управління системи. Необхідна комунікативність досягається шляхом використання органами управління сучасних мереж ЕОМ з розподіленими базами даних.

12. Контрольованість процесів управління – властивість, за якої забезпечується можливість перевірки достовірності даних, що

використовуються органами управління, результатів розрахунків, які ними проводяться, прогнозів, що здійснюються, а також забезпечується перевірка проходження впливів управління між елементами структури.

Для реалізації властивостей системи управління доцільно навести показники ефективності функціонування інформаційно-аналітичної системи забезпечення процесів управління силами безпеки, які характеризують здатність (пристосовність) системи виконувати покладені на неї функції. З реалізованими значеннями цих показників безпосередньо пов’язані значення основних показників, але їх перевагою є те, що вони порівняно легко вимірюються або визначаються при відомих характеристиках окремих елементів конкретної інформаційної (інформаційно-управляючої) системи.

До цих показників відносяться [117]:

1. Показники якості структури інформаційно-аналітичної системи забезпечення, що характеризують її кількісний і якісний склад (кількість елементів за типами, характеристики технічних засобів, що використовуються, можливості та порівняльна ефективність задач і моделей, що реалізуються та ін.), взаємозв’язки між джерелами та споживачами інформації. До цих показників відносяться: показник складності організації структури інформаційної мережі; показник взаємозв’язку вузлів інформаційної мережі; показник нерівномірності інформаційного навантаження вузлів інформаційної мережі; показник ізольованості вузлів інформаційної мережі.

2. Показники, які характеризують можливості системи щодо обробки та передачі інформації відповідного обсягу за заданий інтервал часу. До них відносяться: 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 відносяться: показники якості інформаційних складових (сукупності даних та зведень, згрупованих за ознаками їх використання джерелами, споживачами, за

їх характеристиками та ін.); відомі показники, що характеризують можливості технічних засобів обробки та передачі інформації; 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 дозволяє додати відповідних 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 відносяться [117]: 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.

Низка важливих додаткових показників дозволяє судити як про властивості структури інформаційно-аналітичної системи забезпечення процесів управління, так і про характеристики інформації, що перетворюється у цій системі.

До основних з них відносяться [117]: кількість джерел, кількість споживачів інформації, кількість зв’язків між ними; кількість прямих та транзитних маршрутів розповсюдження (передачі) інформації; кратність

транзитного маршруту; кількість транзитних маршрутів відповідної кратності (характеризує кількість варіантів передачі інформації від джерела до споживача); довжина маршруту розповсюдження інформації; ранг ієрархії структури інформаційно-аналітичної системи та рівень ієрархії її елементів.

Показники дозволяють вимірювати ефективність інформаційно-аналітичної системи забезпечення процесів управління сил безпеки та у подальшому здійснювати вибір варіантів як структур управління, так і рішень, що приймаються відповідними органами управління.

Ефективність інформаційно-аналітичної системи забезпечення процесів управління визначається її призначенням – досягти такої якості забезпечення користувачів інформацією у системі управління військами (силами), яка дозволить отримати визначену бойову ефективність (або підвищити її, реалізувати потенціальну та ін.). При такому підході оцінка ефективності має базуватися на визначенні кінцевого ефекту, тобто досягнутого або очікуваного приросту ефективності бойових дій, який дає створення цієї системи.

Визначити очікуваний приріст ефективності службово-бойових дій без використання відповідних моделей важко. На етапі проектування та створення інформаційно-аналітичної системи забезпечення процесів управління не вдається знайти простих функціональних залежностей ефективності бойових дій від параметрів та показників цієї системи. На етапі застосування інформаційно-аналітичної системи забезпечення процесів управління стає можливим розрахувати реалізовану ефективність службово-бойових дій. На практиці ж визначити, наскільки низька ефективність службово-бойових дій на випадок, коли цієї системи немає, або одержати апостеріорний приріст ефективності службово-бойових дій за рахунок реалізації інформаційно-аналітичної системи забезпечення процесів управління також стає неможливим. Виходом з цього є використання складних моделей функціонування інформаційно-управляючих систем у складі комплексної моделі операції з метою розрахунку значень показників очікуваної ефективності службово-бойових дій при різних варіантах реалізації інформаційно-аналітичної системи

забезпечення процесів управління та наступної оцінки очікуваного приросту, що досягається.

У зв’язку з тим, що інформаційно-аналітична система забезпечення управління сил безпеки існує завжди, незалежно від наявності або відсутності відповідних засобів автоматизації управління, як показник приросту ефективності службово-бойових дій за рахунок реалізації нових властивостей інформаційно-аналітичної системи забезпечення процесів управління доцільно використовувати зважений показник.

Для організації комплексної оцінки якості інформаційно-аналітичної системи забезпечення процесів управління сил безпеки розглянуті показники доцільно звести у такі групи:

основні – показники, що характеризують збільшення ефективності службово-бойових дій сил безпеки за рахунок реалізації інформаційно-аналітичної системи забезпечення процесів управління;

додаткові – показники, що характеризують досягнуті властивості інформаційно-аналітичної системи забезпечення процесів управління;

обмеження – показники економічної доцільності впровадження цієї системи.

Доцільно окремо розглянути один з основних показників ефективності системи управління, який увібрав у себе всі характеристики складових системи, у тому числі й характеристики інформаційно-аналітичної системи забезпечення процесів управління. Цей показник характеризує безперервність процесів управління [51, 117].

Дробаха Г.А. в своїх працях, розглядаючи процес управління службово-бойовими діями сил безпеки, відмічає властиву йому дискретність, пов’язану з тим, що у ході виконання функцій управління будь-який орган управління здійснює на підлеглих управляючі впливи (ставить задачу, доводить команди, сигнали, дані, здійснює контроль за якістю виконання поставлених завдань та ін.) не безперервно, а в деякі моменти часу та з кількістю і тривалістю цих дій, потрібною для такого реагування на зміни обстановки, яке дозволяє досягати

поставлену мету управління (наприклад, забезпечення потрібної ефективності службово-бойових дій).

У зв’язку з цим потрібно конкретизувати поняття безперервності процесу управління та визначити його необхідні і достатні умови. Це у свою чергу дасть можливість знайти необхідні показники та критерії безперервності процесу управління, розробити достовірні методи розрахунку їх значень.

Тривалість часу, протягом якого безпосередньо виконуються функції управління, тісно пов’язана з тривалістю часу виконання поставлених ним завдань. Виконання кожної окремої задачі з тих, що виникають у процесі підготовки та ведення службово-бойових дій, як правило, потребує реалізації органом управління декількох функцій управління. Кожна з таких функцій у свою чергу характеризується кількістю управляючих впливів, потрібних для послідовного доведення даних і постановки (уточнення) задач підлеглим, та часом між їх здійсненням. Потрібна тривалість цього часу залежить від інтенсивності виникнення задач, що вимагають втручання органа управління у дії підлеглих, а та, що реалізується, ще й від часу, який витрачається органом управління на отримання необхідної інформацій, прийняття рішення і доведення його до підлеглих. При цьому у реальному процесі підготовки та ведення службово-бойових дій можливі такі випадки [117]:

1. Моменти здійснення органом управління впливу на підлеглих (постановки задачі, доведення команди, сигналу, даних обстановки та ін.) мають співпадати з потрібним поточним часом здійснення цього впливу, який диктується розвитком обстановки (діями протиборствуючей стороною та станом своїх сил, їх задачами, зміною умов обстановки та ін.).

2. Управляючий вплив на підлеглих здійснюється пізніше, ніж це потрібно за розвитком обстановки, тобто з якоюсь затримкою часу від моменту, потрібного для доведення завдань до підлеглих.

3. Управляючий вплив на підлеглих здійснюється раніше, ніж це потрібно за розвитком обстановки.

4. Ситуація, коли управляючий вплив здійснюється своєчасно (у

контексті того, що розглянуто), але неодноразово, не призводить безпосередньо до втрати управління, а має наслідком перевантаження органа управління та підлеглих надлишковою роботою.

5. Ситуація, коли управляючий вплив здійснюється своєчасно та з необхідною тривалістю післядії, а виконавчий орган (підпорядкований) виконує поставлене завдання (реагує на управляючий вплив) раніше, ніж це потрібно за умовами обстановки, звичайно також не призводить до втрат управління, але дає додатковий час підлеглому для підвищення надійності виконання поставлених завдань.

6. Ситуація, коли управляючий вплив здійснюється своєчасно, але через велику затримку у доведенні інформації до підлеглих або значного, ніж це передбачалося, перевищення витрат ними часу на виконання раніше поставленої задачі виконавчий орган не в змозі одразу реагувати на наступний управляючий вплив, також призведе до часткової втрати управління.

Суттєвим для розуміння поняття безперервності управління є те, що будь-який управляючий вплив (команда, сигнал, передані дані та ін.) має властивість “корисної” післядії. Тобто управляючий вплив завжди зберігає свою актуальність (корисний ефект) протягом деякого часу, а не втрачає її одразу ж з отриманням підлеглим цієї команди, сигналу або даних. Тому, якщо на протязі між двома сусідніми управляючими впливами до моменту, коли підлеглий закінчить виконання поставленого завдання, перший з них зберігає властивість післядії, тобто поставлене завдання (команда, сигнал, дані та ін.) відповідають розвитку обстановки та не вимагають коригування, таке управління буде безперервним. Якщо цього не відбувається, виникає втрата управління, і тоді така властивість, як безперервність управління, не буде йому властива.

Сумарний час, на протязі якого після чергового управляючого впливу (команди) підлеглий здатний успішно вирішувати завдання без додаткового втручання органа управління, характеризується тривалістю післядії, на яку розрахований управляючий вплив. Досвід управління показує, що у командирів сьогоднішніх структур силових формувань 90% робочого часу приділяється

вирішенню питань забезпечення повсякденної діяльності, забезпеченню службово-бойових дій, і лише 10% часу – відпрацюванню бойових завдань з управління підрозділами, зброєю. Це пов’язується із зростанням як завдань забезпечення, так і економічних проблем наповнення воєнного бюджету.

Проведений аналіз дає можливість сформулювати необхідну та достатню умову безперервності управління: щоб бути безперервним, управління повинно бути своєчасним, а інтервали між двома сусідніми управляючими впливами на підлеглих та від початку першого до моменту виконання поставленого завдання підлеглим не повинні перевищувати допустимої тривалості післядії першого з них. При цьому під своєчасністю управління розуміється те, що управляючий вплив буде здійснений не пізніше, ніж це потрібно за умовами розвитку обстановки, а при випереджальному управляючому впливі тривалість його післядій буде більшою, ніж інтервал часу від здійснення управляючого впливу до того останнього моменту, коли за умов обстановки виконавчий орган (підлеглі) буде ще в змозі відпрацювати поставлене завдання або відповідним чином відреагувати на управляючий вплив. Потребує уваги питання, що для сил безпеки таке поняття, як противник не є актуальним. Для ЗСУ таке поняття можна використовувати, тому що існує збройне протистояння та присутня сторона конфлікту. Для сил безпеки більш доцільним було б використання терміну протиборствуюча сторона. Для кожного суб’єкту сил безпеки протиборствуюча сторона представлена в різних формах. Так, наприклад, для Національної поліції протиборствуючою стороною виступають правопорушники, для ДПСУ – порушники державного кордону, для ДСНСУ – це природні, або штучні явища що призвели до надзвичайної ситуації. Для НГУ, крім перелічених форм протиборствуючої сторони, в деяких сценаріях службово-бойових дій можна використовувати термін противник. У якості противника для НГУ можуть виступати незаконні збройні формування (НЗФ), диверсійно-розвідувальні групи (ДРГ), комбатанти.

На користь використання терміну протиборствуюча сторона може виступати той факт, що сили безпеки у своїй діяльності стикаються з громадянами своєї держави.

1.3 Генезіс інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки України

Інформаційно-аналітичне забезпечення (ІАЗ) сил безпеки України є важливою складовою сучасної системи національної безпеки країни. Розвиток цієї галузі в Україні відбувався в контексті викликів і загроз, які виникали внаслідок геополітичних подій, змін у технологічному просторі та необхідності адаптації до міжнародних стандартів.

Період після отримання незалежності (1991-2000 рр.). У перші роки після отримання незалежності в 1991 році, Україна зіткнулася з численними викликами і завданнями, пов’язаними з формуванням власної системи безпеки та оборони. У цей період інформаційно-аналітичне забезпечення (ІАЗ) сил безпеки України ще не було належною розвиненою галуззю, і воно проходило через етапи становлення та організаційного розвитку. У цей період інформаційно-аналітичне забезпечення складалося переважно з застарілих методів інформаційного аналізу.

Основні характеристики ІАЗ у перші роки після отримання незалежності [17].

Цей період характеризується новими викликами та необхідністю в утворенні нової системи безпеки. Розпад Радянського Союзу призвів до створення самостійної системи безпеки для новоствореної держави. Це передбачало формування власних збройних сил, розвідки та інших служб безпеки. Був присутній брак досвіду та власних ресурсів. Україна мала обмежені ресурси та обладнання для впровадження власної системи ІАЗ. Знання та досвід у галузі інформаційної безпеки були обмеженими, і країна стикнулася із завданням відтворення власних оборонних та безпекових структур. У перші роки після незалежності особливу роль у забезпеченні інформаційної безпеки відігравала розвідка. Спеціальні служби фокусувалися на зборі та аналізі інформації щодо зовнішніх та внутрішніх загроз. При цьому існували і традиційні методи інформаційного аналізу. Оскільки сучасні

технології не були ще широко впроваджені, інформаційно-аналітичне забезпечення використовувало традиційні методи збору та обробки інформації. Одним з негативних факторів цього періоду була відсутність стандартизації. У період становлення незалежності відсутність стандартизації в галузі інформаційно-аналітичного забезпечення сил безпеки утруднювала координацію та обмін інформацією між різними структурами.

Протягом перших років незалежності відбувалися зміни в організаційній структурі та стратегії сил безпеки, що вплинуло на розвиток інформаційно-аналітичного забезпечення. Цей період становлення був важливим для подальшого розвитку ІАЗ сил безпеки України, і з часом країна стала активно адаптувати та впроваджувати сучасні технології для вдосконалення своїх здатностей у сфері інформаційної безпеки.

Період модернізації (2000-2014 рр.). У цей період забезпечення інформаційно-аналітичними засобами почало зазнавати модернізації. З'явилися нові технології, включаючи системи автоматизованого збору та аналізу даних. Проте, розвиток був неоднаковим у зв'язку з фінансовими труднощами та іншими факторами.. У цей період країна вдосконалювала свої інформаційно-аналітичні системи, реагуючи на сучасні виклики та враховуючи досвід інших країн. Основні аспекти цього періоду включають:

У цей період Україна створювала нові структури та підрозділи, спрямовані на інформаційне забезпечення сил безпеки. Створення спеціалізованих агентств, які відповідають за аналіз та обробку інформації, покращило систему ІАЗ. Зростання рівня технологічного розвитку призвело до модернізації технічного забезпечення ІАЗ. Використання комп'ютерних технологій, програмного забезпечення для обробки та аналізу інформації стало більш поширеним. У цей період велика увага була приділена розвитку систем аналітики та обробки великих обсягів даних. Це дозволило здійснювати більш точний та швидкий аналіз інформації, що було важливим для оперативного прийняття рішень. В умовах росту інтересу до штучного інтелекту, сили безпеки почали впроваджувати його для автоматизації деяких аспектів аналізу

та прийняття рішень. Це стало важливим етапом у розвитку інтелектуальних систем ІАЗ. З урахуванням росту кількості кіберзагроз та кібератак, акцент був зроблений на підвищенні інформаційної безпеки. Розробка та впровадження кіберзахисту стали важливим елементом ІАЗ. Важливою складовою модернізації було підвищення кваліфікації фахівців в галузі інформаційної безпеки та аналітики. Це включало навчання персоналу за новітніми методиками та технологіями. Зазначений період був ключовим для покращення здатностей сил безпеки України у сфері інформаційно-аналітичного забезпечення, що стало докладною відповіддю на виклики сучасності та підготовкою до подальшого розвитку систем безпеки та оборони.

Події на сході України (з 2014 р.). Події, що розгорталися на сході України та анексія Криму російською федерацією з 2014 року, визначили необхідність стрімкого розвитку інформаційно-аналітичного забезпечення (ІАЗ) сил безпеки України. Ці події створили нові виклики та загрози для національної безпеки, а також потребу в ефективній системі аналізу та розподілу інформації для прийняття оперативних рішень. Основні аспекти цього періоду включають:

Російська федерація активно використовувала інформаційні та психологічні методи для впливу на ситуацію в Україні. Інформаційна війна, дезінформація та кібератаки стали важливими аспектами, які вимагали вдосконалення системи ІАЗ для ефективного виявлення та реагування. Конфлікт вимагав обробки великої кількості інформації, яка надходила з різних джерел, включаючи розвідувальні дані, дані відкритого джерела та інші. Система ІАЗ повинна була забезпечити швидке та ефективне аналітичне опрацювання цієї інформації. Розвиток кіберзагроз та кібератак, використання гібридної війни, вимагав вдосконалення заходів кібербезпеки та використання новітніх технологій для виявлення та запобігання атакам. Однією з характерних рис цього періоду був розвиток кібераналітики. З метою виявлення та аналізу кіберзагроз, силам безпеки було необхідно вдосконалити системи кібераналітики. Це включало в себе аналіз великих обсягів кіберданих та

впровадження нових методів виявлення загроз. Україна створила спеціалізовані штаби та центри інформаційно-аналітичного забезпечення для координації та обміну інформацією між різними службами та військовими підрозділами. Проведені заходи з організації міжнародної співпраці в галузі кібербезпеки та інформаційної безпеки. Україна взаємодіяла з іншими країнами та міжнародними організаціями в галузі кібербезпеки та інформаційної безпеки для обміну досвідом та отримання підтримки у боротьбі з загрозами.

В цілому, події на сході України та анексія Криму визначили стрімкий розвиток інформаційно-аналітичного забезпечення сил безпеки, зробивши його більш адаптованим до сучасних загроз та викликів.

Створення нових структур (з 2014 р.). З метою вдосконалення системи безпеки та оборони, Україна створила нові структури, включаючи Службу зовнішньої розвідки України та інші агентства, які активно використовують інформаційно-аналітичні технології для забезпечення своїх завдань. У зв’язку з реалізацією стратегічних завдань та вдосконаленням системи безпеки та оборони в умовах сучасних загроз, Україна створила нові структури інформаційно-аналітичного забезпечення (ІАЗ). Ці структури спрямовані на підвищення ефективності роботи сил безпеки та забезпечення оперативної та точної інформації для прийняття стратегічних рішень. Деякі з цих структур включають:

Інформаційно-аналітичне управління Міністерства оборони. Створене для централізованого управління та координації інформаційно-аналітичною діяльністю в галузі оборони.

Інформаційно-аналітичний центр Генерального штабу Збройних Сил України. Забезпечує аналіз сучасної ситуації в країні та світі, розробку прогнозів та аналітичних матеріалів для вищого військового керівництва.

Центр кіберзахисту Національної гвардії України. Створений для забезпечення кібербезпеки та захисту від кіберзагроз, включаючи важливі об’єкти та інформаційні ресурси.

Інформаційно-аналітичне управління Служби безпеки України.

Відповідає за збір, аналіз та обробку інформації щодо загроз національній безпеці, внутрішній та зовнішній розвідці.

Управління інформаційно-аналітичного забезпечення Міністерства внутрішніх справ. Створене для обробки інформації щодо внутрішніх загроз, забезпечення ситуаційної обстановки в країні та підтримки операцій підрозділів МВС.

Центр інформаційно-аналітичної діяльності Служби зовнішньої розвідки України. Відповідає за збір, аналіз та обробку інформації в міжнародному контексті, розвідку і захист від зовнішніх загроз.

Створення таких структур ІАЗ сприяло забезпеченню системи безпеки та оборони України сучасними та ефективними інструментами для аналізу інформації, виявлення загроз та вчасного реагування на них. Це важливий крок для захисту національних інтересів та забезпечення безпеки країни в умовах сучасних викликів і загроз.

Застосування новітніх технологій (з 2014 р.): Внаслідок технологічних та інформаційних зрушень, сили безпеки України почали впроваджувати новітні технології для забезпечення ефективності, точності та оперативності в сфері інформаційно-аналітичного забезпечення (ІАЗ), такі як штучний інтелект, кібербезпека, аналіз великих даних та інші інструменти для збору та обробки інформації.

Сили безпеки використовують штучний інтелект для автоматизації процесів аналізу великих обсягів даних, виявлення закономірностей та встановлення зв’язків. Штучний інтелект (ШІ) також може бути використаний для прогнозування ситуацій, виявлення аномалій та автоматизованого прийняття рішень. У зв’язку зі зростанням кількості кіберзагроз, сили безпеки вдосконалюють заходи кібербезпеки та впроваджують сучасні засоби захисту від кібератак. Це включає розвиток систем виявлення та реагування на інциденти, шифрування інформації та забезпечення кіберзахисту критичних об’єктів. Однією з новітніх технологій, що застосовується силами безпеки є аналіз великих даних (Big Data). З використанням аналізу великих обсягів

даних сили безпеки можуть отримати більш повний та глибокий розуміння складних ситуацій, виявляти тенденції та робити стратегічні висновки. Інтернет речей (Internet of Things або IoT) - це концепція, яка вказує на підключення до Інтернету фізичних об’єктів, які раніше не були здатні до цього. Це можуть бути різноманітні пристрої, предмети побуту, технічні системи, автомобілі, електроніка та інші об’єкти, оснащені сенсорами, програмним забезпеченням та можливістю здійснювати обмін даними через мережу Інтернет. Основна ідея IoT полягає в тому, щоб об’єднати реальний світ зі світом Інтернету, де об’єкти можуть взаємодіяти один з одним, збирати та обмінюватися даними, використовуючи мережі і комунікаційні технології. Впровадження технологій Інтернету речей дозволяє збирати та обробляти дані з різних джерел, що полегшує моніторинг та керування об’єктами та ресурсами [17].

Комп’ютерний аналіз зображень та відео аналітика є технологією що отримала широке розповсюдження у повсякденному житті. Використання алгоритмів машинного навчання для обробки та аналізу відеоматеріалів забезпечує можливість виявлення аномалій, розпізнавання об’єктів та подій. Використання новітніх інноваційних засобів зв’язку дозволяє силам безпеки ефективно обмінюватися інформацією в режимі реального часу.

Ці технологічні інновації спрямовані на покращення якості та обсягу інформації, що доступна силам безпеки, забезпечуючи більшу ефективність в управлінні та реагуванні на сучасні загрози.

Після подій 2014 року, Україна активно розвиває міжнародну співпрацю в галузі інформаційно-аналітичного забезпечення (ІАЗ), співпрацюючи з іншими країнами та міжнародними організаціями. Це має на меті обмін інформацією, впровадження новітніх технологій та забезпечення колективного відстою від сучасних загроз. Декілька ключових аспектів міжнародної співпраці в цій сфері включають:

- обмін розвідувальною інформацією. Україна співпрацює з партнерами з інших країн, обмінюючи розвідувальною інформацією щодо загроз та дій проти національної безпеки;

- участь в міжнародних організаціях. Україна є членом різних міжнародних організацій, де співпрацює з партнерами для вирішення сучасних викликів, включаючи питання інформаційної безпеки;

- Україна розвиває безпекові партнерства з іншими країнами, які включають обмін досвідом та навчання з питань інформаційної безпеки та ІАЗ;

- технічна допомога. За допомогою міжнародної співпраці, Україна може отримати доступ до новітніх технологій та інновацій в галузі інформаційного аналізу та безпеки;

- загальні стандарти та норми. Участь в міжнародних форумах дозволяє Україні долучитися до встановлення та вдосконалення загальних стандартів та норм у галузі інформаційної безпеки;

- спільні навчання із партнерами сприяють взаємодії між різними країнами та підвищують готовність до спільного реагування на потенційні загрози.

Ця міжнародна співпраця допомагає Україні покращувати свої інформаційно-аналітичні здатності, отримувати підтримку від партнерів у сфері безпеки та обмінюватися досвідом та найкращими практиками. Вона також сприяє створенню більш єдиної та відповідальної міжнародної системи безпеки.

Загалом, розвиток ІАЗ сил безпеки України визначається потребами часу, загрозами безпеки та здатністю країни адаптуватися до сучасних викликів у сфері інформаційної безпеки та оборони.

Інформаційно-аналітичне забезпечення службово-бойової діяльності сил безпеки України є ключовим аспектом забезпечення національної безпеки та ефективності військових операцій. Це включає в себе збір, аналіз та обробку інформації з різних джерел для прийняття обґрунтованих рішень та виконання завдань в області безпеки.

Основні компоненти інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки включають:

Систематичний збір інформації з різних джерел, таких як розвідка,

датчики, джерела відкритої інформації, сигнали зв'язку тощо. Це може включати технічний розвідувальний збір, інформаційний аналіз та інші методи.

Проведення аналізу інформації з метою виявлення тенденцій, оцінки загроз, визначення стратегій та тактик. Це може включати розвідувальний аналіз, геопросторовий аналіз, аналіз соціальних мереж та інші методи.

Для зручного сприйняття командирів та прийняття рішень отримані дані повинні бути оброблені і візуалізовані. Це може включати створення карт, графіків, інфографіки та інших інструментів візуалізації.

Забезпечення безпеки інформації є важливою частиною інформаційно-аналітичного забезпечення. Заходи до цього можуть включати криптографічний захист, контроль доступу та інші методи забезпечення конфіденційності та цілісності інформації.

Підготовка аналітичних звітів та рекомендацій допоможе приймати обґрунтовані раціональні рішення на основі найновішої інформації.

Постійне навчання і професійне зростання персоналу є важливим елементом, оскільки сучасне інформаційне середовище постійно змінюється. Тренування з використання новітніх технологій та методів аналізу інформації є необхідним для забезпечення ефективної службово-бойової діяльності.

Ці аспекти допомагають створити інтегровану систему, яка дозволяє силам безпеки ефективно використовувати інформацію для досягнення своїх цілей у сфері безпеки та оборони.

Сучасна інформатизація та комунікації у військовій справі характеризуються численними рисами, що визначають нові підходи до ведення війни та оборони. Характерними рисами сучасної інформатизації та комунікації у військовій справі є [72, 233]:

- глобалізація інформаційних процесів у арміях провідних країн світу;

- мініатюризація елементної бази обчислювальної техніки та полегшення її інтеграції зі зразками озброєння;

- зростання надійності та мобільності обчислювальних мереж, які використовуються як матеріальна основа для побудови різних інформаційних систем воєнного призначення;

- використання штучного інтелекту (ШІ) та аналітичних систем для аналізу великих обсягів даних, розпізнавання патернів, прогнозування та прийняття рішень. ШІ може бути використаний для розвідки, планування операцій та виявлення загроз;

- розвиток телекомунікаційних технологій дозволяє швидко та ефективно обмінюватися інформацією між різними рівнями командування та підрозділами;

- розвиток телекомунікаційних технологій дозволяє швидко та ефективно обмінюватися інформацією між різними рівнями командування та підрозділами;

- розвиток роботизованих безпілотних систем розвідки та нанесення високоточних ударів;

- використання систем геолокації та геоінформаційних технологій для ведення операцій, розташування сил та планування маршрутів;

- забезпечення сумісності та взаємодії між різними системами та платформами (інтероперабельність), щоб забезпечити ефективне командування та контроль;

- заходи для захисту військової інформації від несанкціонованого доступу, кібератак та інших загроз.

Основні стратегічні напрями розвитку інформаційного суспільства в Україні включають наступні важливі цілі [72]:

- прискорене розроблення та впровадження сучасних конкурентоспроможних інформаційних технологій в усі сфери суспільного життя, зокрема в економіку, державне управління та місцеве самоврядування;

- розвиток національної інформаційної інфраструктури та її інтеграція із глобальною інфраструктурою;

- створення загальнодержавних інформаційних систем, особливо у таких сферах, як охорона здоров’я, освіта, наука, культура та охорона довкілля;

- поліпшення стану інформаційної безпеки в умовах активного використання новітніх інформаційних технологій.

Сучасні військові конфлікти набувають все більш специфічних рис, які включають рішучість у досягненні політичних цілей, націленість на паралізацію систем державного військового управління та критичної інфраструктури противника, динамічність, швидкоплинність та високу технологічність застосовуваних засобів.

До таких характерних рис можна віднести [72, 233]:

- постійне вдосконалення автоматизованих систем управління військами та озброєнням, що демонструють тенденцію до переходу до автоматичних систем управління зброєю;

- розвиток високоточної зброї, яка завдяки входженню в інформаційне середовище «бойового простору» може отримувати коригування навіть після запуску;

- вдосконалення засобів розвідки, де спостерігається розширення використання різних датчиків та сенсорів, які здатні діяти автономно протягом тривалого часу та на значних відстанях, разом із традиційними засобами безпілотної розвідки;

- вдосконалення зброї, керованої штучним інтелектом, і роботизованих систем ведення бойових дій.

В Міністерстві оборони США вважають, що для досягнення перемоги у збройних конфліктах необхідно отримувати, передавати та обробляти інформацію максимально близько до реального часу [22]. Інформаційна перевага є ключовим фактором, що забезпечує розуміння поточної ситуації на полі бою та своєчасне прийняття рішень, що випереджають дії противника. В межах системи підвищення бойової здатності та мобільності військ США передбачено розробку і використання інтелектуальної зброї та робототехнічних засобів. Серед компонентів нової концепції бойового забезпечення військ

виділяються система оперативного перепланування операцій, що дозволяє суттєво скоротити час, необхідний на перепланування, підсистема оперативного картографування, а також технології навчання військовослужбовців діям у нестандартних умовах.

В Україні також здійснюється суттєве реформування процедур оперативного та комплексного забезпечення виконання оборонних завдань. На основі наукових досліджень вже розроблено сучасні технології автоматизації процесів оборонного планування, а також відповідні програмні та технічні засоби. Серед впроваджених у Збройних Силах України інформаційно-аналітичних та програмних систем базовою є ІАС «Ресурс», яка надає можливість комплексно розв'язувати інформаційні та розрахункові завдання, завдання з моделювання, а також забезпечувати осіб, що приймають рішення, своєчасною, об'єктивною та достатньою інформацією для всебічного аналізу, починаючи від командирів частин і закінчуючи вищим керівництвом країни.

Крім того, за державним замовленням Науково-дослідний інститут автоматизованих комп'ютерних систем «Екотех» розробляє комплекс інформаційно-аналітичних систем, таких як «ІАС підтримки оборонного планування ЗСУ», «ІАС автоматизованого обліку особового складу ЗСУ» та інші. Ці системи наразі проходять перевірку і найближчим часом будуть впроваджені у практичну діяльність Збройних Сил України [22].

Впровадження у роботу органів військового управління стандартизованих процедур етапів планування як форми прийняття військового рішення командирами та штабами за стандартами НАТО [94, 233] породжує ряд проблем, вирішення яких можливе шляхом інтеграції в процес прийняття військових рішень (MDMP – Military Decision-Making Process) сучасних інформаційно-аналітичних технологій. Ці технології поєднують у собі методи збору та обробки інформації, узагальнення висновків з аналізу завдання та оцінки ситуації, специфічні прийоми діагностики, аналізу варіантів та синтезу способів дій підпорядкованих сил і засобів, а також оцінки можливостей досягнення кінцевої мети виконання службово-бойового завдання [94].

Починаючи з 2018 року використовуються окремі інформаційні системи різного рівня: Delta, «Кропива», «Віраж-планшет», GisArta та ін. (табл. 1.1).

Таблиця 1.1 – Перелік інформаційно-аналітичнич систем [39].

Назва	Призначення	Рік
«Укроп» (MyGun)	Розрахунок для стрільби артилерії, офлайн-карта, орієнтування	2009
GisArta	Орієнтування, планування, розрахунок для артилерії	2014
«Кропива»	Розрахунок для стрільби артилерії, планування, нанесення тактичної обстановки, управління підрозділами, розвідка, орієнтування	2014
«ТОПО» (Топик)	Орієнтування, нанесення тактичної обстановки	2014
«Броня»	Розрахунок для стрільби з гранатометів, мінометів, танків, орієнтування	2015
«Термінал»	Тактична обстановка, орієнтування	2015
ComBat Vision	Розвідка, орієнтування, підтримка прийняття рішень	2015
Delta	Орієнтування, тактична обстановка, управління підрозділами	2016
«Дзвін-АС»	Управління та контроль за бойовими діями на рівні командування	2016
«Віраж-планшет»	Збирання, відображення та аналіз інформації про повітряну обстановку	2016
MilChat	Обмін повідомленнями, тактична обстановка, транслювання геопозиції	2018
«Простір»	Управління військами та зброєю на рівні бригади	2021

Усі зазначені системи функціонують на тактичному рівні управління [39]. Комплекс спеціального програмного забезпечення «Віраж-планшет» являє собою автоматизовану геоінформаційну систему (ГІС), призначену для

збирання, обробки, відображення та аналізу інформації про повітряну обстановку. Цю систему створено для радіотехнічних військ Повітряних Сил ЗСУ з метою автоматизації процесів контролю, збереження та надання інформації про повітряну обстановку [16, 39]. Ще одним прикладом є інформаційна система GisArta, яка виконує функцію автоматизованої системи управління артилерійськими частинами, враховуючи специфіку планування та ведення бойових дій, а також вимоги до отримання точних даних про результати бойових операцій [39].

Програмний комплекс «Кропива» є системою управління тактичної ланки, розробленою на базі ГІС для створення інтелектуальних карт у поєднанні з різними пристроями та інструментами для планування, проведення розрахунків та орієнтування на місцевості. На сьогодні цей комплекс активно використовується різними підрозділами сухопутних військ ЗСУ, Національної гвардії України (НГУ) та територіальної оборони (ТРО), включаючи артилерійські, бронетанкові, піхотні та розвідувальні підрозділи [39].

Варто зазначити, що на відміну від військової сфери, в правоохоронній діяльності поки не відбулося значних технологічних проривів в інформаційному забезпеченні, що негативно відобразилося на рівні боротьби зі злочинністю, охороні прав і свобод громадян, а також захисті життєвих цінностей. Криміногенна ситуація в Україні демонструє стійку тенденцію до збільшення кількості звернень громадян щодо кримінальних подій. Це призводить до підвищеного навантаження на працівників оперативних підрозділів органів внутрішніх справ (ОВС), що ускладнює їх роботу, особливо в умовах кадрового дефіциту, накопиченого за останні роки [22].

У зв’язку з цим, для ефективної роботи правоохоронних органів необхідно створити єдину загальнодержавну інформаційну систему. Впровадження такої системи не тільки зменшить навантаження на оперативних працівників, але й дозволить ефективніше використовувати державні інформаційні ресурси в режимі реального часу. Однак, для успішного впровадження концепції інформаційної переваги в оперативно-розшуковій

діяльності (ОРД) необхідно створити ефективну інформаційну модель, яка повинна бути тісно інтегрована із системою управління в органах внутрішніх справ. Важливо відзначити, що ще в 1972 році засновник української кібернетики, академік В.М. Глушков, попереджав, що автоматизація ієрархічної моделі управління є тупиковим шляхом [22, 34].

Під час виконання службово-бойових завдань (СБЗ) силам безпеки потрібні різноманітні інформаційно-аналітичні технології (ІАТ). Наприклад, для Національної поліції України (НПУ) важливо використовувати бази даних (БД), що містять інформацію про правопорушників, кримінальні події тощо. Системи розпізнавання об'єктів розшуку, такі як правопорушники, необхідні не тільки для НПУ, але й для Державної прикордонної служби України (ДПСУ). Ці загальнодержавні бази даних можуть бути використані іншими суб'єктами сил безпеки під час виконання СБЗ, які є специфічними для цих суб'єктів. Автоматизовані системи управління (АСУ) потрібні всім без виключення суб'єктам сил безпеки (ССБ) не лише для взаємодії та обміну даними, а й для загального керівництва, управління підрозділами (угрупованнями) та зброєю на державному рівні.

ССБ, які виконують бойові завдання згідно з призначенням, потребують систем підтримки прийняття рішень (СППР) та геоінформаційних систем (ГІС). Потреби сил безпеки у різноманітних інформаційно-аналітичних технологіях можна побачити в таблиці 1.2. Інформаційно-аналітичне забезпечення сил безпеки України включає специфічні системи підтримки прийняття рішень, імітаційні моделі службово-бойових дій, бази даних та системи розпізнавання об'єктів розшуку. Загальними інформаційними технологіями для сил безпеки, як суб'єкта державної безпеки, є автоматизовані системи управління (АСУ) та системи документообігу.

На сьогодні існують БД суб'єктів сил безпеки, які забезпечують інформаційну підтримку службово-бойової діяльності.

Так, наприклад, у ДПСУ створена БД «Відомості про осіб, які перетнули державний кордон України» [155]. Ця БД розроблена відповідно до Законів

України «Про Державну прикордонну службу України» [150], «Про інформацію» [159], «Про захист інформації в інформаційно-телекомунікаційних системах» [157], «Про Національну програму інформатизації» [147], «Про концепцію Національної програми інформатизації» [160], Положення про порядок надання Державній прикордонній службі та виконання нею доручень правоохоронних і розвідувальних органів щодо осіб, які перетинають державний кордон України [139].

Таблиця 1.2 – Потреби сил безпеки у інформаційно-аналітичних технологіях [212]

№	Суб'єкт сил безпеки	ІАТ					
		БД	АСУ	Системи документообігу	Розп. образів	СППР	ГІС
1	НГУ (МВС)	-	+	+	-	+	+
2	НПУ (МВС)	+	+	+	+	-	-
3	ДСНСУ (МВС)	-	+	+	-	-	+
4	СБУ	+	+	+	+	+	+
5	ДПСУ	+	+	+	+	+	+

Відповідно до [155], Департамент охорони державного кордону Адміністрації Державної прикордонної служби України відповідає за встановлення програмно-технічних комплексів для автоматизації прикордонного контролю (ПТК АПК) «Гарт-1/П», що є частиною інтегрованої інформаційно-телекомунікаційної системи «Гарт» (ІІТС «Гарт»). Ці комплекси встановлюються у всіх пунктах пропуску (пунктах контролю). Також проводиться робота з підключення цих комплексів до телекомунікаційної системи Державної прикордонної служби України, що забезпечує безперервне збирання інформації про осіб, які перетнули державний кордон України, до бази даних «Відомості про осіб». Ця інформація зберігається у центральному сховищі даних центральної підсистеми ІІТС «Гарт», яка обслуговується ПТК

АПК «Гарт-1/П» у пунктах пропуску.

База даних осіб є важливою частиною центрального сховища даних (ЦСД) центральної підсистеми інтегрованої інформаційно-телекомунікаційної системи «Гарт» та міжвідомчої інформаційно-телекомунікаційної системи «Аркан», яка контролює осіб, транспортні засоби та вантажі, що перетинають державний кордон України. Ці системи сприяють забезпеченню безпеки на кордоні та ефективному управлінні даними, що надходять під час контрольних процедур.

Формування бази даних осіб включає можливість інформаційної інтеграції з аналогічними базами даних інших правоохоронних органів, а також з центральними органами виконавчої влади та суб'єктами системи «Аркан», згідно із чинним законодавством. Збір інформації про осіб відбувається через автоматизовані робочі місця «Інспектор» (у стаціонарному, портативному або кишеньковому форматах) і програмно-технічні комплекси автоматизації прикордонного контролю системи «Гарт-1». Ці дані передаються в реальному часі до центрального сховища даних системи «Гарт» за допомогою технічних засобів телекомунікаційної мережі Державної прикордонної служби України.

В системі МВС існують також БД «Розшук» та «Реєстр атестованих судових експертів Експертної служби МВС».

База даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» («ІПНП») створена згідно наказу Міністерства внутрішніх справ України № 534 «Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» [154].

Основними завданням та призначенням БД «Розшук» є – «забезпечення наповнення та підтримання в актуальному стані реєстрів та баз даних, що входять до єдиної інформаційної системи МВС (ЄІС МВС), стосовно осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від відбування покарання або від виконання обов'язків, визначених

законом для суб'єктів пробації, зниклих безвісти, зокрема за особливих обставин, підлягають психіатричній допомозі у примусовому порядку, є боржниками за виконавчими документами, відповідачами у справах про стягнення аліментів або про відшкодування шкоди, завданої каліцтвом, іншим ушкодженням здоров'я або смертю фізичної особи, є дітьми, стосовно яких за виконавчим документом про відібрання дитини за поданням виконавця судом винесено ухвалу про їх розшук, осіб, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком, установлення осіб невпізнаних трупів» [154].

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності включає в себе декілька ключових напрямків, таких як:

Наповнення бази даних «Розшук», яка є частиною ЄІС МВС. Ця база даних використовується для збору та аналізу інформації про осіб, які є предметом оперативно-розшукових заходів.

Автоматизована перевірка статусу осіб, що включає підозрюваних, обвинувачених або підсудних, які ухиляються від відбування покарання або вироку суду, осіб, що зникли безвісти під особливих обставин, а також людей, які через хворобу або неповнолітній вік не можуть надати про себе достовірну інформацію.

Використання реєстрів та баз даних ЄІС МВС для встановлення місцезнаходження осіб або для ідентифікації невідомих осіб. Це включає пошук відповідностей та верифікацію даних через автоматизовані системи.

Таке забезпечення дозволяє ефективно реагувати на різноманітні виклики, які стоять перед правоохоронними органами, і значно підвищує швидкість та точність оперативно-розшукових заходів.

Положення про базу даних реєстру атестованих судових експертів Експертної служби МВС [152] визначає такі завдання для БД: забезпечення утворення систематизованої інформації про кваліфікованих працівників Експертної служби, які мають право на проведення судових експертиз відповідно до законодавства; здійснення комплексного аналізу кваліфікації

експертів для визначення потреб у їх подальшому навчанні та професійному розвитку; планування процедур атестації судових експертів для оцінювання їхніх професійних здібностей та знань; постачання відомостей для державного Реєстру атестованих судових експертів, який веде Міністерство юстиції України відповідно до чинного законодавства.

У рамках питання розвитку інформаційних технологій та інформаційно-аналітичного забезпечення в Україні потрібно розглянути питання їх фінансового забезпечення.

Згідно даних Державної служби статистики України [188], в період з 2010 по 2012 роки фінансове забезпечення, яке виділялось на розвиток програмного забезпечення та баз даних в Україні незміно зростало.

Дані наведено в таблиці 1.3 та на рисунку 1.5.

Фінансове забезпечення інформаційно-аналітичної підтримки сил безпеки є однією з найважливіших складових у забезпеченні національної безпеки та обороноздатності держави. Бюджетування інформаційно-аналітичного забезпечення (ІАЗ) зазвичай здійснюється в межах загального оборонного бюджету країни, який охоплює всі аспекти національної безпеки, включаючи військові витрати, інвестиції в оборонну промисловість, розвідку, кібербезпеку та інші важливі напрямки. Пріоритет надається системам кіберзахисту, розробці власних програмних рішень для обробки даних, аналітичним системам та засобам кіберінтелігенції. Важливим джерелом фінансування ІАЗ стають міжнародні гранти та співпраця з союзниками, що дозволяє залучати додаткові ресурси для реалізації таких проектів.

Серед проблемних аспектів фінансового забезпечення інформаційних технологій можна виділити кілька ключових моментів. Перш за все, це швидкі технологічні зміни: нові технології розвиваються настільки стрімко, що державні закупівлі часто не встигають за потребами в оновленні обладнання та програмного забезпечення. Інша важлива проблема полягає у великій потребі в кваліфікованих фахівцях, здатних ефективно працювати з новітніми технологіями. Однак таких спеціалістів наразі бракує. Також збільшення

фінансування ІАЗ вимагає підвищеного рівня захисту даних, що в свою чергу потребує додаткових витрат на безпеку [207, 288].

Таблиця 1.3 – Статистика виділення бюджетних коштів на розвиток програмного забезпечення та баз даних в Україні з 2010 по 2021роки [188]

Кошти/роки	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Усього бюджетних коштів, млн.грн	180575,5	241286,0	273256,0	249873,4	219419,9	273116,4	359216,1	448461,5	578726,4	623978,9	508217,0	673899,3
Програмне забезпечення та бази даних, млн.грн	2802,4	3254,0	3409,1	3477,6	3207,3	4908,4	6315,5	8196,4	9476,4	10215,3	12411,1	16643,5
Відсоток на ПЗ та БД від загальної кількості коштів, %	1,5519	1,3486	1,2475	1,3917	1,4617	1,7971	1,7581	1,8276	1,6374	1,6371	2,4420	2,4697

Ефективне фінансове забезпечення інформаційно-аналітичних систем є критично важливим для підтримки національної безпеки. Необхідно забезпечити належне фінансування, регулярне оновлення технологічної бази та підготовку висококваліфікованих кадрів, щоб зміцнити обороноздатність країни та забезпечити її захист від сучасних загроз. Розвиток ІАЗ для сил безпеки України безпосередньо пов’язаний з прогресом у технологіях і фундаментальних науках, таких як математика, фізика, хімія. Підвищення продуктивності обчислювальної техніки створює умови для застосування штучного інтелекту в системах підтримки прийняття рішень. На сьогодні

органи управління активно використовують інформаційні технології для ухвалення стратегічних рішень.

Існує нагальна потреба у формуванні вимог до створення загальнодержавної інформаційної системи для сил безпеки, що зможе адекватно реагувати на виклики сучасності. Подальше вдосконалення системи державного управління має включати розробку та впровадження цієї системи, яка стане ключовим елементом у забезпеченні ефективного управління силами безпеки.

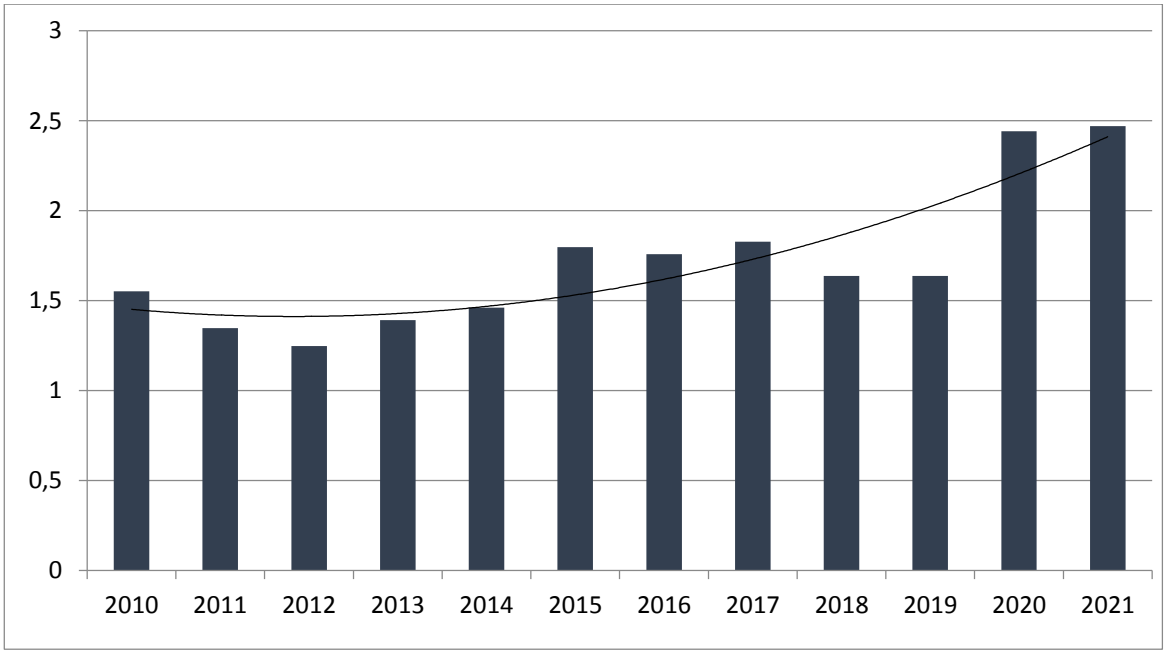

Рисунок 1.5 – Відсоток бюджетних коштів виділених на розвиток програмного забезпечення та баз даних в Україні з 2010 по 2021 роки, тренд змін відсотка

Інформаційна безпека є однією з найважливіших складових національної безпеки. Вона передбачає не лише всебічне і якісне інформування громадян, але й забезпечення їхнього вільного доступу до інформації. Зовнішні загрози, особливо з боку росії, включають дезінформацію та пропаганду, які спрямовані на дестабілізацію суспільно-політичної ситуації в Україні. У цьому контексті розбудова потужної системи інформаційно-аналітичного забезпечення, інтегрованої в національну систему безпеки, є невідкладною необхідністю для протистояння сучасним викликам.

Висновки до розділу 1

1. Проведений аналіз загроз в інформаційній сфері, що спрямовані на державну безпеку України, дозволив визначити ключові функції системи забезпечення інформаційної безпеки країни. Інформаційна безпека в контексті національної безпеки для сил безпеки України розглядається як інтегральний показник, який охоплює такі аспекти, як інформаційно-технічна безпека, протидія кіберзлочинності та інформаційне протиборство. Виділено перелік суб'єктів, які відповідають за виявлення та оцінку інформаційних загроз, а також організовують заходи з протидії цим загрозам. Було розглянуто стратегічні завдання держави, які включають створення та забезпечення функціонування механізмів, що гарантують інформаційну безпеку. Ці механізми передбачають послідовну системну діяльність, впровадження комплексних заходів і створення відповідних державно-правових інституцій, що спрямовані на забезпечення безперешкодної реалізації національних інтересів у інформаційній сфері, захист інтересів громадян і суспільства, а також своєчасне запобігання та оперативне вирішення інформаційних конфліктів.

2. Досягнення та підтримка інформаційної переваги є невід'ємною частиною забезпечення національної безпеки. Це передбачає проведення цілого ряду заходів, спрямованих на нейтралізацію систем управління та прийняття рішень, а також протидію комп'ютерним та інформаційним мережам і системам супротивника. У сучасних умовах новітні інформаційні технології стають основоположним елементом в організації та веденні службово-бойової діяльності сил безпеки. Інформаційна перевага є важливим інструментом, який надає командуванню можливість ефективно використовувати розосереджені сили в ключових операціях, підвищуючи ефективність дій різнорідних силових підрозділів, склад яких найбільш точно відповідає поставленим завданням. Це також дозволяє здійснювати гнучке та цілеспрямоване матеріально-технічне забезпечення, що є критичним для успішного виконання бойових завдань.

3. Світова практика демонструє, що інформаційне навантаження на органи управління постійно зростає, що значно ускладнює процес прийняття управлінських рішень, який вимагає ретельного планування, аналізу і ефективного використання ресурсів. Розглянуто основні підходи до прийняття управлінських рішень, зокрема у контексті інформаційно-аналітичного забезпечення сил безпеки на сучасному етапі. Виявлено ряд проблем, які включають: недостатній рівень розробки нормативно-правової бази у силах безпеки України щодо створення інформаційних ресурсів та продуктів, надання інформаційних послуг та функціонування системи інформаційно-аналітичного забезпечення; відсутність функціональної, технологічної та технічної інтеграції між інформаційно-аналітичними підрозділами сил безпеки; брак єдиної системи класифікації та кодування інформації в силових структурах України; недостатній розвиток загальних інформаційних ресурсів і відсутність інтегрованого банку даних, який має стати важливим елементом загальнодержавної інформаційної інфраструктури. Крім того, відзначається необхідність використання сертифікованого програмно-математичного забезпечення, що вже зарекомендувало себе на практиці, але наразі відсутні сертифіковані засоби захисту інформації. Ще однією проблемою є відсутність чітко визначеного комплексу спеціального програмно-математичного забезпечення для інформаційної діяльності. Важливо також забезпечити підготовку фахівців, здатних працювати з сучасними інформаційно-аналітичними системами, оскільки брак таких спеціалістів негативно впливає на загальний рівень інформаційного забезпечення. Недостатність фінансування, а також відсутність комплексного підходу до організації досліджень, спрямованих на вирішення цих проблем, ускладнюють розвиток ефективної системи інформаційного забезпечення сил безпеки України. На даний момент недостатньо досліджуються такі важливі напрями, як вдосконалення нормативно-правової бази, розвиток інформаційно-аналітичних підрозділів, створення комплексної системи захисту інформації, а також розробка

системних вимог щодо сертифікації засобів інформатизації та інформаційно-телекомунікаційних систем в силових структурах України.

4. Розглянута біполярна модель, яка має у своєму складі два конкуруючих центра управління, що представляються відповідними моделями на декількох рівнях. В основі моделі є складні процеси протистояння двох антагоністичних систем, які вступають між собою в інтелектуальний конфлікт, що передбачається задумами дій сторін. Проведений аналіз моделі дав змогу визначити найбільш важливий аспектуправління, а саме якість прийняття рішення органами управління та контроль виконання поставленихзавдань.

5. Наведена класифікація інформаційних технологій, що використовуються в службово-бойовій діяльності сил безпеки. Визначені показники інформаційно-аналітичного забезпечення сил безпеки, що дозволили якісно оцінити стан системи управління силами безпеки.

6. Інформаційно-аналітичне забезпечення сил безпеки України має специфічні системи підтримки прийняття рішення, імітаційні моделі службово-бойових дій, бази даних та системи розпізнавання об’єктів розшуку. Загальними інформаційними технологіями сил безпеки як суб’єкта державної безпеки є автоматизовані системи управління та системи документообігу.

7. Проведений аналіз проблемних аспектів фінансового забезпечення інформаційно-аналітичного забезпечення, до яких відносяться: швидкі технологічні зміни, іноді державні закупівлі не встигають за потребами оновлення обладнання та програмного забезпечення; існує потреба в кваліфікованих фахівцях, які можуть ефективно працювати з новітніми технологіями, часто зустрічається з обмеженою кількістю таких спеціалістів; збільшення фінансування інформаційно-аналітичного забезпечення вимагає також забезпечення високого рівня захисту даних, що в свою чергу вимагає додаткових витрат. Існує потреба сучасності в забезпеченні адекватного рівня фінансування, оновлення технологічної бази та підготовки кваліфікованих кадрів для зміцнення обороноздатності та захисту держави від сучасних загроз.

8. На сьогоднішній день існує потреба в формуванні вимог дозагальнодержавної інформаційної системи сил безпеки, а у подальшому її створені. Виклики сучасності з якими зіткнулась наша держава потребують негайного вдосконалення системи державного управління. Одним з шляхів вдосконалення системи державного управління є створеннязагальнодержавної інформаційної системи управління силами безпеки.

РОЗДІЛ 2
МЕТОДОЛОГІЧНІ ОСНОВИ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ

2.1 Вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку

Оцінка впливу системи інформаційно-аналітичного забезпечення сил безпеки на державну безпеку України є вкрай складним і багатогранним завданням, яке залежить від безлічі факторів і специфічних умов, в яких вона функціонує. Така система складається з численних компонентів, серед яких варто виділити збір та обробку розвідувальної інформації, аналіз і інтерпретацію даних, кіберзахист, забезпечення координації між різними структурами сил безпеки, і багато інших елементів.

Вплив системи інформаційно-аналітичного забезпечення може бути розглянутий через призму кількох ключових аспектів. По-перше, такі системи відіграють центральну роль у зборі та аналізі розвідувальної інформації, яка є критично важливою для виявлення потенційних загроз національній безпеці. Зокрема, системи інформаційно-аналітичного забезпечення (ІАЗ) сконструйовані для забезпечення високоефективного управління інформацією, що стосується безпеки держави, та сприяють ухваленню стратегічних і тактичних рішень на основі достовірних даних. ІАЗ дозволяють збирати, зберігати та аналізувати різноманітні види даних, такі як інформація з розвідувальних джерел, супутникові знімки, аналітичні звіти та багато іншого. Завдяки використанню аналітичних інструментів, ці системи можуть обробляти великі обсяги структурованих і неструктурованих даних для виявлення потенційних загроз [204, 211].

Застосування геопросторового аналізу дозволяє глибше зрозуміти

географічне розташування інформації та визначити просторові взаємозв'язки, що допомагає у виявленні загроз в реальному часі. Це, своєю чергою, дозволяє оперативно отримувати точні дані для швидкого реагування на виникаючі загрози. Дані, отримані від розвідувальних джерел і проаналізовані через ІАЗ, активно використовуються для розробки стратегічних і тактичних планів, які спрямовані на запобігання або мінімізацію загроз. Крім того, забезпечення ефективного обміну інформацією між різними відомствами та військовими структурами створює можливість для спільного розуміння ситуації і скоординованого реагування на загрози.

Використання сучасних технологій, таких як штучний інтелект, машинне навчання та аналіз даних в режимі реального часу, сприяє автоматизації процесів аналізу і виявлення загроз, що значно підвищує рівень ефективності інформаційно-аналітичного забезпечення. Такі системи відіграють критично важливу роль у підвищенні рівня обізнаності та адекватної відповіді на розвідувальну інформацію, що стосується державної безпеки.

Крім того, забезпечення кібербезпеки та захисту важливих інформаційних ресурсів і критичної інфраструктури є ключовими завданнями для запобігання атакам та ефективного реагування на кіберзагрози. Інформаційно-аналітичні системи можуть використовуватися для постійного моніторингу безпеки критичних об'єктів і інфраструктури, що дозволяє вчасно виявляти та усувати потенційні загрози. Аналітичні інструменти також можуть сприяти ефективному управлінню кризовими ситуаціями та прийняттю рішень на основі комплексних даних із різних джерел.

Забезпечення належної координації та взаємодії між різними силами безпеки, такими як армія, поліція та розвідувальні служби, може значно підвищити загальний рівень безпеки країни. Інформаційно-аналітичні системи можуть відігравати вирішальну роль у запобіганні та ефективному реагуванні на різноманітні загрози, включаючи тероризм, злочинність та інші небезпеки.

Водночас слід враховувати, що ефективність системи інформаційно-аналітичного забезпечення може бути суттєво знижена у разі недостатньої

координації дій, недостатньої підготовки персоналу або ж відсутності сучасних технологій. Крім того, ці системи повинні суворо дотримуватися принципів конфіденційності та приватності, щоб уникнути можливих зловживань отриманою інформацією.

Дослідження питання впливу стану системи інформаційно-аналітичногозабезпечення сил безпеки України на державну безпеку в роботі пропонується за допомогою діаграми Ісікави. Діаграма дозволяє виявити ключові взаємозв'язки між різними факторами й більш точно зрозуміти досліджуваний процес. Діаграма сприяє визначенню головних факторів, що роблять найбільш значний вплив на розвиток розглянутої проблеми, а також попередженню або усуненню дії даних факторів. На рисунку 2.1 представлена розроблена діаграма Ісікави, яка дозволяє оцінити вплив факторів на ІАЗ СБД сил безпеки України.

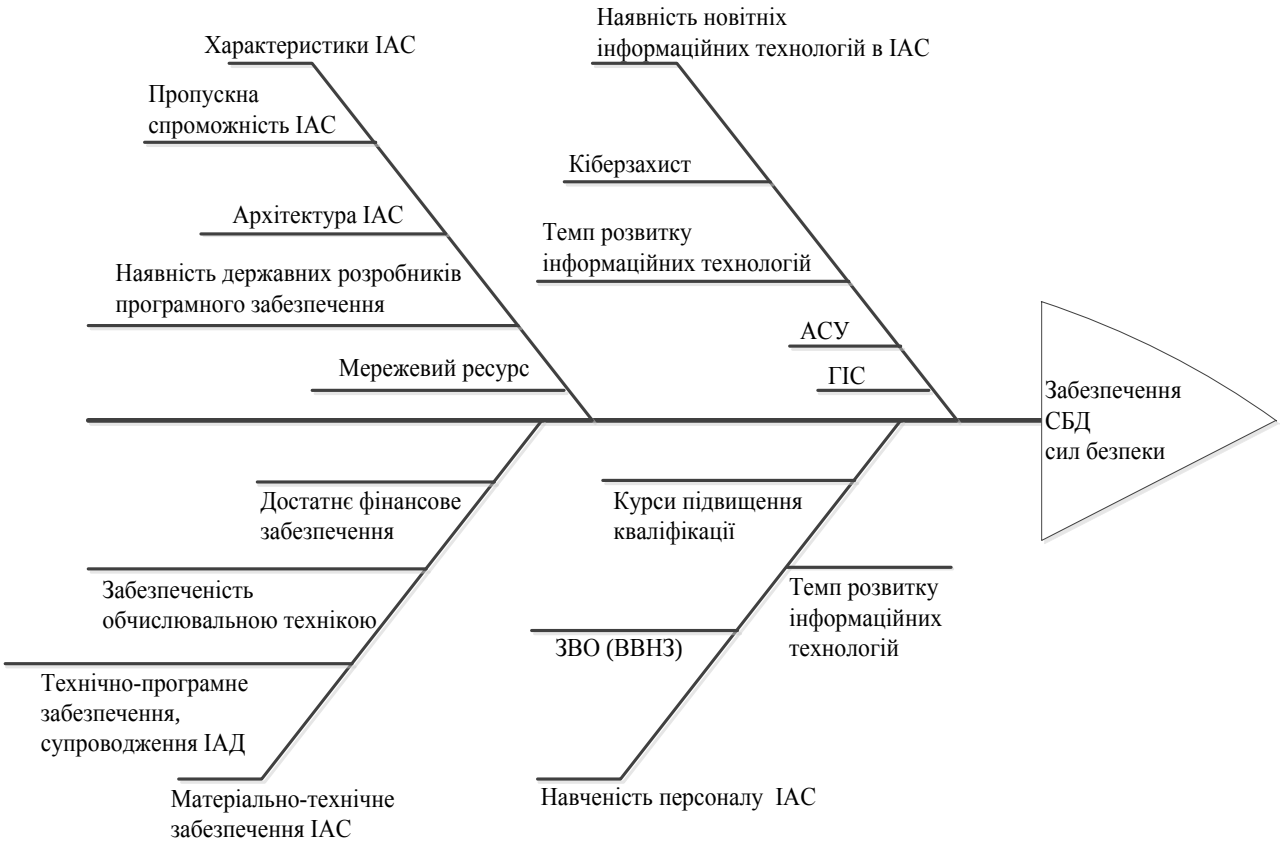

Рисунок 2.1 – Вплив факторів на інформаційно-аналітичне забезпечення сил безпеки України [14]

Основною групою факторів, що об’єднує та описує наявність інформаційних технологій у системі інформаційно-аналітичного забезпечення діяльності сил безпеки, є група, яка включає такі важливі елементи, як система кіберзахисту. Ця система може складатися з підсистем шифрування, обмеження доступу, програмно-технічних модулів захисту інформації. Додатково до цієї групи входять засоби автоматизації управління (АСУ) та геопросторовий аналіз (ГІС). Значущим фактором, який позитивно впливає на розвиток інформаційно-аналітичних систем (ІАС), є темп розвитку інформаційних технологій, який залежить від досягнень у таких фундаментальних галузях науки, як фізика, хімія та інші. Цей фактор відіграє ключову роль у сприянні розвитку ІАС, забезпечуючи поступове вдосконалення технологічної бази.

До іншої групи факторів належить навченість персоналу, відповідального за роботу ІАС. Ця група включає освітні заклади вищої освіти та курси підвищення кваліфікації. Темп розвитку інформаційних технологій у даному контексті виступає як фактор, що може знижувати ефективність навчання, оскільки швидкоплинні зміни у галузі інформаційних технологій, а також поява нових технологій створюють потребу в постійному підвищенні кваліфікації персоналу, який працює з ІАС.

Третя група факторів пов’язана з матеріально-технічним забезпеченням ІАС. До цієї групи входять такі елементи, як фінансове забезпечення ІАС, наявність необхідної обчислювальної техніки та програмно-технічних засобів, а також забезпеченість технічним супроводженням програмного та математичного забезпечення ІАС.

Четверта група факторів охоплює характеристики самої ІАС, що більше стосуються її технічних параметрів. Сюди входять пропускна здатність ІАС, тобто кількість одночасно оброблюваних завдань і обсяг інформації, який здатна обробляти система; архітектура ІАС, яка включає методи та способи побудови системи; наявність вітчизняних розробників програмного забезпечення; та розвинена мережа зв’язку в країні, яка також є важливою складовою.

Додатково слід звернути увагу на стан інформаційно-аналітичного забезпечення (ІАЗ) у різних суб'єктах сил безпеки. Використання ІАЗ під час прийняття рішень у процесах виконання службово-бойових завдань стає надзвичайно важливим аспектом сучасного управління. Вимоги до підвищення ефективності ІАЗ вимагають впровадження новітніх інформаційних технологій [41, 89, 92, 130, 229, 274, 285, 286, 290, 299]. Для подальшого розвитку ІАЗ сил безпеки передбачається створення і застосування сучасних інформаційно-аналітичних систем, основним завданням яких є збір, накопичення, зберігання, динамічне відображення та багатовимірний аналіз накопичених і поточних даних, а також аналіз тенденцій, моделювання і прогнозування наслідків різних управлінських рішень. На сьогоднішній день ІАС може виступати як ефективний інструмент підтримки управлінських рішень, надаючи користувачам необхідну інформацію візуально та оперативно для аналізу ситуації та прийняття рішень.

У всій системі Міністерства внутрішніх справ України (МВСУ) на даний момент практично відсутні ІАС, здатні конструктивно підтримувати прийняття ефективних рішень під час планування та виконання оперативних завдань [195, 228, 299], використовуючи при цьому усі необхідні інформаційні джерела.

Під застосуванням сил безпеки розуміють складові службово-бойових дій суб'єктів сил безпеки, що охоплюють як теорію, так і практику підготовки і ведення оперативних та спеціальних дій (спеціальних операцій) силами безпеки, оперативними резервами оперативно-територіальних об'єднань, з'єднань і частин НГУ, ДПСУ, у складі тимчасово об'єднаних угруповань відомчих або різновідомчих сил, оперативно-розшукову діяльність. Ці завдання відрізняються важливістю цілей, масштабом та тривалістю, виконуються зазвичай за надзвичайних обставин, поза пунктами постійної дислокації, з максимальним напруженням та використанням сил і засобів, іноді одночасно в декількох регіонах країни [228].

Досвід застосування сил безпеки в умовах кризових ситуацій, що виникають за надзвичайних обставин, дозволяє виділити загальні етапи їх дій.

Ці етапи включають: передислокацію сил і засобів до районів виконання завдань та створення різнорідних угруповань; безпосереднє проведення оперативних і спеціальних дій, таких як спеціальні операції, у зонах конфліктів, під час надзвичайних ситуацій або в умовах воєнного стану; та завершальний етап, що передбачає поступове або одночасне виведення сил безпеки до місць постійної дислокації або їхню заміну чи доукомплектування новими підрозділами.

Ефективність дій військових формувань на всіх цих етапах значною мірою залежить від якості та оперативності прийнятих рішень. На першому етапі, ключовим показником ефективності є швидкість прийняття оптимальних рішень щодо залучення оперативних резервів сил безпеки в умовах складної, швидкоплинної і часто неповно визначеної оперативної ситуації. Також важливою є оперативність зосередження цих резервів у визначених районах, відповідно до прийнятого рішення.

Забезпечення оперативного управління, особливо в умовах раптового ускладнення ситуації, де задіяні сили безпеки, є одним із найважливіших завдань органів військового управління. Для оптимізації цього процесу необхідне впровадження сучасних інформаційно-аналітичних систем (ІАС), побудованих на трансдисциплінарному підході.

Експертна аналітична діяльність, що підтримує процес прийняття рішень із залученням сил безпеки, базується на інформаційних ресурсах, які включають не лише дані про службово-бойові завдання, але й широкий спектр інформації з різних джерел, включаючи засоби масової інформації, зокрема Інтернет-видання. Проте без належних аналітичних сервісів ці ресурси залишаються пасивними елементами інформаційного простору сил безпеки України. Неналежна обробка цих ресурсів обмежує їх інтеграцію і суттєво знижує ефективність їх використання, що відображається у сучасному стані інформаційно-аналітичного забезпечення сил безпеки.

Для підвищення ефективності обробки такої інформації необхідне програмно-інформаційне забезпечення, здатне реалізовувати інтелектуальні

когнітивні сервіси для інтегрованого аналітичного оброблення даних службово-бойових завдань. Це повинно включати обробку змісту масових видань, взаємодію з лінгвістично-семантичним та концептографічним контент-аналізом, а також забезпечувати структуроване відображення результатів для використання у всіх системних компонентах, таких як властивості, функціональні характеристики та міжсистемні зв'язки.

Проведений аналіз автоматизації процесів підтримки прийняття рішень щодо застосування сил безпеки показав, що на кожному з напрямів уже створені окремі компоненти інформаційних систем. Однак вони значно відрізняються за часом розробки, ступенем завершеності, використаними технологіями, масштабом охоплення процесів, обсягом розгортання та наповнення даними, а також можливістю інтеграції до єдиного інформаційного середовища. Ця інтеграція має враховувати когнітивний підхід до оброблення інформаційних ресурсів, а також принципи та стандарти, що прийняті в Євросоюзі та НАТО [87, 228, 261, 281].

Сучасний стан інформаційно-аналітичної інфраструктури, яка повинна задовольняти потреби керівного складу структурних сил безпеки, значно відстає від вимог, що диктуються сьогоденними викликами. Це особливо критично під час підтримки процесів прийняття рішень щодо застосування сил безпеки. Наявна інтеграція інформаційних систем за різними напрямами є фрагментарною або взагалі відсутня, що не враховує сучасних вимог до консолідації [21, 123]. Це призводить до дублювання інформації, недостатньої достовірності та неповноти даних, що суттєво ускладнює комплексне управління процесами виконання службово-бойових завдань.

Додатково існує ряд невирішених питань: відсутність єдиних методологічних, науково-технічних та організаційних принципів і обґрунтованих підходів до створення інформаційно-аналітичних систем (ІАС) та впровадження сучасних когнітивних інформаційних технологій; нестача єдиних стандартів обміну даними між інформаційними системами, які б забезпечували взаємодію та інтероперабельність; слабка розробленість заходів

із захисту інформаційних ресурсів; недостатньо розгалужені інформаційно-телекомунікаційні мережі та обмежена пропускна здатність каналів передачі даних; організаційна розпорошеність і функціональна ізольованість існуючих інформаційних систем; недосконалість нормативно-правової бази, що регулює життєвий цикл інформаційних систем у Міністерстві внутрішніх справ України (МВСУ) та Національній гвардії України (НГУ); відсутність єдиної організаційної та мережецентричної інформаційно-технологічної платформи з компонентною архітектурою когнітивних сервісів, яка б забезпечувала семантичну операціональність взаємодії з інформаційними ресурсами [286].

Вирішення цих проблем, пов'язаних із невідповідністю сучасним вимогам інформаційно-аналітичного забезпечення (ІАЗ), потребує розробки комплексу цілеспрямованих заходів, які мають бути скоординовані за часом і обсягами. Ці заходи повинні бути спрямовані на створення сучасної інтелектуальної інформаційно-аналітичної системи (ІАС) в інтересах сил безпеки. Основою цієї системи має стати компонентний підхід до створення агрегованих когнітивних сервісів підтримки прийняття рішень, а в перспективі – формування єдиної інформаційної інфраструктури сил безпеки.

Такі зміни дозволять забезпечити необхідний рівень оперативності, достовірності та повноти інформації, що необхідна для прийняття управлінських рішень у процесі оперативного застосування сил. На основі досвіду та враховуючи вище зазначене, розвиток ІАЗ доцільно здійснювати за такими основними напрямами [21, 46, 83, 123, 227]: впровадження передових інформаційних технологій для прийняття рішень під час виконання службово-бойових завдань; створення нових технічних рішень під час розробки або модернізації ІАС; розвиток і вдосконалення інформаційної інфраструктури сил безпеки з урахуванням національних та міжнародних стандартів; створення ІАС, які забезпечать ефективну взаємодію між наявними і новоствореними інформаційними системами; використання гнучких технологічних платформ для впровадження ІАС; забезпечення відмовостійкості та катастрофостійкості розроблюваних ІАС; впровадження механізмів автоматичної ідентифікації та

автентифікації користувачів ІАС, регламентованого доступу і обміну даними, забезпечення належного рівня захисту інформації від зовнішніх і внутрішніх загроз; удосконалення організаційної структури розроблюваних ІАС.

Створення єдиної інформаційної інфраструктури сил безпеки повинно бути реалізовано на основі принципів відкритих таксономій [21, 46, 83, 123, 227]. Це надасть можливість визначити технологічні умови для консолідованого використання всіх доступних інформаційних ресурсів у процесах прийняття рішень та взаємодії з ними в мережевому середовищі.

Таксономічне відображення системології інформаційних ресурсів забезпечить об'єктивність та високу валідність результатів семантичного аналізу інформації, а також створить передумови для формування онтологічних експертних платформ для оцінки ситуацій та прийняття рішень [232, 286].

Інформаційно-аналітичні системи, що створюються в різних сферах управління, повинні бути орієнтовані на задоволення потреб суспільства в контексті предметно-орієнтованого розвитку, а також враховувати перспективи та завдання формування інформаційного суспільства, де знання виступають рушійною силою людства [113, 136, 138, 144, 227]. У сучасних умовах застосування ІАЗ дозволяє підвищити ефективність управління організацією або установою завдяки об’єктивізації аналітичної діяльності та використанню допоміжних пошукових і експертних інструментів.

Проблематика аналізу початкової або накопиченої інформації значною мірою пов’язана з необхідністю адекватної обробки великих масивів даних. Відповідно до сучасних концепцій ІАЗ, ІАС повинні проектуватися і функціонувати з урахуванням таких ключових аспектів: вибір з різних джерел різнорідних даних, представлених у різних форматах, та їх приведення до єдиного формату і структури; акумулювання інформації, створення великих баз даних, застосування технологій індексації і пошуку; організація надання користувачам необхідної інформації для прийняття рішень, реалізації заходів або програмних дій у сфері їх основної діяльності; використання інструментів оперативного та інтелектуального аналізу, підготовка планового та регулярного

оцінювання стану об'єктів управління, а також надання досліджень у вигляді документальних матеріалів і електронних оглядів та звітів; представлення інформації та результатів аналізу в зручному для користувачів форматі для ефективного сприйняття [10].

Ці аспекти накладають додаткові вимоги на ІАС: підсистеми отримання інформації повинні мати можливість ідентифікувати, аналізувати і верифікувати географічну інформацію, зокрема координати і адреси; система повинна мати здатність перетворювати адреси в географічні координати (виконувати геокодування); внутрішній формат представлення інформації має підтримувати зберігання географічних даних (наприклад, у вигляді текстового рядка з координатами, які згодом можуть бути оброблені електронною картою); одним з форматів представлення інформації користувачам повинна бути електронна карта або повинна існувати можливість перетворення даних у формат, сумісний з існуючими ІАС.

Аналіз стану розвитку інформаційних систем на даний момент дозволяє виокремити три основні проблеми, що потребують вирішення для ефективного створення та впровадження ІАС [176, 193, 194, 195, 229, 255, 256, 257, 258, 259, 281, 286, 297].

По-перше, слід зазначити недосконалість механізмів реалізації інтерактивних сервісів для експертів і користувачів. Це пов’язано з високою гетерогенністю технічних платформ з одного боку та суттєвими відмінностями у рівні підготовки, спеціалізації осіб, що приймають рішення, операторів і споживачів інформації – з іншого.

По-друге, існує відсутність ефективних процедур, механізмів, алгоритмів та методик для використання інтелектуальних засобів обробки інформаційних ресурсів у предметній області. До таких засобів належать, зокрема: контент-аналіз та структурування мережевих інформаційних масивів, агрегування контекстів до обробки інформації; недосконалість механізмів інтеграції засобів здобування та формування знань про керовані процеси; виявлення та ідентифікація латентних об’єктів і процесів у мережецентричному

гіперінформаційному просторі.

По-третє, майже повністю відсутні механізми консолідації інформаційних ресурсів та документів, які використовуються в процесах ухвалення управлінських рішень.

Зупинимося на стані інформаційно-аналітичного забезпечення (ІАЗ) суб'єктів сил безпеки України. На сьогодні для потреб Національної гвардії України (НГУ) розроблено ряд програмних засобів, які частково автоматизують (лише окремі етапи) процес прийняття рішень під час використання угруповань НГУ. До таких засобів належать як локальні, так і мережеві програмні рішення.

До локальних програмних засобів можна віднести [6]: програмні комплекси «Оцінка», «Динаміка», «Розрахунок особового складу угруповання по військовим нарядам», «Визначення кількості особового складу для охорони особливо важливих державних об'єктів», «Пошук»; штатну математичну модель «Ешелон»; інформаційно-розрахункові системи «Варіант» і «Оберіг»; автоматизовану систему «Підтримка»; геоінформаційні системи «Аргумент» і «Інструмент».

Прикладами мережевих програмних комплексів є автоматизована система управління українськими військово-морськими силами «Херсонес» та глобальна автоматизована інформаційна система «Гарт» Державної прикордонної служби України. Вони дозволяють автоматизувати процеси збирання, зберігання та первинного оброблення неструктурованих різнорідних даних [87, 261]. У Дніпрі функціонує, поки ще, єдиний в Україні командний центр безпеки регіону, що здійснює відео спостереження за адміністративними кордонами області та фіксує всі автомобілі, які перетинають межі області [5, 23].

Запровадження таких систем створило умови для оперативного збирання та обробки інформації, підтримання в актуальному стані баз даних загальної, директивної інформації, а також інформації, необхідної для планування та оперативного використання угруповань НГУ. Як вже зазначалося, однією з ключових проблем ефективного використання таких систем для підтримки

прийняття рішень є відсутність єдиного інформаційного простору.

Отже, необхідність створення ІАС для НГУ обумовлена, з одного боку, об'єктивним процесом інформатизації суспільства та розвитком НГУ, а з іншого боку – відставанням у розвитку засобів інформатизації та новітніх інформаційних технологій у НГУ порівняно з загальнодержавним рівнем і рівнем силових структур провідних країн світу [192].

Сучасні поліцейські сили зазвичай використовують ІАС для підтримки оперативно-аналітичної роботи, обробки інформації, ведення баз даних та прийняття рішень. Ці системи можуть включати інструменти для аналізу кримінальної статистики, розслідування злочинів, обробки даних про взаємодію з громадськістю, технічної підтримки спеціальних операцій та інших завдань. Важливо, щоб такі системи відповідали принципам конфіденційності, безпеки та захисту прав людини. Однією з основних функцій цих систем може бути полегшення роботи правоохоронних органів, сприяння прозорості інформації та підвищення загальної безпеки в суспільстві.

Визначальною складовою створення інформаційно-аналітичного забезпечення діяльності всіх підрозділів Національної поліції України (НПУ) є єдина інформаційна система Міністерства внутрішніх справ України (ЄІС МВС). Ця багатофункціональна інтегрована автоматизована система забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супровід їхньої діяльності. ЄІС МВС представляє собою сукупність взаємопов'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів електронної комунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, а також внутрішню та зовнішню інформаційну взаємодію. Це унормовано в межах Положення про єдину інформаційну систему Міністерства внутрішніх справ, затвердженого постановою Кабінету Міністрів України від 14.11.2018 року № 1024 [156]. ЄІС МВС надає можливість ефективного функціонування підрозділів системи МВС, які є її складовими або чия діяльність координується цим центральним органом влади.

Таким чином, комплекс технічних засобів і програмних комплексів, що автоматизують службові процеси підрозділів до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, формує, зберігає, спільно використовує і верифікує інформаційні ресурси ЄІС МВС, які доцільно визначати як функціональні підсистеми ЄІС МВС. Важливим елементом функціонування всіх зазначених підсистем є обсяг інформаційних ресурсів, який складається із сукупності взаємопов'язаних задокументованих одиниць інформації, що формуються та об'єднуються в автоматизованих інформаційних системах суб'єктів ЄІС МВС за певними критеріями. Це включає також ті ресурси, що зазначені в переліку пріоритетних інформаційних ресурсів ЄІС Міністерства внутрішніх справ [93, 108, 254].

Крім того, відповідно до статті 27 Закону [162], поліція має доступ до інформаційних ресурсів інших органів державної влади, включаючи решту пріоритетних інформаційних ресурсів МВС. Ці ресурси можуть бути об'єктом опрацювання в межах компетенції підрозділів Національної поліції України, навіть якщо остання не є суб'єктом ЄІС МВС щодо цих інформаційних ресурсів. Це стосується, зокрема, даних з Єдиного державного реєстру транспортних засобів, Реєстру адміністративних правопорушень у сфері безпеки дорожнього руху, інтегрованої інформаційно-пошукової системи, національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, Єдиного реєстру досудових розслідувань, Єдиного державного реєстру судових рішень та багатьох інших. Додатково до цього слід віднести облік вогнепальної зброї, дактилоскопічний облік, криміналістичний облік експертної служби та персонально-довідковий облік. Наведений перелік не є вичерпним, оскільки навіть Положення виділяє серед них як пріоритетні, так і інші інформаційні ресурси.

Однією з функціональних підсистем ЄІС МВС є інформаційний портал Національної поліції України, який функціонує згідно з Положенням про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» [141]. Завданнями цього порталу є:

– забезпечення інформаційно-аналітичної підтримки діяльності Національної поліції України;

– наповнення та підтримка в актуальному стані інформаційних ресурсів баз даних, що входять до ЄІС МВС;

– підтримка щоденної діяльності органів поліції у сфері трудових, фінансових, управлінських відносин і документообігу;

– забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Отже, підтримка функціонування цієї підсистеми ЄІС МВС є основним завданням підрозділів інформаційно-аналітичної підтримки Національної поліції України. Ця підтримка реалізується через такі дії:

– формування інформаційних ресурсів ЄІС МВС;

– обробка інформації, отриманої під час діяльності поліції;

– аналітична обробка даних з автоматичної фото- і відеотехніки;

– забезпечення оперативного доступу до інформаційних ресурсів ЄІС МВС;

– генерація інтерфейсів та вебсервісів для інформаційної взаємодії органів поліції з іншими державними органами, органами правопорядку іноземних держав, міжнародними організаціями;

– здійснення пошукових і аналітичних функцій для використання даних з баз даних поліції, МВС та інших органів державної влади відповідно до рівня доступу та повноважень;

– застосування програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичного оновлення зображення об’єктів залежно від зміни їх характеристик, зміни масштабу та деталізації картографічної інформації;

– забезпечення автоматизації процесів управління силами та засобами поліції;

– організація електронного документообігу в органах поліції та обміну електронними документами з МВС;

– забезпечення комплексного захисту інформації та обмеження доступу до даних, що зберігаються в базах системи ІПНП.

Враховуючи вищезазначене, інформаційні ресурси ІПНП, окрім ресурсів ЄІС МВС, включають також дані, що утворюються в процесі діяльності поліції. Вони використовуються для формування баз даних, необхідних для управлінських відносин, виконання повноважень поліції, а також для підтримки її щоденної діяльності у сфері трудових відносин, фінансового забезпечення та документообігу.

Інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» [140] є структурованою автоматизованою базою даних, що використовується для збору, зберігання, обліку, пошуку, узагальнення, захисту, перевірки достовірності даних, їх перетворення та відображення, а також для забезпечення доступу до інформації про притягнення особи до кримінальної відповідальності, наявність або відсутність судимості та обмежень, передбачених кримінальним процесуальним законодавством України.

Згідно з пунктом 5 [140] Департамент інформатизації Міністерства внутрішніх справ України відповідає за наступні завдання:

– методичне та методологічне забезпечення функціонування інформаційно-аналітичної системи (ІАС);

– проведення аналізу структури та змісту інформаційних ресурсів ІАС з метою підвищення рівня інформаційної взаємодії з іншими державними інформаційними системами;

– перевірка повноти та актуальності відомостей, що містяться в ІАС, та вжиття заходів щодо усунення виявлених недоліків у роботі системи;

– визначення механізмів інформаційного обміну;

– моніторинг та аналіз якості функціонування ІАС;

– здійснення контролю за дотриманням користувачами ІАС вимог законодавства щодо доступу до інформаційних ресурсів у межах їхніх повноважень;

– корегування інформації, що зберігається в ІАС;

– впровадження та модернізація програмного забезпечення з централізованою технологією обробки запитів фізичних осіб за допомогою ІАС, що дозволяє формувати витяги в електронному вигляді;

– надання користувачам можливості віддаленого доступу до ІАС через спеціалізоване програмне забезпечення, що дозволяє надсилати запити та отримувати відомості з бази даних;

– ведення електронного реєстру запитів, отриманих через віддалені робочі місця, та витягів в електронному вигляді;

впровадження та модернізація сервісу для перевірки достовірності виданих витягів на офіційному вебсайті МВС [140].

Ця система відіграє ключову роль у забезпеченні належного рівня обліку та обробки інформації щодо притягнення осіб до кримінальної відповідальності, надаючи користувачам зручний доступ до достовірних даних, необхідних для виконання їхніх повноважень та прийняття обґрунтованих рішень.

Однією з сучасних інформаційних технологій є OSINT. OSINT (від англійської Open-Source Intelligence) - це метод збору інформації, який базується на використанні відкритих джерел. Це включає в себе збір, аналіз та інтерпретацію даних, які доступні громадськості або вільно розповсюджуються.

Основна ідея OSINT - використання інформації, яка вже існує в відкритому доступі, такі як публічні звіти, веб-сайти, соціальні мережі, новини, фотографії, відео та інше, для отримання розуміння конкретної ситуації або визначення різних аспектів певної теми. На сьогоднішній день використовується під час розвідувальної діяльності Службою безпеки України (СБУ).

До основних джерел OSINT можна віднести:

- ЗМІ: Газети, журнали, телебачення та радіо, які можуть надавати інформацію про події, людей і тенденції.

- Інтернет: Веб-сайти, блоги, новинні портали та інші онлайн-ресурси. Це також включає бази даних, такі як ті, що використовуються для наукових досліджень або ринкових аналізів.

- Соціальні мережі: Профілі та дописи на платформах, таких як Facebook, Twitter, LinkedIn, де користувачі діляться особистою інформацією, думками та новинами.

- Геопросторові дані: Відкриті дані про місцезнаходження, отримані через такі сервіси, як Google Maps або OpenStreetMap.

- Відеоматеріали та зображення: Відео та фотографії, які користувачі або компанії публікують онлайн.

- Державні та муніципальні ресурси: Офіційні публікації, законодавчі та регуляторні бази даних, публічні записи.

Процес OSINT може включати наступні етапи: планування та визначення цілей – чітке розуміння, що саме потрібно дізнатися, і формулювання конкретних питань, на які треба знайти відповіді; збір інформації – використання різних інструментів та методів для пошуку і збору даних з відкритих джерел; обробка та аналіз – відсіювання нерелевантної інформації, перевірка достовірності фактів, аналіз зібраних даних для отримання цінних інсайтів; оцінка та інтерпретація – визначення важливості інформації та її можливого впливу на вирішення поставлених задач; розподіл або доповідь – представлення отриманих даних зацікавленим сторонам у формі звітів, презентацій або інформаційних бюлетенів.

Для ефективного виконання OSINT аналітики використовують різноманітні інструменти, які можуть включати:

- Пошукові системи: Google, Bing, Yandex та інші;

- Спеціалізовані пошукові інструменти: Shodan (пошук в інтернеті речей), Foca (для аналізу метаданих);

- Інструменти для аналізу соціальних мереж: Maltego, Hootsuite;

- Геопросторові аналітичні інструменти: Google Earth, ArcGIS;

- Інструменти для збору даних з веб-сайтів: Scrapy, Import.io.;

OSINT несе в собі певні ризики і обмеження, такі як можливість отримання неправдивої або маніпулятивної інформації, проблеми з її актуальністю або повнотою, а також юридичні та етичні питання доступу до даних.

Розвиток технологій і зростання кількості відкритих даних робить OSINT незамінним інструментом у багатьох сферах, включаючи безпеку, розвідку та бізнес. Однак для ефективного використання OSINT необхідно не тільки використовувати сучасні технічні засоби, але й розуміти можливі ризики та вміти критично оцінювати інформацію.

Інформаційно-аналітична діяльність у Державній прикордонній службі України (ДПСУ) передбачає роботу посадових осіб та органів управління, спрямовану на отримання, обробку та перетворення інформації у форми, необхідні для обґрунтування і прийняття управлінських рішень у сфері захисту і охорони державного кордону (ДК) [43, 82, 85, 86].

Сутність інформаційно-аналітичного забезпечення полягає в організації процесів збирання, передавання, обробки, накопичення, зберігання, захисту, пошуку, перетворення та розповсюдження інформації з метою вирішення оперативно-службових та інших завдань. Це включає формування інформаційних ресурсів ДПСУ, надання необхідної інформації споживачам для виконання їхніх функціональних обов’язків, розробку прогнозів щодо розвитку ситуації на державному кордоні, як у підрозділах, так і навколо них. Інформаційно-аналітична діяльність також спрямована на вироблення варіантів ефективних управлінських рішень, визначення стратегії і тактики діяльності підрозділів, органів і управлінь ДПСУ, а також оцінку відповідності їхніх дій поточним умовам обстановки [43, 82, 85, 86].

До основних вимог, що висуваються до інформаційно-аналітичного забезпечення, належать: наукова обґрунтованість оцінки подій і явищ, оперативність отримання, збору та обробки інформації, безперервність інформаційних потоків, достовірність отриманих даних, системність у висвітленні проблем, конфіденційність аналітичних процедур, своєчасність

інформування керівництва про важливі проблеми, а також чітке визначення цілей та інтересів посадових осіб, які можуть використовувати аналітичну інформацію [2, 71, 127].

Основними принципами, що застосовуються в процесі інформаційно-аналітичної роботи, є:

– наявність чітко визначеної мети, що дозволяє сформувати масштаб, форми і методи аналітичної роботи;

– точне та однозначне визначення понять, яке дозволяє встановити конкретний зміст кожного терміна;

- використання різних джерел інформації, що дозволяє оцінити можливості та межі використання кожного з них, ступінь довіри до них і низку інших аспектів [2, 71, 127].

Основними складовими інформаційно-аналітичного забезпечення є сили, засоби, методи і дії (табл. 2.1).

Таблиця 2.1– Складові інформаційно-аналітичного забезпечення ДПСУ

Сили	Засоби	Методи	Дії
1. Органи управління та підрозділи ДПСУ. 2. Інформаційно-аналітичні підрозділи ДПСУ (управління, відділи, відділення тощо). 3. Інформаційно-аналітичні підрозділи інших суб'єктів інтегрованого управління кордонами	1. Засоби масової інформації. 2. Інтернет. 3. Інтранет. 3. Внутрішні та зовнішні бази даних. 4. Внутрішня звітна та облікова документація.	1.Кількісні 2. Якісні. 3. Змішані.	1. Активні: участь у нарадах, семінарах, конференціях, бесіда, опитування, спостереження тощо. 2. Пасивні: аналіз інформації зі ЗМІ, Інтернету, документації тощо.

Інформаційно-аналітичне забезпечення є одним із ключових напрямів діяльності ДПСУ, спрямованим на забезпечення ефективної охорони та захисту державного кордону. Це досягається шляхом підготовки інформації, на основі якої керівник може приймати обґрунтовані рішення в умовах значної невизначеності обстановки на кордоні. Завдяки цьому суттєво знижуються ризики, різного роду втрати, витрати на підготовчі заходи, а також підвищується ефективність і результативність оперативно-службової діяльності ДПСУ. Успішність застосування того чи іншого методу та позитивний результат значною мірою залежать від виду, обсягу та достовірності вихідних даних. Тому важливо створити систему для формалізації, збору, зберігання та видачі даних у ДПСУ. Для впровадження запропонованих підходів необхідна розробка адекватних моделей, методів та методик інформаційно-аналітичного забезпечення.

2.2 Досвід функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу

Після Другої світової війни розвиток теорії управління військами в США значною мірою був зумовлений впливом нових наукових дисциплін, які виникли ще в попередньому столітті. Однією з таких дисциплін стала кібернетика, засновником якої був Норберт Вінер, а також системний аналіз, дослідженням якого активно займалася відома компанія RAND Corporation [236].

У теоретичних та нормативних розробках, спрямованих на вдосконалення управління військовими силами, особливу популярність здобула теорія управління, запропонована Джоном Бойдом, яка відома під назвою «петля OODA» (Observation, Orientation, Decision, and Action) [269, 272]. Ця концепція управління протягом багатьох років слугувала основою для наукового аналізу та навчання на різних рівнях військового управління—тактичному, оперативному та стратегічному.

Теорія Джона Бойда стала однією з трьох ключових концепцій, які лягли в основу розробки теорії застосування Військово-Повітряних Сил США. Вона доповнювалася теорією паралельної війни та моделлю п’яти кілець, запропонованою Джоном Ворденом [269, 272].

Значною мірою популярність концепції петлі OODA пояснюється її інтуїтивною простотою та легкістю сприйняття. Для ілюстрації своєї ідеї Джон Бойд порівнював раціональну поведінку людини або організації з процесом вирішення чотирьох основних завдань: спостереження, орієнтації, прийняття рішення та дії. Він об’єднав ці етапи в єдиний цикл прийняття рішень, назвавши його петлею OODA (Observation, Orientation, Decision, and Action) (рис. 2.2).

Згодом Бойд узагальнив цю концепцію до рівня загальної теорії конфлікту, яка стала застосовною як на оперативному, так і на тактичному рівнях управління військами. Він також розглядав маневрову або швидкоплинну війну як важливий аспект своєї теорії, підкреслюючи її значення для ефективного управління в умовах сучасних військових конфліктів.

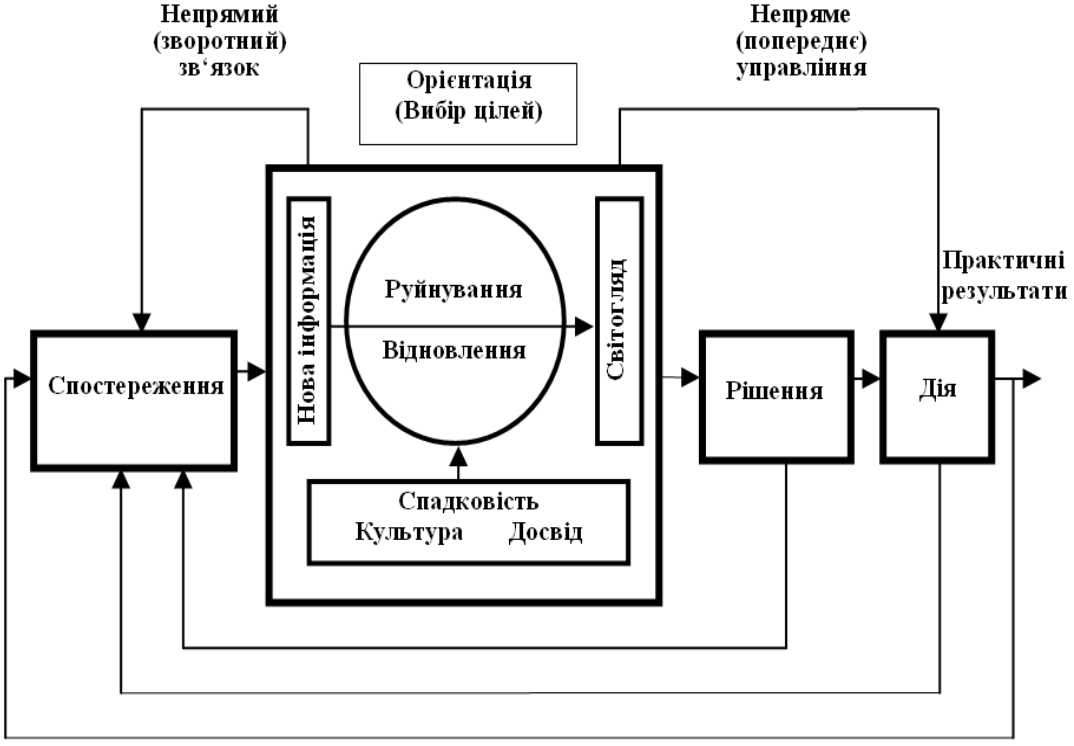

Рисунок 2.2 – Схема концепції управління (петлі Дж. Бойди) OODA [233]

Згідно з цією теорією, основна мета війни полягає в зломі морального та психологічного стану противника, створенні для нього умов, що викликають раптовість, дезорієнтацію, та загрозливі оперативні й стратегічні ситуації. Для досягнення цього необхідно діяти з більшою швидкістю та рішучістю, ніж противник. Іншими словами, мета маневреної війни полягає в тому, щоб позбавити ворога можливості адаптуватися до швидко змінюваних і невизначених умов бойових дій, не дозволяючи йому розгорнути свої сили для ефективної відповіді. Бойові операції спрямовані на створення та підтримання стану постійної невизначеності та небезпеки для ворога; на порушення його організаційних структур або на їх руйнування; на зниження бойових можливостей противника, що унеможливлює його пристосування до нових умов.

Аналізуючи минулу і сучасну військову історію, Дж. Бойд виділив чотири ключові характеристики успішних дій: ініціативу, координацію, різноманітність підходів та швидкість виконання. Для досягнення максимальної ефективності необхідно планувати різноманітні способи атак на ворога, які можуть бути виконані з максимальною швидкістю.

На оперативному рівні, при плануванні бойових дій, важливо спрямувати зусилля на руйнування здатності противника виконувати початкові та подальші плани операцій і бойових дій. Оперативна мета повинна бути зосереджена на порушенні здатності противника обробляти інформацію, приймати рішення та виконувати відповідні дії. З часом це призведе до того, що противник не зможе оцінити та зрозуміти, що відбувається проти нього, і не буде здатний адекватно реагувати. Зрештою, це погіршить його положення, що може призвести до втрати бойової спроможності або змусити припинити опір.

Технологічні та організаційні аспекти управління силами безпеки та перспективи їхнього розвитку, засновані на концепції циклу OODA, були досліджені в роботі [280]. На думку авторів [280], для ефективного функціонування циклу OODA необхідно об’єднання та розвиток п’яти ключових технологій:

– технології збору інформації, яка повинна надавати особі, що приймає рішення, повний спектр даних від різних джерел, створюючи повну картину ситуації на полі бою. Це відповідає функції спостереження у циклі OODA;

– технології комунікаційних систем, що забезпечують в реальному часі доступ до будь-якої бази даних та створюють необхідний потік інформації для управління;

– технології комп’ютерної обробки даних;

– технології створення інтелектуального програмного забезпечення, яке здатне обробляти різноманітні типи та джерела інформації, допомагаючи особам, що приймають рішення, у розробці та прийнятті відповідних рішень, підтримуючи функції орієнтації та формування рішень у циклі управління;

– технології, що забезпечують повну інтеграцію людини та комп’ютера.

У недалекому минулому для прийняття рішень часто не вистачало інформації, тому подальший розвиток інформаційних технологій був спрямований на створення більшого обсягу інформації для забезпечення якості бойового управління [276]. Однак, без певної інтелектуальної підтримки та сучасних комп'ютерних технологій існує ризик інформаційного перевантаження командирів, що може призвести до прийняття помилкових рішень.

Цикл OODA все більше залежить від зростаючого обсягу інформації, значна частина якої може виявитися незначущою для вирішення поставлених завдань. Це призводить до труднощів у фільтрації необхідної інформації. В умовах бойових дій більшість командувачів мають обмежений час на вирішення певних завдань, і зростання обсягу інформації, що надходить до них, активує природні механізми захисту, які обмежують сприйняття надлишкової інформації [283]. Одна з небезпек цього механізму полягає в тому, що командир може пропустити важливу інформацію. Інша небезпека полягає в тому, що командир може не встигнути вчасно усвідомити помилковість раніше отриманих даних і переорієнтувати свої плани.

Ключовим напрямком для забезпечення ефективної роботи командувача є пошук шляхів розвитку технологій інтелектуального програмного забезпечення. Створене людиною інтелектуальне програмне забезпечення повинно забезпечити аналіз та інтерпретацію отриманої інформації, моделювання можливих дій сторін, формування оцінки альтернатив та видачу рекомендацій.

Поняття інтелектуального програмного забезпечення набуває все більшого значення в сучасному світі, проте його практичне застосування все ще не відповідає вимогам, які ставить перед нами кібернетична війна. На даний момент вимоги до розробки таких програм залишаються недостатньо визначеними, що ускладнює їх впровадження. Для глибшого розуміння потенційних можливостей використання інтелектуального програмного забезпечення варто розглянути парадигму «поведінки» інтелектуальних систем, які наділені здатністю формувати управляючі впливи і приймати рішення.

Інтелектуальним системам, незалежно від того, чи вони біологічного або технічного походження, притаманні п’ять основних видів дій [262]:

- сприйняття навколишнього середовища;
- інтерпретація отриманої інформації з урахуванням наявних знань про це середовище;
- формування плану дій на основі внутрішньої моделі світу;
- реалізація запланованих дій для досягнення поставлених цілей;
- підтримка комунікації з іншими агентами для координації зусиль і досягнення спільних цілей.

Ці дії демонструють певну схожість з елементами циклу OODA. Виходячи з цього підходу до інтелектуальних систем, створення інтелектуального програмного забезпечення можна описати як завдання розвитку чотирьох ключових технологій [262].

Перша технологія, відома як IU-технологія (Image Understanding), спрямована на розуміння зображень. Вона передбачає розробку механізмів, які здатні аналізувати та описувати зовнішнє середовище на основі інформації,

отриманої від сенсорних пристроїв, навіть у випадку неповної або викривленої інформації. Довгострокова мета цієї технології полягає в створенні теорії та методів застосування машинного зору, які перевершували б можливості людського ока у сприйнятті інформації з усього спектра електромагнітного випромінювання в різних середовищах. Комерційні продукти цієї технології вже використовуються в програмах промислового впізнавання, системах візуального контролю і навігації для роботів. Проте, у військових цілях ця технологія вимагає значних інвестицій з боку держави.

Друга технологія – це інтелектуальна інтеграція інформації, яка передбачає обробку і узагальнення даних, отриманих з різноманітних джерел, що мають різну структуру, мови опису та семантику. Це важливий аспект для забезпечення цілісності інформаційної системи та підвищення її ефективності.

Третя технологія – підтримка процесів планування і прийняття рішень. Інструменти для підтримки цих процесів повинні включати методи міркувань для генерації змістовних планів і графіків. Такі інструменти допомагають користувачам уникнути інформаційного перевантаження, дозволяючи їм зосередитися на прийнятті оптимальних рішень у стислий термін. Вони також сприяють розробці більшої кількості альтернативних варіантів рішень, які заслуговують на увагу.

Четверта технологія – це взаємодія людини з комп’ютером. Сучасний розвиток біо- та мікропроцесорних технологій відкриває нові можливості для вирішення завдання прямої взаємодії комп’ютера з мозком людини. Це завдання поділяється на дві частини: перша пов’язана з представленням комп’ютерної інформації у формі, сприйнятливій для людського мозку, а друга - з інтерпретацією та представленням комп’ютером інформації, що надходить від мозку людини.

У більш пізніх роботах [284, 300] американські воєнні теоретики дійшли висновку, що просте перенесення концепції петлі OODA, яка була розроблена для опису дій пілота у повітряному бою, на більш складні багаторівневі організації, такі як угруповання збройних сил, є недостатнім. Сучасні

багаторівневі організаційно-технічні системи сил безпеки вимагають більш складних інструментів для організації процесів управління.

Петля OODA, за своєю суттю, є занадто спрощеним підходом, який не дозволяє врахувати всю складність управлінських процесів в автоматизованих системах управління (C^4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), без яких сучасне управління військами неможливе.

На відміну від логіки, закладеної в петлю OODA, де розумові процеси завершуються прийняттям рішення або вибором альтернативи, процеси в системах C^4ISR мають значно складніший характер і передбачають формування замислу командувача, що є результатом взаємодії численних факторів і рівнів управління.

Сучасний процес формування замислу командувача, який функціонує в автоматизованих системах управління (АСУ), суттєво відрізняється від традиційних підходів. Замість одностороннього ухвалення рішень, замисел командувача сьогодні є результатом багаторівневого діалогу між командувачем (командиром) та його підлеглими на різних рівнях управління. Після того, як замисел визначено, він трансформується у рішення, яке далі реалізується у формі планів.

Ці військові плани можуть мати різні форми: від усних наказів до об’ємних письмових документів з численними додатками. Незалежно від їхнього формату, кожен план має п’ять ключових складових:

– загальна мета і завдання, які ставляться перед підлеглими підрозділами;

– визначення сил і засобів, які будуть використані, із зазначенням конкретних підрозділів та їхньої підпорядкованості;

– послідовність дій та графіки проведення бойових операцій підрозділами;

– визначення меж відповідальності в географічних та функціональних аспектах;

– планування на випадок непередбачених обставин, коли може знадобитися внесення змін до плану.

Після формування рішення (плану) воно перетворюється в директиви, які передаються підлеглим підрозділам для підготовки та ухвалення відповідних рішень на рівні командирів з подальшою організацією бойових дій. Щоб замисел командувача був дійсно ефективним, його необхідно своєчасно довести до всіх залучених осіб через систему C^4ISR (командування, управління, зв'язок, комп'ютери, розвідка, спостереження та розвідка).

Важливо, щоб усі зацікавлені сторони, які працюють у системі C^4ISR, розуміли загальну мету та завдання. Це дозволяє підлеглим командирам глибше усвідомлювати свої завдання та взаємодіяти з іншими підрозділами для досягнення спільних цілей.

Процес формування замислу, або «sensemaking», залишається надзвичайно складною та неформалізованою діяльністю, яка поки що є виключно людською сферою. Формальні методи аналізу, які викладаються у військових академіях США, покликані допомогти майбутнім командирам у прийнятті складних рішень. Проте, сучасні системи C^4ISR поки що не можуть замінити людей у цьому процесі, вони лише забезпечують підтримку при ухваленні складних рішень.

Подальший розвиток теорії управління військами пов'язаний із продовженням революції в сфері безпеки (Revolutions in Security Affairs) та військової справи (Revolutions in Military Affairs) [279, 292].

Сучасні збройні сили США та інших країн НАТО перебувають у процесі переходу від армій індустріальної епохи до армій інформаційної епохи.

В арміях минулої індустріальної епохи управлінські функції були висококонцентрованими, зокрема через централізацію планування, що частково компенсувалося децентралізованим виконанням. Через технічні обмеження індустріальної епохи центр мав монополію на інформацію, яка була необхідна для ухвалення оптимальних рішень. Всі дані збиралися в центрі, оброблялися для прийняття рішення, і у вигляді директив передавалися до війська.

Централізована система управління, характерна для індустріальної епохи, функціонувала циклічно, оскільки кожне ухвалене рішення підлягало затримкам через механізми обробки та передачі інформації. Популярність циклу OODA у збройних силах США відображає їхнє визнання циклічного підходу до управління військами. Цей підхід акцентує увагу на ролі командувача як центральної фігури, яку обслуговує підлеглий управлінський персонал.

У перспективній моделі децентралізованого управління, яку просувають американські фахівці, концепція змінюється: командувач створює умови для творчої роботи підлеглого персоналу, який забезпечує виконання управлінських функцій. Ця теорія децентралізованого управління базується на принципах системного підходу індустріальної епохи, таких як декомпозиція, спеціалізація, ієрархія, оптимізація, координація, централізоване планування та децентралізоване виконання.

Таким чином, перехід до нових принципів управління, адаптованих до умов інформаційної епохи, передбачає більш складні моделі, де командувач має можливість не лише контролювати, але й активно сприяти реалізації творчого потенціалу своїх підлеглих, інтегруючи їхні зусилля в єдину ефективну систему управління.

Централізоване планування та децентралізоване виконання являють собою логічний наслідок принципів, сформованих в індустріальну епоху, а також обмежень технічного характеру, які стосувалися можливостей передачі інформації та комунікації. В умовах динамічних і складних ситуацій з високим рівнем невизначеності централізоване планування, яке спрямоване на пошук оптимального рішення, часто стає недієздатним. Воно перетворює організацію на неповоротку та неефективну структуру, нездатну швидко реагувати на змінні умови.

Сучасна інформаційна епоха ставить перед військовими організаціями жорсткі вимоги, такі як швидкість реакції, гнучкість та здатність до адаптації. Швидкість реакції стає ключовим показником ефективності управління,

оскільки вона визначає здатність організації миттєво реагувати на раптово виникаючі виклики та знаходити нові шляхи виконання бойових завдань. Умови невизначеності або ознаки розпаду, які можуть призвести до ослаблення або навіть втрати деяких можливостей, не повинні «заганяти в кут» такі організації. Висока швидкість реакції в управлінні залежить від здатності командних структур об'єднувати зусилля колективів для забезпечення узгодженої відповіді на виклики, що виникають.

З точки зору військового управління, однією з найбільш значущих змін, які відбуваються в процесі трансформації збройних сил з індустріальної епохи в інформаційну, є необхідність розширення децентралізації управління завдяки технологічному прогресу. У найближче десятиліття розвиток нових інформаційних технологій дозволить усунути існуючі обмеження на швидкість обробки інформації та пропускну здатність каналів зв'язку. Це відкриє можливість зняти технічні бар'єри, які перешкоджають ефективному розподілу управлінських функцій, і сприятиме більш тісній взаємодії в області розумової діяльності між різними рівнями командування.

Унікальний підхід США до опису процесів розвитку збройних сил, який часто має «художній» характер, відображає не тільки бажання вирішити наявні проблеми в теорії управління, але й підкреслює важливість функціонального поєднання централізованого та децентралізованого управління. Це поєднання є необхідним за багатьма критеріями, такими як ефективність і оперативність, і полягає у розподілі сфер відповідальності між стратегічним, оперативним та тактичним рівнями управління. На кожному рівні функціонує своя власна петля OODA, яка відповідає за моніторинг специфічних для цього рівня умов обстановки, поведінки та стану військ, а також за прийняття рішень згідно з відповідними критеріями.

Враховуючи інтерес США до розвитку науки управління, можна зробити кілька важливих висновків [225]:

– Підготовка і прийняття рішень (тобто формування замислу) відносяться до вищих форм інтелектуальної діяльності людини, яка погано

піддається формалізації та поки що не має повноцінного втілення у комп’ютерних технологіях;

– Американські науковці та їхні партнери по НАТО активно працюють над впровадженням у практику військового управління технологій інтелектуального програмного забезпечення, зокрема систем C^4ISR;

– Неможливість повної формалізації процесу формування замислу рішення підкреслює необхідність розробки інтелектуальних комп’ютерних технологій, які підтримуватимуть процеси розумової діяльності людини. Це включає фільтрацію інформації за якісними та кількісними показниками, створення відповідних образів сприйняття, проведення складних математичних розрахунків для підготовки формалізованих висновків і пропозицій тощо;

– Основою процесу підготовки і прийняття рішень є концепція цілеутворення, яка визначає сутність технологічних рішень у роботі органів управління під час прийняття рішень для ведення бойових дій;

– Теорія прийняття рішень не обмежується лише вибором між альтернативами, а являє собою методологію розробки варіантів замислу, їх обґрунтування, оптимізації запропонованих рішень, прийняття остаточного рішення та подальшого планування дій підпорядкованих військових підрозділів.

Таким чином, сучасна інформаційна епоха вимагає від військових структур не тільки нових технологічних рішень, але й переосмислення підходів до управління, щоб забезпечити ефективність і адаптивність у складних і швидкозмінних умовах бойових дій.

«Управління військами» (англомовний аналог «command and control») у глосарії NATO [201] визначається як діяльність командуючих, командирів, штабів та інших органів управління щодо підтримки постійної готовності військ (сил), підготовки операцій (бойових дій) і керівництва військами (силами) при виконанні ними поставлених завдань. Воно включає безперервне добування, збір, вивчення, відображення, аналіз і оцінку даних обстановки; прийняття рішення на операцію (бій); постановку завдань військам (силам);

планування операції (бою); організацію й підтримку взаємодії всіх сил і засобів, а також здійснення всіх видів забезпечення; організацію управління; підготовку підпорядкованих органів управління й військ (сил) до бойових дій; організацію контролю й здійснення допомоги підпорядкованим командуючим (командирам), штабам, військам (силам); безпосереднє керівництво діями військ (сил) при виконанні ними бойових завдань.

Наведене визначення відображає лише зовнішній прояв функції управління й не розкриває його сутнісних сторін. Для виявлення тенденцій і прогнозування напрямків розвитку цього складного поняття необхідний спеціальний науковий підхід.

Із трьох основних системологічних підходів щодо дослідження управління військами найбільш природним є кібернетичний.

Одна з основних теорем кібернетики – теорема необхідної розмаїтості, запропонована Р. Ешбі [35].

Якщо перекластиїї на мовууправління організацією (у тому числі й військової), то зміст можна трактувати так: щоб успішно протистояти середовищу, складність і швидкість прийняття рішень в організації повинні відповідати складності й швидкості змін, що відбуваються в середовищі.

З усієї множини характеристик, які визначають найбільш істотні риси управління військами, можна виділити три ключові [270]:

- розподіл прав прийняття рішення;

- організація взаємодії (співробітництва) між особами, що беруть участь у підготовці (виробленні) рішень;

- розподіл інформації між учасниками процесу управління.

Зазначені характеристики утворюють простір, у якому можуть існувати різні типи управління військами (рис. 2.3).

Місце розташування організації у просторі типів управління військами відбивається як відносно окремих функцій управління, так і відносно динаміки переходу від одного типу управління до іншого.

Наприклад, функції збору розвідувальної інформації можуть

відображатися в іншій частині простору уявлення, ніж функції проведення гуманітарної допомоги й достатньо відрізнятися від того, як будуть уявлятися функції управління військами при веденні бойових дій.

Точно так само, місце розташування організації в просторі уявлення управління військами при відсутності кризової ситуації буде іншим, ніж в умовах кризи.

Сучасні збройні сили США й збройні сили інших держав (але в різному ступені) перебувають у стані перетворення (трансформації) від так званих збройних сил індустріальної епохи до збройних сил постіндустріальної (інформаційної) епохи [271].

Для збройних сил індустріальної епохи характерним є високий ступінь концентрації управлінських функцій. При існуючих технічних обмеженнях на темп обробки й доставки інформації центр був монополістом на найбільш повну інформацію. Тільки в центрі, що забезпечений найбільш повною інформацією, могло бути вироблене найкраще (оптимальне) рішення. У такій системі управління вся інформація збирається в центрі, перетворюється до зручного для розробки рішення вигляду й потім як детальні директиви і плани доводиться військам (силам).

На рисунку 2.3 на початку координат показана область, що відповідає класичному централізованому ієрархічному управлінню військами, характерному для збройних сил індустріальної епохи. У протилежній вершині координатного куба показана область, яка відповідає децентралізованому мережному управлінню військами і буде реалізована в збройних силах майбутньої інформаційної епохи. Тенденцію еволюції класичного управління військами від централізованого до децентралізованого мережного управління можна розглядати як процес адаптації військових організацій до змін, що відбуваються в операційному навколишньому середовищі. Важливо показати, яким чином зміни, що відбуваються, неминуче ведуть у зовнішньому операційному середовищі до еволюції системи управління військами.

Зміни у зовнішньому операційному середовищі можна охарактеризувати

такими факторами: збільшенням динамізму, обумовленого технологічним прогресом; ускладненням, пов’язаним зі збільшенням розмаїтості засобів і способів дій асиметричних сил конфліктуючих сторін; збільшенням невизначеності в діях протилежної сторони.

Зазначені фактори можна подати у трьох вимірах [270]:

- ступінь зміни операційної обстановки (статична – динамічна);
- ступінь ознайомлення з ситуаціями (висока – низька);
- міцність інформаційного положення (сильна – слабка).

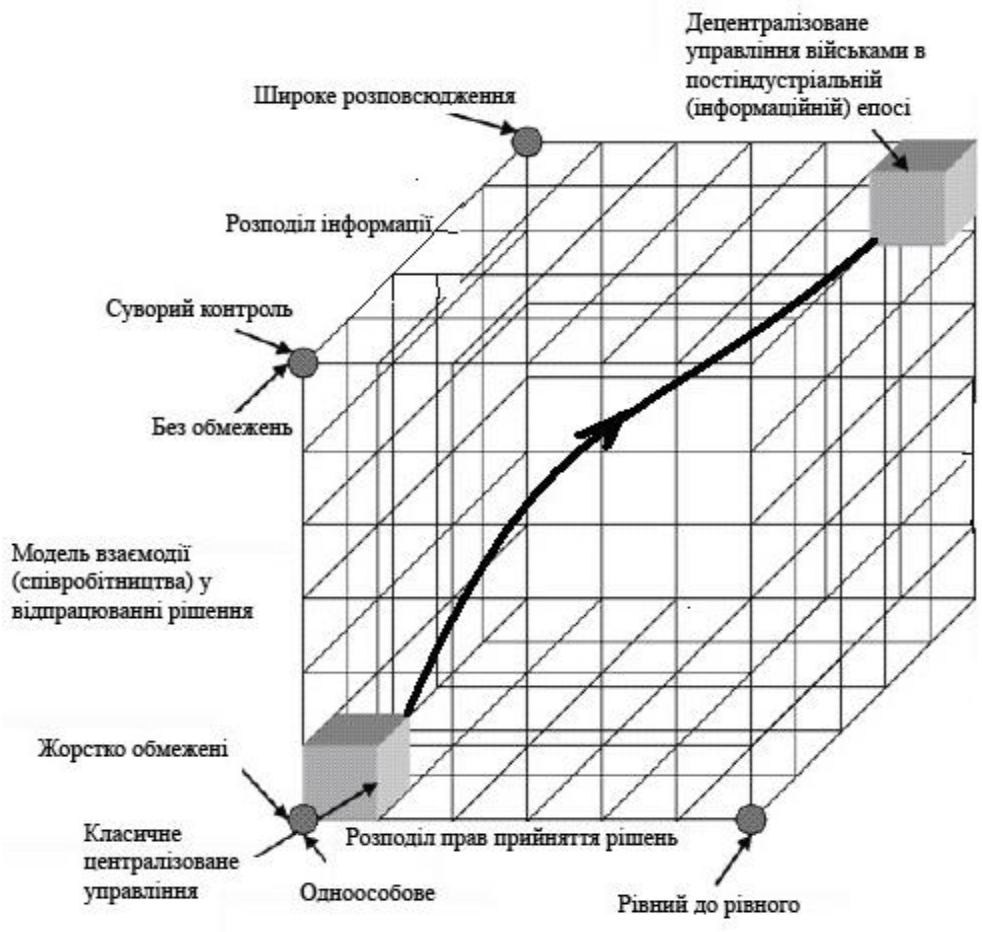

Рисунок 2.3 – Простір типів управління силами [233]

На рисунку 2.4 показаний простір зовнішньої операційної обстановки й напрямок її еволюції від «холодної війни» до воєн і конфліктів XXI століття.

Динамічне операційне навколишнє середовище (обстановка), на відміну від статичного, є непостійним, у ньому сторони конфлікту створюють різні

ситуації із швидким темпом оновлення.

У більш статичному операційному навколишньому середовищі переважає централізоване прийняття рішення, у якому дії військ можуть бути оптимізовані на основі найбільш повної інформації, якою володіє центр. Однак у динамічному операційному навколишньому середовищі централізоване прийняття рішення може бути не своєчасним і малопридатним для ведення успішних бойових дій.

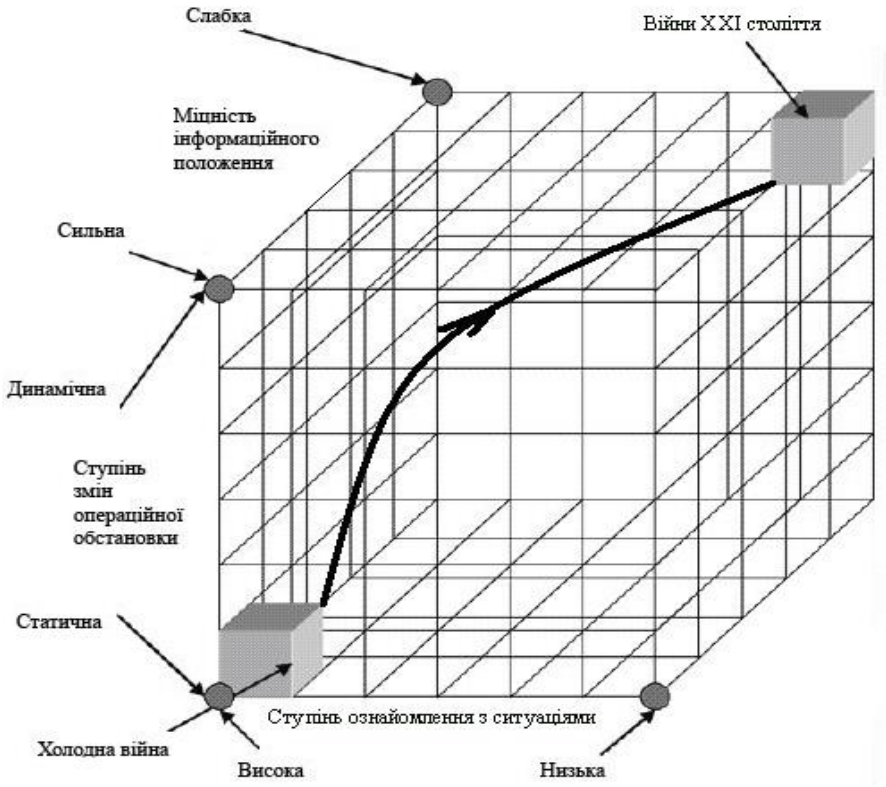

Рисунок 2.4 – Простір характеристик операційного навколишнього середовища [233]

Коли характер службово-бойового завдання добре відомий, усі дії відбуваються за спрощеною схемою.

По-перше, зрозумілими є інформаційні вимоги, тобто кому й яка інформація потрібна для ведення ефективних бойових дій.

По-друге, відомо, як повинна здійснюватися взаємодія. Це дозволяє приймати чіткі рішення з відповідним розподілом прав щодо прийняття

рішення.

Ступінь знання операційного навколишнього середовища не обов'язково обумовлена його статичністю. Наприклад, і НАТО, і збройні сили держав-учасниць колишнього Варшавського договору передбачали динамічний характер можливої світової війни. Однак після десятиліть планування, підготовки й збору розвідданих кожна сторона сподівалася, що є чітке розуміння того, як може розвертатися ймовірний військовий конфлікт. Як наслідок, вони розвивали високо спеціалізовані сили й деталізували плани щодо можливої участі й порядку дій у цьому конфлікті.

Інформаційне положення організації характеризується ступенем задоволення її інформаційних вимог.

Незалежно від ступеня динамізму й ступеня знання ситуації, міцність інформаційного положення має важливий вплив на застосування того або іншого типу управління військами.

Організація з дуже простими інформаційними вимогами може мати сильне інформаційне положення, хоча обсяг інформації може бути незначним.

У той самий час сили (війська), що прагнуть використати різнорідні системи зброї для проведення успішних дій проти терористів, можуть мати у своєму розпорядженні більший обсяг інформації, але одночасно відносно слабке інформаційне положення через високі інформаційні вимоги.

Цілком природно, що інформаційне положення організації також впливає на розподіл права прийняття рішень.

Перелічені вище ключові виміри типів управління військами не є цілком незалежними. Відносини між ними проілюстровані на рисунку 2.5. Найбільш фундаментальним виміром є розподіл прав прийняття рішень. Він впливає на характер взаємодії (співробітництва) між рівнями управління й розподілу інформації між ними. У той же час характер взаємодії (співробітництва) при розробці рішень може приводити до змін у розподілі прав прийняття рішень.

Коли ситуація вимагає швидкої реакції (наприклад, засідка на тактичному рівні), командири на більш низьких рівнях підпорядкованості не будуть

(відповідно до доктрини найсучасніших збройних сил) консультуватися з більш високим штабом про відхилення від плану або чекати нового плану, а швидше за все будуть брати ініціативу у свої руки, приймаючи рішення з негайним реагуванням на обстановку. Вони повідомлять пізніше вищий штаб про те, що відбулося, які дії були виконані й прохання про підтримку, якщо загроза не минула. Якщо ці дії не передбачені існуючими планами керівництва, воно змушене змінити розподіл прав прийняття рішення.

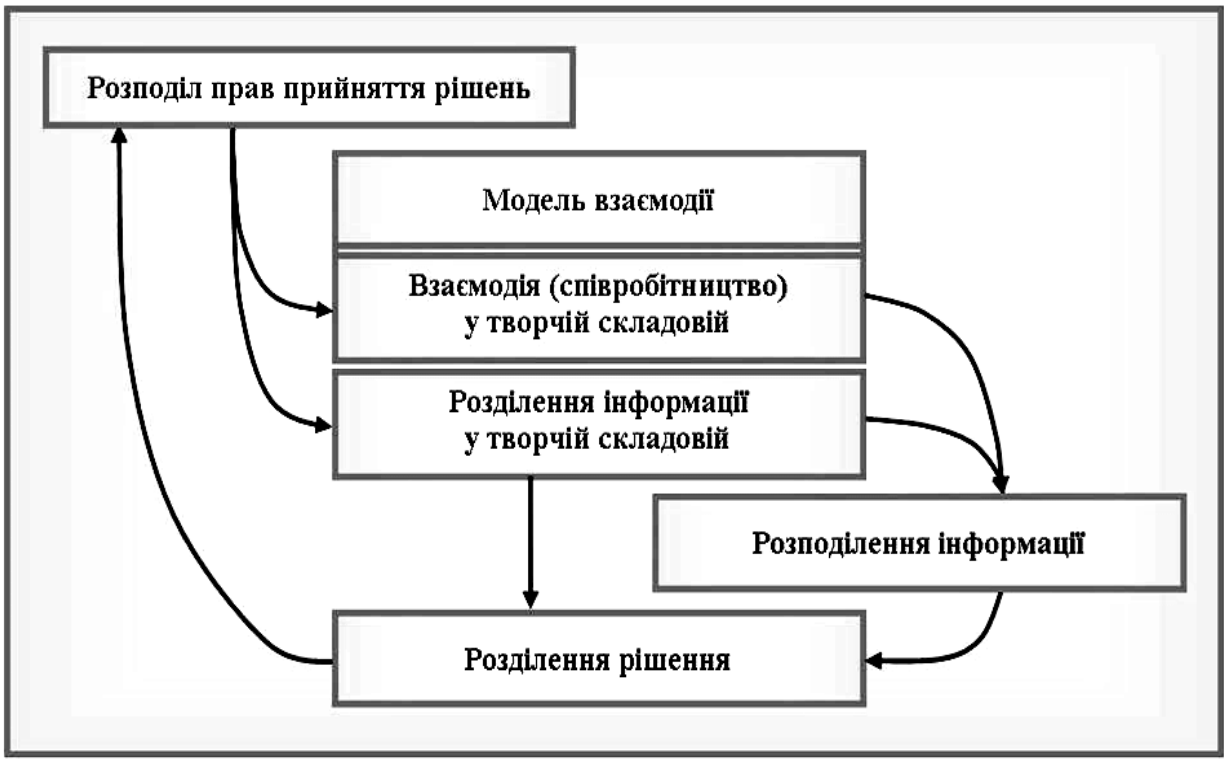

Рисунок 2.5 – Взаємний вплив ключових факторів управління силами

Можливий розподіл прав прийняття рішення має два протилежні логічні полюси: один полюс – повна централізація (усі права прийняття рішень зосереджені в однієї особи), інший полюс – повна децентралізація (кожний учасник управлінського процесу має рівні права у прийнятті рішення).

Як повну концентрацію або централізацію права прийняття рішень, так і повну рівність або повну децентралізацію права прийняття рішень можна знайти в маленьких колективах, однак жодна з цих крайностей, імовірно, не реалізується повністю в жодній конкретній організації.

Для збройних сил «індустріальної епохи» була характерна централізація права прийняття рішень.Відображенням стилю централізації збройних сил цієї епохи була практика видання наказів (розпоряджень) від імені командира, навіть коли накази стосувалися деякої спеціалізованої функціональної області.

Існує велика кількість як емпіричних, так і теоретичних підтверджень того, що широка участь у підготовці рішень збільшує їхню якість. Однак існує й зворотний бік цієї переваги, пов'язаний з тим, що широка участь у підготовці рішень може призвести до збільшення часу підготовки й прийняття рішень. Однак це правило не поширюється на підготовку й прийняття рішень у повторюваних або простих ситуаціях. Повторювані або прості ситуації відрізняються тим, що вони є знайомими, мають кінцеву кількість гарно зрозумілих альтернативних дій, і для них правильна дія може бути відібраною відповідно до правила або алгоритму [19].

Взаємодія між рівнями управління може обмежуватися обміном даних або інформацією, або бути на рівні творчого співробітництва, що впливає на досягнення загальної мети. У збройних силах «індустріальної епохи» всі види взаємодії будувалися таким чином, щоб гарантувати контроль з боку центру.

Традиційним було те, що інформація повинна була проходити по каналах, контрольованих командиром, і, що вся інформація як би належить командирові. Як наслідок, взаємодія індустріальної епохи зберегла подобу ієрархічної структури військової організації.

У багатьох випадках обмежена смуга пропускання контуру управління для проходження множинних рішень, комунікацій і великого обсягу дій приводила до необхідності створення декількох ієрархічних рівнів, що істотно впливало на процеси управління військами, управління зброєю й логістикою. До того ж кожна зі служб мала унікальні системи комунікацій. Проблема полягає в тому, що ці спеціалізовані ієрархії істотно ускладнювали горизонтальне співробітництво й взаємодію.

У збройних силах інформаційної епохи на зміну ієрархічним системам взаємодії (співробітництва) приходять мережні структури взаємодії.

Розподіл інформації у межах організації частково залежить від розподілу прав прийняття рішень, частково – від прийнятої структури взаємодії, частково – від ступеня готовності розділити інформацію, частково – від ступеня готовності індивідуумів користуватися цією інформацією і частково – від інструментів і навичок, яких вони мають набути.

В остаточному підсумку, розподіл інформації визначає здатність органів управління розробити смислову частину рішень, причому з використанням як індивідуального, так і колективного методів прийняття рішень.

Розподіл інформації як координата простору, виміряються від повністю централізованих, строго контрольованих баз даних (наприклад, стара універсальна ЕОМ, що містила всі дані для компанії або організації, і доступ кожного користувача був визначений і управлявся адміністратором) до повністю розподілених (мережних) баз даних, коли кожний має доступ до всієї інформації.

В організаціях індустріальної епохи інформація розподілялася згідно з певними потребами кожного користувача. Це вимагало попереднього планування й ідентифікації «власника» кожного інформаційного елемента.

Розроблювачі систем управління військами витрачали багато часу, обґрунтовуючи вимоги до інформаційного обміну. Саме вони визначали: хто мав потребу в доступі, до якої інформації й при яких обставинах. Все це стримувало взаємодію, обмежувало розподіл інформації відповідно до припущень. При цьому заздалегідь відомі загрози й обставини припускали застосування конкретної воєнної сили й адекватних проектів систем управління військами.

В організаціях інформаційної епохи вся інформація стає доступною всім об’єктам із обмеженнями, а також мінімізованою й зосередженою для забезпечення необхідної інформаційної безпеки (таємність, вірогідність, точність та ін.). Однак інформаційна безпека не забезпечується сама по собі. Користувачі для цього повинні мати інструменти пошуку необхідної інформації, розуміння того, яка інформація є їм доступною, також повинна

враховуватися здатність користувачів обробити інформацію, «переварити», щоб зробити свій внесок у розробку смислової частини рішення.

При розгляді інформаційної безпеки необхідно враховувати розподіл зберігання інформації для її захисту від втрат при навмисних нападах, при природних катаклізмах, відмовах системи з її можливістю швидко перерозподілити інформацію в динамічно мінливих і непередбачених обставинах.

Стійкість системи до можливих помилок і надмірності інформації залежить від ключових елементів, які служать для підтримання ефективного інформаційного розподілу інформації протягом заданого часу й забезпечення виконання необхідних функцій.

На практиці закордонні держави розробляють різні стратегії та методики 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 існує 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 в сфері інформації. Ці органи не тільки займаються моніторингом і виявленням кібератак, але й розробляють національні стратегії кібербезпеки, проводять навчання і координують заходи між різними державними та приватними структурами.

Агентство національної безпеки (NSA), США. NSA займається збором і аналізом інформації та даних для зовнішньої і внутрішньої безпеки. Відомство також відіграє ключову роль у захисті урядових мереж, розробляючи стандарти кібербезпеки і технології шифрування.

Агентство національної безпеки (АНБ), (National Security Agency (NSA)) – агентство криптологічної розвідки Сполучених Штатів Америки. АНБ є

частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж уряду США. АНБ є складовою частиною системи безпеки країни разом зЦРУта іншими агентствами, однак на відміну від ЦРУ не займається використанням агентів в інших країнах. Згідно з федеральним законом, діяльність агентства обмежена збором та моніторингом іноземної розвідувальної інформації, однак з'являлися численні підозри у використанні агентства для збору інформації також і у США.

Структура кібервійськових сил США включає кілька ключових військових і цивільних організацій, відповідальних за забезпечення кібербезпеки, проведення кібервійськових операцій і захист від кіберзагроз. Основними складовими цієї структури є:

1. Кіберкомандування Сполучених Штатів (USCYBERCOM) – центральний орган, що відповідає за всі аспекти кібервійськової діяльності та кіберзахисту у військовій сфері США. USCYBERCOM займається координацією заходів кібербезпеки і проведенням кібероперацій спільно із збройними силами та іншими відповідними військовими структурами.

2. Національне агентство з кібербезпеки та інфраструктури (CISA) – агентство, що входить до складу Міністерства національної безпеки США, яке відповідає за захист критичної інфраструктури країни і координацію кіберзаходів у цивільному секторі.

3. Військові кібервійськові частини – кібероперації проводяться також у межах окремих видів військ, таких як Армія США (Army Cyber Command), ВМС США (U.S. Fleet Cyber Command / U.S. 10th Fleet), Авіація США (Air Force Cyber Command) і Морська піхота США (Marine Corps Cyberspace Command). Кожен з цих родів військ має власні підрозділи, що займаються кібербезпекою та кібератаками.

4. Кіберцентри національних розвідувальних агентств – такі розвідувальні агентства, як Національне управління з розвідки (NSA) і Центральне розвідувальне управління (CIA), мають свої кіберпідрозділи, які

спеціалізуються на зборі розвідувальної інформації, кібероперація х за кордоном та виявленні кіберзагроз.

5. Приватний сектор – багато компаній, які забезпечують критично важливу інфраструктуру, зокрема в галузях енергетики, транспорту, фінансів, також мають власні команди з кібербезпеки, що захищають від кіберзагроз і забезпечують безперебійну роботу їхніх систем.

Кібервійськові сили США мають складну та розгалужену структуру з підрозділами, що функціонують у різних родах військ. Внутрішня організація включає кілька ключових підрозділів, серед яких виділяються Кіберкомандування США (USCYBERCOM) та Спільна робоча група ARES. Кіберкомандування США (USCYBERCOM) є одним з одинадцяти уніфікованих командувань Міністерства оборони США, відповідальним за операції у кіберпросторі. Його основні функції включають зміцнення кіберзахисту, інтеграцію та розвиток кібернетичного досвіду в Міністерстві оборони. Хоча USCYBERCOM спочатку було створено для вирішення завдань оборони, тепер воно також виконує функції наступальної сили.

З 2018 року статус USCYBERCOM підвищено до рівня повноцінного та незалежного командування. До його складу входять такі підрозділи, як U.S. Army Cyber Command, Fleet Cyber Command (10th Fleet), Sixteenth Air Force (Air Forces Cyber) та Marine Corps Forces (Cyberspace Command). Головною метою USCYBERCOM є керування, синхронізація та координація планування і виконання операцій у кіберпросторі для захисту та просування національних інтересів США в тісній співпраці з внутрішніми та міжнародними партнерами.

Основними напрямками діяльності USCYBERCOM є:

1. Захист інформаційної мережі Міністерства оборони (DoDIN) – забезпечення захисту критичних мереж та інфраструктури від кібератак.

2. Підтримка командирів бойових дій – надання можливості командирам здійснювати свої місії по всьому світу, забезпечуючи їм необхідну кіберпідтримку.

3. Посилення національної здатності до реагування на кібератаки – зміцнення національної кібербезпеки та покращення здатності країни протистояти кібератакам.

USCYBERCOM також займається розробкою структури кіберсил, вимог до підготовки та стандартів сертифікації, що дозволяють формувати кіберсили, здатні виконувати специфічні місії. Крім того, командування активно співпрацює з міжвідомчими та міжнародними партнерами, щоб ефективно виконувати критичні завдання у сфері кібербезпеки.

Кіберкомандування Сполучених Штатів (USCYBERCOM) здійснює широкий спектр операцій у кіберпросторі, зосереджених на забезпеченні кібербезпеки, веденні кібервійни та захисті національних інтересів США. Основні операції включають:

1. Захист від кібератак – пошук, виявлення і нейтралізація кібератак на інфраструктуру, мережі та інформаційні системи США та їхніх союзників. Це включає розробку заходів кіберзахисту, аналіз кіберзагроз та забезпечення стійкості систем.

2. Кібероперації – проведення операцій, спрямованих на підтримку військових дій, розвідки, протидії ворожим кіберзагрозам і забезпечення військової переваги у кіберпросторі.

3. Кіберрозвідка – збір та аналіз інформації про ворожі інформаційні системи, кіберзагрози та потенційні цілі, які можуть бути використані в майбутніх операціях.

4. Відповідь на кібератаки – у разі нападу на США або їхніх союзників, USCYBERCOM розробляє та застосовує відповідні кібероперації для мінімізації шкоди, нейтралізації атакуючих і відновлення нормального функціонування інфраструктури.

5. Партнерство та співпраця – взаємодія з іншими військовими командуваннями, урядовими агенціями, союзниками та партнерами для обміну інформацією, спільних навчань і виконання операцій з метою підвищення кібербезпеки та забезпечення захисту в кіберпросторі.

Таким чином, кіберкомандування США відіграє ключову роль у забезпеченні національної безпеки в умовах постійно зростаючих кіберзагроз, використовуючи для цього найсучасніші технології та тісно співпрацюючи з численними партнерами по всьому світу.

Загалом, діяльність USCYBERCOM охоплює широкий спектр операцій у кіберпросторі, спрямованих на забезпечення національної безпеки та захист стратегічних інтересів США. Основними завданнями підрозділу є інтеграція та проведення комплексних операцій у кіберпросторі, включаючи радіоелектронну боротьбу та інформаційні операції. Це забезпечує свободу дій дружніх сил у кіберпросторі та інформаційному середовищі, одночасно захищаючи їх від потенційних загроз з боку супротивників.

Кіберкомандування флоту США (FCC) Десятий флот (C10F) є важливим компонентом цієї структури, забезпечуючи оперативні сили чисельністю понад 14 000 активних і резервних моряків та цивільних осіб, які об'єднані в 28 діючих команд і 40 підрозділів Сил кібермісії. Ці підрозділи діють по всьому світу, забезпечуючи ефективну роботу та захист інформаційних мереж ВМС, а також виконують наступальні та оборонні операції в кіберпросторі. Окрім того, FCC відповідає за космічні операції, розвідку сигналів та забезпечення безпеки в інформаційному середовищі.

Десятий флот США, як оперативний підрозділ Кіберкомандування флоту, виконує свою місію через структуру оперативної групи, аналогічно іншим командуючим військовим діям. Серед основних операцій, що виконуються цим підрозділом, можна виділити:

1. Моніторинг кіберзагроз та проведення детального аналізу їх характеристик, таких як методи атак, використані вразливості, цілі та наміри атакуючих. Це дозволяє ідентифікувати потенційні загрози та вживати заходів для їх попередження та нейтралізації.

2. Агентство CISA активно попереджає та реагує на кіберінциденти, працюючи у тісній співпраці з державними органами, приватним сектором та іншими партнерами. Це включає реагування на кібератаки на критичну

інфраструктуру, державні установи, а також надання допомоги у виявленні, аналізі та ліквідації кіберподій, сприяючи відновленню нормального функціонування пошкоджених систем.

3. Розробка та поширення кіберзаходів є важливою частиною роботи CISA. Це включає розробку та поширення кіберзаходів, таких як патчі, керівництва з кібербезпеки та інші рекомендації, спрямовані на захист інформаційних систем від вразливостей і загроз. CISA також співпрацює з федеральними, місцевими та приватними секторами, а також з міжнародними партнерами для обміну інформацією, координації дій та підвищення рівня кібербезпеки.

4. Підтримка кібернавчань та освіти – ще одна важлива сфера діяльності CISA. Агентство проводить навчальні заходи, тренінги та освітні програми для різних аудиторій, включаючи державні установи, підприємства та громадян, з метою підвищення обізнаності та відповідальності у сфері кібербезпеки. Це сприяє формуванню культури кібербезпеки на всіх рівнях суспільства.

Таким чином, CISA відіграє ключову роль у захисті критичної інфраструктури та інформаційних систем США від кіберзагроз, а також у реагуванні на кіберінциденти та підвищенні рівня кібербезпеки у всіх секторах економіки.

Європейське агентство з кібербезпеки (ENISA), створене у 2004 році, займає важливе місце в підвищенні рівня кібербезпеки серед держав-членів ЄС. ENISA розробляє політики, проводить навчальні програми та здійснює аналізи кіберзагроз, сприяючи обміну інформацією та кращими практиками між країнами ЄС і приватним сектором. Агентство також допомагає Європейській комісії, державам-членам ЄС та бізнесу виконувати вимоги мережевої та інформаційної безпеки, включаючи чинне та майбутнє законодавство ЄС.

ENISA тісно співпрацює з Європолом та Європейським центром кіберзлочинів (EC3), а також підтримує інші установи ЄС, зокрема Європейське агентство з питань правоохоронної підготовки (CEPOL), Орган європейських регуляторів електронних комунікацій (BEREC) та Європейське агентство

оперативного управління великомасштабними IT-системами (eu-LISA). Ці організації відіграють ключову роль у захисті національних інтересів у цифровому просторі, особливо в умовах зростаючих інформаційних загроз, що можуть походити від злочинних угруповань, терористичних організацій та інших недружніх акторів.

Таким чином, діяльність USCYBERCOM, CISA та ENISA є надзвичайно важливою для забезпечення кібербезпеки на національному та міжнародному рівнях, адже вони разом формують комплексну систему захисту від кіберзагроз, забезпечуючи безпеку та стабільність у кіберпросторі.

2.3 Методологічні засади функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

Методологічні засади функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України можуть включати ряд ключових принципів та підходів. Зазначимо деякі з них.

Принцип стратегічного планування. Визначення стратегічних цілей та завдань системи інформаційно-аналітичного забезпечення в контексті потреб національної безпеки України. Система інформаційно-аналітичного забезпечення в контексті національної безпеки України виконує ключову роль у зборі, обробці, аналізі та поширенні інформації, необхідної для ефективного прийняття рішень та реагування на потенційні загрози та виклики. Визначення стратегічних цілей та завдань для ІАЗ у цьому контексті може включати наступні аспекти [214]:

1. Забезпечення конфіденційності та цілісності інформації. Розробка та впровадження заходів з кіберзахисту для запобігання несанкціонованому доступу до інформації. Реалізація систем шифрування та контролю цілісності даних;

2. Моніторинг та аналіз загроз. Виявлення, аналіз та оцінка потенційних загроз для національної безпеки. Розвиток інструментів для вчасного виявлення змін в ситуації та трендів у кіберпросторі;

3. Створення ефективних процедур та механізмів реагування на кіберінциденти та кібератаки. Розробка планів відновлення роботи систем у разі порушення їх функціонування;

4. Забезпечення доступу до інформації для прийняття рішень. Розвиток систем обробки та аналізу великих обсягів даних (Big Data) для вивчення та прогнозування ситуацій в області безпеки. Забезпечення доступу до релевантної та актуальної інформації для органів управління та прийняття рішень;

5. Розвиток механізмів співпраці з іншими країнами, міжнародними організаціями та партнерами у сфері безпеки. Забезпечення ефективного обміну інформацією з різними секторами національного управління та правоохоронними органами;

6. Розвиток кадрового потенціалу та освіти. Підготовка та підвищення кваліфікації спеціалістів у галузі інформаційно-аналітичного забезпечення безпеки. Забезпечення своєчасного доступу до новітніх технологій та методик в сфері кібербезпеки.

Ці стратегічні цілі та завдання допомагають створити ефективну та гнучку систему ІАЗ, яка спроможна адекватно реагувати на сучасні виклики у сфері національної безпеки.

Принцип координації та інтеграції. Забезпечення ефективної координації між різними органами та відомствами, що відповідають за інформаційно-аналітичне забезпечення сил безпеки, вимагає інтеграції різних компонентів системи для забезпечення єдиної та згуртованої реакції на загрози. При створенні такої системи потребують врахування наступні вимоги. Це створення центрального пункту управління, який би був відповідальний за координацію та моніторинг інформаційно-аналітичного забезпечення. Розробка стандартів та протоколів обміну інформацією між різними органами безпеки. Уніфікація та

стандартизація інформаційних технологій, які використовуються різними органами безпеки. Розробка інтегрованих інтерфейсів для обміну даними між системами. Організація тренінгів та семінарів для представників різних органів для забезпечення єдності в розумінні методик та процедур. Спільна підготовка до реагування на кризові ситуації та вправи для вдосконалення співпраці. Утворення центрального пункту аналізу, який відповідатиме за здійснення інформаційного аналізу та видачу рекомендацій. Застосування передових аналітичних та прогностичних інструментів. Розробка безпечних та шифрованих каналів для обміну конфіденційною інформацією між різними агентствами. Створення системи для швидкого та ефективного обміну оперативною інформацією. Чітке визначення ролей та відповідальностей кожного органу в системі координації. Розробка механізмів взаємодії та вирішення конфліктів між різними органами. Розробка стійкої інформаційної архітектури, що враховує можливі кіберзагрози. Забезпечення заходів кіберзахисту для запобігання несанкціонованому доступу.

Ці заходи можуть сприяти створенню ефективної та координованої системи інформаційно-аналітичного забезпечення сил безпеки, яка буде готова до відповіді на різноманітні загрози та виклики.

Розробка та впровадження стандартів для забезпечення єдності та взаємодії системи ІАЗ базується на системному підході, який враховує взаємозв’язок різних компонентів та функцій системи [291].

Проведення аналізу функціональних та технічних вимог до системи ІАЗ. Визначення основних завдань, які система повинна вирішувати для досягнення цілей національної безпеки. Розробка стандартів для обміну та обробки інформації між різними компонентами системи. Визначення протоколів забезпечення безпеки та конфіденційності під час обміну даними. Визначення стандартної архітектури системи ІАЗ, включаючи функціональні блоки та їх взаємозв’язки. Розробка загальних принципів побудови та інтеграції компонентів. Розробка єдиної методології роботи з даними та інформацією в системі. Встановлення стандартних підходів до збору, обробки, зберігання та

аналізу інформації. Визначення стандартів та термінології, щоб уникнути непорозумінь між різними органами та відомствами. Забезпечення єдиності та узгодженості у використанні термінів та визначень. Створення системи моніторингу для визначення ефективності роботи різних компонентів системи. Запровадження засобів оцінки результативності та відповідності стандартам. Впровадження системи постійного вдосконалення та оптимізації процесів. Проведення регулярних аудитів для визначення можливостей для покращень.

Системний підхід допомагає створити єдину та взаємодіючу систему інформаційно-аналітичного забезпечення, яка ефективно вирішує завдання національної безпеки та забезпечує стійку реакцію на потенційні загрози.

Розробка та впровадження заходів з кіберзахисту має на меті усунення або зменшення ризиків, пов’язаних із зловживанням, втратою або несанкціонованим доступом до інформації та інфраструктури. Кроки для забезпечення кіберзахисту наступні. Проведення системного аудиту безпеки для виявлення потенційних вразливостей та слабких місць у системі. Аналіз конфігурацій, політик безпеки та здатності систем до атак. Встановлення та налаштування брандмауера та інших засобів фільтрації мережевого трафіку. Використання віртуальних приватних мереж (VPN) для шифрування комунікацій. Впровадження механізмів шифрування для захисту конфіденційної інформації під час передачі та зберігання. Використання сучасних алгоритмів шифрування для найвищого рівня безпеки. Встановлення систем моніторингу для виявлення незвичайної активності та потенційних загроз безпеці. Впровадження систем виявлення вторгнень (IDS) та виявлення вразливостей (Vulnerability Scanning). Встановлення сильних методів аутентифікації, таких як двофакторна аутентифікація. Налаштування точних політик авторизації для контролю доступу до різних рівнів інформації. Вчасне оновлення всіх програмних та апаратних компонентів системи. Автоматизація процесу встановлення патчів та виправлення вразливостей. Запровадження політик безпеки щодо внутрішнього персоналу та обмеження доступу до критичної інформації. Моніторинг активності внутрішніх користувачів та

систем для виявлення аномалій. Розробка та використання безпечних програм та додатків. Аудит додатків на вразливості та побудова міцних систем захисту. Розробка планів реагування на інциденти для швидкого та координованого реагування. Проведення тренінгів та симуляцій для персоналу щодо виявлення та вирішення кіберінцидентів.

Ці заходи є важливою частиною комплексного підходу до кіберзахисту, спрямованого на забезпечення надійності, конфіденційності та доступності інформаційних ресурсів системи.

Аналітичні служби (підрозділи) почали створюватися у всіх вузлових точках інформаційної інфраструктури, тобто в усіх сферах діяльності, де відбувалося накопичення, обробка та аналіз значних інформаційних потоків з метою прийняття соціально значимих управлінських рішень. Це стосувалося широкого спектра сфер, включаючи органи державного та військового управління, міністерства і відомства, засоби масової інформації, сферу бізнесу, політичні партії та рухи. Основною відмінною рисою цих служб є їхня глибока інтеграція в відповідні сфери діяльності, забезпечення функціонального та організаційно-діяльного симбіозу з соціальними інститутами, конкретними організаціями та органами управління (ОУ).

Стан інформаційно-аналітичної інфраструктури, що використовується для забезпечення потреб керівного складу структурних сил безпеки, не відповідає сучасним викликам, які виникають під час підтримки прийняття рішень щодо застосування сил. Інтеграція інформаційних систем за окремими напрямами відсутня або здійснюється фрагментарно, що не враховує сучасні вимоги щодо консолідації [92, 130, 275]. Це призводить до дублювання, недостатньої достовірності та неповноти інформації, що негативно впливає на процес комплексного управління службово-бойовими завданнями.

Окрім цього, залишається багато невирішених питань, таких як: відсутність єдиних методологічних, науково-технічних та організаційних принципів для створення ІАС та впровадження сучасних когнітивних інформаційних технологій; відсутність єдиних стандартів обміну даними між

інформаційними системами, що є необхідним для забезпечення їхньої взаємосумісності (інтероперабельності); недостатня розробленість аспектів захисту інформації та інформаційних ресурсів; обмежена розгалуженість інформаційно-телекомунікаційних мереж та відсутність швидких каналів передавання даних; організаційна розпорошеність і функціональна роз'єднаність існуючих інформаційних систем; недосконаліть нормативно-правового регулювання життєвого циклу інформаційних систем у МВСУ та НГУ; відсутність єдиної організаційної та мережецентричної інформаційно-технологічної платформи з компонентною архітектурою когнітивних сервісів, які забезпечують семантичну операціональність взаємодії з інформаційними ресурсами [87, 214, 287].

Методологічні основи функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України включають комплексний підхід до забезпечення ефективної роботи інформаційних систем, аналітичних засобів та процесів прийняття рішень у сфері національної безпеки. Цей підхід передбачає розробку та впровадження стандартів, методів та процедур, які гарантують збирання, аналіз, зберігання та передачу інформації, необхідної для підтримки діяльності сил безпеки [14]. Ефективне функціонування та розвиток механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України вимагає комплексного підходу, регулярного оновлення технологій та методів аналізу, а також забезпечення високого рівня безпеки та захисту інформації. Інтеграція інформаційних систем та стандартизація процесів обробки даних є основоположними елементами, що забезпечують ефективність, безпеку та надійність управління інформаційними ресурсами в силових структурах. Ці процеси дозволяють синхронізувати діяльність різних підрозділів, забезпечуючи їхню здатність швидко реагувати на мінливі умови та загрози.

Інтеграція інформаційних систем потребує узгодження технічних і програмних компонентів для забезпечення безперебійного обміну даними між різними платформами та базами даних. Це включає:

1. Сумісність форматів даних. Важливо забезпечити, щоб усі системи могли «читати» та «розуміти» дані одна одної, використовуючи загальноприйняті формати.

2. Встановлення стандартних протоколів. Для безпечного обміну даними між системами необхідно впроваджувати стандартизовані протоколи.

3. API (Application Programming Interface). Розробка та використання API дозволяє забезпечити взаємодію між різними програмними додатками, що сприяє покращенню їхньої інтеграції.

4. Мідлваре (Middleware). Використання програмного забезпечення, яке діє як посередник між різними програмними компонентами та базами даних, спрощуючи їх взаємодію.

Забезпечення сумісності та інтеграції різних інформаційних систем і баз даних, які використовуються в силових структурах, є необхідним для безперервного доступу до актуальної інформації та підвищення загальної ефективності системи інформаційно-аналітичного забезпечення.

Стандартизація процесів обробки даних є критично важливим аспектом для забезпечення ефективного та безпечного управління інформаційними ресурсами. Розробка та впровадження чітких стандартів для обробки, зберігання та передачі даних дозволяють не лише оптимізувати роботу з інформацією, але й значно підвищити надійність та захищеність інформаційних систем. Стандартизація охоплює встановлення єдиних правил і методик обробки, зберігання та передачі інформації, що забезпечує високий рівень захисту та цілісності даних.

Ключовими елементами цієї стандартизації є наступні:

1. Розробка стандартів даних. Це включає визначення структури даних, форматів їх зберігання, а також методів їхньої обробки. Важливим завданням є встановлення чітких правил і процедур для захисту інформації від

несанкціонованого доступу, модифікації або втрати. Ці стандарти мають враховувати вимоги безпеки та конфіденційності, що є ключовими для забезпечення цілісності даних в умовах сучасних загроз.

2. Аудит та контроль якості даних. Регулярний перегляд та аналіз якості даних, а також систем, що займаються їх обробкою, є необхідними для забезпечення відповідності встановленим стандартам. Це допомагає виявляти та усувати можливі недоліки, що можуть виникнути в процесі обробки або зберігання даних. Крім того, це дозволяє забезпечити високу якість і точність інформації, що використовується для прийняття управлінських рішень.

3. Політики керування доступом. Впровадження чітких політик, які регулюють доступ до даних, є важливим аспектом забезпечення безпеки інформаційних ресурсів. Це включає визначення того, хто, коли та як може отримувати доступ до певної інформації, що дозволяє ефективно захищати дані від несанкціонованого доступу.

Розвиток аналітичних засобів та створення ефективних систем підтримки прийняття рішень є ключовими для підвищення ефективності управлінських процесів, особливо в контексті національної безпеки та оборони. Для сил безпеки України особливо важливо мати можливість швидко приймати обґрунтовані рішення, оскільки це може мати стратегічне значення в умовах постійно змінюваних загроз.

1. Використання сучасних методів аналітики. Застосування машинного навчання (МН) та штучного інтелекту (ШІ) для обробки великих обсягів даних стає незамінним інструментом для виявлення потенційних загроз. Сучасні аналітичні засоби, що базуються на МН та ШІ, здатні ефективно аналізувати великі масиви інформації, виділяючи з них корисну інформацію та виявляючи потенційні загрози.

– Прогнозування та виявлення загроз. МН та ШІ дозволяють аналізувати патерни поведінки та історичні дані, щоб прогнозувати можливі загрози. Це надає силам безпеки можливість діяти проактивно, запобігаючи реалізації загроз до їх виникнення.

– Обробка природної мови (NLP). Технології обробки природної мови дозволяють автоматично аналізувати текстові дані, такі як розвідувальні звіти, новини та інформацію з соціальних мереж, що сприяє виявленню корисної інформації та підвищенню рівня ситуаційної обізнаності.

– Аналіз візуальних даних. Використання алгоритмів комп'ютерного зору для аналізу зображень та відео сприяє виявленню загроз, моніторингу об'єктів та інших важливих завдань, що підвищує ефективність оперативної діяльності сил безпеки.

2. Розробка інформаційно-аналітичних систем, що надають оперативну інформацію та рекомендації для прийняття рішень на різних рівнях управління, є критично важливим для покращення управлінських процесів. Системи підтримки прийняття рішень (СППР) забезпечують керівництво сил безпеки актуальною інформацією та аналітичними рекомендаціями, що є вирішальним для ефективного реагування на виклики.

– Інтерактивні дашборди. Ці інструменти надають швидкий доступ до ключових показників ефективності (KPI), аналітики в реальному часі та інших важливих даних, що дозволяє оперативно реагувати на зміни в ситуації.

– Моделювання та симуляція. Ці технології використовуються для оцінки різних сценаріїв та їхнього потенційного впливу на безпеку. Вони допомагають керівництву сил безпеки розуміти можливі наслідки своїх рішень, що підвищує їхню стратегічну обґрунтованість.

– Системи експертних оцінок. Такі системи забезпечують аналіз ситуацій на основі даних та досвіду експертів, пропонуючи рекомендації щодо прийняття рішень, що дозволяє значно підвищити якість управлінських процесів.

3. Інтеграція з іншими системами. Ефективна інтеграція СППР з іншими інформаційними системами забезпечує безперервний доступ до даних та аналітики, що є вирішальним для підтримки високого рівня національної безпеки. Це дозволяє забезпечити синхронізацію та узгодженість діяльності

різних підрозділів, що є важливим для оперативного реагування на змінні умови та виклики.

Застосування цих технологій і підходів може значно підвищити ефективність управління, а також сприяти швидкому та ефективному реагуванню сил безпеки України на різноманітні виклики, забезпечуючи національну безпеку на найвищому рівні.

Використання сучасних криптографічних методів для захисту інформації, яка передається або зберігається в інформаційних системах силових структур, є ключовим елементом забезпечення безпеки національної інформаційної інфраструктури. Криптографічний захист даних та забезпечення інформаційної безпеки є надзвичайно важливими аспектами для гарантування цілісності, конфіденційності та доступності інформаційних ресурсів, що мають стратегічне значення в умовах сучасних загроз.

Забезпечення інформаційної безпеки вимагає впровадження комплексного підходу, що охоплює різноманітні заходи адміністративного, технічного та фізичного характеру для надійного захисту інформаційних систем і даних. Основні складові цього підходу включають:

1. Розробка та впровадження політик безпеки. Створення чітких політик, що регулюють правила роботи з інформацією та інформаційними системами, є основою для організації захисту даних. Такі політики визначають принципи поводження з інформацією, які повинні бути дотримані всіма співробітниками та користувачами систем.

2. Контроль доступу до інформаційних систем і даних. Встановлення строгих процедур контролю доступу включає використання передових механізмів аутентифікації та авторизації, що дозволяють гарантувати, що лише уповноважені особи можуть отримати доступ до конфіденційної інформації.

3. Захист від вірусів та шкідливого програмного забезпечення. Використання сучасного антивірусного програмного забезпечення, а також інших засобів захисту, спрямованих на виявлення та запобігання дії шкідливих

програм, є необхідною умовою для підтримання безпеки інформаційних систем.

4. Захист мережевої інфраструктури. Важливим елементом є впровадження файрволів, систем виявлення та запобігання вторгнень, які захищають мережі від несанкціонованого доступу та можливих атак.

5. Регулярне резервне копіювання даних та розробка планів відновлення. Для забезпечення доступності інформації навіть у випадку збоїв або втрат, необхідно здійснювати регулярне резервне копіювання важливих даних та мати чітко визначені плани відновлення.

Криптографія виступає ключовим інструментом для забезпечення безпеки інформації, що передається через мережі або зберігається в інформаційних системах. До основних заходів криптографічного захисту відносяться:

1. Використання сильних алгоритмів шифрування. Застосування потужних алгоритмів шифрування гарантує конфіденційність даних під час їх передачі та зберігання, що унеможливлює їх прочитання сторонніми особами.

2. Цифрові підписи для забезпечення цілісності та автентичності. Використання цифрових підписів дозволяє гарантувати, що електронні документи та повідомлення не були змінені після їх створення, а також підтверджує їхнє авторство.

3. Управління криптографічними ключами. Впровадження надійних процесів управління криптографічними ключами є важливим для запобігання їх неправомірному використанню або втраті, що може скомпрометувати безпеку всієї системи.

4. Інфраструктура відкритих ключів (PKI). Розробка та впровадження PKI забезпечує централізоване управління цифровими сертифікатами та ключами, що є основою для побудови довірчої інформаційної інфраструктури.

Комплексне застосування цих заходів є необхідним для захисту інформаційних систем і даних від різноманітних загроз, що виникають у сучасному цифровому середовищі. Це забезпечує цілісність, конфіденційність

та доступність інформації, що є критично важливим для ефективного функціонування силових структур.

Окрім технічних заходів, важливим є створення та регулярне оновлення нормативно-правових актів, які регулюють діяльність системи інформаційно-аналітичного забезпечення. Важливість правового регулювання полягає в забезпеченні законності, прозорості та ефективності роботи системи, особливо у сфері національної безпеки та оборони.

Розробка законодавчої та нормативної бази включає такі ключові етапи:

1. Визначення правових, технічних та оперативних вимог, необхідних для ефективного функціонування системи інформаційно-аналітичного забезпечення. Це створює основу для регулювання діяльності таких систем, забезпечуючи їх відповідність сучасним викликам та стандартам.

2. Підготовка законопроектів та нормативних актів, які регулюють збір, обробку, зберігання, передачу та захист інформації в системах національної безпеки. Такі документи повинні бути розроблені з урахуванням найкращих світових практик і стандартів.

3. Залучення експертів та громадськості до обговорення проектів законів та нормативних актів. Це забезпечує їх комплексність та відповідність реальним потребам суспільства та держави, а також сприяє їх подальшій легітимізації.

4. Офіційне прийняття, публікація та введення в дію законів та нормативних актів. Важливо забезпечити, щоб нове законодавство було чітко донесене до всіх зацікавлених сторін та почало застосовуватись на практиці.

5. Навчання та інформування співробітників про нові вимоги та процедури. Організація навчальних заходів для співробітників, які працюють у сфері національної безпеки, є важливим етапом впровадження нових правових норм.

6. Постійний моніторинг і оцінка впливу нового законодавства. Необхідно здійснювати регулярний моніторинг ефективності правового регулювання та, за потреби, вносити зміни для адаптації до нових викликів.

Законодавство має забезпечувати баланс між захистом національної безпеки та дотриманням прав і свобод громадян. Це включає захист особистих даних, гарантії прозорості процесів збору та обробки інформації, а також гармонізацію національних норм із міжнародними стандартами.

Програми підготовки та навчання персоналу, залученого до роботи з інформаційно-аналітичними системами, є одним із ключових аспектів забезпечення ефективності та безпеки діяльності організацій. Розробка та впровадження цільових навчальних програм сприяють не лише підвищенню кваліфікації співробітників, але й зміцненню загальної інформаційної безпеки.

1. Аналіз навчальних потреб. Перед розробкою навчальної програми важливо провести глибокий аналіз специфічних вимог до знань та навичок для кожної ролі або відділу. Це допоможе виявити прогалини в компетенціях та сформувати цілеспрямовані плани навчання.

2. Гнучкість та адаптивність навчальних програм. Навчальні програми повинні бути гнучкими та адаптованими до конкретних потреб організації. Вони можуть включати лекції, воркшопи, тренінги, а також онлайн-курси для самостійного навчання, що дозволить максимально ефективно засвоїти необхідні знання.

3. Кваліфіковані інструктори та тренери. Навчальні заходи повинні проводитися кваліфікованими інструкторами, які мають глибокі знання та практичний досвід у сфері інформаційних технологій та безпеки. Це забезпечить високу якість навчання та підвищить його ефективність.

4. Регулярний перегляд та оновлення навчальних програм. У зв’язку з швидкими змінами в технологіях та загрозах, навчальні програми потребують регулярного перегляду та оновлення, що дозволить співробітникам залишатися в курсі останніх тенденцій та інновацій.

5. Оцінка ефективності навчання. Збір зворотного зв’язку від учасників та аналіз результатів їхньої роботи після завершення навчання є важливим для вдосконалення програм та підвищення їхньої ефективності.

6. Мотивація до навчання. Використання ігрових елементів, надання сертифікатів та визнання досягнень може суттєво підвищити залученість та зацікавленість співробітників у навчальному процесі.

7. Застосування знань на практиці. Важливо забезпечити можливість застосування отриманих знань у реальних робочих ситуаціях, що сприятиме закріпленню навичок та підвищенню загальної ефективності роботи з інформаційно-аналітичними системами.

Таким чином, ефективні програми підготовки та навчання персоналу є невід'ємною частиною стратегії розвитку будь-якої організації, особливо в сферах, де високий рівень кваліфікації та обізнаність персоналу мають безпосередній вплив на національну безпеку.

Розвиток інформаційно-аналітичного забезпечення (ІАЗ) необхідно здійснювати за такими ключовими напрямами: впровадження передових інформаційних технологій для прийняття ефективних рішень під час виконання службово-бойових завдань; створення та вдосконалення нових технічних рішень у процесі розробки або модернізації інформаційно-аналітичних систем (ІАС); удосконалення інформаційної інфраструктури сил безпеки з урахуванням вимог національних та міжнародних стандартів. Важливо також враховувати необхідність створення ІАС, які забезпечують взаємодію між наявними та новими інформаційними системами в силових структурах. Використання гнучких технологічних платформ під час впровадження ІАС є критично важливим для підвищення їхньої ефективності та надійності. Особливу увагу слід приділяти вимогам до відмовостійкості та катастрофостійкості ІАС, а також впровадженню механізмів автоматичної ідентифікації та автентифікації користувачів, забезпечення регламентованого доступу та обміну даними, і надійного захисту інформації від зовнішніх та внутрішніх загроз. Удосконалення організаційної структури ІАС є також важливим аспектом, що сприяє підвищенню їхньої ефективності.

Центральним моментом у розумінні процесів розвитку управління військами в сучасних умовах є раціональний розподіл повноважень щодо

прийняття рішень, вибір оптимальної структури та схеми взаємодії під час підготовки та прийняття рішень, а також адекватний розподіл необхідної інформації відповідно до зовнішньої операційної обстановки.

Забезпечення ефективної взаємодії між різними підрозділами сил безпеки через інтегровані інформаційні системи стає пріоритетним завданням, оскільки це дозволяє швидко та ефективно обмінюватися даними та аналітичними звітами. Впровадження сучасних технологій обробки даних, таких як штучний інтелект, машинне навчання та аналіз великих даних, суттєво підвищує ефективність аналітичної роботи. Постійне навчання та підвищення кваліфікації співробітників сил безпеки, особливо в галузі новітніх технологій та аналітичних методів, є невід'ємною частиною цієї стратегії. Також критично важливою є розробка та впровадження заходів з кібербезпеки, що забезпечують захист інформаційних систем та даних від зовнішніх і внутрішніх загроз.

Актуалізація законодавства у сфері державного управління інформаційно-аналітичним забезпеченням має також ключове значення. Вона включає оновлення правил обробки та розподілу інформації з урахуванням сучасних реалій. Важливим аспектом є розвиток партнерських відносин з міжнародними організаціями та іншими країнами для обміну досвідом, технологіями та інформацією, що сприятиме підвищенню рівня національної безпеки. Впровадження систем моніторингу та оцінки для аналізу ефективності роботи інформаційно-аналітичних систем дозволить приймати своєчасні та обґрунтовані управлінські рішення.

Для реалізації цієї стратегії необхідний комплексний підхід, що включає технічні, організаційні, нормативні та освітні аспекти. Прогнозування розвитку ІАЗ органів державної влади на найближчі десять років передбачає розгляд кількох ключових напрямів.

Очікується, що стрімкий прогрес у галузях штучного інтелекту (ШІ), машинного навчання, аналізу великих даних та квантових обчислень значно підвищить ефективність ІАЗ. ШІ стане важливим інструментом для глибокого аналізу даних, прогнозування та автоматизації рутинних процесів. У зв'язку з

постійним зростанням загрози кібератак, особливу увагу буде приділено посиленню кібербезпеки. Розробка та впровадження нових механізмів виявлення, запобігання вторгненням та реагування на інциденти будуть пріоритетними завданнями для забезпечення захисту критично важливих інформаційних ресурсів.

Впровадження єдиної інформаційної системи, яка забезпечить ефективний обмін даними між різними відомствами та рівнями влади, сприятиме значному підвищенню ефективності ІАЗ. Міжвідомче та міжнародне співробітництво також буде активно розвиватися, що дозволить обмінюватися досвідом та передовими технологіями.

Підвищення уваги до освіти та підготовки фахівців у галузях ІТ, аналітики даних та кібербезпеки стане критично важливим фактором для забезпечення високого рівня ІАЗ. Навчальні програми та курси підвищення кваліфікації будуть спрямовані на розвиток спеціалізованих навичок та знань. Адаптація законодавства, яке регулює питання ІАЗ, включаючи захист даних, приватність та використання ШІ, матиме велике значення для збалансованого розвитку цієї сфери. Крім того, етичні аспекти, особливо в контексті використання ШІ та аналітики даних, набуватимуть дедалі більшої ваги. Забезпечення прозорості, відповідальності та дотримання прав людини стане ключовим пріоритетом у розвитку ІАЗ.

Загалом очікується, що інформаційно-аналітичне забезпечення стане більш інтегрованим, автоматизованим та захищеним, з акцентом на співпрацю, освіту та високі етичні стандарти [72, 125, 223, 233].

Для забезпечення держави новітніми технологіями необхідно реалізувати всебічну стратегію, що включає такі важливі кроки. Перш за все, слід здійснювати значні інвестиції у наукові дослідження та вищу освіту, щоб створити міцний фундамент для технологічних інновацій. Це передбачає фінансування університетів, дослідницьких інститутів та лабораторій, що займаються передовими дослідженнями. Держава повинна також активно підтримувати дослідницькі та розробницькі (R&D) ініціативи, надаючи

фінансову та інфраструктурну підтримку підприємствам та організаціям, які працюють у ключових технологічних галузях. Для стимулювання інноваційної діяльності як у приватному, так і державному секторах, можна використовувати різні інструменти, зокрема податкові пільги, гранти, субсидії та інші заходи.

Важливим є створення середовища, що сприяє інноваціям, шляхом налагодження тісної співпраці між університетами, дослідницькими інститутами, промисловими підприємствами та урядом для обміну знаннями та комерціалізації технологій. Для досягнення успіху необхідно забезпечити підготовку висококваліфікованих фахівців у галузі високих технологій через освітні програми, стажування, майстер-класи та перепідготовку кадрів. Надійна правова база, яка гарантує захист інтелектуальної власності, сприятиме інвестиціям у дослідження та розробки, забезпечуючи захист прав на інновації та винаходи. Крім того, держава повинна активно сприяти міжнародному співробітництву в галузі науки та технологій, що дозволить обмінюватися знаннями, брати участь у міжнародних дослідницьких проєктах та мати доступ до глобальних інновацій.

Просування цифрової трансформації у всіх секторах економіки сприятиме швидкому впровадженню та поширенню нових технологій. Для підтримки розвитку стартапів та технологічних підприємств необхідно створити сприятливі умови, включаючи легкий доступ до фінансування, консультаційні послуги та ринки для реалізації їхніх продуктів. Важливим аспектом є регулярне оцінювання та аналіз ефективності технологічних та інноваційних програм, що дозволить оптимізувати стратегії та політики. Реалізація цих заходів сприятиме активному розвитку та впровадженню новітніх технологій, що, в свою чергу, підвищить економічний розвиток країни та покращить її конкурентоспроможність на світовому ринку.

Прогнози щодо розвитку нових технологій зазвичай зосереджуються на кількох ключових галузях, де очікуються значні інновації та прориви. Передбачається, що алгоритми машинного навчання та штучного інтелекту досягнуть нового рівня, що дозволить їм виконувати більш складні завдання,

починаючи від автоматизації виробничих процесів до управління міською інфраструктурою. Квантові обчислення мають потенціал для революції в обробці даних, відкриваючи можливості для вирішення завдань, які наразі є недосяжними для класичних комп'ютерів, наприклад, у криптографії, матеріалознавстві та фармацевтиці. Інновації в галузі виробництва, зберігання та використання енергії, зокрема розвиток відновлюваних джерел енергії, таких як сонячна та вітрова енергія, а також технологій уловлювання та зберігання вуглецю, відіграватимуть ключову роль у боротьбі зі зміною клімату. Застосування нанотехнологій має потенціал радикально змінити багато галузей, від медицини до виробництва матеріалів, дозволяючи створювати продукти з новими унікальними властивостями.

Подальша інтеграція цифрових технологій у повсякденне життя, розвиток інтернету речей, який дозволить пристроям та системам взаємодіяти більш тісно, збираючи та аналізуючи дані у реальному часі, стане важливим етапом технологічного прогресу. Ці прогнози відображають поточні тенденції досліджень та розробок, і можуть змінюватися в залежності від технологічного прогресу, ринкових умов та політичних рішень. Успіх у здобутті нових технологій залежатиме від здатності держави та приватного сектора інвестувати у дослідження, підтримувати інновації та створювати сприятливі умови для їх комерціалізації.

Розвиток фундаментальних наук також сприяє інтеграції різних наукових дисциплін, що є важливим для комплексного підходу до аналізу складних проблем. Міждисциплінарний підхід значно підсилює здатність інформаційно-аналітичних служб справлятися з різноманітними завданнями. Крім того, фундаментальні науки відіграють важливу роль в освіті та підготовці кваліфікованих фахівців, які володіють необхідними знаннями та навичками для виконання аналітичної роботи. Поглиблене розуміння цих наук дозволяє аналітикам критично оцінювати інформацію, виявляти приховані зв'язки і тенденції. Застосування таких технологій, як нанотехнології і нові матеріали,

може призвести до створення інноваційних пристроїв і методів для збирання, зберігання і передачі даних, що розширює можливості аналітичних служб.

Організація безперервного навчання співробітників сил безпеки у сфері новітніх технологій і аналітичних методів має вирішальне значення для підвищення їхньої ефективності і готовності до сучасних викликів. Для досягнення цієї мети слід вжити кілька важливих кроків. Початковим етапом є проведення аналізу та оцінки поточного рівня компетенцій персоналу, що допоможе визначити конкретні потреби у навчанні. Це дозволить виявити прогалини в знаннях і скласти навчальний план, орієнтований на важливі технології та методики. На основі результатів оцінки необхідно розробити навчальні програми, які включатимуть тренінги, семінари, воркшопи та курси з актуальних тем, таких як кібербезпека, аналітика даних, штучний інтелект та сучасні методи розвідки. Для проведення навчання важливо залучати досвідчених тренерів і фахівців з відповідних областей, включаючи як внутрішніх, так і зовнішніх експертів. Теоретичні знання повинні доповнюватися практичними тренінгами, що дозволить співробітникам відточувати свої навички у реальних або симульованих умовах. Важливо також забезпечити умови для практичного застосування нових знань.

Після завершення навчальних заходів слід оцінити їхню ефективність, аналізуючи здобутки та недоліки, і коригувати подальші плани навчання. Для цього можуть використовуватися анкети, інтерв’ю, тести та практичні завдання, які допоможуть оцінити рівень засвоєних знань і навичок. Оскільки технології та аналітичні методи швидко розвиваються, важливо забезпечити систематичне оновлення навчальних програм та регулярне навчання персоналу [222].

Висновки до розділу 2

1. Вивчення впливу стану інформаційно-аналітичного забезпечення сил безпеки України на національну безпеку було здійснене за допомогою діаграми Ісікави, що дозволила виявити та проаналізувати ключові фактори, які

найбільше впливають на розвиток проблем у цій сфері. Використання цієї діаграми також дало можливість знайти способи попередження або нейтралізації негативного впливу виявлених факторів. Під час дослідження всі чинники були поділені на чотири основні групи. Перша група охоплює фактори, пов’язані з наявністю та рівнем розвитку інформаційних технологій у системі інформаційно-аналітичного забезпечення сил безпеки, включаючи такі важливі аспекти, як система кіберзахисту, автоматизовані системи управління (АСУ) та технології геопросторового аналізу (ГІС). Значущим фактором є також темпи розвитку інформаційних технологій, які залежать від наукових досягнень у таких галузях, як фізика, хімія та інші. Друга група факторів стосується рівня підготовки персоналу, що включає діяльність закладів вищої освіти та курси підвищення кваліфікації. У цій категорії особливо важливим є вплив темпів розвитку інформаційних технологій, що може знижувати ефективність навчання через постійні зміни в галузі та необхідність безперервного підвищення кваліфікації працівників. Третя група охоплює матеріально-технічне забезпечення, яке включає фінансування, забезпеченість обчислювальною технікою, програмно-технічними засобами, а також технічне обслуговування програмного та математичного забезпечення. Нарешті, четверта група включає характеристики самої системи ІАЗ, серед яких важливими є пропускна здатність (кількість одночасно оброблюваних завдань та обсяг оброблюваної інформації), архітектура системи, наявність вітчизняних розробників програмного забезпечення та розвинута система зв’язку.

2. Впровадження інформаційно-аналітичного забезпечення (ІАЗ) у процеси підтримки прийняття рішень при виконанні службово-бойових завдань набуває особливої ваги в сучасних умовах. Для підвищення ефективності ІАЗ необхідне впровадження новітніх ІТ-технологій, що дозволяє забезпечити якісне підґрунтя для прийняття управлінських рішень. У перспективі розвитку ІАЗ сил безпеки важливо створювати сучасні інформаційно-аналітичні системи, які будуть здатні виконувати такі завдання, як збір, накопичення, зберігання, динамічне відображення та багатовимірний аналіз даних. Крім того, важливим

є аналіз тенденцій, моделювання та прогнозування результатів управлінських рішень. На сьогодні ІАС є надзвичайно ефективним інструментом, який забезпечує користувачів всією необхідною інформацією для глибокого аналізу та прийняття оптимальних рішень.

3. Проведене дослідження дало змогу визначити ключові напрямки подальшого розвитку ІАЗ, що включають в себе кілька важливих аспектів. Серед них впровадження новітніх інформаційних технологій, які сприятимуть прийняттю рішень під час виконання службово-бойових завдань, розробка та впровадження нових технічних рішень для модернізації ІАС, а також удосконалення інформаційної інфраструктури сил безпеки з урахуванням як національних, так і міжнародних стандартів. Додатково важливим є створення ІАС, які забезпечують взаємодію між існуючими та новими інформаційними системами сил безпеки, використання гнучких технологічних платформ під час впровадження цих систем, а також врахування вимог до їхньої відмовостійкості та катастрофостійкості. Важливим завданням також є впровадження автоматичної ідентифікації та автентифікації користувачів ІАС, регламентованого доступу та безпечного обміну даними, що забезпечить високий рівень захисту інформації від зовнішніх та внутрішніх загроз. Удосконалення організаційної структури ІАС є також критично важливим для забезпечення ефективності їхнього функціонування.

4. Аналіз міжнародного досвіду показав, що у провідних країнах світу функціонування систем інформаційно-аналітичного забезпечення силових структур здійснюється на основі розроблених стратегій та методик протидії інформаційним загрозам. Ці стратегії, зазвичай, враховують політичні, економічні та технологічні можливості кожної країни. Одним із найпоширеніших підходів є створення спеціалізованих органів, що займаються кібербезпекою та захистом інформації. Формування таких установ є важливим кроком, який дозволяє країнам ефективно протидіяти кіберзагрозам та забезпечувати національну безпеку в інформаційному просторі. Ці організації не тільки здійснюють моніторинг та виявлення кібератак, але й займаються

розробкою національних стратегій кібербезпеки, проводять навчання фахівців та координують діяльність між різними державними та приватними структурами.

5. Системи інформаційно-аналітичного забезпечення (ІАЗ) відіграють надзвичайно важливу роль у зборі, обробці та аналізі розвідувальної інформації, що є ключовим для виявлення та ефективного реагування на загрози національній безпеці України. Використання сучасних технологій, зокрема штучного інтелекту та машинного навчання, дозволяє значно підвищити ефективність ІАЗ, автоматизуючи процеси аналізу даних та виявлення загроз. Геопросторовий аналіз сприяє точному визначенню місця розташування потенційних загроз, що є важливим для швидкого та ефективного реагування. Оперативний та ефективний обмін інформацією між різними відомствами та військовими структурами дозволяє досягти кращого розуміння ситуації та скоординованих дій у відповідь на загрози. Забезпечення кібербезпеки та захисту інформаційних ресурсів є критичним завданням для запобігання кібератакам та забезпечення ефективної відповіді на них. Оскільки інформаційні технології стрімко розвиваються, системи ІАЗ потребують постійного оновлення та удосконалення, а персонал – регулярного навчання для підтримки високого рівня компетенцій. Однак, існують певні виклики, такі як недостатнє фінансування, потреба у висококваліфікованих фахівцях, забезпечення конфіденційності та приватності, що можуть обмежувати ефективність ІАЗ без належної координації та впровадження сучасних технологій.

РОЗДІЛ 3
СУЧАСНИЙ СТАН ФУНКЦІОНУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ

3.1 Системи підтримки прийняття рішень у державному управлінні силами безпеки України

У сфері державного управління силами безпеки складні організаційні ієрархічні системи (СОІС) відіграють ключову роль у забезпеченні координації та виконанні різних функцій для підтримання безпеки країни. Проте такі системи часто стикаються з низкою викликів. Із зростанням кількості служб і підрозділів виникає проблема координації як по вертикалі, так і по горизонталі. Недостатній рівень взаємодії між підрозділами може призвести до дублювання функцій або утворення прогалин у системі безпеки.

У великих і складних організаційних структурах також може виникнути проблема бюрократизації, що затримує процес прийняття та реалізації рішень. Це особливо критично у сфері безпеки, де швидкість реагування може мати вирішальне значення. Складні ієрархічні структури часто є менш гнучкими та реагують повільніше на швидко змінювані умови, що ускладнює адаптацію до нових загроз або викликів [117, 233].

Силами безпеки України охоплюється широкий спектр завдань та функцій, що може спричинити проблеми з ефективністю комунікації між різними рівнями та підрозділами. Це впливає на обмін інформацією та координацію дій. Крім того, складні ієрархічні системи стикаються з викликами у сфері управління ресурсами та бюджетом, що робить оптимізацію розподілу ресурсів у багаторівневій ієрархії досить складним завданням.

Для подолання цих викликів організаційні структури шукають шляхи покращення комунікації, впровадження технологій для підтримки прийняття

рішень та вдосконалення систем координації. Реформи та пошук оптимального балансу між ієрархічністю та гнучкістю можуть підвищити ефективність систем управління силами безпеки.

Процес прийняття рішень у СОІС і в її ланках має низку особливостей [18]. По-перше, більшість рішень приймаються в умовах, які раніше не траплялися, оскільки ідентичність ситуацій у військовій, економічній чи політичній сферах є майже неможливою. По-друге, вибір варіантів дій зазвичай відбувається в умовах високого ступеня невизначеності, пов'язаної як із випадковістю процесу, так і з неоднозначністю цілей, критеріїв, альтернатив дій та їхніх наслідків. По-третє, рішення, навіть найвідповідальніші, приймаються в умовах обмеженого часу, що додає тиску на процес прийняття рішень.

Ці особливості висувають вимоги як до організації роботи органів управління, так і до математичного забезпечення процесу прийняття рішень у СОІС. Організація процесів прийняття рішень та розробка математичного забезпечення в цих умовах має низку викликів. Вони виникають як при аналізі системи в цілому, так і при розгляді її окремих елементів, діяльність яких регламентується вимогами вищих органів управління та спрямована на керівництво підпорядкованими системами.

Одним з основних викликів є описання функціонування СОІС з позиції цілісності та ієрархічності. Найскладніше – відобразити ієрархічну структуру зв’язків і відносин у ході функціонування СОІС. Потрібен компактний і наочний математичний опис системи, що водночас враховує велику кількість змінних, необхідних для відображення всіх суттєвих властивостей і особливостей СОІС. Також необхідно формалізувати процеси управління в СОІС.

Наступним викликом є інформаційне забезпечення процесу прийняття рішень. У ньому можна виділити два основні аспекти: з одного боку, є завдання переробки інформації. Інформація, що надходить з вищих інстанцій, потребує деталізації, тоді як інформація від підлеглих вимагає узагальнення. Тобто

необхідно адаптувати інформацію до рівня управління, який її отримує. Оскільки переклад є неоднозначним, потрібно шукати способи усунення цієї невизначеності. З іншого боку, необхідно будувати гіпотези про стан підпорядкованої системи на основі наявної інформації [32]. Математична задача оцінки надійності можливих гіпотез про стан підсистем зрештою визначає якість прийнятого рішення. Ще одним важливим питанням є вибір критерію якості рішення. Розглядаються дві задачі: формалізований опис і вимірювання невизначеностей, з якими стикаються органи управління під час прийняття рішень, та вибір показників, які дозволяють врахувати як суб'єктивні, так і об'єктивні фактори, що впливають на рішення.

Дослідження в галузі теорії прийняття рішень часто ігнорують важливий аспект – впевненість особи, що приймає рішення, у правильності вихідних даних і висновків, які можуть вплинути на оцінку неформалізованих факторів. Це створює додаткові складнощі при формуванні прийнятних альтернатив поведінки підсистеми. Задача ускладнюється, коли кількість можливих альтернатив і гіпотез є значною [117, 233].

Вирішення цих проблем передбачає створення формального апарату для якісної оцінки групи альтернатив, що мають спільні ознаки. Прогноз результатів для будь-якої альтернативи значною мірою залежить від факторів, що не піддаються формалізації, таких як неповні знання про функціонування підсистеми або психологічні фактори. Єдиним способом вирішення цього типу невизначеності є експертна оцінка, заснована на інтуїтивно-логічному аналізі процесу [117, 134, 233].

Зрештою, основним викликом є переведення інтуїтивних оцінок у кількісні без участі особи, що приймає рішення. Це завдання потребує створення практично придатних формалізованих методик для забезпечення процесів прийняття рішень у СОІС.

Формальний апарат повинен забезпечувати високу оперативність процесу прийняття рішень, бути простим і зручним у використанні, а також видавати наочні й інформативні результати. Рішення цих проблем дозволить враховувати

більше об’єктивних факторів у процесі прийняття рішень, підвищуючи наукову обґрунтованість рішень. Такий апарат допоможе особі, що приймає рішення, усвідомити логічну структуру вибору найкращого варіанту дій і прийняти рішення, що відповідає цій логіці [117, 233]. Таким чином, постановка цієї проблематики дозволить зосередити наукову діяльність на створенні інформаційно-аналітичної системи для підтримки управлінських процесів, використовуючи комплекс засобів автоматизації.

Основи теорії прийняття рішень охоплюють широкий спектр складних завдань, має різноманітні напрямки, які займаються аналізом можливих варіантів дій для знаходження найраціональнішого рішення в конкретних умовах. Загальна теорія прийняття рішень сформувалася як самостійна наукова дисципліна на початку 1960-х років. Основна мета цієї теорії полягала у раціоналізації процесу прийняття рішень. У подальші роки була розроблена прикладна теорія статистичних рішень, яка дозволяє аналізувати та вирішувати широкий спектр управлінських завдань, пов'язаних з обмеженим ризиком, таких як вибір, розподіл, розміщення ресурсів та інші питання.

Разом із розвитком кібернетики, теорії дослідження операцій, математичної теорії управління (зокрема теорії автоматичного регулювання – ТАР), ці результати активно впроваджувалися у створення нових та модернізацію існуючих технічних систем. Це також сприяло появі нових підходів у розробці математичних моделей соціальних і економічних систем. Виникли такі теорії, як теорія активних систем (ТАС), теорія ієрархічних ігор (ТІІ) та теорія управління організаційними системами [117, 17]. На сьогодні теорія прийняття рішень застосовується переважно для аналізу таких ділових проблем, які можна чітко та однозначно формалізувати, а результати дослідження легко інтерпретувати. Методи цієї теорії широко використовуються у різних галузях управління, зокрема при проектуванні складних технічних і організаційних систем, плануванні розвитку організацій, виборі економічних стратегій розвитку регіонів, організації нових економічних зон тощо.

Використання підходів і методів теорії прийняття рішень в управлінні є необхідним у зв’язку зі швидким розвитком та ускладненням економічних зв’язків, а також через виявлення взаємозалежності між складними процесами та явищами, які раніше здавалися несумісними. Це ускладнює прийняття обґрунтованих рішень, збільшує витрати на їх реалізацію, робить наслідки помилок все більш серйозними. Звернення до професійного досвіду та інтуїції не завжди гарантує вибір найкращої стратегії. Впровадження методів теорії прийняття рішень дозволяє вирішувати ці проблеми швидко та з достатнім рівнем точності.

Протягом всієї історії людства процес прийняття рішень був у центрі уваги суспільства, оскільки від результатів прийнятих рішень нерідко залежала доля цілих народів і держав. У сучасному світі цей процес набуває ще більшого значення, що робить його центральною складовою діяльності людства. Хоча економічна діяльність сьогодні сприяє розвитку теорії прийняття рішень, перший поштовх для її розвитку виник у військовій сфері. Незважаючи на це, військова галузь залишається певною мірою відокремленою від нових методів прийняття рішень, зокрема способів обробки інформації, оцінки ситуацій та аналізу факторів, що впливають на зміст рішень [117, 233].

Фахівці сил безпеки зазвичай розглядають процес прийняття рішення як одномоментний акт, коли командир, проаналізувавши результати попередньої роботи та врахувавши всі фактори, ухвалює рішення про необхідність дій певного характеру. Прийняте рішення, як правило, має офіційне оформлення, особливо у військових – це може бути карта «Рішення…» та пояснювальна записка до неї. Рішення закріплюється в бойових наказах, розпорядженнях або у звичайних наказах для вирішення питань повсякденної діяльності.

Коли говорять про те, що «рішення готується» або «приймається», мається на увазі підготовка пропозицій до цього рішення. Цей процес включає формування ідей, логічний аналіз, проведення розрахунків, узагальнення результатів і експертний аналіз. Командир, керуючи цим процесом, наближає момент прийняття рішення. Лише командир відчуває готовність до ухвалення

рішення і має право зупинити процес підготовки пропозицій та оголосити саме рішення.

Поняття «варіанти рішень» передбачає різні варіанти замислу до рішення, яке в кінцевому підсумку має бути одне. Уся копітка робота колективу спрямована на формування пропозицій, щоб командир міг обрати найкращий варіант. Процес управління нерозривно пов'язаний із процесом підготовки й ухвалення рішень.

Цикл управління включає кілька етапів: безперервний збір інформації, формування та аналіз ситуацій, оцінку обстановки, підготовку й ухвалення рішень, постановку завдань та контроль за їх виконанням, а також збір нової інформації для прийняття наступних рішень (рис. 3.1).

Більшість функцій, зазначених на рисунку (від 1 до 9), є невід’ємною частиною процесу підготовки до прийняття рішення. Сам акт прийняття рішення (10) включає в себе постановку завдань і контроль за їх виконанням (11, 12). Важливо зазначити, що процеси управління та підготовки й прийняття рішення не можна формально відокремити один від одного, оскільки всі зазначені функції органів управління є складовими саме процесу управління. Таким чином, процес управління можна формально поділити на такі складові: збір інформації, підготовка пропозицій до рішення, прийняття рішення, постановка завдань і контроль за їх виконанням.

У сучасних умовах, коли службово-бойові дії розгортаються дуже швидко, деталізація всіх завдань для великої кількості підлеглих командиру протягом обмеженого часу може бути майже неможливою. Завдання, які ставляться перед силами безпеки, визначають зміст дій підлеглих командирів та організацію всього процесу управління. В рамках управління силами безпеки можна виділити такі функції:

- Організація та проведення заходів із підвищення бойової та мобілізаційної готовності сил;
- Безперервний збір, обробка, аналіз та оцінка даних обстановки;

- Вироблення та ухвалення поточних і планових рішень, доведення завдань до підлеглих;
- Планування операцій та службово-бойових дій;
- Організація та забезпечення взаємодії між підрозділами;
- Організація та проведення заходів із різних видів забезпечення;
- Забезпечення стійкого та безперервного функціонування системи управління;
- Підготовка підпорядкованих сил та органів управління;
- Здійснення контролю та надання допомоги підлеглим;
- Безпосереднє управління діями сил під час виконання завдань.

Рисунок 3.1 – Безперервний цикл управління та процеси підготовки прийняття рішень [18]

Особливістю останньої функції є її інтегрований характер, що передбачає прийняття багатьох часткових рішень з усіх перелічених питань, включаючи бойову готовність, збір і оцінку даних, організацію підготовки та взаємодії.

Системи підтримки прийняття рішень у державному управлінні силами безпеки є критично важливими для України в умовах сучасних викликів. Ці системи включають широкий спектр інструментів, процедур та технологій,

спрямованих на забезпечення ефективного управління безпекою країни. Це особливо важливо для України, яка проходить через складний історичний період, пов’язаний із геополітичними та внутрішньополітичними викликами.

Загалом, розвиток і вдосконалення систем підтримки прийняття рішень у сфері державного управління силами безпеки є безперервним процесом, який потребує стратегічного бачення, технічної компетентності та здатності адаптуватися до нових викликів та загроз [198].

Розглянемо процес ухвалення управлінських рішень у сфері національної безпеки, який представляє собою комплекс взаємозалежних механізмів, таких як політичні, економічні, соціологічні, юридичні та психологічні, які визначаються внутрішнім та зовнішнім контекстом соціальних відносин. При цьому, у юридичній науці цей процес зазвичай розглядається як виконавчо-розпорядча діяльність, орієнтована на розробку відповідних правил поведінки для державних органів, організацій, посадових осіб і громадян. Основний фокус приділяється інституціонально-правовому аспекту, який має форму законодавчо встановленої процедури створення нормативно-правових актів, ігноруючи інші важливі складові. Серед недостатньо освітлених аспектів можна виокремити: формування і приоритизацію цілей, координацію цілей між собою; збір і системний аналіз інформації, необхідної для розробки, прийняття та виконання управлінських рішень; визначення можливих альтернатив і вибір найбільш раціональної; аналіз проблематики створення та ефективної роботи системи моніторингу реалізації управлінських рішень, особливо з урахуванням змін у середовищі діяльності.

Аналіз ролі, місця та взаємозв’язків зазначених елементів у процесі прийняття управлінських рішень повинен будуватися на кількох ключових принципах [198]:

- принцип поліцентричності передбачає визнання зовнішнього середовища як рівноправного учасника в процесі прийняття рішень. Поняття «середовище» розглядається як складний об’єкт або процес, який залежно від цілей дослідження може виступати як система або як елемент (підсистема)

іншої системи. Наприклад, міжнародна безпека може бути визначена як середовище (система), в якому формується національна безпека, тоді як національні цілі розглядаються як результат оцінки ситуації в різних сферах національної безпеки, а також як результат декомпозиції національних інтересів;

- принцип ієрархії стверджує, що процес визначення цілей управління повинен бути організований ієрархічно. Це дозволяє структурувати цілі за рівнями важливості та забезпечує можливість систематизації та координації зусиль на різних рівнях управління, забезпечуючи таким чином ефективність реалізації прийнятих рішень. Ієрархічний підхід дозволяє також ефективно розподілити ресурси та визначити пріоритетні напрямки діяльності в рамках більш широких стратегічних завдань;

- принцип ентропійності вимагає від розробників управлінських рішень структурувати управлінську ситуацію, виходячи з рівня невизначеності, що присутня в ній. Цей принцип стає особливо актуальним у контексті національної безпеки, де управлінські ситуації часто характеризуються високим рівнем невизначеності, пов’язаним із непередбачуваністю динаміки зовнішніх і внутрішніх змін. Важливо, щоб кожна управлінська ситуація була чітко аналізована з метою визначення потенційних загроз національним інтересам та розроблення стратегій, спрямованих на мінімізацію ризиків;

- принцип оптимальності передбачає кількісну оцінку витрат і результатів, необхідних для реалізації кожного варіанту управлінського рішення, а також проведення багатокритеріальної оцінки для вибору найкращого варіанту. Цей принцип дозволяє забезпечити, що управлінські рішення не тільки досягають поставлених цілей, але й оптимізують використання ресурсів, мінімізуючи при цьому витрати та максимізуючи потенційні переваги. Вибір найкращого рішення залежить від ретельної оцінки всіх можливих альтернатив з урахуванням комплексу факторів, включаючи ризики, вартість, часові рамки, стратегічну значимість та інші критичні параметри;

- принцип адекватності мети і результату підкреслює необхідність забезпечення відповідності між поставленою метою та кінцевим результатом управлінських рішень. В контексті національної безпеки, альтернативні рішення мають супроводжуватися оцінкою рівня захищеності національних інтересів. Це забезпечує, що вжиті заходи адекватно відповідають викликам, з якими стикається країна, і що вони дійсно сприяють зміцненню безпеки. Принцип адекватності управлінських рішень рівню загроз вимагає, щоб усі розроблені альтернативи адекватно реагували на існуючі або потенційні загрози національним інтересам. Неадекватність рішень може не тільки не вирішити проблему, але й спровокувати подальше зростання загроз, що зумовлює необхідність точної відповідності між розміром загрози та силою застосованої відповіді;
- принцип багатоваріантності визначає необхідність розробки широкого спектру можливих альтернатив при ухваленні управлінських рішень. У процесі прийняття рішень органами державного управління важливо мати на вибір ряд різноманітних варіантів, що забезпечує гнучкість і здатність адаптуватися до швидкозмінних обставин. Такий підхід дозволяє уникнути ризиків, пов’язаних з обмеженістю вибору, та забезпечує вищу ймовірність вибору найбільш оптимального рішення.

Ці принципи взаємопов’язані та разом формують основу для розуміння і вдосконалення процесу прийняття управлінських рішень, особливо в умовах, що вимагають високого рівня відповідальності та стратегічного мислення, таких як забезпечення національної безпеки.

У будь-якому випадку процес прийняття рішення обов’язково включає й процес його підготовки, що об’єктивно відображається в теорії прийняття рішень. З точки зору теорії прийняття рішень, вибір застосовуваних методів підготовки й прийняття рішень органами управління залежить від умов обстановки, поставленої мети, типу завдань, які треба виконати, а також такий вибір стосується свідомої організаційної діяльності особи, що приймає рішення (ОПР), експертів, які залучаються до підготовки і оцінки пропозицій.

За допомогою методів підготовки й прийняття рішення визначаються в першу чергу ті операції, прийоми мозкової діяльності органів управління, що дозволяють усвідомити поставлене завдання, оцінити обстановку, зрозуміти проблеми, сформувати мету практичної діяльності, способи її досягнення, обґрунтувати їх раціональність та провести критерійну оцінку результатів.

У той же час сам метод в основному визначається змістом мозкової і організаційної діяльності органів управління при прийнятті рішень, способами організації їх діяльності. Наприклад, в залежності від наявного часу застосовуються способи послідовної або паралельної роботи органів управління всіх рівнів підпорядкування або їх комбінація. Метод прийняття рішення це, в першу чергу, спеціальна технологія управлінської діяльності, а не математичні методи вирішення поставлених задач.

Під методом підготовки й прийняття рішення розуміється сукупність прийомів та операцій практичного (організаційна робота органів управління) і теоретичного (принципи і методи дослідження) засвоювання поставлених завдань, проблем і обстановки, яка (сукупність) дозволяє для організації ефективної (за результатами прогнозу) військової діяльності вирішити багатокритерійну (однокритерійну) задачу за відповідною кількістю цільових функцій (рис. 3.2).

Тим самим передбачається, що у заданих припущеннях та обмеженнях у розглянутих ситуаціях прийняті рішення за результатами прогнозу повинні забезпечити досягнення поставленої мети.

Невизначеність завжди присутня у процесах прийняття рішень. Саме у визначенні мети діяльності полягає та частина загальної невизначеності, яка супроводжує органи управління. Невизначеність мети діяльності проявляється через показники і критерії її досягнення.

По-перше, мету можна характеризувати показниками: співвідношення сил та засобів сторін при організації службово-бойової діяльності; ефективність дій суб’єкту сил безпеки.

Рисунок 3.2 – Узагальнена схема методу підготовки й прийняття рішення

По-друге, при обранні одного з показників досягнення мети службово-бойових дій постає інша невизначеність – яке значення показника обрати для опису критерійної оцінки. Яке значення буде вважатися достатнім для характеристики мети службово-бойових дій як досягнутої?

Саме тому схема методу включає окремі блоки, якими описуються прийоми формування мети бойових дій, визначення показників і критеріїв її досягнення (бл.1), прийому формування обрису бажаного результату (бл.2), згідно з яким, наприклад, передбачається описування структури суб'єкту сил безпеки, його елементів, характеристик, показників та критеріїв її ефективності.

По мірі визначення (обрання) тієї чи іншої мети, обрису об'єкта управління для реалізації мети на кожному кроці послідовно знижується рівень невизначеності. Таких кроків зниження невизначеності в схемі (рис. 3.2) передбачається шість, але не їх кількість є відмінністю схеми методу, а сам цей підхід.

ОПР на кожному кроці підготовки рішення невизначену інформацію його елементів змінює на детерміновану, конкретну для обраної обстановки (одного з варіантів, що досліджується). Кожен наступний крок у цьому процесі робить ситуацію більш визначеною для прогнозу, наприклад, ефективності службово-бойових дій, що наприкінці дає можливість отримати конкретні значення всіх показників, які виносилися для аналізу.

Методи багатокритерійного аналізу дозволяють на відповідних кроках зниження невизначеності обстановки послідовно вирішувати проблему комплексної критерійної оцінки варіанта рішення. Якщо на виході етапу формування замислу дій (бл. 4, 5) результати прогнозу відповідають одному з критеріїв оцінки рішення, органи управління переходять до наступного кроку у підготовці варіантів рішення. Кількість таких кроків багатокритерійної оцінки варіанта рішення є змінною величиною і залежить від кількості обраних критеріїв.

Виходячи з фізичного змісту процесів підготовки й прийняття рішення такі кроки багатокритерійної оцінки пов'язані з визначенням стратегій

досягнення мети (бл. 3), з визначенням ресурсного забезпечення (бл. 6) та із здійсненням вибору одного варіанта із альтернатив (бл. 10).

Для кожної конкретної ситуації, що складається в системі управління, схема методу уточнюється і деталізується відповідно до системи переваг ОПР, для отримання значень всіх заявлених показників і критеріїв ефективності тих процесів, що досліджуються в ході підготовки й прийняття рішення.

В основі методу підготовки й прийняття рішення лежить дослідження операції. Під операцією в цьому випадку розуміється процес досягнення певної мети системою (з урахуванням її взаємодії із зовнішнім середовищем). Дослідження операції полягає в оцінці й порівнянні можливих способів її проведення з урахуванням наявних обмежень. Обмеження, як правило, пов’язані з часовими, матеріальними, людськими або іншими видами ресурсів, які перебувають у розпорядженні сторони, що оперує (суб’єкта операції).Таким чином, спосіб проведення операції визначається стратегією використання наявних ресурсів. Тому замість виразу «спосіб проведення операції» частіше використовують термін «стратегія».Така термінологія обумовлена ще й тим, що поява цього розділу математики пов’язана з дослідженням воєнних операцій. Стратегії, що задовольняють накладеним обмеженням, називаються припустимими. Поняття «припустима стратегія» є відносним: множина припустимих стратегій змінюється, якщо змінюються обмеження (або наявні ресурси).

Реалізація тієї або іншої припустимої стратегії приводить до різних наслідків операції. Якість проведення операції, її «успішність» оцінюється з позицій особи, що приймає рішення. ОПР має власну систему переваг, до якої в першу чергу входять міра ефективності проведеної операції та вирішальне правило, на підставі якого обирається та чи інша стратегія досягнення мети операції.

Якщо система переваг ОПР має властивості повноти й спрямованості, то може бути побудована модель переваг ОПР. Слово «модель» у цьому випадку означає формалізований опис відповідних категорій, що забезпечує повторення

процедури вибору в однотипних ситуаціях при різних вихідних даних. Крім того, модель переваг ОПР може бути використана для автоматизації процесу пошукурішення.

Існуюча класифікація методів прийняття рішень [52, 231] в основному зведена до їх упорядкування за математичними методами здійснення вибору одного варіанта стратегії з множини їх альтернатив, що описують шляхи досягнення мети системи.

Саме математичні методи обґрунтування способів вирішення практичних завдань створюють ознаки для класифікації методів прийняття рішень у різних умовах обстановки, у тому числі і за характеристиками особи, що приймає рішення. У організаційній системі кожного суб'єкту сил безпеки є ОПР, яка відповідає за всю систему, і є ОПР підпорядкованих структур (підсистем). Наприклад, для системи управління НГУ підсистемами є територіальне управління, відділи, служби, в яких відповідні керівники при відпрацюванні пропозицій командувачу здійснюють опрацювання відповідної інформації та приймають часткові рішення щодо елементів загального рішення. Разом з основним органом управління – командувачем НГУ – всі підлеглі йому керівники складають колективний образ ОПР, на який покладається завдання підготовки й прийняття рішень. Модель переваг такого колективного образу ОПР складається з часткових моделей та набуває властивості системності лише у злагодженому колективі.

У той же час необхідно відзначити, що на практиці переваги ОПР непостійні й можуть змінюватися навіть в одній і тій же ситуації вибору. У зв'язку з цим важливе значення має поняття концепції раціональної поведінки ОПР. Та лінія поведінки («концепція»), якої дотримується ОПР, і визначає вибір правила, на основі якого будуть порівнюватися стратегії.

Тому класифікація методів підготовки й прийняття рішень залежатиме від характеристик системи переваг ОПР. Відповідно до теорії прийняття рішень, ОПР може використати одну з трьох концепцій раціональної поведінки: придатності, оптимальності або адаптивності.

При використанні концепції придатності прийнятноювважається будь-яка стратегія, що забезпечує значення показника ефективності не гірше заданого.

Концепція оптимальності вимагає, щоб з усієї множини припустимих стратегій була обрана тільки та, котра відповідає кращому («екстремальному») значенню показника ефективності.

Концепція адаптивної поведінкиприпускає, що правило вибору може змінюватися відповідно до змінених характеристик розглянутої ситуації.

Класифікація методів підготовки й прийняття рішення здійснюється в залежності від умов невизначеності обстановки. Так, існують методи рішення задач в умовах визначеності вхідних даних і методи рішення задач в умовах невизначеності (стохастичної, нестохастичної) обстановки. Остання класифікація більше впливає на технологію процесів прийняття рішень, яка має важливе значення, якщо розглядати процеси й підготовки й прийняття рішень.

Звідси доцільно розглядати класифікацію методів підготовки й прийняття рішення, що базується на визначенні відмінностей технологій прийняття рішення в умовах визначеності і в умовах невизначеності обстановки.

Задачі прийняття рішень в умовах визначеностіхарактеризуються наявністю повної й достовірної інформації про проблемну ситуацію, мету, обстановку, обмеження й наслідки прийнятих рішень. У таких задачах заздалегідь, до початку дій, відомо, до якого результату приведе кожна зі стратегій. Це зокрема означає, що всі зовнішні фактори відомі, враховані, і вони не можуть будь-яким непередбаченим чином вплинути на результат операції. Тобто, коли обстановка характеризується детермінованою інформацією, технологія підготовки й прийняття рішення повинна базуватися на застосуванні математичних методів теорії дослідження операцій і нормативних вимог керівних документів. Такий метод можна назвати нормативним методом підготовки й прийняття рішень в умовах визначеності обстановки.

Характерна риса всіх задач підготовки й прийняття рішень в умовах невизначеностіполягає в тому, що результат операції залежить не тільки від стратегій ОПР і фіксованих факторів, але й від невизначених факторів, не

контрольованих ОПР і не відомих йому на момент прийняття рішення (або недостовірновідомих). У результаті кожна стратегія виявляєтьсяпов'язаною з множиноюможливихрезультатів операції, що істотно ускладнює процесвироблennярішення [206].

Задачі підготовки й прийняття рішень в умовах невизначеності обстановки розділяють на задачістохастичної і нестохастичної невизначеності [19].

У випадку стохастичної невизначеності кожній стратегії відповідає деяка кінцева множинарезультатів, причому ОПР відомі їх імовірнісні характеристики. Але навіть якщо ОПР буде орієнтуватися на найбільш імовірний результат, це не означатиме, що операція буде розвиватися саме за даним сценарієм. Тому задачі такого типу називають також прийняттям рішень в умовах ризику. Вони мають місце в тих випадках, коли на результат операції можуть вплинути ті або інші випадкові фактори.

Задачі підготовки й прийняття рішень в умовах нестохастичної невизначеностірозділяються, у свою чергу, на задачі, що вирішуються в умовах природної й поведінкової невизначеності.

Такі задачі виникають у тих випадках, коли ОПР не має у своєму розпорядженні ймовірнісних характеристик можливихрезультатів операції або вони взагалі не є випадковими. У найкращому випадку відомі лише діапазони їх значень.

Якщо обмеженість інформації обумовлена недостатньою вивченістю природи розглянутих явищ, то говорять про задачіз «природною» невизначеністю. Якщо ж нестача інформації обумовлена впливом на хід операції інших суб'єктів крім ОПР, то має місце завдання з «поведінковою» невизначеністю. Для вирішеннязавдань із «поведінковою» невизначеністю використовуються методи теорії ігор. Іншим суб'єктом для органів управління виступає «протилежна сторона», яка створює умови поведінки її сил, що вимагає відповідного рішення ОПР протилежної сторони.

За характером залежності проблемної ситуації від часу розрізняють

статичні й динамічні задачіпідготовки й прийняття рішень. У динамічних задачах параметри (характеристики) проблемної ситуації змінюються у часі.

У загальному випадку в умовах невизначеності обстановки технології підготовки й прийняття рішення базуються на двох принципах: один принцип полягає у формуванні замислу рішення щодо виконання поставленого завдання, виходячи з аналізу наявних сил та засобів (наявних ресурсів), другий – у формуванні замислу рішення, спираючись на концепцію цілеутворення, саме аналіз шляхів досягнення мети дає підстави щодо визначення необхідних для цього сил та засобів. Ці два принципи відрізняються рівнем невизначеності обстановки, другий з них ближче до умов повної невизначеності обстановки, коли визначення самої мети може стати головним завданням у процесах прийняття рішення.

Слід зауважити, що з системних позицій усі методи підготовки й прийняття рішень мають одну сукупність прийомів та операцій практичного і теоретичного засвоювання поставлених завдань, проблем і обстановки, але ця сукупність трансформується в методах по різному. В одних методах основними виступають прийоми й операції цілеутворення, в інших – ресурсного забезпечення; деякі методи приділяють більше уваги практичному досвіду органів управління, інші – науковим способам обґрунтування пропозицій до рішення.

Розглянемо послідовно основні класичні етапи будь-якого методу підготовки й прийняття рішення.

Важливим для прийняття рішення є етап визначення цілей.

Для організації практичної діяльності на першому місці є та ціль, що стоїть перед колективом. Обрис об’єкта управління у майбутньому залежить, насамперед, від особистих оцінок і суджень осіб, відповідальних за прийняття рішень. Після визначення цілей можна окреслити ті фактори, механізми, закономірності, ресурси, які впливають на розвиток ситуації.

При прийнятті важливих рішень з вагомими наслідками реалізації бажані цілі необхідно уявляти чітко. Існують методи формування дерева цілі, що

дозволяє визначити ієрархічну структуру системи цілей, і дерева критеріїв, що дозволяє оцінити ступінь досягнення цілей.

Цілі можуть бути конкретними та розподіленими. Наприклад, конкретна мирна ціль – це підвищення рівня підготовки для отримання високої оцінки на підсумкових тактичних навчаннях. Загальні критерії для встановлених цілей включають комплексність, систематичність, узгодженість, досяжність, конкретність, гнучкість та прийнятність. При формуванні цілей також критично важливо визначити час, необхідний для їх досягнення, тому всі підпорядковані цілі повинні бути скоординованими як за змістом, так і за часом з цілями вищого рівня управління. Зазвичай, цілі охоплюють аспекти службово-бойової діяльності частин і підрозділів, описуючи бажаний стан у конкретних напрямках, які оцінюються за певними показниками [117]:

- службово-бойової діяльності (загальна ефективність дій ОГП, кількісні показники задіяного персоналу, імовірнісні показники виконання завдань та ін.);
- ефективності системи управління підрозділами, командами (час прийняття рішення, ступінь раціональності, складність системи управління, якість планування дій і повсякденної діяльності тощо);
- ефективності підготовки (рівень підготовки підрозділів (загонів) за період часу, на поточний момент, якість підготовки кадрів тощо);
- ефективності систем забезпечення сил безпеки і їх діяльності (рівень забезпечення по видах, своєчасність забезпечення та ін.);
- забезпеченості соціальних умов у мирний час (медичного, фінансового обслуговування, відпочинку, забезпечення житлом тощо).

У процесах формування цілей можна використовувати такі підходи [52, 238], як аналітичне вивчення обстановки та стану сил, каузальний імперизм, вивчення документів.

Аналітичне вивчення передбачає моделювання ситуації і систем для отримання більш детальної картини про вхідні і вихідні параметри, ті або інші змінні. Такий аналіз дозволяє отримати більш чітке уявлення про цілі на всіх

ієрархічних рівнях, у тому числі і сусідніх, з якими взаємодіють.

Підхід каузального імперизму передбачає спостереження за процесом прийняття рішення і виявлення цілей різного ієрархічного рівня за підсумками такого спостереження.

Як правило, у під час виконання службово-бойових заходів використовуються всі зазначені підходи.

Процес формування цілей звичайно йде від більш високих ієрархічних рівнів управління до нижчих. Але у деяких випадках (під час здійснення взаємодії) мета підлеглого рівня управління передбачає формування мети службово-бойових дій і на старших рівнях. При відсутності часу для прийняття рішення організується паралельний спосіб роботи органів управління, коли можуть вибірково використовуватися зазначені методи формування цілей.

Зберігання інформації та її обробка для подібного дерева цілей можуть здійснюватися за допомогою апарату матричної алгебри [117, 231].

При побудові дерева цілей вважається доцільним [117, 240] переходити до цілей більш нижчого ієрархічного рівня до тих пір, поки:

- не здійснено не тільки вербальне, але й кількісне описування цілі;
- ціль надалі не розгорнеться у часі;
- для цілей не будуть визначені вагові коефіцієнти відносної важливості.

У процесі формування цілей:

- розглядаються їх різні альтернативні варіанти;
- виключаються цільові заходи з низькою важливістю;
- виключаються цільові заходи з їх відносно низькою ефективністю;
- виключаються заходи, для виконання яких недостатньо ресурсів.

Оскільки мета – це бажаний стан об’єкта управління, до досягнення якого прагне відповідний керівний орган управління, то, для того щоб мати можливість реально управляти об’єктом, необхідно вміти вимірювати ступінь досягнення мети.

Головне, заради чого це необхідно, полягає в тому, що, тільки маючи можливість оцінювати ступінь досягнення мети, можна своєчасно скоригувати

управлінські впливи під час практичного управління бойовими діями. Саме тому завчасно прийняте рішення набуває можливості реалізуватися у ході ведення бойових дій.

У той же час оцінювати ступінь досягнення мети можна лише з використанням відповідного критерію. З одного боку, критерій повинен адекватно відображати процес досягнення мети службово-бойових дій, а з іншого – складові показники критерійної оцінки мають бути обчислюваними, тобто треба мати можливість їх розраховувати.

В залежності від наявного часу можна досягати значної глибини досліджень за всіма складовими рішення на службово-бойових дії. Якщо так підходити до процесу формування пропозицій до рішення, тоді доцільно застосовувати термінологію «проектування» службово-бойових дій.

Дерева цілей широко використовуються при програмно-цільовому плануванні на державному рівні. Такі методи доцільно використовувати при розробці програм розвитку суб'єкту сил безпеки, при проведенні робіт щодо розробки і прийняття на озброєння нових видів зброї і військової техніки. Дерева цілей необхідні і при плануванні службово-бойових дій – від суб'єкту сил безпеки до окремого підрозділу (загону). При цьому обов'язково розглядається мета старшого рівня управління, відповідна їй власна мета і узгоджені цілі діяльності на підлеглих рівнях управління.

Велике значення має визначення пріоритетності цілей, оскільки досвід показує, що при реальному управлінні доводиться здійснювати відповідний вибір. Не можна невиправдано розпорошувати сили. Ресурси, які витрачаються при функціонуванні організації, як правило, обмежені.

Під час визначення цілей функціонування організації здійснюється оцінка обстановки, що характеризується станом об'єктів управління, умовами зовнішнього середовища. Оцінка обстановки повинна дати можливість виявити фактори, що визначають динаміку розвитку ситуації. У ході оцінки обстановки здійснюється формування ознак, за якими оцінка обстановки змінює свою характеристику. Наприклад, «проста» обстановка перейде до рангу «складної»,

якщо ознака «кількість сил та засобів протилежної сторони в оперативній глибині прикордонної смуги перевищує деяке значення» буде істиною. Такі ознаки є і в оцінці воєнно-політичної обстановки, і в оцінці стану своїх сил, і в оцінці кліматичних умов та ін. Такий підхід дозволяє формалізувати процес визначення ступеня досягнення мети функціонування організації, здійснити контроль за розвитком ситуації, прийняти відповідні рішення щодо стану об'єктів управління.

Таким чином, на даному етапі прийняття рішення необхідно усвідомити завдання, оцінити обстановку, сформувати оціночну систему цілей, яка включає:

- критерії, що характеризують об'єкт системи;
- шкали, за допомогою яких оцінюється об'єкт по кожному з критеріїв;
- принципи вибору, за якими визначається загальна оцінка або порівняльна оцінка раціональних альтернативних варіантів.

Мета і стратегія визначають сценарій (послідовність) дій сил, порядок використання засобів для досягнення поставленої мети.

Стратегія охоплює всі можливі ситуації і їх комбінації, що дає можливість формувати варіанти застосування сил безпеки або окремих їх суб'єктів. Передбачається, що декілька стратегій можуть забезпечувати досягнення визначеної мети службово-бойових дій. При цьому спектр варіантів повинен бути повним, але в той же час не збитковим.

Стратегія як узгоджена за часом, місцем, планом визначена послідовність дій сил з використанням тих або інших прийомів і способів, повинна мати окрему назву – скорочене формулювання основного змісту стратегії, номер варіанта, вхідні параметри ситуації (обстановки), стану сил і вихідні дані – показники ефективності службово-бойових дій. Це дасть змогу здійснити критерійну оцінку стратегій досягнення визначеної мети службово-бойових дій.

Визначення стратегій, застосовуваних для реалізації службово-бойових дій, дає можливість переходити до формування завдань. Можна сказати, що після побудови дерева цілей, дерева стратегій по кожній цілі умовно закінчився

етап формування замислу службово-бойових дій. Зазначені стратегії повинні перетворитися в конкретні завдання. Тобто на даному етапі визначається склад сил та засобів для реалізації стратегії, здійснюється оцінка ресурсного забезпечення реалізації як стратегій, так і досягнення мети службово-бойових дій.

На даному етапі видно основу рішення – замисел службово-бойових дій, який системно створювався з певних цілей, обраних стратегій та у якому можна побачити такі елементи, наприклад: ділянки прикриття державного кордону; район виконання службово-бойових дій; місце створення правопорушення; розподіл сил і засобів згідно із завданнями; кількість службовців задіяних в виконанні службово-бойових дій; об’єкти охорони та оборони; кількість правопорушників, наявність у них засобів або озброєння; кількість службовців задіяних для ОГП; наявність та кількість техніки.

Щоб отримати ці дані на карті, але в системному вигляді, необхідно формалізувати процес побудови замислу ведення службово-бойових дій, тобто знайти формальний опис послідовності дій сторін, визначення цілей, стратегій дій сторін.

У загальному випадку формальний опис дій сторін передбачає визначення:

- сукупності якісних і кількісних показників, що характеризують протиборчі сторони, їх територіальне розміщення;
- дерева цілей і дерева стратегій;
- вербально-кількісного опису кожної мети прогнозованих дій військ (сил);
- переваг, устремлінь сторін (є залежність виграшу від дій військ, дії цілеспрямовані, раціональні і кожна сторона зацікавлена в максимізації виграшу);
- сукупності можливих дій сторін у вигляді стратегій (послідовності прогнозних практичних дій);
- інформованості сторін (перелік інформації, якою володіють обидві

сторони на даний час), включаючи порядок і час уведення в оману дій сторін;

- порядку ведення дій (порядок і послідовність вибору «ходів» сторін).

Всі ці дані є вхідними даними для проведення моделювання динаміки службово-бойових дій, для реалізації певної стратегії. При цьому заповнюються бази даних, визначається стан сил, їх положення, цілі (чого бажають), можливі стратегії (порядок дій), їх можливості (що можуть), їх інформованість про протилежну сторону (що знають) і порядок розіграшу очікуваних дій сторін. Можна сказати, що перелічені дані задають певну гру. Математичні методи опису дій протиборчих (антагоністичних) сторін складають зміст теорії ігор, які доцільно використовувати при відпрацюванні пропозицій до рішення, а саме замислу ведення службово-бойових дій. У теорії ігор для того, щоб передбачити результат гри – знайти рішення гри (або рівновагу гри), необхідно порівняти між собою множину раціональних і сталих стратегій дій сторін [224]. На сьогоднішній день у теорії ігор не існує універсальної концепції рівноваги [42, 52, 242]. Приймаючи ті або інші припущення стосовно принципів прийняття рішення сторонами, можна отримати різні по суті рішення. Тому основною задачею, що розглядається, є побудова рівноваги гри.

Прогнозування – одна з основних складових управлінського процесу. Без прогнозування, без уявлень про хід очікуваних подій, розвиток ситуацій не можливе прийняття ефективного рішення.

По-перше, застосовуючи ті або інші методи прогнозу, органи управління суб’єкту сил безпеки отримують для порівняльної оцінки прогнозовані значення показників своїх можливостей, значення показників ефективності службово-бойових дій, завдань всебічного забезпечення дій.

По-друге, прогноз результатів практичних дій дозволяє сформувати зміст команд управління в ході підготовки та ведення службово-бойових дій, які дозволять отримати саме ті прогнозовані результати.

Різниця між реальними і прогнозованими результатами формує «сигнал помилки» процесу управління та вимагає від органів управління знову приймати рішення, здійснювати прогноз і формувати нові команди управління.

За існуючими методиками прогнозу майбутнього є можливість вирішення проблеми проведення кількісної оцінки отриманих результатів, проведення критерійного аналізу для того, щоб на підставі порівняння результатів прийняти відповідне рішення.

На наступному етапі прийняття рішення – етапі визначення завдань за обраними стратегіями дій – здійснюється конкретизація сил (підрозділів), які б були здатними забезпечити реалізацію стратегії дій. Якщо сили та засоби, ресурси щодо забезпечення реалізації стратегії стають недостатніми, змінюються або способи досягнення бажаного результату, або стратегія дій, або взагалі змінюється мета службово-бойових дій. При зміні замислу або мети дій етапи підготовки й прийняття рішення повторюються. Такий ітераційний процес є необхідним, щоб вирішити багатокритерійну задачу при плануванні підготовки та ведення дій.

Процес узгодження критерійних оцінок у загальному випадку є значною проблемою, але задачу багатокритерійної оцінки командири вирішують у будь-якому випадку. З цього випливає необхідність знаходження шляхів формалізації цього складного процесу.

За зазначеною схемою методу прийняття рішення (рисунок 3.1) відбираються всі раціональні варіанти, які відповідають встановленим вимогам. Настає відповідальний момент, коли всі експерти сказали своє слово, настає та мить, заради якої великі колективи здійснювали «мозковий штурм». Цей момент належить командирові (начальнику) для здійснення завершального акту – прийняття рішення.

На підставі чого керівник зупиняє процес підготовки пропозицій до рішення? Крім інтуїції, яка сьогодні є рушійною силою у діяльності командира, існує необхідність у проведенні аналізу повноти інформації для прийняття рішення, достатності ступеня обґрунтування пропозицій експертів. Саме це характеризує якість рішення, але ця оцінка дається керівником, тому для об’єктивності цієї оцінки необхідно мати відповідне підґрунтя у вигляді окремого показника якості рішення, «правильності» рішення, «впевненості»

керівника у рішенні, яке він збирається оголосити. У загальному випадку керівник проводить багатокритерійну оцінку варіантів рішення.

Відомо, що багатокритерійна оптимізація, яка є достатньо складною проблемою з суто математичної точки зору, залишається проблемою прийняття рішень навіть після свого компромісного вирішення (наприклад, після побудови значної кількості варіантів пропозицій до рішення) – проблемою вибору остаточного єдиного компромісного рішення, що є прерогативою ОПР.

Результати експертиз стосовно порівняльної оцінки альтернативних варіантів рішення або одного варіанта рішення (якщо розробка альтернативних варіантів не передбачалася) надходять до ОПР. Вони є базою для прийняття управлінського рішення.

Поряд з результатами експертизи при прийнятті рішення ОПР ураховує додаткову інформацію про об’єкт прийняття рішення, яка може бути доступною лише йому як керівнику.

Крім того, як особистість ОПР може схилятися до різного ступеня ризику, віддавати перевагу тим або іншим способам досягнення результату, володіти різним досвідом реалізації тих або інших способів управлінського впливу на ситуацію, з різним ступенем розвинення почуття інтуїції.

Володіючи правом остаточного вибору і в повній мірі відповідаючи за прийняте рішення, ОПР віддає перевагу тому чи іншому альтернативному варіанту рішення.

Слід зауважити, що при прийнятті складних багатоаспектних рішень роль суджень спеціалістів, які професійно володіють проблемами, що впливають на рішення, значно зростає.

Колективне формування пропозицій до рішення – одна з найбільш важливих процедур процесу прийняття управлінських рішень. На відміну від процедури визначення експертних оцінок передбачається не тільки обробка результатів колективної експертизи, але також:

- використання спеціальних методів відкритого заслуховування спеціалістів, обговорення варіантів пропозицій до рішення;

- додатковий обмін інформацією між спеціалістами-експертами, що беруть участь у розробці пропозицій до рішення;

- узгодженість пропозицій до рішення з кожної проблеми, з кожної протилежної точки зору;

- взаємний вплив пропозицій до рішення стосовно кожного напрямку, з кожної проблеми та ін.

В силових структурах колективне обговорення доцільно лише на етапі формування пропозицій до рішення. У той же час акт прийняття рішення завжди є прерогативою одної особи – керівника. Для цього існують індивідуальні методи прийняття рішення, наприклад, метод одного експерта [231].

Право вибору стратегії досягнення мети діяльності віддається командиру, тому що на нього покладена вся відповідальність за виконання поставленого завдання.

Методи теорії прийняття рішень однакові для органів управління всіх галузей людської діяльності, її процеси визначаються об’єктивними закономірностями, існують деякі відмінності у діяльності силових структур.

Положення керівника, що приймає рішення, визначається:

- високим рівнем відповідальності за прийняті рішення;

- внутрішнім екстремальним середовищем, в якому організується його діяльність (психологічна, емоційна, фізична, мозкова напруженість, обмеження в часі);

- зовнішнім екстремальним середовищем, в якому здійснюється діяльність;

- положенням її в ієрархічній структурі суб’єкта сил безпеки;

- делегуванням людині повноважень, за які вона несе відповідальність;

- наданням людині прав і обов’язків для виконання поставлених завдань;

- можливістю делегування своїх повноважень і обов’язків іншим особам, які виступають у ролі підлеглих органів управління;

- професійним рівнем людини, що приймає рішення;
- організаційною культурою спілкування керівника з собі рівними і підлеглими.

На відміну від цивільних у організаціях сил безпеки передбачені спеціальні органи управління (командувач (командир), штаб), які за визначеними алгоритмами здійснюють процеси підготовки й прийняття рішення. В таких організаціях створюються спеціальні підрозділи, на які покладаються питання збору та обробки інформації, оцінки обстановки, формування пропозицій до рішення, оформлення відповідних документів, зберігання та доведення до виконавців завдань, контроль за їх виконанням.

Задача командувача (командира) полягає в організації спільної діяльності тих структур, що забезпечують підготовку рішень та контроль за їх виконанням.

Повсякденна діяльність колективів вимагає від командирів і начальників готовності постійно приймати відповідні рішення, що пов’язуються з менеджментом, тобто налагодженням зв’язків із зовнішнім середовищем для організації повсякденного життя, вирішенням та виконанням внутрішніх повсякденних завдань, що у цілому спрямовується на підготовку всього підрозділу до виконання завдань у бойовій обстановці.

У цьому сенсі будь-який командир (начальник) повинен бути відмінним менеджером. Чим вище професіоналізм менеджера-командира, тим ефективніші рішення він приймає, тим більший процент рішень, які дозволяють представникам сил безпеки досягати поставлених цілей.

Для менеджера з низьким професійним рівнем характерні або надлишкова обережність у прийнятті рішень, коли, побоюючись за свою кар’єру, він не має можливості прийняти сміливе, іноді єдине можливе рішення, або здійснює прийняття легких, недостатньо виправданих управлінських рішень без розуміння реальних наслідків, які можуть статися при прийнятті того або іншого рішення. Рішення, які можуть виявитися «непопулярними», деякі командири спрямовують або на старший рівень, або на

підлеглий ієрархічний рівень управління, або намагаються переадресувати задачу іншим структурам у горизонтальній площині управління.

Таким чином, методи людської діяльності, за якими здійснюються всі процеси прийняття рішень, є одним з важливих факторів щодо визначення методу прийняття рішень.

Суть методу прийняття рішення має визначати спосіб формування замислу рішення, що й дає назву методу прийняття рішень. Першим з них є нормативний метод підготовки й прийняття рішень.

Слід зауважити, що іноді для прийняття рішення не потрібно проводити взагалі ніяких розрахунків, рішення стосується, наприклад, організації діяльності відповідно до вимог керівних документів.

Цей метод застосовується в умовах визначеності обстановки, коли задача, яку необхідно вирішити, відноситься до конкретного складу сил та засобів, наявних ресурсів, тобто описується детермінованими вхідними даними. Рішення в даному випадку в основному приймається на підставі керівних документів з розрахунком окремих показників, які будуть підставою для прийняття рішення. У даних задачах, як правило, використовуються математичні методи теорії дослідження операцій.

Таким чином, можна зазначити, що нормативний метод стосується проблем поточного управління та оперативного прийняття рішень. У той же час цей метод може бути елементом інших більш складних методів прийняття рішень.

Експертом для прогнозу ситуацій може виступати сам командир або група його заступників, начальників відділів, служб, які є фахівцями з окремих напрямків військової діяльності. При прийнятті рішення нормативним методом, як правило, рішення стосується вибору способу виконання поставленого завдання. У критерійній оцінці якості прийнятого рішення будуть враховуватися не тільки отримані значення показників ефективності виконання завдання, але й відповідність чинності обраного способу виконання завдання вимогам керівних документів.

Даний метод формування пропозицій й прийняття рішення органами управління передбачає їх повну інформованість про загальну обстановку, тому задача полягає у виборі раціонального способу виконання завдання (із існуючих, що визначені керівними документами).

Метод базується на знаннях експертів вимог керівних документів з тих або інших питань діяльності. Якість прийнятого рішення характеризується часом, в межах якого було прийнято рішення, що забезпечило виконання поставленого завдання.

Можна характеризувати якість рішення ступенем відповідності результату вимогам щодо досягнення поставленої мети, значенням відносного показника відповідності застосованого способу виконання завдання при обмеженнях, що стосуються дотримання вимог керівних документів.

Багато прикладів складних умов можна навести при вирішенні проблем прийняття рішень в конкретній визначеній обстановці, коли у певних обставинах прийняте рішення має свої особливості.

При формуванні пропозицій до рішення сам командувач (командир) виступає як експерт в галузі конкретних знань, а якщо є потреба провести додаткові розрахунки, врахувати більш глибокі знання у спеціальних питаннях, командир може залучати інших експертів.

У задачах теорії прийняття рішення людина (або група осіб) стикається, як правило, з необхідністю розгляду декількох альтернативних варіантів пропозицій до рішення. Необхідність вибору може бути викликана будь-якою проблемною ситуацією, у якій є два стани: бажаний і дійсний, а способів досягнення бажаної мети (стану) – не менш двох. Таким чином, у людини в такій ситуації є деяка свобода вибору між декількома альтернативними варіантами. Кожний варіант вибору (вибір альтернативи) приводить до відповідного результату. У людини є свої уявлення про переваги й недоліки окремих результатів, своє власне відношення до них, а отже, і до варіантів рішення. Таким чином, у людини, що приймає рішення, є система переваг.

У загальному випадку процес прийняття рішення передбачає вибір

найбільш кращого варіанта рішення з множини припустимих альтернатив. У той же час людина, що приймає рішення, може й не формувати декілька варіантів пропозицій до рішення, бо саме рішення «лежить на поверхні», обумовлено керівними документами і залишається лише визначити деталі тих завдань, які необхідно поставити для виконання.

Але в той же час нормативний метод підготовки й прийняття рішень в умовах інформаційної невизначеності може стати неефективним, через те, що в ньому або відсутній процес прогнозування результату, або в процесі прогнозування (на окремому етапі прийняття рішення) застосовуються менш достовірні методи.

В умовах, коли органи управління стикаються з невизначеністю обстановки, можуть застосовуватися інші методи синтезу інваріантного рішення або поліваріантного аналізу.

Метод синтезу інваріантного рішення здійснюється шляхом декомпозиції загальної задачі на часткові з наступним синтезом пропозицій по часткових задачах в один варіант рішення. Особливість цього методу полягає в тому, що підлеглі нижчих рівнів управління, начальники служб, підрозділів після проведення досліджень проблем за своїм напрямком відповідальності у визначеній командиром послідовності та під його особистим керівництвом формують пропозиції до майбутнього рішення в єдиному для сприйняття форматі документів.

Процес підготовки й прийняття рішення має прескриптивний характер, що передбачає керуючий вплив командира на підлеглі органи управління; саме командир вказує їм, які пропозиції-альтернативи відповідають його уявленням про об’єкт управління.

Основною відмінністю цього методу є те, що після оцінки обстановки формування замислу рішення на службово-бойові дії здійснюється органами управління, виходячи з оцінки наявних сил та засобів, з оцінки співвідношення сил, з розстановки наявних сил на місцевості в тому чи іншому порядку. При цьому мета службово-бойових дій за своєю значущістю відходить на другий

план, а оцінка її досягнення відображається через оцінку прогнозу результатів виконання поставленого завдання, пошук шляхів виконання якого здійснюється в межах наявних ресурсів.

Пропозиції, що надаються командирові за окремими напрямками відповідальності, аналізуються ним особисто у поточному часі. За кожним напрямком відповідальності підлеглих органів управління відбираються і включаються до замислу рішення придатні варіанти пропозицій згідно з визначеним командиром критерієм. Розроблені пропозиції, якщо вони затверджені командиром під час аналізу, стають змістом замислу та набувають сили під час оголошення рішення.

Замисел після його затвердження дає можливість сформувати зміст завдань через авторизацію виконавців, відповідальних за виконання часткових завдань, які складали загальне завдання.

Інваріантність рішення в цьому випадку полягає в незалежності змісту рішення від рівня невизначеності обстановки та кількості відповідних пропозицій-альтернатив. Діяльність органів управління в даному методі спрямовується на зменшення часу щодо організації процесу формування пропозицій й прийняття рішення та зменшення часу на підготовку до службово-бойових дій [238, 242].

У даному методі в процесі підготовки пропозицій до рішення підлеглі начальники родів військ, служб стають експертами з проблем стосовно окремих спеціальних напрямків відповідальності (рисунок 3.3).

Керівник, що прийматиме рішення, на етапі підготовки пропозицій активно виступає основним експертом із загальних питань та самостійно здійснює у поточному часі відбір відповідних пропозицій до замислу рішення. Тобто за безпосередньою участю керівника, заступників, служб ще на початковому етапі формування пропозицій-альтернатив замислу у ритмі роботи органів управління створюються умови цілісності загального рішення для досягнення головної мети практичних дій.

За єдиний формат у ході узагальнення пропозицій до рішення прийнято

робочу карту командира (карту-замисел, карту-рішення), на яку послідовно, обговорюючи кожну складову рішення під керівництвом командира, наносяться елементи загального рішення. Всі варіанти пропозицій відповідних посадових осіб у ході обговорення (заслуховування) аналізуються командиром, відбираються кращі варіанти методом парето-оптимізації, після чого наносяться на карту, а текстуальна частина пропозицій включається до змісту пояснювальної записки до рішення.

Такий метод прийняття рішення застосовується в умовах стохастичної невизначеності, коли поставлене завдання у певних умовах обстановки і стану сил за обмежений час вимагає розглядати декілька варіантів пропозицій до рішення, а виникнення ситуацій і подій описується ймовірнісними законами. Обґрунтування пропозицій до рішення здійснюється за допомогою математичних методів дослідження операцій. Аналіз пропозицій здійснюється на етапі обговорення елементів замислу рішення, а обґрунтовані пропозиції відбираються самим командиром. У випадку, коли є значний час підготовки до службово-бойових дій, створюється можливість розглядання великої кількості варіантів пропозицій до рішення. У даних умовах доцільно використовувати метод поліваріантного аналізу і альтернативного вибору рішення.

Відмінність цього методу підготовки й прийняття рішення від попереднього полягає в тому, що на перший план виходить процес цілеутворення. Цей процес формує вимоги до кількісно-якісної оцінки сил та засобів, способів виконання завдань для досягнення сформованої мети. Сам процес має дескриптивний характер та дозволяє широко описувати можливі варіанти стану об’єкта дослідження [237, 238, 239, 240, 241].

Метод поліваріантного аналізу і альтернативного вибору рішення доцільно використовувати, наприклад, на етапі завчасного планування службово-бойових дій. При цьому для послаблення впливу невизначеності на результати прогнозу діяльності передбачається покрокове проведення декомпозиції головного завдання (головної мети ведення дій) з усім переліком наявних проблем по напрямках відповідальності підлеглих керівників-

експертів, органів управління.

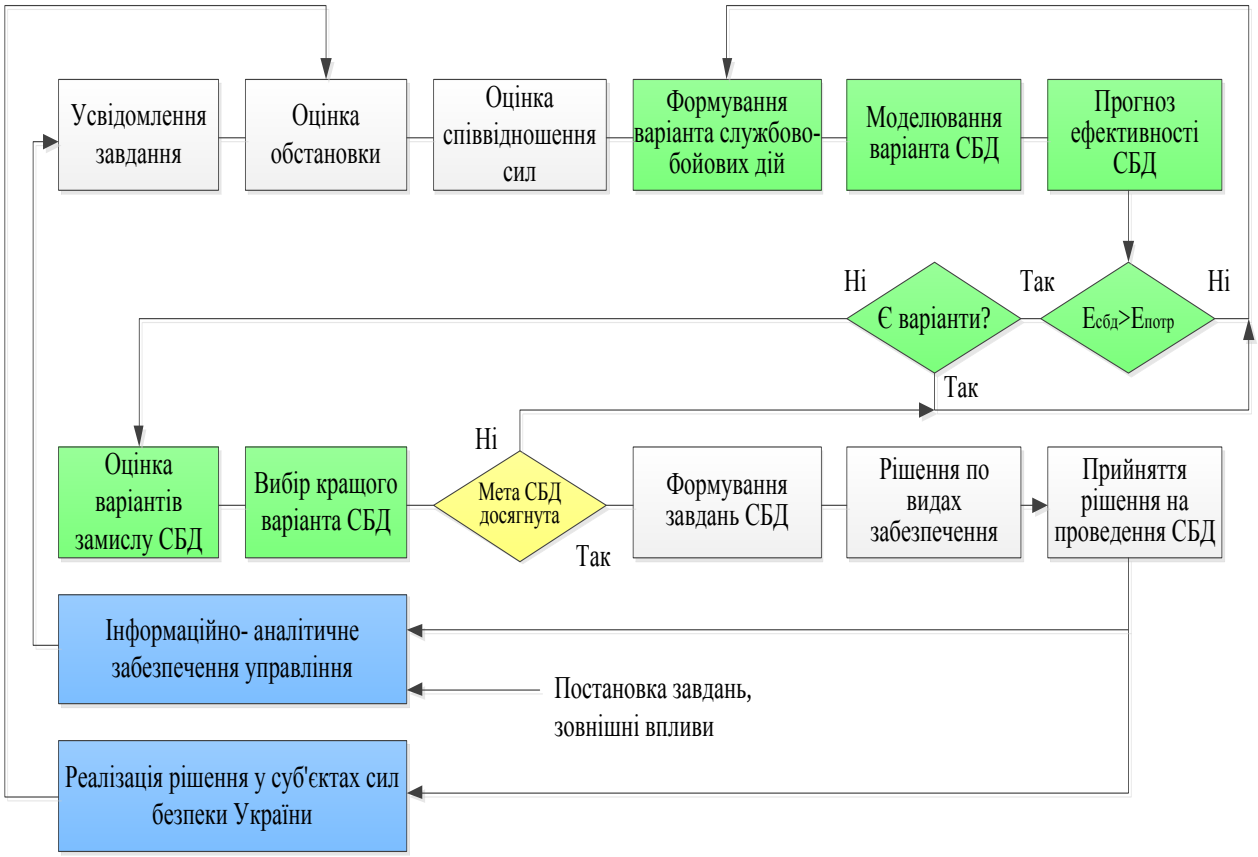

Рисунок 3.3 – Схема реалізації методу синтезу інваріантного рішення (зеленим кольором показаний етап формування замислу службово-бойових дій, жовтим кольором – перевірка узгодженості замислу і мети ведення дій, блакитним – блок інформаційного забезпечення) [238]

Кожен з них як би приймає своє окреме рішення по часткових складових загального варіанта службово-бойових дій. З комбінацій дій складаються варіанти дій підрозділів у цілому. Під час прогнозування результатів конкретного варіанта в заданих органами управління умовах вхідна інформація для процесу прийняття рішення вважається як би відомою. Командир при цьому виступає як головний експерт, який узагальнює варіанти часткових дій в єдині варіанти-альтернативи, що аналізуються методом моделювання з застосуванням спеціальних математичних методів теорії ігор, теорії

ймовірностей, нечітких множин та ін. [239].

Прогнозування в процесі прийняття рішення має велике значення. Прогноз як погляд у майбутнє дає можливість оцінити можливі шляхи розвитку подій, наслідків тих або інших рішень. Іноді прогноз базується на добре відомих закономірностях, тоді результати прогнозу мають більшу ступінь довіри. В умовах же природної (нестохастичної) невизначеності необхідно обирати таку кількість варіантів пропозицій до рішення, щоб перекрити діапазон варіантів всіх можливих дій протилежної сторони. Частиною тих варіантів, які не ввійдуть до повної сукупності розіграшів дій сторін, буде характеризуватися ступінь достовірності рішення, що приймається.

Якщо в методі формування інваріантного рішення прогноз результатів дій за декількома варіантами займає значну частину часу у загальному процесі прийняття рішення і відображає зміст самого рішення, то в методі поліваріантного аналізу прогнозування виступає як елемент складової процесу прийняття рішення – процесу створення пропозицій-альтернатив замислу службово-бойових дій для їх порівняльної оцінки. Причому сформована сукупність варіантів замислу службово-бойових дій як результат процесу підготовки й прийняття рішення зберігається на рівні безперервної готовності для подальшого аналізу та вибору альтернативи як рішення (рисунок 3.4).

Метод поліваріантного аналізу і альтернативного вибору рішення на відміну від методу формування інваріантного рішення застосовується в умовах природної (нестохастичної) невизначеності та передбачає технологію формування замислу органами управління, починаючи не від аналізу наявних сил та засобів, а від обґрунтування мети ведення службово-бойових дій. Процес цілеутворення в даному методі прийняття рішень є фундаментальним, і він об’єднує всі інші процеси метода в систему.

Технологія прийняття рішення з використанням даного методу передбачає реалізацію відповідної діяльності органів управління (рисунок 3.4).

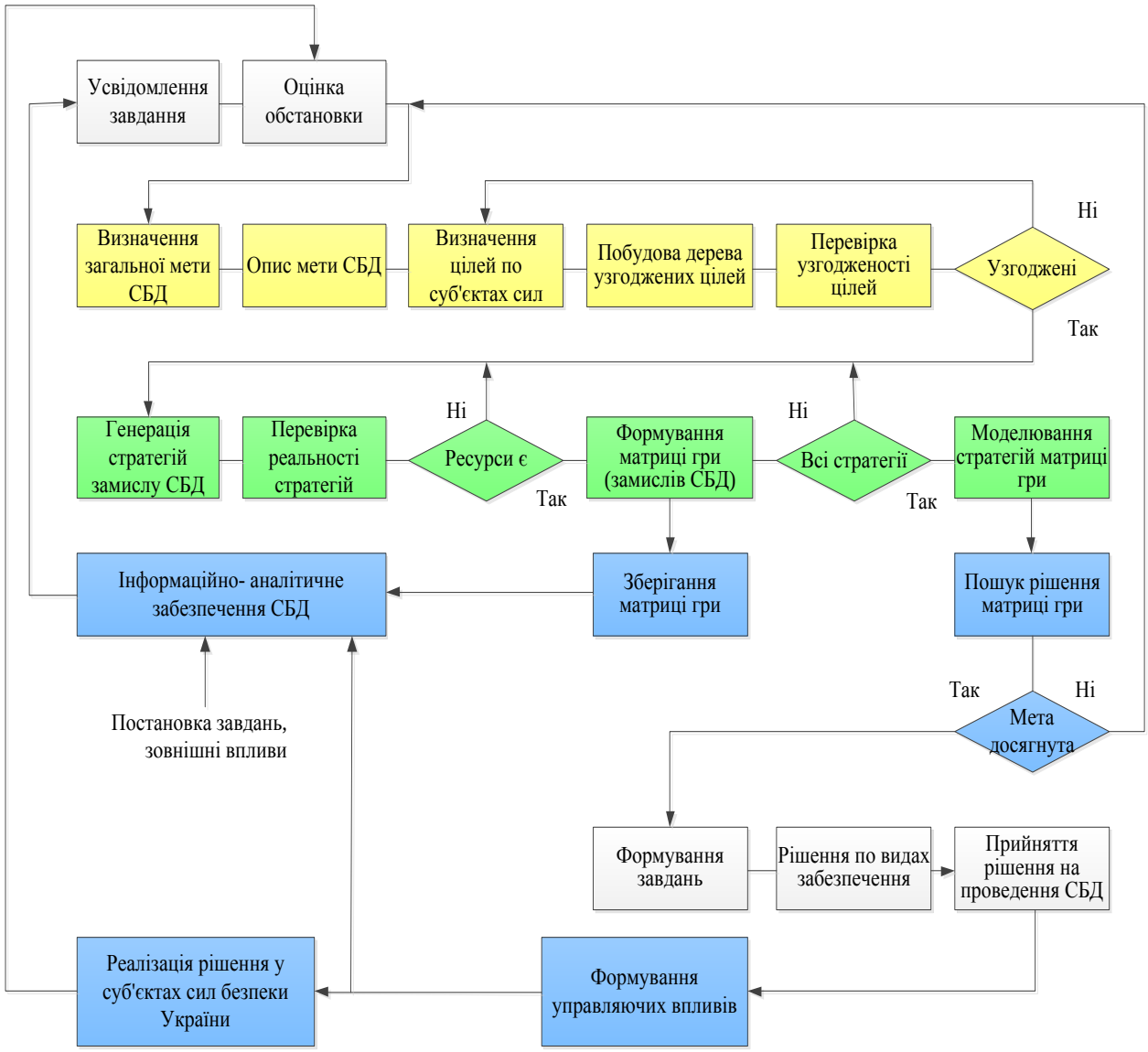

Рисунок 3.4 – Схема реалізації методу поліваріантного аналізу і альтернативного вибору рішення (жовтим кольором показаний етап цілеутворення, зеленим кольором показаний етап формування замислу службово-бойових дій, блакитним кольором показані блоки інформаційного забезпечення) [239]

3.2 Підсистеми захисту інформації в системі державного управління силами безпеки України

Система державного управління силами безпеки України охоплює численні підсистеми захисту інформації, оскільки захист інформації є

ключовим елементом забезпечення національної безпеки в сучасному світі. До основних складових цієї системи входять декілька підсистем, кожна з яких виконує важливу роль у забезпеченні безпеки інформації.

Однією з таких є інформаційно-аналітична підсистема, яка відповідає за збір, обробку, аналіз і використання інформації для прийняття управлінських рішень у сфері національної безпеки. Вона також включає системи зберігання і захисту конфіденційних даних, забезпечуючи їх цілісність та доступність.

Друга важлива складова – інформаційно-технічна підсистема, яка охоплює різні технічні засоби захисту інформації. Сюди входять системи шифрування, мережеві засоби безпеки, антивірусні програми та інші технічні рішення, спрямовані на захист інформаційних ресурсів від загроз.

Інформаційно-правова підсистема відіграє роль у розробці та впровадженні правових актів, що регулюють сферу захисту інформації в державі. Це включає закони про кібербезпеку, правила обробки конфіденційної інформації, відповідальність за порушення норм захисту інформації та інші важливі аспекти правового забезпечення інформаційної безпеки.

Ще одна важлива складова – організаційно-методична підсистема, яка забезпечує розробку та впровадження методик, стандартів, інструкцій та інших документів, що регулюють організаційні аспекти захисту інформації. Вона охоплює процедури аудиту безпеки, навчання персоналу та інші заходи, спрямовані на підвищення рівня захищеності інформації.

Технологічна підсистема захисту інформації відповідає за впровадження сучасних технологій, таких як системи ідентифікації та аутентифікації, контроль доступу, механізми виявлення і реагування на кіберзагрози. Ця підсистема є важливим елементом забезпечення цілісності, конфіденційності та доступності інформації.

Всі ці підсистеми взаємодіють між собою, забезпечуючи ефективний захист інформації в системі державного управління силами безпеки України. Вони також частково інтегровані в підсистеми захисту інформації кожного з суб'єктів сил безпеки.

Сьогодні до проблемних питань підсистеми захисту інформації в системі державного управління силами безпеки України належать [217]:

- несформованість актуального нормативно-правового поля;
- відсутність єдиного підходу до захисту інформації;
- зростання новітніх викликів щодо захисту інформації;
- широке впровадження іноземних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

Захист інформації є складною та багатогранною проблемою, яка включає як теоретичні, так і практичні аспекти, такі як технологія проєктування та створення захищених систем і засобів захисту.

Значний внесок у дослідження проблемних аспектів захисту інформації в системах управління суб'єктів сил безпеки та оборони України внесли такі вчені, як Мацько О. Й., Микусь С. А., Солонніков В. Г., Дробаха Г. А., Олещенко О.А., Іохов О.Ю., Горелишев С.А., Сафошкіна Л.В., Лісіцин В. Е. та інші. Також питання забезпечення інформаційної безпеки держави розглянуті у працях таких науковців, як Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І., Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є., Климчук О. О., Петрик В. М., Присяжнюк М. М., Мужанова Т.М.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. [68, 119], кібербезпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Це включає забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі».

Повноваження щодо протидії основним видам загроз кібербезпеці, таким як кіберзлочинність, кіберагресія та кібертероризм, покладаються на правоохоронні органи, сферу оборони, оборонно-промисловий комплекс і сферу державної безпеки [68, 119].

Закон [68] встановлює правові й організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження та обов'язки державних органів у цій сфері і основні принципи координації їх діяльності.

Відповідно до Закону, об'єктами кібербезпеки та кіберзахисту є:

- конституційні права і свободи людини і громадянина;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- об'єкти критичної інфраструктури.

Об'єктами кіберзахисту є комунікаційні системи різних форм власності, в яких обробляються національні інформаційні ресурси або які використовуються в інтересах органів державної влади, місцевого самоврядування, правоохоронних органів та військових формувань, створених відповідно до законодавства. До таких об'єктів також належать критичні інформаційні інфраструктури та комунікаційні системи, які забезпечують задоволення суспільних потреб та реалізацію правовідносин у сферах електронного урядування, державних послуг, електронної комерції та електронного документообігу [59, 68, 90, 119].

Одним з важливих досягнень Закону України «Про основні засади забезпечення кібербезпеки України» стало офіційне закріплення базових понять у сфері кібербезпеки на законодавчому рівні, а також чітке визначення прав і обов'язків державних органів у цій сфері [119].

Згідно з цим Законом, Національна система кібербезпеки складається з сукупності суб'єктів, що забезпечують кібербезпеку, та взаємопов'язаних заходів різного характеру: політичного, науково-технічного, інформаційного,

освітнього, організаційного, правового, оперативно-розшукового, розвідувального, контррозвідувального, оборонного, інженерно-технічного, а також заходів криптографічного та технічного захисту національних інформаційних ресурсів і кіберзахисту об’єктів критичної інформаційної інфраструктури [68].

Повноваження щодо забезпечення безпеки в кіберпросторі надані Президенту України, який керує Радою національної безпеки і оборони (РНБО), а також Національному координаційному центру кібербезпеки, що діє як робочий орган РНБО. Важливу роль у формуванні та реалізації державної політики у сфері кібербезпеки відіграє Кабінет Міністрів України, який не тільки захищає права і свободи громадян, національні інтереси в кіберпросторі та бореться з кіберзлочинністю, але й організовує та забезпечує функціонування національної системи кібербезпеки, формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, за винятком банківської системи України.

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція, Служба безпеки України, Міністерство оборони та Генеральний штаб ЗСУ, розвідувальні органи, а також Національний банк України. Крім того, суб’єктами, які безпосередньо здійснюють заходи з кібербезпеки у межах своїх повноважень, є різні міністерства та центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності, ЗСУ та інші військові формування, створені відповідно до законодавства. До них також належать підприємства, установи та організації, які відносяться до об’єктів критичної інфраструктури, суб’єкти господарювання, громадяни України та їх об’єднання, інші особи, які здійснюють діяльність або надають послуги, пов’язані з національними інформаційними ресурсами, електронними послугами, правочинами, комунікаціями, захистом інформації та кіберзахистом [59, 68, 90, 119]:

Законом передбачено, що суб’єкти забезпечення кібербезпеки у межах своїх повноважень здійснюють широкий спектр заходів, зокрема:

- запобігання використанню кіберпростору для воєнних, розвідувально-підривних, терористичних та інших незаконних і злочинних цілей;
- виявлення та реагування на кіберінциденти та кібератаки, усунення їх наслідків;
- організація інформаційного обміну щодо реалізованих і потенційних кіберзагроз;
- розробка та впровадження запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;
- проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;
- здійснення інших заходів, спрямованих на забезпечення розвитку та безпеки кіберпростору.

Згідно із Законом України, розподіл функцій і повноважень у сфері кіберзахисту між органами державної влади організовано таким чином [68]:

Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язок) відповідальна за кіберзахист об’єктів критичної інформаційної інфраструктури. Її функції включають координацію діяльності інших суб’єктів кібербезпеки, забезпечення створення та функціонування національної телекомунікаційної мережі, а також запобігання, виявлення та реагування на кіберінциденти та кібератаки. Держспецзв’язок також займається усуненням наслідків таких інцидентів, інформуванням про кіберзагрози та методи захисту, а також проведенням аудиту інформаційної безпеки на об’єктах критичної інфраструктури. Крім того, цей орган встановлює вимоги до аудиторів інформаційної безпеки та визначає порядок їх атестації та переатестації;

Національна поліція України (НПУ) має завдання попереджати, виявляти, припиняти та розкривати кіберзлочини, що є важливою частиною загальної стратегії кібербезпеки країни;

Міністерство оборони України та Генеральний штаб Збройних Сил України (ЗСУ) відповідають за кібероборону військових об’єктів, кіберзахист критичної інфраструктури під час війни та надзвичайного стану, а також за відбиття військової агресії у кіберпросторі;

Служба безпеки України (СБУ) в межах своїх повноважень займається попередженням, виявленням, припиненням та розкриттям злочинів проти миру та безпеки людства в кіберпросторі, боротьбою з кібертероризмом та кібершпигунством, а також проведенням таємних перевірок на об’єктах критичної інфраструктури;

Національний банк України (НБУ) виступає регулятором з питань кібербезпеки у банківській сфері, встановлює власні стандарти безпеки та організовує перевірку їх дотримання. Завдання НБУ включають визначення порядку, вимог та заходів щодо кіберзахисту та інформаційної безпеки в банківській системі, створення центру кіберзахисту та реєстру об’єктів критичної інформаційної інфраструктури в банківському секторі.

Законодавство передбачає активну співпрацю між державою та приватним сектором у сфері кібербезпеки. Система своєчасного виявлення, попередження та нейтралізації кіберзагроз може бути побудована із залученням волонтерських організацій. Планується підвищення цифрової грамотності громадян та розвитку культури безпеки поведінки у кіберпросторі. Окрім цього, заплановано створення консультаційних пунктів для громадян, промисловості та бізнесу, а також систему підготовки кадрів і підвищення компетентності фахівців у різних сферах, пов’язаних з кібербезпекою [68].

Отже, на законодавчому рівні закладено нормативно-правову основу для розбудови національної системи кібербезпеки України. Розподілено повноваження між органами державної влади та визначено роль Національного координаційного центру кібербезпеки, який відповідає за координацію та контроль діяльності суб’єктів сектору безпеки і оборони, що займаються кібербезпекою. Основне завдання центру – координувати дії цих суб'єктів, встановлювати процедури взаємодії та забезпечувати комплексні заходи

реагування на кіберзагрози, а також здійснювати роботу щодо попередження кіберзлочинів.

Однак, у сфері кібербезпеки України все ще існують значні виклики. Відсутні систематизовані нормативні документи, які б детально описували загрози у кіберпросторі, надавали їх чітке визначення та формували основу для цілісної державної політики з кібербезпеки. Крім того, експерти відзначають недостатню кількість кваліфікованих кадрів у сфері кібербезпеки, що пов’язано з низькою якістю підготовки, швидким розвитком технологій, труднощами у залученні практиків та небажанням молодих спеціалістів працювати у державних структурах. Відсутність профільних науково-дослідних інститутів, які б займалися комплексними дослідженнями з інформаційної та кібербезпеки, також ускладнює розвиток цієї сфери [119].

Значною проблемою є технологічна залежність України від іноземних програмних продуктів та матеріально-технічної бази. Це створює ризики для національної безпеки, оскільки важко виявити можливі загрози, пов'язані з використанням іноземних технологій. Важливим питанням залишається створення національної операційної системи, відновлення виробничих потужностей у сфері телекомунікаційного обладнання та розробка вітчизняного антивірусу [119, 125].

Крім того, українське суспільство, включаючи державні органи та установи, характеризується низьким рівнем культури кібербезпеки. Це відображається у недостатньому усвідомленні необхідності дотримання вимог безпеки та потенційних наслідків, що можуть виникнути через нехтування цими вимогами [119, 125].

Сучасне суспільство можна описати як інформаційне, де жодна галузь не може існувати і розвиватися без залучення кіберпростору. Глобальна інформатизація впливає на діяльність держав у всьому світі, а інформаційні технології використовуються для вирішення завдань національної, військової та економічної безпеки. Водночас, одним із ключових наслідків широкомасштабної інформатизації державних і приватних секторів є створення

нового середовища для конкурентного протиборства у кіберпросторі. Інтернет та інформаційні технології відкривають перед людством безліч можливостей, але й породжують нові серйозні загрози. Обсяги інформації, що циркулюють онлайн, зростають, і сьогодні у світі підключено понад 20 мільярдів пристроїв до Інтернету, що значно перевищує чисельність населення Землі. На серверах зберігаються мільярди гігабайтів даних. Цей відкритий світ вимагає створення нових правил взаємодії [200].

Сучасний світ неможливо уявити без інтенсивного впровадження інноваційних інформаційних технологій, які торкаються всіх сфер життя, включаючи органи державної безпеки. Застосування сучасних технологічних рішень відіграє важливу роль у прискоренні та оптимізації робочих процесів сил безпеки, але одночасно вносить певні виклики та ризики, особливо в контексті кібербезпеки.

Сили безпеки, залучаючи передові інформаційні технології, отримують змогу значно покращити ефективність своїх операцій. Цифровізація допомагає в аналізі великих обсягів даних, швидкому обміні інформацією між підрозділами та партнерами, а також у реалізації комплексних міжнародних операцій. Проте, ці ж технології можуть створювати потенційні загрози для кібербезпеки, оскільки зростає залежність правоохоронної системи від цифрового простору, що робить її вразливою перед обличчям кібератак.

Кіберзагрози для правоохоронних органів варто розглядати з двох основних позицій. По-перше, правоохоронні органи повинні активно працювати над запобіганням та протидією кіберзагрозам, розробляючи і впроваджуючи заходи кібербезпеки. Це включає створення спеціалізованих підрозділів, розробку і виконання стратегій захисту інфраструктури та даних, а також навчання персоналу ефективним методам протидії кіберзлочинності. По-друге, правоохоронні структури самі можуть стати об’єктами кіберзагроз, що вимагає від них розробки особливих механізмів захисту, зокрема впровадження сучасних технологій шифрування, використання захищених каналів зв’язку та застосування надійних систем ідентифікації і аутентифікації.

Така двоїстість впливу інформаційних технологій на правоохоронну діяльність актуалізує необхідність комплексного підходу до забезпечення кібербезпеки. Розробка державної політики в цій сфері має бути спрямована не тільки на формування ефективної системи захисту державних інформаційних ресурсів, але й на створення умов для сталого розвитку інформаційних технологій у секторі безпеки.

Не менш важливим є взаємодія між різними правоохоронними агенціями та іншими державними та приватними секторами, а також міжнародна співпраця у цій області. Обмін знаннями, технологіями та кращими практиками може значно підвищити загальний рівень кіберзахисту та ефективно протидіяти транснаціональним кіберзагрозам.

Розуміння цих аспектів та впровадження комплексних мір безпеки стануть ключовими у забезпеченні стабільності та безпеки не тільки в національних масштабах, але й на міжнародному рівні.

У сучасному світі, де інформація стала ключовим ресурсом, кібербезпека набуває вирішального значення. З кожним роком наукові дослідження в цій сфері активізуються, оскільки вчені та експерти намагаються відповісти на виклики, що постійно змінюються через швидкий розвиток технологій. Кібербезпека і її окремі аспекти перетворились на предмет багатьох наукових праць, проте розуміння цієї складної проблеми досі залишається неповним. Це частково пояснюється невідповідністю темпів теоретичних досліджень до швидкості змін у цифровому світі.

З розвитком цифрових технологій відбувається стрімке зростання впливу інформаційних систем на суспільні відносини, що веде до появи нових загроз громадській безпеці. Це, у свою чергу, вимагає негайного реагування та адаптації систем безпеки до сучасних умов. Виникає потреба не тільки у захисті інформаційної інфраструктури, але й у захисті самих громадян від нових форм кіберзлочинів.

Саме поняття кібербезпеки потребує переосмислення в контексті глобальних змін у феномені інформації. Зі збільшенням обсягу даних, які

обробляються та зберігаються в цифровому форматі, зростає й рівень потенційних кіберзагроз. Такі загрози можуть виникати не тільки ззовні, але й всередині самісіньких організацій, змушуючи їх постійно вдосконалювати методи захисту та відновлення даних.

Крім технологічного аспекту, кібербезпека торкається й правових питань. Створення ефективного законодавства, яке б відповідало сучасним вимогам кіберпростору, є складним завданням. Вимоги до законодавчих змін мають бути гнучкими, щоб адаптуватися до нових технологічних реалій, забезпечуючи при цьому захист прав громадян і приватності.

Наукове співтовариство, у свою чергу, повинне активізувати міждисциплінарні дослідження, залучаючи експертів з різних галузей для розробки нових підходів до розуміння та вирішення проблем кібербезпеки. Це включає вивчення соціологічних, психологічних та економічних аспектів кіберзахисту, а також аналізування впливу кіберзагроз на національну та міжнародну безпеку.

Зростаюча «інформаційність» світового співтовариства ставить перед ученими, політиками та правоохоронцями нові виклики. У відповідь на ці виклики необхідно не тільки розробляти нові технології та методики, але й формувати нову культуру кібербезпеки, яка б включала підвищення обізнаності та відповідальності серед звичайних користувачів Інтернету [107].

Питання кібербезпеки, в цілому, та кібербезпеки правоохоронної системи досліджували в своїх працях: С. Абрамов, А. Аносенко, А. Актонюк, В. Білоус, І. Бородін, В. Горбулін, В. Григор’єв, В. Гусєва, В. Гулай, П. Демідов, О. Доренський, О. Дзьобань, Ю. Заболотна, В. Зверев, Т. Карабін, А. Качинський, І. Кушнір, О. Криворучко, А. Кубаєнко, О. Корнейко, Я. Кулешник, В. Кудінов, О. Косаревська, К. Ісмайлов, А. Ландіна, Я. Лазур, А. Легеза, Ю. Лісовська, І. Лях, В. Маковій, Я. Малик, Й. Мастяниця, С. Мельник, Н. Нижник, О. Орлик, В. Пашорін, Д. Прокопович-Ткаченко, О.Прокоф’єва-Янчиленко, В. Прокопчук, С. Рзаєва, Радутний, В. Рассамакін, Г. Ситник, В. Світличний, Т. Савченко, М. Савчин, В. Сеник, О. Соснін, О. Сільмак, Д. Ткаченко, О. Трофименко, Н.

Черняк, В. Щирська, Г. Форос, Т. Шевчук, Л. Шиманський та інші.

Зазначені вчені розглядали різні аспекти прояву кібербезпеки у правоохоронній діяльності, проте, на сьогодні, невирішеними залишилися питання механізмів державної політики щодо забезпечення кібербезпеки правоохоронної системи.

Можна погодитись з думкою Євдокімова В.В. та Грицишина Д.О., що «XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі. Питома вага кіберзагроз у спектрі загроз національній безпеці країн зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить лише не забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об’єктів противника шляхом руйнування інформаційних систем, які управляють такими об’єктами» [102 с. 517, 226].

У сучасному світі, який характеризується швидким розвитком інформаційних технологій, відчути себе повністю захищеним у кіберпросторі

стає дедалі складніше. Зі збільшенням кількості цифрових пристроїв та послуг, різноманітність та кількість кіберзлочинів зростають з неймовірною швидкістю, що робить кіберзлочинність однією з найбільших загроз XXI століття. На цьому фоні з'являються нові сфери суспільного життя, які в свою чергу породжують нові виклики та загрози для безпеки громадян.

Державна влада та правоохоронні органи повинні активно реагувати на ці виклики, забезпечуючи захист національних інтересів, а також інтересів кожного громадянина в кіберпросторі. Це включає не тільки захист персональних даних і приватності, але й забезпечення стабільності та безпеки на державному рівні. Забезпечення кібербезпеки стає одним із ключових елементів національної безпеки.

Кіберпростір є безмежним і неконтрольованим, що надає досвідченим хакерам можливість діяти інкогніто, використовуючи свої навички та засоби для здійснення атак. Ці атаки можуть завдавати шкоди не тільки індивідуальним особам та компаніям, але й цілим країнам, підриваючи їхню економічну та політичну стабільність.

Сучасні технології, такі як смартфони та соціальні мережі, хоч і приносять значні переваги для зв'язку та доступу до інформації, також роблять користувачів вразливими перед обличчям кіберзагроз. Наші цифрові відбитки містять часто більше інформації про нас, ніж ми можемо усвідомлювати, і ці дані можуть бути використані зловмисниками для завдання шкоди.

Відповідь на ці виклики вимагає комплексного підходу, що включає законодавчі зміни, технологічні інновації та міжнародну співпрацю. Законодавство повинно адаптуватися до нових реалій, забезпечуючи ефективний захист від кіберзлочинів та зловмисників. Технологічні інновації мають зосередитися на розробці більш безпечних систем та методів аутентифікації, які зможуть виявляти та блокувати загрози. Міжнародна співпраця є ключовою, оскільки кіберзлочини не знають кордонів і можуть бути здійснені з будь-якої точки світу [84].

На думку Грицишина Д.О. [102] кіберзагрози для держави, в цілому, та

правоохоронної системи можуть проявлятися різними наслідками: соціальними, політичними, економічними, матеріальними, людськими жертвами, психологічними та іншими. Кіберзлочини чинять вплив, як на соціально-економічні відносини в певній державі, так і на світову економіку. «Хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів або 820 мільярдів євро. Про це свідчать оприлюднені дані американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнароднихдосліджень (CSIS). Завданий цього року хакерами збиток є на 50 відсотків вищим, ніж був у 2018 році, встановили дослідники. Таким чином збитки, завдані хакерами у 2020 році, становлять понад один відсоток світового ВВП, інформує агенція AFP» [88, 102 с.518]. «Кіберзлочинність у всьому світі що року завдає збитків на десятки мільярдів доларів США як державам, так і приватним компаніям. Чого лиш варта атака вірусу «Petya», який призвів до зупинення багатьох державних інституцій світу та бізнесу, зокрема й в Україні» [186].

Статистичні дані щодо кіберзлочинів в Україні свідчать про особливу їх загрозу (табл. 3.3) для національної безпеки.

Таблиця 3.3 – Статистичні дані щодо кіберзлочинів в Україні у 2020-2023 роки за даними Національної поліції [74]

Роки	2020	2021	2022	2023
Кількість кіберзлочинів, тисяч	4,2	10	14,9	17,3

Дана статистика, в цілому, показує, що кількість кіберзлочинів неухильно зростає. Важливе значення у забезпеченні кібербезпеки системи державного управління правоохоронної системи, зокрема, покладається на запобігання та протидію хакерським атакам, що значно активізувалися у довоєнний та воєнний періоди:

- довоєнний період: «За останні місяці Україна не вперше зазнає кібератак: найбільша з них до 15 лютого булла зафіксована ще 14-15 січня. В «Українському кіберальянсі» заявляють, що зловмисникам вдалося не лише зламати сайти міністерств та застосунок «Дія», а й викрасти персональні дані мільйонів людей із бази МВС країни. Однак в СБУ повідомили, що витоку даних внаслідок кібернападу не відбулося. Втім, деякі електронні сервіси, наприклад, сервіс перевірки полісу страхування цивільної відповідальності автовласників, не працювали після цієї атаки ще кілька тижнів» [102 с. 520, 174];

- воєнний період: «За місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення, DDoS-атаки» [53]. «Загалом за місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року: 198 проти 76. Проте більшість із них безуспішні та майже не впливають на роботу критичної інформаційної інфраструктури» [89, 102].

Проблема кібератак характерна і для інших країн світу, що представлено в табл. 3.4 та табл. 3.5.

Хакерські атаки у світі у період 2020 р. по 2023 р. найбільше здійснювалися проти таких країн, як США (46%), Україна (19%), Великобританія (9%), Бельгія (3%), Німеччина (3%), Ізраїль (2%), Молдова (2%), Португалія (1%), Саудівська Аравія (1%) та інших (10%). Так, більша частина хакерських атак (79%) була спрямована на корпоративні цілі. Головними секторами, проти яких були спрямовані хакерські атаки стали: державного управління, неурядові організації та аналітичні центри, освіта, міжнародні міжурядові організації, ІТ, медіа, охорона здоров'я, енергетика та інші. Протягом досліджуваного періоду, найбільшу кількість хакерських атак було зафіксовано з території рф (58%), друге місце у цьому рейтингу посідає КНДР (23%). Наступна країна за місцем походження хакерських атак с Іран

(11%). Незначний відрив від Ірану має Китай, з території якого було здійснено 8% хакерських атак. Також, атаки були зафіксовані з території Південної Кореї, В'єтнаму, Туреччини та інших країн [102].

Таблиця 3.4 – Хакерські атаки в світі за 2020-2023 роки [102, 202]

Країни, проти яких були спрямовані хакерські атаки						
США	Україна	Великобританія	Бельгія	ФРН	Ізраїль	Інші
46%	19%	9%	3%	3%	2%	15%
Хакерські атаки за країнами походження						
рф	КНДР	Іран	КНР	Півд. Корея	В'єтнам	Туреччина
58%	23%	11%	8%	≤1%	≤1%	≤1%
Сектори, проти яких були спрямовані хакерські атаки у світі						
Державне управління		Неурядові організацій та аналітичні центри			Освіта	
48%		31%			3%	
Міжнародні міжурядові організації		IT			Медіа	
3%		2%			1%	
Охорона здоров'я		Енергетика			Інші	
1%		1%			10%	

Найбільш активною хакерською группою можна назвати російське угрупування Nobelium, активність якого сягає 59%. Дане угрупування здійснювало хакерські атаки на сектори державного управління, дипломатії, оборони, неурядових організацій, IT, телекомунікацій та аналітичних центрів. Друге місце за активністю посідає угрупування Thallium, яке здійснює свою діяльність із території КНДР. Від діяльності зазначеного угрупування найбільше постраждали сектори дипломатії, науки та аналітичних центрів. Загалом, активність групи сягає 16%. Варто зазначити, що на території КНДР

також діє група Cetrium, яка здійснювала атаки на об’єкти аналітичних центрів, дипломатії, оборони, науки, аерокосмічної галузі. Загалом, активність даного угрупування сягає 5%.

Таблиця 3.5 – Найбільш активні хакерські групи [102 с.521, 202]

Об’єкти хакерських атак	Група та країна знаходження							
	рф	КНДР	Іран	КНДР	КНР	КНР	Іран	Інші
	Nobelium	Thallium	Phosphorus	Cetrium	Zirconium	Nickel	Curium	
Державне управління	+				+	+	+	
Дипломатія	+	+	+	+	+	+		
Оборона	+			+			+	
Ядерна політика			+					
Неурядові організації	+							
ІТ	+						+	
Телекомунікації	+							
Аналітичні центри	+	+		+				
Наука		+	+	+				
Журналістика			+					
Економіка					+			
Аерокосмічна галузь				+				
Активність групи	59%	16%	9%	5%	3%	2%	2%	4%

Також активне хакерське угрупування Phosphorus, якє здійснює напади на сектори дипломатії, ядерної політики, науки та журналістики. Дана группа базується на території Ірану, так само, як і угрупування Curium. Curium здійснює хакерські атаки на об’єкти державного управління, оборони та ІТ. Zirconium та Nickel є китайськими угрупуваннями, активність яких сягає 35%

та 12%, відповідно. Об’єктами їх атак стали сектори державного управління та оборони. Групою Zirconium були здійснені атаки на сектори економіки. Варто зазначити, що понад 4% активності хакерських угрупувань досі не визначено кому належать [102].

«Однією з перших держав, що сприйняла кібербезпеку як питання державного рівня, була США, де 2003 року було опубліковано Національну стратегію безпеки в кіберпросторі. У наступні роки в Європі поширювались плани заходів та стратегії, покликані розв’язати подібну задачу. Через кібератаку 2007 року Естонія стала однією з перших держав-членів Євросоюзу, яка опублікувала 2008 року національну стратегію кібербезпеки, у якій особливу увагу зосереджено на безпеці ІКТ» [250].

Правова основа для забезпечення кібербезпеки в Україні ґрунтується на низці важливих документів, серед яких Конституція України, законодавчі акти, що регулюють основи національної безпеки, внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів, а також інформації, захист якої встановлено законом. До цієї основи входить і Конвенція про кіберзлочинність, інші міжнародні договори, які були ратифіковані Верховною Радою України, укази Президента України, акти Кабінету Міністрів України та інші нормативно-правові акти, що ухвалюються для реалізації законів України [8, 166].

Правове забезпечення механізмів кібербезпеки, особливо для сил безпеки України, складається з кількох ключових нормативно-правових актів:

Зокрема, Кримінальний кодекс України містить статті, спрямовані на запобігання та протидію кіберзлочинам і забезпечення кібербезпеки. Це такі статті, як [103]: ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку; ст. 361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а розповсюдження або збут, ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в

електронно-обчислювальних автоматизованих машинах (комп'ютерах), системах, комп'ютерних мережах або на носіях такої інформації; ст. 362 несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; ст. 363 порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

- Закон України «Про основні засади забезпечення кібербезпеки України» встановлює основи правового регулювання у сфері кібербезпеки. Він визначає правові основи забезпечення кібербезпеки, об'єкти кібербезпеки та кіберзахисту, специфіку діяльності суб'єктів кібербезпеки, а також принципи забезпечення кібербезпеки. У Законі визначено напрями розвитку національної системи кібербезпеки, включаючи взаємодію державних суб'єктів з приватним сектором, міжнародними організаціями та іншими країнами, фінансове забезпечення заходів кібербезпеки та моніторинг їх виконання [166]. Національна система кібербезпеки, відповідно до Закону, охоплює сукупність суб'єктів, що забезпечують кібербезпеку, а також заходи політичного, науково-технічного, інформаційного, освітнього, організаційного, правового, оперативно-розшукового, розвідувального, оборонного, інженерно-технічного та криптографічного характеру. Ця система також включає заходи кіберзахисту об'єктів критичної інформаційної інфраструктури.

Відповідно до цього Закону, формування механізму державної політики у сфері кібербезпеки для сил безпеки має відповідати цим правовим нормам. Зокрема, терміни, визначені у законі, такі як «кібербезпека», «кібератака», «кіберзагроза» та «кіберзахист», слугують базовими поняттями, що формують

основи для державної політики у цій сфері.

Державна політика щодо забезпечення кібербезпеки в Україні враховує той факт, що сили безпеки є не лише інструментом для запобігання кіберзагрозам, але й об'єктом таких загроз. Тому існує необхідність забезпечення кібербезпеки як усіх сил безпеки, так і окремих суб'єктів або видів службово-бойової діяльності. Це забезпечення повинно здійснюватися в контексті загальної державної інформаційної політики та політики захисту інформаційної безпеки, що разом утворює систему кібероборони.

Значну увагу у країнах Європи приділяють принципам, на яких повинна базуватися державна політика забезпечення кібербезпеки, як загалом, так і в окремих секторах, зокрема (табл. 3.6). у правоохоронній системі. Сучасні системи управління, що побудовані на базі обчислювальних мереж, особливо потребують розробки та впровадження новітніх систем захисту інформації [166].

У кожному суб'єкті сил безпеки існує власна підсистема захисту інформації, яка має свої специфічні вимоги до рівня захищеності. Відсутність уніфікованого підходу до цих підсистем знижує загальну ефективність державного управління у сфері інформаційної безпеки. Оскільки сили безпеки України є ключовим елементом у забезпеченні державної безпеки, захист інформації, яка циркулює в їхніх мережах, має безпосередній вплив на національну безпеку. Витоки конфіденційної інформації можуть призвести не тільки до серйозних іміджевих втрат для держави, але й до значних втрат на полі бою, що особливо небезпечно в умовах військового конфлікту.

Розробка та вдосконалення механізмів державного управління системами захисту інформації у силових структурах України є надзвичайно актуальним завданням, враховуючи нові виклики, з якими стикається держава. Збройна агресія рф проти України виявила нові загрози для інформаційної безпеки, які потребують негайної та ефективної реакції з боку сил безпеки та оборони.

Таблиця 3.6 – Принципи забезпечення кібербезпеки у нормативних документах країн Європи [102]

Нормативний акт	Принципи
Німеччина	
Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) [266]	узгодження набору інструментів для реагування на кібератаки
	регулярна оцінка ситуаці, ризиків та прийняття відповідних засобів захисту
	регулярні тренування персоналу та тестування обладнання
	зміцнення IT-безпеки у сфері державного управління
Естонія	
Стратегія кібербезпеки Естонії (Cyber Security Strategy) [267]	кібербезпека с невід'ємною частиною національної безпеки, підтримує функціонування конкурентоспроможність держави економіки суспільства, інновацій, забезпечується на основі принципу пропорційності, беручи до уваги існуючі та потенційні ризики і ресурси
	гарантується дотриманням основних прав і свобод, а також захисту особистої інформації та особистості
	починається з індивідуальної відповідальності за безпечне використання засобів ІКТ
	підтримується інтенсивністю конкурентоспроможністю досліджень і розвитку на міжнародному рівні
	забезпечується на узгодженій основі в рамках співпраці між державним, приватним та третім сектором, беручи до уваги взаємозв'язок і взаємозалежність існуючої інфраструктури і сервісів в кіберпросторі
	забезпечується за допомогою міжнародного співробітництва з союзниками і партнерами

продовження таблиці 3.6

Польща	
Стратегія кібербезпеки Польщі (Cyberspace Protection Policy of the Republic of Poland) [268]	законодавчих заходів
	процедурних і організаційних заходів (система менеджменту)
	виховання, навчання та підвищення обізнаності в галузі безпеки
	технічних дій (збільшення кількості команд для реагування на інциденти безпеки у державних установах, тестування рівня безпеки, розвиток системи попередження, запобігання інцидентам і прийняття профілактичних рішень)
Чорногорія	
Стратегія кібербезпеки Чорногорії (Strategy on Cyber Security of Montenegro to 2017) [296]	визначення інституційної та організаційної структури в сфері кібербезпеки в державі
	захист критичних інформаційних структур
	зміцнення потенціалу державних правоохоронних органів
	реагування на інциденти
	посилення ролі Міністерства оборони та військових Чорногорії в кіберпросторі
	державно-приватне партнерство
	підвищення обізнаності громадськості та захисту користувачів
Австрія	
Стратегія кібербезпеки Австрії (Austrian Cyber Security Strategy) [263]	дотримання закону
	самоврегулювання
	пропорційність
	ієрархічність
	конфіденційність
	цілісність
	автентичність
	доступність, приватність
	захист даних
Угорщина	
Стратегія кібербезпеки Угорщини (National Cyber Security Strategy of Hungary) [289]	співпраця на різних рівнях
	підвищення рівня обізнаності та освіченості громадян в сфера кібербезпеки
	захист дітей у кіберпросторі
	розвиток нормативно-правової та технічної бази
	мотивація комерційного сектору

Ці загрози ставлять перед Україною складні завдання, що вимагають модернізації та покращення існуючих систем захисту інформації. Необхідно забезпечити інтеграцію новітніх технологій і підходів до захисту інформації, які відповідають сучасним вимогам безпеки. Це передбачає створення ефективних механізмів виявлення, попередження та реагування на інформаційні загрози, а також забезпечення координації дій між різними суб'єктами державної безпеки.

Особливої уваги потребує питання захисту інформації в умовах кіберзагроз, які стають дедалі складнішими і технологічно просунутими. Важливим завданням є також навчання та підготовка персоналу сил безпеки у сфері інформаційної безпеки, щоб забезпечити їхню готовність до протидії новим викликам.

Таким чином, для забезпечення національної безпеки необхідно не тільки покращити існуючі підсистеми захисту інформації у силах безпеки України, але й розробити нові, більш ефективні стратегії та механізми, які будуть відповідати сучасним умовам і викликам.

3.3 Засади автоматизації інформаційних систем управлінського призначення сил безпеки передових країн ЄС та НАТО

Основною функцією сил безпеки та оборони України є забезпечення потрібного рівня державної безпеки. Державне управління силами безпеки та оборони має багатогранні аспекти. В умовах широкого розповсюдження систем інформатизації та автоматизації процесів управління виникає гостра необхідність в забезпеченні сил безпеки засобами автоматизації [56]. На думку фахівців, як закордонних так і вітчизняних автоматизація інформаційних систем управлінського призначення є ключовим елементом у забезпеченні ефективності та оперативності рішень у сфері національної безпеки та оборони передових країн ЄС та НАТО. В умовах зростаючих загроз і викликів, ефективна обробка, аналіз та розподіл інформації здатні значно підвищити

реагування та адаптивність сил безпеки. Автоматизація інформаційних систем обумовлена потребою збільшення швидкості обробки даних, зниження впливу людського фактора на процеси прийняття рішень і підвищення їх об'єктивності. Основою автоматизації є використання сучасних інформаційних технологій, зокрема, штучного інтелекту, машинного навчання, великих даних та обчислювальної техніки [233].

В ЄС та НАТО активно впроваджуються стандартизовані рішення, такі як NATO Architecture Framework (NAF), що сприяє інтеграції та сумісності систем між країнами-членами. Використання хмарних технологій, кібербезпеки та шифрування забезпечує захист інформації та її конфіденційність [125]. Інноваційні рішення, такі як системи безпілотних літальних апаратів (БПЛА) для розвідки та моніторингу, використання штучного інтелекту для аналізу великих даних, забезпечують нові можливості для сил безпеки. Автоматизовані системи управління (АСУ) стають вирішальним елементом в сучасних військових конфліктах, дозволяючи забезпечити швидке реагування, високу точність прийняття рішень та ефективне управління військовими ресурсами. Країни ЄС активно інтегрують новітні технології в свої військові системи для підвищення обороноздатності та сумісності зі структурами НАТО.

Прийнятий курс держави на вступ до НАТО понукає шукати шляхи взаємосумісності державних систем управління силами безпеки з аналогічними система країн ЄС та НАТО.

Значний внесок у дослідження проблемних питань автоматизації інформаційних систем управлінського призначення сил безпеки та оборони України зробили таківчені як: Мацько О. Й., Микусь С. А., Солонніков В. Г., Дробаха Г. А., Олещенко О.А., Іохов О.Ю., Горелишев С.А., Сафошкіна Л.В., Лісіцин В. Е.ін.

В епоху повномасштабного конфлікту між Україною та російською федерацією, автоматизація керування військовими силами стає надзвичайно важливою. Структури безпеки та оборони, подібно до інших державних органів, неустанно розвиваються, адаптуються та стають складнішими. Це

супроводжується появою нових видів озброєнь, створенням нових військових формувань, виділенням нових завдань, а також зміною методик і стратегій ведення бойових дій. В контексті ведення бойових операцій, ключовим фактором є швидкість збору, обробки, перетворення, передачі та використання інформації, а також методи її збереження.

Розвиток та впровадження концепції автоматизованих систем управління військами (АСУВ) та її технологічних можливостей можна умовно розбити на кілька ключових періодів [183, 233]:

1960-1980-ті роки: Цей період характеризується розробкою та впровадженням у військові структури комп'ютерних мереж, включаючи бортові обчислювальні комплекси, що знайшли застосування у повітряних, підводних силах, ракетних та радіотехнічних військах. Це також час, коли методи моделювання почали активно використовуватися для планування воєнних операцій, а в США були розроблені перші військові автоматизовані системи управління, зокрема система глобального управління та контролю (Worldwide Military Command and Control System) у 1962 році [183, 233].

1980-1990-ті роки: Цей час ознаменувався подальшим розвитком концепції автоматизації на тлі технологічного прогресу, включаючи створення перших АСУ тактичного рівня, як-от АСУ боєм "Маневр" у СРСР у 1983 році та Battlefield Management System у США протягом 1986-1987 років. Також була розпочата робота над інтеграцією окремих АСУ в єдині системи управління, наприклад, Joint Operations Tactical System у США у 1992 році та Army Tactical Command and Control System, розробка якої стартувала в 1987 році [183, 233].

З 1990-х років до сьогодення: Період, протягом якого було створено єдині системи управління, які охоплюють всі військові структури без винятку, тим самим визначивши АСУВ у сучасному її розумінні як конгломерат різноманітних автоматизованих систем управління. Серед прикладів можна вказати Global Command and Control System у США (1996 рік) та Joint Consultation, Command and Control Information Exchange Data Model в НАТО (2007 рік) [183, 233].

Таким чином, історія розвитку АСУВ, як на Заході, так і в СРСР, свідчить про довгий шлях еволюції цих систем. Значні інвестиції урядів багатьох країн світу у цю сферу (з ринком АСУ, що становив $33 мільярди у 2022 році та очікуваним зростанням до $44,9 мільярда у 2027 році) підкреслюють стратегічну важливість автоматизованого управління військами для підвищення ефективності та реактивності військових операцій [183].

Використання автоматизованих систем управління силами безпеки та оборони із відповідними підсистемами може дозволити швидко оцінити ситуацію, отримуючи необхідні дані в режимі реального часу через системи управління на рівні бригад і батальйонів. Є численні приклади, де такий підхід може бути застосований: від підготовки карти для командира конкретного підрозділу, моделювання службово-бойових дій, коригування вогню, передачі даних про цілі для протиповітряної оборони, моніторингу переміщення танків та бронетехніки, до забезпечення миттєвої координації між сухопутними підрозділами та авіацією.

Автоматизація процесів управління силами безпеки та оборони виключає бюрократичні перепони, пов’язані з обробкою великої кількості паперової документації, тим самим звільняючи час для розробки та ухвалення додаткових стратегічних рішень, що можуть бути більш обдуманими та виваженими. Цей аспект набуває особливого значення в умовах воєнного стану, коли ресурси, як матеріальні, так і людські, обмежені, а кожен одиниця бронетехніки та боєприпасів на вазі золота, особливо коли противник має значну перевагу в кількості.

Крім того, автоматизація управління силами безпеки та оборони спрямована на мінімізацію впливу людського фактора, а саме помилок і неточностей, що можуть виникнути під час ручного збору, обробки, перетворення та передачі даних. В умовах, де кожен крок потребує точності, суб’єктивні оцінки та помилки можуть призвести до неправильного трактування важливої інформації, що, у свою чергу, створює ризики не тільки для втрат у техніці та живій силі, але й для погіршення загальної тактичної та

стратегічної ситуації.

Отже, автоматизація управління силами безпеки та оборони є критично важливим кроком у підвищенні ефективності та здатності сил до швидкого та адекватного реагування на виклики сучасності, що дозволяє силам безпеки та оборони перейти на якісно новий рівень оперативних можливостей.

Автоматизовані системи управління (АСУ) відіграють вирішальну роль у сучасних військових конфліктах, що визначається їхнім впливом на ефективність, оперативність і точність службово-бойових дій.

Експерти в безпекової галузі визначають такі переваги АСУ в сучасних конфліктах, як [209]:

Підвищення оперативності реагування. АСУ дозволяють особам що приймають рішення (ОПР) і операторам швидко обмінюватися інформацією, забезпечуючи миттєве реагування на змінні умови бойових дій.

Точність прийняття рішень. Завдяки аналізу великих обсягів даних і використанню алгоритмів штучного інтелекту АСУ сприяють прийняттю обґрунтованих і точних рішень, мінімізуючи людські помилки.

Інтеграція сил і засобів. АСУ забезпечують ефективну координацію дій різних видів військ і підрозділів, включаючи сухопутні війська, авіацію, флот та спеціальні операції.

Автоматизація процесів управління. АСУ автоматизують рутинні процеси управління, звільняючи час і ресурси для зосередження на стратегічному плануванні та оперативному керуванні.

Підвищення ефективності використання ресурсів. Оптимізація логістики, управління запасами та розподілу ресурсів знижує витрати та підвищує ефективність службово-бойових дій.

Управління комплексними операціями. В умовах сучасних конфліктів, що часто характеризуються асиметричністю та високою динамікою, АСУ дозволяють ефективно управляти складними багаторівневими операціями, забезпечуючи їх координацію та синхронізацію.

Забезпечення інформаційної переваги. Швидкий збір, обробка та аналіз

інформації дозволяють забезпечити інформаційну перевагу над противоборствуючей стороною, що є ключовим фактором успіху в сучасних конфліктах.

Контроль за виконанням службово-бойових задач. АСУ сприяють точному моніторингу виконання службово-бойових задач і оперативному коригуванню планів у відповідь на зміни обстановки.

Мінімізація ризиків для особового складу. Автоматизація дозволяє знизити ризики для життя та здоров'я військовослужбовців, зокрема, за рахунок використання безпілотних технологій та дистанційного управління.

Адаптація до гібридних загроз. АСУ забезпечують ефективне протистояння гібридним загрозам, що включають кібератаки, інформаційно-психологічні операції та інші неконвенційні методи ведення війни.

Автоматизовані системи управління в силах безпеки країн Європейського Союзу мають ряд стратегічних та тактичних цілей, спрямованих на підвищення ефективності, оперативності та здатності до адаптації у відповідь на сучасні виклики безпеки. Основні цілі включають [56, 183, 233]:

1. Підвищення оперативної сумісності. Забезпечення сумісності та інтеграції з системами країн-членів НАТО та ЄС для спрощення спільних операцій та маневрів. Стандартизація процесів та уніфікація процедур управління та комунікації для підвищення ефективності міжнародного військового співробітництва.

2. Забезпечення інформаційної переваги. Миттєвий доступ до оперативної інформації для підтримки прийняття рішень на всіх рівнях керування. Аналіз і інтерпретація великих даних з різноманітних джерел для прогнозування та відповіді на потенційні загрози.

3. Підвищення ефективності військових операцій. Мінімізація людських помилок та підвищення точності через автоматизацію критичних процесів управління. Ефективне розподілення та використання військових ресурсів, включаючи персонал, озброєння, техніку та логістику.

4. Забезпечення безпеки та захисту інформації. Захист військових мереж

та даних від кібератак і несанкціонованого доступу. Забезпечення конфіденційності та цілісності інформації під час передачі даних.

5. Підвищення гнучкості та адаптивності. Можливість швидкого перенастроювання та адаптації до змінних умов бойових дій та загроз. Розробка систем, які можуть бути легко модифіковані або розширені для відповіді на нові виклики та потреби.

6. Підтримка прийняття рішень. Використання штучного інтелекту та машинного навчання для підтримки прийняття обґрунтованих рішень на основі актуальної інформації. Розробка сценаріїв та моделювання потенційних військових операцій для оцінки ризиків і планування.

АСУ в силах безпеки країн ЄС є ключовим елементом у підтримці сучасної військової стратегії, спрямованої на підвищення обороноздатності, ефективності та міжнародної інтеграції в умовах швидко змінюваного глобального безпекового середовища.

Автоматизовані системи управління можуть бути класифіковані за рівнями управління на тактичні, оперативні та стратегічні. Кожен тип системи має свої специфічні завдання, функції та характеристики, які відповідають рівню управління, для якого вони призначені.

Завданнями та функціями тактичних АСУ є: безпосереднє керуванні військовими підрозділами в полі або на окремому театрі воєнних дій. Забезпечують збір, обробку та аналіз інформації, необхідної для ведення службово-бойових дій, розподілу військ та управління вогнем. Використовуються для координації дій між різними за призначенням підрозділами на полі бою. До основних характеристик таких АСУ відносяться: висока мобільність та здатність до швидкого розгортання, робота в умовах високого рівня невизначеності та динаміки.

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 розробки оптимальних планів дій. До основних їх характеристик відносяться: інтеграція з ширшими інформаційними системами для обміну даними з тактичним та стратегічним рівнями, способність до довготривалого планування та управління ресурсами.

Завданнями та функціями стратегічних АСУ є: призначені для підтримки прийняття рішень на найвищому рівні військового та політичного керівництва. Забезпечують аналіз загальної обстановки, стратегічне планування, розробку довгострокових стратегій та моніторинг виконання стратегічних завдань. Враховують політичні, економічні, соціальні та міжнародні фактори, що впливають на оборонну політику.

Характеристиками стратегічних АСУ є: інтеграція з цивільними інформаційними системами та міжнародними партнерами для обміну стратегічною інформацією, висока ступінь захисту інформації та кібербезпеки, враховуючи чутливість оброблюваної інформації.

Кожен тип АСУ має свої унікальні технологічні рішення, інтерфейси, засоби зв’язку та обчислювальні можливості, які оптимізовані для виконання специфічних завдань відповідного рівня управління. Розробка та впровадження таких систем вимагає комплексного підходу, що включає аналіз потреб, вибір технологій, розробку програмного забезпечення, інтеграцію з існуючими системами та навчання персоналу.

На сьогоднішній день у силах безпеки та оборони України використовується декілька абсолютно різних АСУ – «Дзвін» (управління та контроль стратегічного рівня), «Дельта» – (спостереження та рекогностування), «Ореанда ПС» (авіація та ППО), «Віраж-планшет» (відстеження повітряного простору), «Кропива» (управління тактичного рівня), «Гермес-С2» (управління тактичного рівня) та ряд інших перспективних розробок [183, 233]. Однак на сьогоднішній день на озброєння прийнята лише АСУ «Ореанда ПС», інші використовуються або в якості експерименту, або в якості волонтерської допомоги. АСУ у силах безпеки та оборони успішно застосовуються під час

ведення службово-бойових дій. Однак, по-перше, їх досить мало і їхній вплив та значення мають фрагментарний характер [183]. По-друге, відсутня система-ядро по прикладу тих, які є у США, країнах НАТО, Швейцарії, Ізраїлі, Туреччині. І це є основною перепоною на шляху розбудови Єдиної АСУ силами безпеки та оборони України, потреба в якій назріла ще в 2014 році і, особливо, зараз, в умовах широкомасштабного вторгнення російської федерації, коли інформація має отримуватися, оброблятися, перетворюватися і передаватися від сотень підрозділів до вищих штабів і навпаки в найкоротший час [183].

Автоматизовані системи управління відіграють ключову роль у забезпеченні обороноздатності країн ЄС, підвищуючи ефективність, точність та швидкість управління військовими ресурсами. Розвиток та вдосконалення АСУ є пріоритетним напрямком для забезпечення національної безпеки та оборони. Напрямками подальших досліджень може бути питання сумісності та взаємодії АСУ країн ЄС та НАТО з АСУ управління силами безпеки та оборони України.

Висновки до розділу 3

1. У рамках дослідження розглянуто теоретико-методологічні основи функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України в умовах сучасних викликів. Ці системи підтримки включають широкий спектр інструментів, методик і технологій, що спрямовані на забезпечення ефективного управління безпекою країни. Вдосконалення та розвиток систем підтримки прийняття рішень у цій сфері є безперервним процесом, який вимагає поєднання стратегічного бачення, технічних знань і гнучкості у відповідь на нові виклики та загрози.

2. Визначено роль і значення інформаційно-аналітичного забезпечення в процесі управління силами безпеки під час прийняття управлінських рішень. Це забезпечення має ґрунтуватися на ключових принципах, таких як поліцентричність, ієрархічність (організація процесу визначення цілей

управління на ієрархічних засадах), ентропійність, оптимальність, адекватність між метою та результатом, а також багатоваріантність. Ці принципи є взаємозалежними та разом формують основу для ефективного управлінського процесу, особливо в ситуаціях, що вимагають високого рівня відповідальності та стратегічного мислення, таких як забезпечення національної безпеки.

3. Вивчено вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на виконання службово-бойових завдань для забезпечення державної безпеки. Обґрунтовано вимоги до цього забезпечення під час виконання завдань, зокрема: наукова основа для оцінки подій і явищ; оперативність у зборі, отриманні та обробці інформації; безперервність у зборі та обробці даних; достовірність отриманої інформації; системність у висвітленні проблем; конфіденційність проведення аналітичних процедур; своєчасне інформування керівництва про важливі проблеми; чіткість у визначенні цілей і інтересів посадових осіб, для яких може бути корисна аналітична інформація.

4. Досліджено теоретико-методологічні аспекти функціонування підсистеми захисту інформації в суб’єктах сил безпеки України на основі комплексного підходу до кібербезпеки. Це включає взаємопов’язані заходи політичного, науково-технічного, інформаційного, освітнього характеру, а також організаційні, правові, оперативно-розшукові, розвідувальні, контррозвідувальні, оборонні, інженерно-технічні заходи, криптографічний і технічний захист національних інформаційних ресурсів і кіберзахист об’єктів критичної інформаційної інфраструктури.

5. Аналіз засад автоматизації інформаційних систем управлінського призначення в силових структурах передових країн ЄС та НАТО показав, що активно впроваджуються стандартизовані рішення, такі як NATO Architecture Framework (NAF), які сприяють інтеграції та сумісності систем між країнами-членами. Застосування хмарних технологій, посилення кібербезпеки та шифрування забезпечує надійний захист інформації та її конфіденційність. Інноваційні технології, такі як безпілотні літальні апарати (БПЛА) для розвідки

та моніторингу, використання штучного інтелекту для аналізу великих даних, відкривають нові можливості для сил безпеки. Автоматизовані системи управління (АСУ) стають критично важливими в умовах сучасних військових конфліктів, забезпечуючи швидке реагування, точність прийняття рішень і ефективне управління військовими ресурсами. Країни ЄС активно інтегрують передові технології у свої військові системи для посилення обороноздатності та забезпечення сумісності зі структурами НАТО.

РОЗДІЛ 4
РОЗВИТОК МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ УКРАЇНИ

4.1 Поліпшення засобів інтелектуалізації інформаційної діяльності та організаційні аспекти управління інформаційними ресурсами

У сучасному світі, в умовах масової комп'ютеризації, розвитку комунікацій і впровадження передових інформаційних технологій, спостерігається стрімкий прогрес у таких сферах, як освіта, наука, економіка і соціальне життя. Інформація перетворилася на глобальний ресурс, а людство фактично вступило в нову еру свого розвитку – еру інформаційної цивілізації. Згідно з проведеним аналізом, інформаційно-аналітичне забезпечення посідає одне з провідних місць у складному процесі інформаційного супроводу системи державного управління. Проте, наразі відсутнє єдине, усталене розуміння цього важливого поняття, а в наукових та публіцистичних матеріалах воно трактується по-різному. Як наслідок, виникає проблема, що ускладнює як розробку методологічних основ інформаційного забезпечення в державному управлінні, так і його практичне впровадження. Для адекватного розуміння сутності інформаційно-аналітичного забезпечення в контексті державного управління, необхідно, перш за все, дослідити існуючі теоретичні підходи до визначення цього поняття, здійснити їх узагальнення та запропонувати дефініцію, яка б найбільш повно відповідала його суті, а також визначити його роль і місце в загальній системі державного управління [215]. Проблемні питання державного управління інформаційними ресурсами України висвітлюються у роботах таких науковців, як Варенко В.М., Пеньков С.В., Шендрик В.В., Чечетова Н.Ф., Лелюк Н.Є., Саричев Ю.О., Дробаха Г.А., Єрмошин М.О., Смірнов Є.Б., Іохов О.Ю., Бєлай С.В. та інших. Інформатизація

є комплексом заходів організаційного, правового, політичного, соціально-економічного та науково-технічного характеру, спрямованих на створення умов для задоволення інформаційних потреб населення та суспільства через розробку, розвиток і використання інформаційних систем, мереж і технологій. Цей процес охоплює широке застосування інформаційних технологій у всіх сферах життя з метою підвищення ефективності управління та використання інформаційних ресурсів. В Україні інформатизація включає заходи на рівні законодавчих та виконавчих органів влади, підтримку підприємництва, управління соціальними процесами та охорону довкілля.

Однак, на жаль, рівень інформатизації національної економіки та соціальних сфер в Україні залишається на досить низькому рівні. Згідно із законодавством, інформатизація країни значно відстає від розвинутих західних держав, а інвестиції в ІТ на душу населення є значно меншими порівняно з іншими країнами. Серед основних проблем можна виділити технічне відставання, недостатню надійність та обсяг телекомунікаційних послуг, а також нерозвинену мережу передачі даних.

Ключові чинники, що гальмують процес інформатизації, включають економічну кризу, низький рівень виробництва та впровадження обчислювальної техніки, слабкий розвиток програмного забезпечення та інформаційних технологій, а також недостатню комп’ютерну грамотність населення. Для прискорення розвитку інформаційного суспільства в Україні необхідно зміцнити правове поле інформаційної діяльності та забезпечити більшу підтримку держави для проектів інформатизації.

В цілому, ситуація в Україні щодо інформатизації національної економіки та інших сфер людської діяльності залишається незадовільною, що підтверджується Законом України «Про концепцію Національної програми інформатизації». За даними Варенка В.М. [24], рівень інформатизації українського суспільства становить лише 2–2,5% від рівня розвинутих західних країн. Загальний стан впровадження інформаційних технологій в Україні наразі не можна вважати навіть близьким до задовільного.

За загальновизнаною методикою, цей показник оцінюється у витратах на інформаційні технології на душу населення за рік. Так, у США цей показник становить 1100 євро, в Японії – 700, у країнах Західної Європи – 500, у провідних країнах Східної Європи (Чехія, Угорщина, Словенія, Естонія та ін.) – близько 90, Польщі – 40, Румунії та Болгарії – близько 10 євро. В Україні цей показник ще менший [24].

Внаслідок загальної кризи та технологічного відставання, галузі, які забезпечують розробку та використання інформаційних засобів і компонентів, опинилися в тяжкому становищі. Україна, колись виробник сучасного обладнання, тепер стала споживачем застарілих іноземних моделей обчислювальної техніки, що призвело до зниження вітчизняного науково-технічного потенціалу і втрати здатності створювати конкурентоздатні продукти. Телекомунікаційні системи та мережі передачі даних в Україні стикаються з технічними відставаннями, недостатньою пропускною спроможністю та низькою надійністю зв’язку, що обмежує якість та обсяг надаваних послуг. Ефективність інформаційної інфраструктури, яка включає системи та мережі зв’язку, важлива для забезпечення доступу до інформаційних мереж, систем та ресурсів, а також для отримання різноманітних інформаційних послуг державними установами, підприємствами, ЗМІ та громадянами [25].

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.

Інтелектуалізація інформаційної діяльності не лише спрощує збір та аналіз інформації, але й сприяє глибшому розумінню отриманих даних.

Використання адаптивних алгоритмів дозволяє системам самонавчання та адаптації до змінних умов, що особливо важливо в динамічних секторах, таких як фінанси, медицина, енергетика та національна безпека. Ці засоби допомагають виявляти закономірності, які можуть залишитися непоміченими при традиційних підходах аналізу [210].

Основою поліпшення інтелектуалізації є розвиток і впровадження новітніх технологій. Наприклад, нейронні мережі та глибинне навчання вже застосовуються для обробки великих обсягів даних та розпізнавання складних зразків у даних. Такі технології, як обробка природної мови (NLP) та комп'ютерний зір, відкривають нові можливості для автоматизації та оптимізації інформаційних процесів.

Поліпшення інтелектуалізації важливе не тільки в технічних чи економічних областях, але й у соціальних аспектах, таких як медицина та освіта. У освіті, наприклад, вони можуть допомогти у створенні персоналізованих навчальних програм, що враховують індивідуальні особливості кожного студента. Це може значно покращити ефективність навчального процесу, адаптуючи матеріал під конкретні потреби і швидкість сприйняття інформації, тим хто навчається. Використання адаптивних алгоритмів дозволяє системам збирати дані про успішність та стиль навчання студентів, аналізувати ці дані та на основі отриманих результатів коригувати подальший навчальний план.

Одним із напрямків розвитку інтелектуалізованих освітніх технологій є створення віртуальних асистентів, які можуть вести діалог зі студентом, відповідати на його запитання, проводити оцінку знань і навіть підтримувати мотивацію до навчання. Такі системи можуть використовувати штучний інтелект для визначення слабких місць у знаннях студента та запропонувати додаткові ресурси або завдання для їх усунення.

Крім того, інтелектуалізація дозволяє використовувати великі дані (big data) для аналізу успішності студентів на макрорівні, дозволяючи освітнім установам виявляти загальні тенденції та покращувати методики навчання.

Завдяки цьому можливе не тільки адаптування навчального процесу під індивідуальні потреби, але й оптимізація освітньої програми, що підвищує загальну якість освіти.

Надзвичайно важливим є те, що інтелектуалізовані освітні системи можуть забезпечити рівний доступ до якісної освіти для студентів з різних соціальних та географічних середовищ. Наприклад, дистанційні освітні платформи з елементами штучного інтелекту дозволяють студентам з віддалених або недостатньо обслуговуваних регіонів отримувати освіту порівнянну з тією, яка доступна у великих містах або більш розвинених країнах.

Також інтелектуалізація сприяє інклюзивності у освіті, адаптуючи навчальний процес для осіб з особливими освітніми потребами. Через це студенти, які мають певні обмеження, можуть в повній мірі брати участь у навчальному процесі та розвивати свої здібності нарівні з іншими.

Розробка і впровадження інтелектуалізованих освітніх систем вимагає значних ресурсів, включаючи інвестиції в технології, підготовку науково-педагогічних кадрів та розробку відповідного контенту. Однак, переваги, які пропонує такий підхід, значно перевищують витрати, відкриваючи нові можливості для розвитку освітньої галузі та підвищення її доступності і ефективності.

Розвиток інтелектуалізації інформаційної діяльності також пов’язаний з певними викликами. Зокрема, питання конфіденційності даних, етичні аспекти використання штучного інтелекту, і потенційна втрата робочих місць у деяких секторах через автоматизацію. Також важливо забезпечити безперервність навчання фахівців, щоб вони могли ефективно використовувати новітні інструменти в своїй роботі.

На додаток до цих викликів, існують значні можливості для подальших досліджень та інновацій. Збільшення обсягів доступних даних та швидкість їх обробки продовжують відкривати нові шляхи для розвитку інтелектуалізації в різних областях діяльності.

Завдяки постійному розвитку технологій та методологій, поліпшення інтелектуалізації інформаційної діяльності залишається в центрі уваги багатьох організацій, спрямованих на оптимізацію інформаційних процесів та підвищення їхньої ефективності.

Людина, яка приймає рішення, повинна володіти знаннями й навиками передбачення. Передбачення – це припущення, бачення заздалегідь того, що повинно (може) відбутися. Поняття «передбачення» включає [38, 51]:

- пророкування (однозначне твердження майбутнього стану об’єкта або настання будь-якої події);
- прогноз (найбільш імовірний (можливий) стан об’єкта або можливість настання події);
- припущення (опис одного або декількох можливих варіантів-гіпотез майбутнього стану об’єктів).

Таким чином, передбачення – це відображення майбутнього стану об’єктів або тих змін, які можуть у них відбутися, або інформація про події, які можуть здійснитися. Передбачати – значить давати випереджальну картину можливої дійсності, що характеризується системою впливових факторів, яка забезпечує їх урахування та потенційно сприятливий розвиток обстановки.

Передбачати можна хід процесів, появу подій, стан об‘єктів дослідження, розвиток ситуацій. Передбачення здійснюється шляхом визначення кількісних і якісних (некількісних) параметрів, показників, що описують процеси, події, стан об’єктів і розвиток ситуацій.

Розглядають передбачення [38, 51]:

- іррегулярних подій (майбутні результати бойових дій, рівень бойової підготовки новосформованої військової частини), неповторюваних унікальних ситуацій, нових об’єктів дослідження;
- менш регулярно повторюваних подій, ситуацій (рівень бойової підготовки військової частини у поточному навчальному році), відомої поведінки об’єктів;
- тенденцій загального розвитку певних, наприклад, воєнно-політичних

подій (розвитку збройних сил та їх видів).

Усі типи передбачення описуються некерованими (слабокерованими) параметрами. При розробці управлінського рішення органи управління стикаються з невизначеністю некерованих параметрів, ступінь якої може бути різним – від повної невідомості їх величини до випадків визначення необхідного параметра у порівняно вузькому діапазоні. Передбачення дає можливість знизити ступінь невизначеності. Передбачення в цілому здійснює тільки людина, яка приймає рішення, а його допоміжні органи управління можуть брати участь у розробці прогнозів при описі припущень.

Під час здійснення управління всередині військової організації передбачення має відповідати таким вимогам:

- спрямовуватися на досягнення поставленої мети (завдання);
- бути чітко пов’язаним з реальністю, тобто результати передбачення повинні бути досяжними;
- відбивати особисту переконаність ОПР;
- ураховувати бойовий потенціал військової організації;
- служити базою для реалізації довготривалого плану бойових дій;
- виражати інтереси всіх підрозділів військової організації.

Сформовані органами управління припущення складають основу прогнозу. Ті результати прогнозу, що ОПР визнаються як однозначно здійсненними, відносяться до пророцтва. Але пророцтва не додають якості процесам прийняття рішень, не формують більш зваженого рішення, тому цей вид передбачення недоцільно використовувати в термінології воєнної науки. Характерними для застосовування у воєнній науці є терміни «припущення» і «прогнозування».

Прогнозування – одна з основних складових управлінського процесу. Без прогнозування, без уявлення очікуваного ходу розвитку подій неможливо прийняти ефективне управлінське рішення.

Державні діячі минулого, полководці приймали підчас блискучі управлінські рішення. При цьому, як правило, використовувалися елементи

прогнозування, які в кращому випадку відносяться до мистецтва прогнозування. Сама наука прогнозування почала формуватися лише в середині XX століття [131].

В енциклопедичному словнику наводиться таке визначення [54, с. 716]: «Прогноз(від грецького prognosis – передбачення, пророкування) – конкретне пророкування, судження про стан будь-якого явища в майбутньому». У [201] прогноз визначається як деяке судження щодо невідомих, особливо майбутніх подій. Терміни «судження» і «подія» отримують тут вільне тлумачення. Зовсім необов’язково, щоб це судження з'явилося в письмовій формі, було опубліковане або подане будь-яким іншим способом. Описувана подія може виражати навіть відсутність деяких явищ.

Доцільно визначити позитивний конструктивний підхід до прогнозування як до активного впливу на майбутнє шляхом планування, програмування, проектування й управління явищами й процесами. У рамках цього підходу прогнозування не є самоціллю, а становить основу для прийняття рішень [231]. При прогнозуванні за параметри мають фігурувати управляючі змінні (тобто мають аналізуватися різні сценарії), і для здійснення характеристики місця прогнозу в прийнятті рішень можна виділити такий ланцюжок операцій: «прогноз – план – програма – проект – управління» [231].

Взаємозв’язок прогнозу і акту прийняття рішення розглядається також у [117], де зазначається, що:

1) знання ОПР дійсного стану об‘єктів управління описується певними змінними;

2) розрізняються керовані (інструментальні) і некеровані змінні;

3) оцінка майбутніх значень некерованих змінних здійснюється залежно від значень керованих змінних, при цьому отримуються умовні прогнози (сценарії);

4) оцінюються результати сценаріїв, описаних у п. 3, тобто порівнюються наслідки обраних операцій;

5) здійснюється вибір значень керованих змінних, тобто приймається

рішення.

Інакше кажучи, формулювання рішення залежить від поточного стану об’єкта управління та відбиває політику ОПР по відношенню до цього об’єкта (тобто відображає саме технологію прийняття рішення).

При організації прогнозу має місце гра одного активного гравця (ОПР) з пасивним гравцем, який називається у дослідженні операцій «природою», у військовій справі додатково визначається й «противник». Вплив прогнозу ОПР щодо поведінки інших самостійних суб'єктів управління враховується пасивно – через прогнозування некерованих змінних, тобто прогнозування у даному випадку є не методом управління, а методом усунення невизначеності (за обраною стратегією управління).

У загальному випадку прогноз може застосовуватися для виконання різних завдань управління, наприклад, для вирішення таких економічних проблем, як оцінка майбутньої фінансової діяльності підприємства, оцінка прибутків від обраної інвестиційної політики. Прогнозування може проводитися відносно оцінки наслідків діяльності у медичній галузі, як, наприклад, розвиватиметься хвороба тощо. У подібних випадках досліджується процес функціонування конкретних об‘єктів у будь-якій галузі діяльності суспільства, у тому числі прогноз може характеризувати й функціонування військової організації. Якщо об‘єктом дослідження є поле бою з активними діями протиборчих сторін, то результатом прогнозу повинні стати значення показників ефективності бойових дій, бойових можливостей сторін після закінчення бойових дій. Такий прогноз стосовно отримання науково-обґрунтованих результатів функціонування об’єктів дослідження можна назвати функціональним прогнозом.

Прогноз може відноситися й до передбачення процесів розвитку технологій у тій або іншій галузі. У цьому прогнозі застосовується трансформування технологій з найнижчих рівнів до вищих або навпаки. Такий прогноз називається технологічним.

Прогнозування має дві сторони або площини конкретизації:

пророкувальну (дескриптивну); передвказівну (прескриптивну). Пророкування означає опис можливих або бажаних перспектив, станів, рішень проблем майбутнього. Передвказування означає вирішення цих проблем шляхом використання інформації про майбутнє у цілеспрямованій діяльності.

Таким чином, у прогнозуванні розрізняють два аспекти: теоретико-пізнавальний і управлінський. У [117], наприклад, розрізняють пошуковий і нормативний прогнози.

Під пошуковим прогнозом розуміється визначення можливих станів об'єкта прогнозування в майбутньому. Завдання нормативного прогнозу полягає у визначенні шляхів і строків досягнення бажаних станів прогнозованого об’єкта в майбутньому.

Іншими словами, нормативний прогноз – передбачення, мета якого полягає в тому, щоб викликати інтерес і спонукати до дії [117]. Тому нормативний прогноз може розглядатися як управління в явному вигляді.

У [117] підкреслюється, що фахівець, який приймає рішення на підставі прогнозу, намагається запобігти наслідкам несприятливого прогнозу й передбачити позитивні результати сприятливого прогнозу.

Існують дві «крайності» у впливі прогнозу на управління. У [117] зазначається, що самоздійснюваний прогноз – це такий прогноз, який виявляється достовірним тільки тому, що був зроблений; самоанульований прогноз – такий прогноз, який, навпаки, стає недостовірним тільки тому, що був зроблений. Аналогічні властивості політичних прогнозів обговорюються в [38].

У [117] також виділяється активний і пасивний прогноз, і обговорюються проблеми апріорної й апостеріорної оцінки якості прогнозу. Пасивний прогноз – такий, для якого результат прогнозу не впливає й, по суті, не може впливати на об'єкт прогнозування. Якщо ж впливом прогнозу на об’єкт прогнозування не можна знехтувати (такий прогноз називається активним), то логіка прогнозування різко змінюється й ускладнюється, тому що сам прогноз повинен ураховувати ефект результатів прогнозування. Отже, активними є будь-які нормативні прогнози, а також такі пошукові прогнози, які використовуються при

прийнятті управлінських рішень. Для активного прогнозу збіг прогнозованих показників з реальними не є доказом високої якості прогнозу.

Свою специфіку має технологічний прогноз. У прикладах, таблиця 4.1 показані рівні технологічного прогнозування розвитку військової організації. У термін «технологічне прогнозування» вкладається за аналогією з [233] не традиційний смисл, а розширене розуміння терміну «технологія», що означає широку галузь цілеспрямованого застосування воєнної науки для оцінки поведінки об‘єктів дослідження як складових військової організаційно-технічної системи.

Технології прогнозування стану військової організаційно-технічної системи розділені на 7 рівнів у порядку зростання, починаючи від виникнення перших ідей у наукових ресурсах військового мистецтва і закінчуючи їх реалізацією у суспільстві, де відносини суспільства до військової організації визначатимуть рівень безпеки самого суспільства.

Перехід від більш низького рівня реалізації ідей до більш високого називається переміщенням технології. Технологічне прогнозування також розділяється на пошукове і нормативне.

Пошукове або дослідницьке прогнозування має у своїй основі орієнтацію на уявні можливості, визначення тенденцій розвитку ситуацій на підставі інформації, яка отримується при розробці прогнозу. При цьому здійснюється перехід від засобів і можливостей до потреб і цілей.

Прикладом пошукового прогнозування може бути прогноз результатів ведення бойових дій певного угруповання військ (сил) у тих або інших умовах обстановки. При цьому характерним є використання таких методів, як екстраполяція, моделювання, написання сценаріїв та ін., що базуються на аналізі точних емпіричних даних. Перевага віддається кількісній інформації, хоча використання якісної (некількісної) інформації також можливо.

В основі нормативного прогнозування лежить орієнтація на місію організації, на ті потреби і цілі, до досягнення яких вона прагне.

Таблиця 4.1 – Основні рівні переміщення технології прогнозування стану організаційно-технічної системи (ОТС)

Стадії реалізації	Рівні застосування технологій прогнозу щодо розвитку ОТС	Приклади
1	Наукові ресурси управлінського мистецтва	Виявлення нових законів і закономірностей управлінського мистецтва
2	Технологічні ресурси управління складними організаційними системами	Методи управління силовими організаціями, угрупованнями
		Методи прийняття рішень
3	Службово-бойове застосування сил під час виконання завдань за призначенням (моделювання)	Нові форми, способи і тактичні прийоми проведення службово-бойових дій
3	Службово-бойове застосування сил під час виконання завдань за призначенням (моделювання)	Нові форми, способи і тактичні прийоми проведення службово-бойових дій
		Нові оперативно-тактичні вимоги щодо необхідних технічних засобів
4	Технічні ресурси	Нові зразки технічних засобів
		Ринок військово-промислового комплексу
5	Інформаційне середовище	Мережево-центричні структури систем управління військами (силами), керування інформаційними потоками
6	Військова організація	Організаційний, технічний, психологічний стан окремого військовослужбовця, обслуги, підрозділу, частини, з’єднання, об’єднання
7	Суспільство	Взаємний вплив суспільства і його складової –організації сил безпеки

Нормативному прогнозуванню відповідає переміщення технологій з більш високого рівня реалізації ідей на більш нижчі рівні. При цьому здійснюється перехід від потреб і цілей до засобів їх реалізації.

Прикладом нормативного прогнозування може бути прогноз розвитку виду збройних сил на визначений період зі створенням програми реалізації сформованих завдань.

До основних методів, що використовуються при нормативному прогнозуванні, слід віднести методи [38, 131, 231, 233] ПАТТЕРН, Дельфи, прогнозного графа Глушкова, Поспєлова та ін.

Для всіх видів прогнозування дуже важливе значення відіграє характер інформації, що аналізується. Як для процесу збору, так і для процесів аналізу, обробки даних, важливим є характер інформації: кількісна або якісна (некількісна).

Кількісна інформація, якщо вона достатньо надійна, має переваги щодо використання точних математичних методів і моделей та визначення тенденцій розвитку ситуацій з достатньою точністю, з вказуванням довірчих інтервалів, можливих похибок під час проведення розрахунків тощо.

Однак на жаль кількісна інформація не завжди є надійною. Тим більше, що коло тих проблем, для яких вдається розробити адекватні математичні моделі, виявляється значно вужчим, ніж множина ситуацій, в яких треба приймати реальні рішення.

У той же час там, де можна знайти адекватні математичні моделі на математичній мові та отримати достовірні результати аналізу, це необхідно робити.

У переважній більшості випадків під час розробки прогнозів органи військового управління мають справу з якісною інформацією, яка подається у вигляді вербальних (словесних) описувань. За цих умов отримання якісних оцінок здійснюється за допомогою вербальних або вербально-кількісних шкал, а рішення приймається на основі порівняльних оцінок альтернативних варіантів.

У випадках, коли прийняття рішення здійснюється за допомогою вербальних або вербально-кількісних шкал, застосовуються експертні методи прогнозування розвитку ситуацій, процесів, передбачається майбутній облік об’єктів управління.

В експертних системах прийняття рішень торкаються питань тих сфер діяльності, які важко формалізуються, де стандартні математичні технології моделювання виявляються практично непридатними. Експертні системи забезпечують процеси прийняття рішень щодо виконання слабко структурованих завдань, у яких, зокрема, важко очікувати наявності достовірних кількісних оцінок за різними варіантами.

Взагалі, під «експертною системою» слід розуміти цілісну взаємно доповнювану інформаційно-аналітичну систему людини і машини, в якій на базі програмно-технічного комплексу діє інтерактивна діалогова програма, що включає знання фахівців про деяку конкретну проблемну область і яка в цій досить вузькій і спеціалізованій галузі здатна забезпечити приймання ОПР обґрунтованих рішень [233]. Замість машини може залучатися достатня кількість окремих людей-експертів, здатних в певних галузях забезпечити прийняття рішень.

Вибір методу прогнозування виступає значним фактором, який дозволяє обрати необхідний метод прийняття рішення. Існуючі методи прогнозування результатів дослідження стану об‘єктів, процесів, ситуацій пов‘язуються з організацією колективного або індивідуального «розуму».

У рамках сучасної теорії прийняття рішень розроблено багато методів організації колективного й індивідуального «розуму», методів прогнозування результатів практичної діяльності. До таких способів прогнозування можуть відноситися методи екстраполяції, моделювання, методи аналогії, сценаріїв, в яких застосовуються способи використання індивідуального і колективного «розуму» (мозкова атака, мозковий штурм) та ін.

Мозкова атака – оперативний метод вирішення проблем на основі стимулювання творчої активності, коли учасникам обговорення пропонується

висувати якнайбільше варіантів рішення, у тому числі найфантастичніших. Потім із загальної кількості висунутих ідей відбираються більш вдалі, які можуть бути використані на практиці.

Для проведення мозкової атаки створюються дві групи:

- учасники, які пропонують нові варіанти вирішення завдання;
- члени комісії, які обробляють запропоновані рішення.

Розрізняють індивідуальні й колективні мозкові атаки.

Мозковий штурм – груповий метод творчої генерації ідей. Основним фактором, що забезпечує високу продуктивність даного методу, є заборона на критику будь-яких пропозицій. Ця методика широко застосовувалася в 50-х рр. минулого століття у таких країнах, як США, Франція, переважно під час обговорення технологічних завдань, а також проблем планування й прогнозування.

Практика використання цієї методики призвела до скептичних оцінок її ефективності, а експериментально-психологічна перевірка не підтвердила її переваг при виконанні творчих завдань, хоча й до сьогоднішнього часу методика знаходить своє відображення в практиці роботи владних структур.

Прогнозування в західній літературі розглядається як дослідження майбутнього або аналіз майбутнього. До основних базових концептуальних підходів щодо аналізу майбутнього можуть бути віднесені: метод Дельфі; сценарний підхід; альтернативні варіанти майбутнього; «темні конячки».

Перші два підходи були розроблені наприкінці 40-х – початку 50-х років минулого століття й послужили основою для подальшого розвитку методів прогнозування. Основним завданням у подібних методах є зниження невизначеності, що принципово пов’язано з майбутнім.

Нічого не містить у собі більше невизначеності, ніж майбутнє. Методи роботи з майбутнім будуються на спробі тим або іншим способом визначити наші інтуїтивні уявлення, зробити з них той інструмент, що за рівнем науковості відповідатиме прийнятим стандартам.

Як тип технології аналізу майбутнього він виник у 1944 р., коли військові

замовили розробку методик, спрямованих на передбачення майбутніх технологій. Метод Дельфі являє собою спосіб збору й обробки інформації від експертів за допомогою запитальника й складається з таких десяти кроків:

- відбір групи експертів;
- розробка переліку запитань для першого раунду;
- перевірка переліку запитань на предмет точності (двозначності або невизначеності слів);
- передача першого переліку запитань і відповідей експертам;
- аналіз відповідей першого раунду;
- підготовка переліку запитань для другого раунду;
- передача переліку запитань і відповідей експертам;
- аналіз відповідей другого раунду;
- підготовка результатів групою аналізу.

Робота з групою експертів, а не з одним з них, дозволяє поступово знижувати суб'єктивність, властиву будь-якій окремій думці. Вважається, що передбачення групи людей частіше виявляться більш вірними, ніж передбачення тими ж окремими індивідами, але працюючими поодинці (ефект Макгрегора).

Сценарний підхід був розроблений у РЕНД (РЕНД – це корпорація (Великобританія і США), яка була організована ще у 1945 році. Основною місією її на той час була місія мозкового центру. Скорочена її назва йде від англійських слів «Research and Development». Сьогодні ця корпорація займається дослідженнями майже всього інформаційного простору планети) наприкінці 40-х років минулого століття. Сценарії давали можливість активізувати такі типи дій:

- стимулювати уявлення;
- прояснити й визначити основні проблеми, досліджувати альтернативні політичні проекти й контексти;
- поліпшити інтелектуальне спілкування аналітиків;
- поліпшити здатність визначати нові моделі, тренди, поворотні пункти й

кризи;

- розуміти їх значущість, спираючись на історичні аналогії, метафори й аналітичні (математичні) моделі.

У сценарному підході присутні дві основні складові:

- покроковий рух до певного майбутнього стану;
- можливі альтернативи на кожному з кроків, які дозволяють полегшити або призупинити можливий розвиток, що дає підґрунтя для процесу прийняття рішень.

Найбільш відомі розробки сценарного підходу були зроблені компанією Шелл [293]. У свій час сценарії стали досить серйозним відкриттям інструментарію дослідження майбутнього. Авторами нових розробок сценарного підходу постійно підкреслюється, що сценарії не є пророцтвом. Однак сценарії дозволяють підготуватися до набору можливих варіантів майбутнього, оскільки вони формулюються в сценарії.

Якщо сценарії являють собою набір подій у рамках причинно-наслідкових зв'язків, то альтернативне майбутнє концентрується вже на кінцевому етапі.

На думку автора, Dewar, J.A. [273], існує майже нескінченна кількість можливих варіантів майбутнього. Ніякий кінцевий список сценаріїв не може повністю закрити всі можливі несподіванки. Робота йде як над більш імовірним розвитком подій, так і над ситуаціями, які можуть бути менш імовірними, але є найбільшим ризиком.

Цінністю альтернативних варіантів майбутнього як підходу до аналізу віддаленого майбутнього є те, що в такий спосіб можна вибудувати захист проти невизначеності, вважає Gordon J. [277].

«Темні конячки» (wild cards) являє собою метод прогнозу, коли розглядаються події, значущі за наслідками, але малоймовірні з погляду сьогоднішнього дня. Однак ними не можна нехтувати, оскільки, якщо вони настануть, то це кардинальним чином змінить сценарії розвитку подій. У методі «Темні конячки» інформація слабко піддається прогнозуванню.

Оскільки сучасна ідеологія оперування з невизначеністю опирається на поняття захисту, то це дозволяє думати й над тим, як убезпечити себе у разі настання навіть малоймовірних подій. Прогноз або аналіз майбутнього відноситься до того етапу стратегічного планування, коли цілі ще не набули конкретного змісту. Основне завдання такого аналізу полягає у створенні ясного розуміння можливостей розвитку, його перспектив і уявлень про те, які цілі можуть бути реально визначені. У нормативних документах подібний аналіз прийнято називати підготовкою вихідних або початкових даних для стратегічного планування. За методиками прогнозу майбутнього постає проблема проведення кількісної оцінки отриманих результатів, проведення критерійного аналізу для того, щоб на підставі порівняння результатів прийняти відповідне рішення.

Для органів управління можуть виникати завдання щодо порівняльної оцінки елементів складного процесу. Причому елементи не завжди мають зрівнянні показники, за значеннями яких проводиться вибір кращої сукупності елементів. У такому випадку застосовуються методи експертного оцінювання, до яких відноситься і метод Сааті – метод «одного експерта» [233].

Сукупністю переваг, притаманних кожному експерту, у тому числі й ОПР, визначається змістовність і якість рішень, що приймаються. Практика проведення оперативної підготовки у Збройних Сил України наприкінці 90-х років минулого століття показує, що при відпрацюванні навчальних завдань планування дій декількома керівниками в однакових умовах обстановки прийняті рішення відрізнялися між собою не тільки обраним бойовим порядком, але й вибором способів і тактичних прийомів виконання поставленого завдання. Це ще раз підкреслює важливість системи переваг кожного командира при прийнятті ним відповідних рішень, яку не враховувати в інформаційно-аналітичній системі забезпечення процесів управління неможливо.

Для реалізації саме таких подібних завдань пошуку прийнятних варіантів рішень відомий американський математик Томас Сааті запропонував новий методологічний підхід – метод аналізу ієрархій (MAI) [264]. Цей метод являє

собою систематичну процедуру для ієрархічного уявлення елементів, які визначають суть проблеми – складові рішення або критерії, за якими остаточно здійснюється вибір варіанта рішення.

Метод складається з декомпозиції проблеми на все більш прості складові і подальшої обробки суджень ОПР попарним порівнянням. Метод аналізу ієрархій включає процедури синтезу множини суджень, отримання пріоритетності критеріїв і знаходження альтернативних рішень. Отримані значення є оцінками за шкалою відношень і відповідають так званим жорстким оцінкам. MAI може використовуватися для визначення парето-оптимального стану складної системи.

Управління інформаційними ресурсами в державному управлінні потребує від організацій раціонального планування, чіткого розподілу ролей та відповідальностей між усіма учасниками процесу. Організаційні структури можуть значно відрізнятися в залежності від розмірів та специфіки конкретної державної інституції, проте існують загальні принципи та підходи, які застосовуються в будь-якому випадку.

Центральні органи управління в Україні, відповідальні за розробку та впровадження національної політики у сфері інформаційного забезпечення адміністративних послуг, відіграють важливу роль у процесі цифровізації та модернізації державного управління. Ці органи забезпечують стратегічне керівництво, регулювання та координацію в сфері інформаційно-аналітичного забезпечення (ІАЗ), спрямовуючи процеси цифрової трансформації. Вони займаються розробкою інформаційних систем, стандартів і нормативів, а також інтеграцією та координацією діяльності місцевих органів влади. У наступному огляді детально розглянуті ключові центральні органи управління, їхні ролі та обов’язки.

Одним з найважливіших центральних органів управління в Україні, що відповідає за розробку та реалізацію національної політики у сфері інформаційного забезпечення, є Міністерство цифрової трансформації України (МЦТ) [191]. Це відомство несе відповідальність за стратегічне планування в області цифрової трансформації держави, включаючи розвиток електронного

урядування. Воно також розробляє політику та нормативно-правові акти для регулювання сфери ІТ та ІАЗ, координує проекти з цифровізації державних послуг для громадян та бізнесу через платформу «Дія», і впроваджує стандарти інформаційної безпеки та захисту даних [191].

До визначених цілей МЦТ до кінця 2024 року входять: забезпечення доступу громадян та бізнесу до 100% публічних послуг онлайн, покриття 95% населення, соціальних об'єктів і головних автошляхів швидкісним інтернетом, залучення 6 мільйонів українців до програми розвитку цифрових навичок, та збільшення частки ІТ у ВВП країни до 10% [191].

Міністерство цифрової трансформації України також активно працює над впровадженням нових проектів, спрямованих на цифрову трансформацію в різних сферах державного управління. До таких проектів належать:

Цифрова трансформація надання послуг у територіальних центрах комплектування та соціальної підтримки (е-ТЦК та СП): створення єдиного порталу, що дозволить громадянам отримувати публічні послуги в електронній формі, усуваючи черги та мінімізуючи корупційні ризики шляхом ведення прозорого реєстру.

Цифрова трансформація системи освіти (е-Університет): автоматизація процесів вступу, організація набору та навчання іноземців, замовлення документів про освіту європейського зразка, електронне ліцензування, модернізація державної електронної бази з питань освіти та створення системи моніторингу працевлаштування випускників.

Цифрова трансформація державної реєстрації бізнесу (е-Бізнес): впровадження електронних та автоматизованих послуг з реєстрації бізнесу, громадських об’єднань, подання інформації про кінцевих бенефіціарних власників, модернізація Єдиного державного реєстру юридичних осіб і фізичних осіб-підприємців.

Цифрова трансформація екологічного нагляду (е-Екоконтроль): створення електронної системи екологічного контролю, автоматизація функцій повідомлення про протиправну діяльність, планових та позапланових перевірок

з можливістю публічного звітування.

Електронна демократія (е-Демократія): впровадження інструментів електронної демократії, таких як електронні петиції, опитування, обговорення проектів нормативно-правових актів, громадський бюджет та звернення громадян [191].

Ці ініціативи спрямовані на суттєве покращення якості надання державних послуг, підвищення ефективності державного управління та забезпечення прозорості й підзвітності уряду перед громадянами.

Основним державним органом України, що відповідає за питання інформаційної безпеки, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) [187].

Ця установа регулює та контролює діяльність, пов'язаної із захистом інформації в інформаційно-телекомунікаційних системах. ДССЗЗІ відповідає за забезпечення національної інформаційної безпеки, включаючи захист критично важливих об'єктів інфраструктури та персональних даних громадян. В її обов'язки входить сертифікація засобів захисту інформації, проведення аудиту безпеки інформаційних систем, а також експертиза в галузі технічного захисту інформації. Крім того, ДССЗЗІ займається криптографічним захистом інформації та здійснює технічне регулювання у сфері інформаційної безпеки.

Згідно з законодавством, інформація, яка належить державі або має обмежений доступ, повинна оброблятися в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах із застосуванням комплексних систем захисту інформації, що відповідають встановленим стандартам. Така відповідність підтверджується результатами державної експертизи, яка проводиться згідно з визначеними законодавством процедурами [187].

Іншим важливим органом державного управління є Державне агентство з питань електронного урядування України (ДАЕУ). Цей орган займається розвитком електронного урядування та підтримкою впровадження електронних послуг. ДАЕУ здійснює управління державними інформаційними ресурсами та системами електронного урядування, координує розвиток міжвідомчих

електронних взаємодій, а також забезпечує інтеграцію даних між різними державними реєстрами та базами даних [142].

ДАЕУ є центральним органом виконавчої влади, діяльність якого координується Кабінетом Міністрів України. Агентство реалізує державну політику в галузі інформатизації, електронного урядування, формування та використання національних електронних інформаційних ресурсів, а також сприяє розвитку інформаційного суспільства.

Основні завдання ДАЕУ включають реалізацію державної політики в зазначених сферах, узагальнення досвіду застосування законодавства, підготовку пропозицій щодо його вдосконалення, а також організацію прогнозно-аналітичних досліджень, присвячених розвитку інформаційного суспільства та електронного урядування.

До основних завдань Агентства відносяться [142]:

- реалізація державної політики у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

- узагальнює практику застосування законодавства з питань, що належать до його компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України та в установленому порядку вносить їх на розгляд Кабінету Міністрів України;

- організовує проведення прогнозно-аналітичних досліджень стану розвитку інформаційного суспільства, електронного урядування та сфери інформатизації;

- виконує функції генерального державного замовника Національної програми інформатизації,

- координує діяльність органів виконавчої влади, пов’язану із створенням та інтеграцією електронних інформаційних систем і ресурсів в Єдиний веб-портал органів виконавчої влади та наданням інформаційних та інших послуг.

Крім того, ДАЕУ виконує функції генерального державного замовника

Національної програми інформатизації, координує діяльність органів виконавчої влади з питань створення та інтеграції електронних інформаційних систем і ресурсів в Єдиний веб-портал органів виконавчої влади, а також забезпечує надання інформаційних послуг громадянам [63, 143, 181].

Національне агентство з питань державної служби України (НАДС) також відіграє ключову роль у сфері державного управління, зокрема в управлінні інформаційно-аналітичним забезпеченням (ІАЗ). НАДС займається розвитком нормативно-правової бази у сфері державної служби, підвищенням кваліфікації державних службовців, зокрема в галузі інформаційних технологій та цифрової грамотності. Основні функції НАДС охоплюють забезпечення формування та реалізації державної політики у сфері державної служби, управління персоналом у державних органах, участь у формуванні політики щодо служби в органах місцевого самоврядування та здійснення функціонального управління державною службою.

Місією НАДС є сприяння розвитку професійної, ефективної, стабільної та політично нейтральної державної служби, яка відповідатиме принципам належного управління, стандартам та кращим практикам країн-членів Європейського Союзу [63, 143, 181].

Місцеві органи управління в Україні реалізують національну політику у сфері інформаційного забезпечення адміністративних послуг, адаптуючи централізовано розроблені стратегії до унікальних потреб та особливостей місцевого контексту. Вони забезпечують практичне впровадження, моніторинг, та коригування ініціатив, спрямованих на цифрову трансформацію та модернізацію державного управління на регіональному та місцевому рівнях.

Місцеві органи влади впроваджують та адаптують національні директиви, нормативно-правових акти, стандарти і норми у сфері інформаційно-аналітичного забезпечення (ІАЗ). Вони не лише впроваджують ці політики на місцевому рівні, але й враховують специфічні потреби та умови регіону, забезпечуючи таким чином ефективну інтеграцію центральних ініціатив у локальний контекст. Завдяки цьому національні стратегії стають більш

ефективними та практичними в конкретних умовах, що сприяє їх успішному виконанню.

Місцеві органи влади також забезпечують постійний зворотний зв’язок із центральними органами управління, інформуючи їх про досягнення, труднощі та потреби на місцевому рівні. Це дозволяє центральним органам коригувати та вдосконалювати свої стратегії та політики, враховуючи реальні умови їх впровадження. Одним із найважливіших завдань місцевих органів є адаптація загальнонаціональних ініціатив до конкретних потреб і умов місцевих громад. Це включає в себе розробку індивідуальних підходів до розвитку місцевої інфраструктури, покращення послуг та забезпечення доступу до інформації, що робить цифрові послуги більш доступними та зручними для різних верств населення.

Крім того, місцеві органи влади відповідальні за моніторинг та оцінку ефективності впроваджених ініціатив у сфері ІАЗ. Вони збирають дані про використання цифрових послуг, аналізують задоволеність користувачів і ефективність систем, що дозволяє своєчасно вносити необхідні корективи та удосконалення. Місцеві органи також ініціюють і реалізують власні проекти та програми, спрямовані на підвищення якості та доступності державних послуг. Це включає розвиток місцевої ІТ-інфраструктури, підтримку цифрової грамотності громадян та створення нових можливостей для використання сучасних технологій.

Сучасні виклики вимагають від державних органів здатності швидко адаптуватися до новітніх технологічних змін. Організаційні структури мають бути достатньо гнучкими, щоб ефективно інтегрувати нові технології та методи обробки даних. Важливим елементом підвищення ефективності управління інформаційними ресурсами є також постійне підвищення кваліфікації співробітників і розвиток їхніх компетенцій у сфері ІАЗ [15].

Розглянемо приклади успішного управління інформаційними ресурсами в державному управлінні України, особливо в контексті цифрової трансформації, яка спрямована на підвищення прозорості, ефективності та доступності

державних послуг.

1. Електронне урядування. Проект: «Дія» – електронна платформа для надання державних послуг в цифровому форматі. Реалізація платформи «Дія» стала революційним кроком у спрощенні доступу громадян до широкого спектру державних послуг. Цей проект забезпечив інтуїтивно зрозумілий інтерфейс для користувачів, знизив бюрократичні бар'єри, підвищив ефективність державного управління, зменшив ризики корупції та значно покращив загальний рівень задоволення громадян державною підтримкою та послугами [189].

Завдяки цифровізації та автоматизації процесів, «Дія» не лише спростила взаємодію громадян з урядом, але й значно знизила можливості для корупції, підвищила прозорість державного управління, та зміцнила загальну структуру національної безпеки.

Електронна платформа «Дія» стала символом інноваційного підходу до державного управління. Запровадження цифрових ліцензій, електронної реєстрації бізнесу та інших послуг через один інтуїтивно зрозумілий інтерфейс значно знизило часові та фінансові витрати громадян, сприяючи зростанню економічної активності та підприємницького духу. Завдяки автоматизації багатьох процесів, «Дія» мінімізує людський фактор у взаємодіях з державою, що різко знижує потенціал для корупції. Наприклад, електронні декларації чи реєстрація нерухомості через платформу виключають необхідність безпосереднього контакту з чиновниками, зменшуючи можливості для хабарництва та зловживань.

«Дія» також вносить свій вклад у національну безпеку, спрощуючи моніторинг та управління важливими аспектами життя громадян. Завдяки інтеграції з іншими державними базами даних, платформа дозволяє ефективніше реагувати на надзвичайні ситуації, аналізувати та прогнозувати соціальні та економічні процеси в країні.

Розвиток «Дії» також викликає питання безпеки даних та захисту приватності. Важливо забезпечити, щоб заходи з кібербезпеки були на

високому рівні, а права та свободи громадян неухильно дотримувались. Неперервне вдосконалення технологічної інфраструктури та правових рамок є ключовим для забезпечення, що платформа відповідатиме викликам сучасного цифрового світу та продовжуватиме сприяти розвитку держави в безпечному та стабільному середовищі.

Таким чином, «Дія» не лише спрощує життя громадянам, а й вносить значний вклад у стабільність, безпеку та прозорість державного управління, формуючи новий стандарт для взаємодії громадян з урядом.

2. Прозорість державних закупівель. Проект «Prozorro» – система електронних закупівель, що забезпечує відкритий та прозорий процес тендерів. Реалізація системи Prozorro дозволяє всім учасникам ринку отримувати рівний доступ до державних тендерів, а державним органам – здійснювати закупівлі ефективніше та економічніше [182].

Проект «Prozorro» став значущим кроком у боротьбі з корупцією в Україні, забезпечуючи прозорість та відкритість у сфері державних закупівель [182]. Ця система електронних торгів не лише сприяла економії бюджетних коштів, а й значно вплинула на зміцнення державної безпеки, створюючи стійкішу та надійнішу систему управління державними ресурсами. Однією з основних переваг Prozorro є значне зменшення можливостей для корупційних схем у процесі закупівель. Прозорість системи забезпечується завдяки повному відкриттю інформації про тендери: від моменту оголошення до підписання контракту. Це не тільки зменшує простір для маніпуляцій та зловживань, а й підвищує довіру громадськості та міжнародних партнерів до української держави, що є критично важливим для економічної стабільності країни.

Prozorro дозволяє державі використовувати бюджетні кошти більш ефективно, забезпечуючи конкурентне середовище, в якому учасники тендерів змушені пропонувати кращі умови та ціни. Це призводить до зниження вартості закупівель, що дозволяє державі заощаджувати значні суми коштів, які можуть бути перерозподілені на інші важливі напрямки, такі як оборона, охорона здоров’я, освіта та інфраструктурні проекти.

Prozorro сприяє не тільки економічному виміру безпеки, але й зміцненню демократії та правової держави в Україні. Система забезпечує високий рівень підзвітності державних органів, обов’язково публікуючи результати всіх торгів, що робить можливим громадський контроль за діяльністю уряду та зменшує ризики зловживань.

Національна безпека також посилюється через забезпечення стабільності та передбачуваності в державних закупівлях. Міцна економіка та відсутність корупції зменшують внутрішні та зовнішні загрози, забезпечуючи кращий захист національних інтересів.

Незважаючи на успіхи, системі Prozorro все ще доводиться вирішувати деякі виклики, включаючи потребу в подальшій інтеграції з іншими державними інформаційними системами, покращенні інтерфейсу користувачів та забезпеченні більшої кількості навчань для учасників процесу. Розвиток цифрової грамотності серед державних службовців і постійне оновлення законодавства також є критично важливими для підтримки ефективності та прозорості системи.

Загалом, Prozorro є яскравим прикладом того, як технологічні інновації можуть сприяти зміцненню державної безпеки, економічної стабільності та демократичних інститутів в країні, стаючи важливим інструментом у руках уряду для боротьби з корупцією та неефективністю.

3. Цифровізація реєстрів. Проект цифровізації реєстрів, зокрема земельного кадастру та реєстру нерухомості, став ключовим етапом у модернізації державного управління. Завдяки цьому проекту вдалося централізувати та автоматизувати доступ до даних про земельні ділянки та об'єкти нерухомості, що значно спростило процес реєстрації прав власності та інші пов'язані з цим процедури. Ця ініціатива суттєво підвищила прозорість ринку нерухомості, скоротила час на обробку запитів і збільшила доходи держави від реєстраційних зборів [180].

Україна досягла значних успіхів у сфері управління інформаційно-аналітичними ресурсами, особливо через впровадження цифрових ініціатив, які

спрямовані на вдосконалення державного управління та покращення надання послуг населенню. Ці успішні приклади демонструють важливість інтеграції сучасних технологій у сферу ІАЗ для підвищення ефективності, прозорості та доступності державних послуг.

Одним з головних викликів залишається подальше розширення та адаптація цифрових сервісів до зростаючих потреб громадян і економіки, а також забезпечення високого рівня захисту даних і конфіденційності.

Організаційні структури та ролі в управлінні інформаційними ресурсами державного управління є критично важливими для успішної реалізації стратегій ІАЗ. Вони забезпечують координацію, ефективність та безпеку в обробці й використанні інформаційних ресурсів, що є необхідним для досягнення стратегічних цілей державного управління.

4.2 Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки Україні

Ефективність інформаційно-аналітичної діяльності в суспільстві може бути забезпечена лише при наявності належного правового регулювання. В Україні правові норми, які керують інформаційною діяльністю, поділяються на такі категорії:

- законодавчі акти, присвячені інформації;
- закони, що захищають права інтелектуальної власності;
- окремі положення інших актів, що впливають на інформацію та інтелектуальну власність.

З моменту здобуття незалежності, Україна активно впроваджує міжнародні норми у вітчизняну практику регулювання інформаційних процесів, що відображено у Конституції.

Основний правовий акт у цій сфері – Закон України «Про інформацію», який набув чинності 2 жовтня 1992 року і зазнав численних змін. Цей закон охоплює інформаційні відносини у всіх сферах діяльності, визначає права на

інформацію, статус учасників, регулює доступ до інформації та її захист, а також встановлює основи обігу інформації.

Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», прийнятий 9 січня 2007 року, визначає розвиток інформаційного суспільства як пріоритет, наголошуючи на важливості вільного доступу до інформації та обміну нею. Закон підкреслює недостатність розбудови інформаційного суспільства в країні порівняно з глобальними тенденціями та вимагає прискореного розвитку цієї сфери, особливо у контексті використання сучасних інформаційних технологій (ІТ).

Закон «Про доступ до публічної інформації» від 13 січня 2011 року сприяє транспарентності та відкритості влади, встановлюючи механізми доступу до інформації, яка є важливою для суспільства, і визначаючи особливі категорії інформації з обмеженим доступом.

Таким чином, українське законодавство забезпечує комплексний підхід до регулювання інформаційної діяльності, що охоплює захист інтелектуальної власності, розвиток інформаційного суспільства та визначення правил доступу до інформації.

Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є важливим аспектом зміцнення національної безпеки та обороноздатності держави. Інформаційно-аналітичне забезпечення є критично важливим для оперативного реагування сил безпеки України на загрози внутрішньої та зовнішньої безпеки. Актуальність теми обумовлена зростаючою кількістю інформаційних операцій проти України та необхідністю адекватного протистояння цим викликам. Розробка та впровадження законодавчих ініціатив для удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення (ІАЗ) сил безпеки України є критично важливим кроком у забезпеченні національної безпеки та обороноздатності країни. Розглянемо деякі аспекти впливу нормативно-правової бази ІАЗ на ефективність службово-бойових дій сил безпеки [203].

Юридична визначеність та прозорість. Сучасне, добре структуроване

законодавство забезпечує чіткі правила та процедури для діяльності сил безпеки, сприяючи їхній прозорості та передбачуваності. Відсутність юридичної визначеності може призводити до затримок у реагуванні на загрози, а також до зловживань та порушень прав людини.

Адаптація до сучасних викликів. Ефективність сил безпеки значною мірою залежить від їх здатності швидко адаптуватися до нових загроз, таких як кібератаки, гібридна війна, тероризм тощо. Нормативна база, яка не відображає сучасних реалій, серйозно обмежує цю здатність.

Міжвідомча координація. Наявність чіткого законодавчого регулювання сприяє кращій координації між різними силами безпеки та відомствами, уникненню дублювання функцій і зусиль, а також оптимізації розподілу ресурсів.

Міжнародна співпраця. Спроможність України до міжнародної співпраці в сфері безпеки також залежить від її законодавчої бази. Сумісність національного законодавства з міжнародними стандартами та угодами є ключовою для ефективної міжнародної взаємодії та підтримки.

Інновації та технології. Нормативно-правова база має сприяти впровадженню новітніх технологій і методик у діяльність сил безпеки. Відсутність правових механізмів для інновацій може обмежувати використання сучасних технологічних рішень.

Гармонізація з міжнародними стандартами. Забезпечення відповідності національного законодавства міжнародним нормам і стандартам для підвищення ефективності міжнародної співпраці.

Посилення міжвідомчої координації. Розробка та впровадження механізмів для зміцнення взаємодії між різними органами сил безпеки.

Для аналізу поточного стану нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України визначимо основні проблеми та виклики.

Наразі, Україна має низку законів та нормативних актів, які регулюють діяльність сил безпеки, включаючи Закон «Про національну безпеку України»,

Закон «Про державну таємницю», Закон «Про боротьбу з тероризмом» та інші. Однак, динаміка сучасних загроз вимагає постійного оновлення та доповнення існуючої нормативної бази. Багато існуючих нормативних актів були розроблені та прийняті 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. В деяких випадках, існуюче 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, потребується додаткова робота для гармонізації внутрішнього законодавства з міжнародними нормами, особливо в контексті кібербезпеки та захисту інформаційного простору.

Основними проблемами нормативно-правової бази є її застарілість, невідповідність сучасним вимогам інформаційної безпеки та відсутність інтегрованого підходу до збору, обробки та аналізу даних. Міжнародний досвід показує, що ефективне інформаційно-аналітичне забезпечення досягається через впровадження передових технологій обробки даних, законодавчу підтримку діяльності спецслужб і посилення міжвідомчої взаємодії. Потребують впровадження сучасні ІТ-рішень для збору, обробки та аналізу даних та існує необхідність постійного підвищення кваліфікації фахівців інформаційно-аналітичних підрозділів.

Дослідженнями проблемних питаньінформаційно-аналітичного забезпечення сил безпеки та оборони України зробили такі вчені як:Мацько О. Й., Микусь С. А., Солонніков В. Г., Дробаха Г.А., Єрмошин М.О., Смірнов Є.Б., Шемчук В.В., Олещенко О. А., Іохов О.Ю., Лісіцин В. Е., Горєлишев С. А. та ін. Вклад в дослідження питань державного управління силами безпеки внесли: Бєлай С.В., Бондаренко О.Г., Єманов В.В. та ін.

До основних нормативно-правових актів щодоінформаційно-аналітичного

забезпечення сил безпеки України можна віднести:

1. Закон України «Про основні засади забезпечення кібербезпеки України» [68]. Метою закону є створення комплексної юридичної основи для захисту кіберпростору України, включаючи захист критичної інфраструктури, персональних даних громадян, а також державних інформаційних систем. Цим законом встановлюються вимоги до кібербезпеки для операторів критичної інфраструктури. Розроблені механізми реагування на кіберінциденти. Створена національна інфраструктури для виявлення та запобігання кіберзагроз. Законом про кібербезпеку регулюються взаємодії між державними органами, приватним сектором та міжнародними організаціями у сфері кібербезпеки.

Україна приділяє значну увагу зміцненню своїх кібербезпекових можливостей у контексті наростаючих глобальних кіберзагроз. Закон України про кібербезпеку є ключовим документом, що визначає правові та організаційні засади забезпечення кібербезпеки в державі, включно з аспектами, що стосуються інформаційно-аналітичного забезпечення сил безпеки.

Закон визначає органи державної влади, відповідальні за кібербезпеку, включаючи ті, що забезпечують інформаційно-аналітичну підтримку сил безпеки, такі як Служба безпеки України, Державна спеціальна служба зв’язку та інформації, Міністерство оборони тощо.

Закон встановлює загальні заходи щодо забезпечення кібербезпеки, які включають розробку та впровадження політик кібербезпеки, захисту інформаційних систем, а також ідентифікацію та реагування на кіберзагрози. Також окреслені механізми збору, обробки та аналізу даних про кіберзагрози, а також розробку стратегічних та оперативних аналітичних матеріалів для підтримки рішень у сфері національної безпеки та оборони. Визнання важливості міжнародної співпраці в галузі кібербезпеки, включаючи обмін інформацією про кіберзагрози, спільні навчання та розробку міжнародних стандартів кібербезпеки. Встановлені правові норми, що регулюють відповідальність за порушення у сфері кібербезпеки, з метою захисту національних інтересів та забезпечення безпеки інформаційного простору.

2. Закон України «Про засади інформаційної безпеки України» [65].Метою закону є забезпечення захисту інформаційного простору України від дезінформації, пропаганди та інших інформаційних операцій, які можуть загрожувати національній безпеці.Визначені основні загрози інформаційній безпеці та механізмів їх протидії.Створена система моніторингу та аналізу інформаційного простору. Розроблені стандарти для ЗМІ та інших інформаційних ресурсів щодо публікації та розповсюдження інформації. Встановлена відповідальність за розповсюдження недостовірної інформації.

Закон «Про засади інформаційної безпеки України», охоплюючи інформаційно-аналітичне забезпечення сил безпеки, створює юридичну основу для комплексного підходу до захисту інформаційного простору України. Це включає не тільки технічні та організаційні заходи, але й важливі аспекти міжвідомчої координації, міжнародної співпраці, освіти та правового регулювання.

3. Закон України «Про розвідку» [69]. Метою закону єнормативне регулювання розвідувальної діяльності в Україні для підвищення ефективності збору, обробки та аналізу розвідувальної інформації. Закономвизначаються правові основи розвідувальної діяльності, включаючи збір, аналіз і розповсюдження розвідданих.Регулюється взаємодія розвідувальних служб з іншими органами державної влади та міжнародними партнерами,встановлюються механізми контролю та нагляду за діяльністю розвідувальних служб.

Законом України «Про розвідку» встановлені чіткі правові основи для проведення розвідувальної діяльності, визначені основні завдання, принципи та методи розвідки, а також органи, які уповноважені проводити розвідувальні операції. Також регулевані питання класифікації, зберігання, захисту та розголошення інформації, отриманої в ході розвідувальної діяльності, з метою захисту державної таємниці та інших конфіденційних даних. Визначені механізми парламентського та громадського контролю за діяльністю розвідувальних служб, а також внутрішніх процедур контролю і оцінки

ефективності розвідувальної роботи.

Закон України «Про розвідку»є ключовим елементом національної безпекової архітектури, який забезпечує правові та організаційні рамки для ефективної роботи розвідки. Через свою роль у зборі, аналізі та використанні розвідданих, розвідувальні служби є невід'ємною частиною інформаційно-аналітичного забезпечення сил безпеки, сприяючи своєчасному виявленню та нейтралізації загроз національній безпеці.

4. Закон про «Про державну таємницю» [64]. Метою закону є визначення нормативів щодо захисту державної таємниці з метою адаптації до сучасних викликів у сфері інформаційної безпеки.

Закон України «Про державну таємницю» регламентує взаємовідносини, пов'язані з захистом інформації, яка становить державну таємницю, та встановлює юридичні, організаційні та технічні засади її збереження. В рамках інформаційно-аналітичного забезпечення сил безпеки України закон визначає критерії, за якими інформація може бути визнана державною таємницею, в тому числі інформація, що стосується обороноздатності та безпеки держави. Це охоплює військові, технічні, наукові, розвідувальні дані, які мають значення для забезпечення національної безпеки. Закон встановлює вимоги до захисту інформації, яка належить до державних таємниць, включаючи забезпечення її конфіденційності, інтеграції та доступності. Це має вирішальне значення для ефективного управління та використання інформаційних ресурсів у силових структурах. Закон передбачає відповідальність за незаконне отримання, передачу, розголошення або втрату інформації, що становить державну таємницю. Це створює правові основи для притягнення до відповідальності осіб, які порушили режим таємниці, забезпечуючи тим самим додатковий захист інформації. Закон окреслює повноваження та обов'язки органів державної влади, установ та організацій щодо забезпечення режиму державної таємниці, включаючи органи сил безпеки. Це включає розробку та впровадження заходів безпеки, атестацію робочих місць, навчання персоналу тощо. Закон регламентує порядок надання доступу до державних таємниць,

визначає процедури перевірки осіб, їх допуску до роботи з таємними матеріалами, що є ключовим для інформаційно-аналітичної діяльності військових і спецслужб.

Хоча закон «Про державну таємницю» безпосередньо не зосереджується на інформаційно-аналітичному забезпеченні сил безпеки, він створює правову основу для захисту і використання інформації, що має важливе значення для національної безпеки і оборони.

5. Закон України «Про національну безпеку України» визначає правові та організаційні основи забезпечення національної безпеки і оборони країни, а також задає основні принципи діяльності держави в цих сферах [66]. Інформаційно-аналітичне забезпечення сил безпеки України в контексті цього закону охоплює наступні аспекти.

Закон визначає інформаційну безпеку як важливу складову національної безпеки, підкреслюючи необхідність захисту інформаційного простору країни від зовнішніх і внутрішніх загроз. Окремі положення закону стосуються розвідувальної діяльності, яка є частиною інформаційно-аналітичного забезпечення. Вказується на необхідність забезпечення дієвої розвідки для виявлення та протидії потенційним загрозам національній безпеці. Закон акцентує увагу на забезпеченні кібербезпеки як елементу захисту критичної інформаційної інфраструктури держави та сил безпеки, встановлюючи основи для протидії кіберзагрозам. Положення закону передбачають координацію діяльності різних сил безпеки та оборони України, в тому числі через обмін інформацією та аналітичними даними для підвищення ефективності виконання завдань національної безпеки. Закон визначає повноваження президента, Верховної Ради, Уряду, Міністерства оборони, Служби безпеки України та інших органів у сфері забезпечення національної безпеки, включно з інформаційно-аналітичним забезпеченням.

Процеси інформатизації сил безпеки істотно відрізняються від ринкових, вимагають більш жорсткого керування. Тому стосовно них повинна бути розроблена нормативно-правова база й інформатизацію доцільно розглядати як

організований процес створення оптимальних умов для задоволення інформаційних потреб особового складу, посадових осіб органів управління силами на основі формування і раціонального використання інформаційних ресурсів у новому технологічному середовищі [125].

Сили безпеки України використовують у своїй службово-бойової діяльності нормативно-правову базу Збройних Силах України у питаннях інформатизації. Ці питання визначаються низкою документів, серед яких слід виділити такі:

1. Концепція інформатизації Міністерства оборони України є важливою частиною стратегічного розвитку військової інфраструктури країни, спрямована на підвищення її обороноздатності та ефективності за допомогою сучасних інформаційних технологій [121]. Вона передбачає комплексний підхід до розвитку, інтеграції та використання інформаційних систем та технологій в усіх аспектах діяльності Збройних Сил. Концепція інформатизації охоплює такі основні аспекти:

Інтеграція інформаційних систем. Це передбачає створення єдиної інформаційної мережі, що дозволяє ефективно управляти ресурсами, координувати дії підрозділів і швидко обмінюватися даними між різними рівнями командування. Автоматизація процесів управління. Впровадження сучасних інформаційно-керуючих систем для автоматизації процесів планування, управління бойовими діями, логістики та інших важливих аспектів діяльності Збройних Сил. Забезпечення кібербезпеки. Розробка та впровадження заходів для захисту військових інформаційних систем від кібератак, шпигунських програм і інших загроз. Розвиток системи зв’язку. Модернізація та розширення систем зв’язку для забезпечення стабільного, безперебійного та безпечного обміну інформацією в умовах бойових дій. Підготовка кадрів. Організація навчання та підвищення кваліфікації військовослужбовців у сфері використання сучасних інформаційних технологій.

Для реалізації концепції інформатизації необхідна ефективна

нормативно-правова база, яка включає: закони та нормативні акти, які регулюють використання інформаційних технологій в Збройних Силах, забезпечення кібербезпеки, захисту інформації та персональних даних. Стандарти та регламенти, які визначають технічні вимоги до інформаційних систем, засобів зв'язку, програмного забезпечення та обладнання. Директиви та інструкції, які регулюють порядок розробки, впровадження та експлуатації інформаційних систем в військовій сфері. Міжнародні угоди та співпраця, що включають участь України в міжнародних проєктах і програмах з розвитку військових інформаційних технологій, обмін досвідом та знаннями з країнами-партнерами.

Концепція інформатизації Міністерства оборони України є ключовим елементом стратегії національної безпеки та оборони, спрямованої на підвищення ефективності та готовності військових сил до дій у сучасних умовах. Реалізація цієї концепції вимагає комплексного підходу, включаючи розвиток нормативно-правової бази, інтеграцію сучасних інформаційних технологій, забезпечення кібербезпеки, розвиток систем зв'язку та підготовку кадрів.

2. Концепція створення єдиної автоматизованої системи управління (ЄАСУ) Збройних Сил України орієнтована на інтеграцію всіх рівнів управління та видів збройних сил у єдину інформаційну структуру [65, 68, 70]. Це має на меті забезпечити ефективне управління, оперативне реагування на змінні умови та злагоджену взаємодію між різними підрозділами та відомствами. Реалізація такої системи передбачає комплексний підхід до автоматизації управління військовими діями, логістики, розвідувальної інформації та інших ключових аспектів діяльності Збройних Сил.

Концепція складається з таких елементів: ЄАСУ має інтегрувати в собі різноманітні інформаційні системи і бази даних, що використовуються в Збройних Силах, забезпечуючи їх взаємосумісність та єдиний формат обміну даними. Основна мета ЄАСУ - максимальна автоматизація процесів прийняття рішень, планування, управління військами та контролю за виконанням завдань.

Високий рівень захисту від зовнішніх та внутрішніх кіберзагроз є критично важливим для надійної роботи ЄАСУ. Система має бути гнучкою до модифікацій та розширення, щоб адаптуватися до змін у структурі Збройних Сил та вимогам сучасного бойового поля. Важливою складовою є створення єдиної, захищеної системи зв'язку, яка забезпечує передачу даних між всіма рівнями управління. ЄАСУ повинна забезпечувати взаємодію не тільки в межах Збройних Сил, а й з іншими відомствами, силами безпеки та оборони України, а також міжнародними партнерами.

Створення єдиної автоматизованої системи управління Збройних Сил України є стратегічно важливим завданням, що сприятиме підвищенню обороноздатності країни, оперативності управління та ефективності виконання поставлених завдань. Успішна реалізація цієї концепції потребує не тільки технічного забезпечення та розробки програмного забезпечення.

3. Положення про науково-інформаційну діяльність у Збройних Силах України визначає правові, організаційні та методологічні основи проведення наукових досліджень, розробки, впровадження та використання наукових знань та інформаційних технологій з метою підвищення обороноздатності та безпеки держави [120]. Основні аспекти такого положення можуть включати: підвищення ефективності управління Збройними Силами через впровадження сучасних наукових досягнень та інформаційних технологій, розвиток наукової бази для забезпечення потреб оборони та безпеки, оптимізація процесів збору, обробки, зберігання та передачі інформації військового призначення, забезпечення інформаційної безпеки в умовах сучасних викликів та загроз.

4. Доктрина «Зв'язок та інформаційні системи» розроблена з урахуванням вимог союзної об'єднаної публікації НАТО AJP-06 «Allied Joint Doctrine for Communication and Information Systems (Edition A Version 1)» (Союзна об'єднана доктрина для зв'язку та інформаційних систем) [49]. Ця Доктрина забезпечує загальне стратегічне керівництво із застосування зв'язку та інформаційних систем у Збройних Силах України та інших складових сил оборони під час їх застосування та підготовки, у т.ч. під час проведення

спільних навчань (тренувань) тощо. Вона вводить термінологію в галузі зв'язку та інформаційних систем, сумісну із термінологією, прийнятою в НАТО, описує характеристики зв'язку та інформаційних систем, поняття інформаційного менеджменту, архітектури побудови зв'язку та інформаційних систем, захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах, функції та завдання у відношенні до зв'язку та інформаційних систем, визначає загальні положення із планування та застосування зв'язку та інформаційних систем, а також визначає аспекти взаємосумісності систем зв'язку та інформаційних систем.

У Національної гвардії, як суб'єкта сил безпеки, з питань ІАЗ діє Концепція державної цільової програми розвитку Національної гвардії України на період до 2020 р. та Концепція розвитку сектора безпеки і оборони України що введена Указом Президента України від 14.03.2016 р. № 92/2016 [125, 246]. Концепція розвитку Національної гвардії України втратила актуальність, терміни дії програми закінчились, реалізація концепції була не повна.

Концепція розвитку сектора безпеки і оборони України є стратегічним документом, що визначає основні напрямки та пріоритети у формуванні та розвитку здатностей сектору безпеки і оборони країни, в тому числі інформаційно-аналітичного забезпечення (ІАЗ) сил безпеки.

До нормативно-правової бази ІАЗ сил безпеки можна віднести і ряд стандартів та нормативних документів, які визначають вимоги до захисту інформації у різних сферах, включаючи державне управління, банківську сферу, телекомунікації та інші галузі.

1. Державний стандарт України DSTU 4145-2002 «Інформація. Захист інформації. Основні терміни та визначення»: Цей стандарт визначає основні терміни та визначення, що використовуються в сфері захисту інформації.

2. Державний стандарт України DSTU ISO/IEC 27001:2015 «Інформаційна технологія. Безпека інформації. Системи управління інформаційною безпекою. Вимоги»: Цей стандарт встановлює вимоги до

систем управління інформаційною безпекою та надає рекомендації щодо їх впровадження.

3. Державний стандарт України DSTU 3731:2001 «Інформаційна технологія. Захист інформації. Загальні положення»: Цей стандарт встановлює загальні положення щодо захисту інформації, включаючи принципи захисту інформації та основні вимоги до захисту.

4. Стандарт Payment Card Industry Data Security Standard (PCI DSS): Цей стандарт встановлює вимоги до захисту конфіденційної інформації про платіжні картки та інших даних, які зберігаються та обробляються в платіжних системах.

5. ISO/IEC 27001 – Міжнародний стандарт, що встановлює вимоги до системи управління інформаційною безпекою (СУІБ). Хоча це міжнародний стандарт, його принципи та практики можуть бути адаптовані на національному рівні для забезпечення захисту інформації в силових структурах.

6. NIST Cybersecurity Framework – розроблено Національним інститутом стандартів та технологій США, цей фреймворк пропонує структуру для управління та зниження кібербезпекових ризиків. В Україні може бути розроблено подібний національний стандарт або адаптовано існуючий для потреб сектора безпеки.

Ці стандарти і нормативні документи визначають базові вимоги та методи захисту інформації в різних сферах діяльності в Україні. Державні установи повинні дотримуватися цих вимог для забезпечення безпеки інформації та відповідності законодавству.

Дослідження міжнародного досвіду в сфері нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки дозволяє визначити передові практики та інноваційні підходи, які можуть бути адаптовані та впроваджені в Україні [56]. Наведемо декілька прикладів з різних країн:

1. Сполучені Штати Америки. Patriot Act: Закон, прийнятий після терактів 11 вересня 2001 року, значно розширив повноваження американських правоохоронних органів та спецслужб у сфері нагляду та збору інформації для

боротьби з тероризмом. Він включає положення, які дозволяють владі вести нагляд без судового ордера за певних умов, що сприяло покращенню інформаційно-аналітичного забезпечення.

Cybersecurity Information Sharing Act (CISA) 2015: Закон, що спрощує обмін інформацією про кіберзагрози між урядом США та приватним сектором. Цей акт сприяє кращій координації та ефективності виявлення та відповіді на кібератаки.

2. Ізраїль розробив комплексний підхід до кібербезпеки, який включає різні законодавчі та регуляторні ініціативи. Вони зосереджені на захисті критичної інфраструктури та зміцненні національної кібербезпеки через співпрацю між державним та приватним секторами. Це забезпечує ефективний обмін інформацією та ресурсами для протидії кіберзагрозам.

3. Естонія є світовим лідером у сфері е-урядування та кібербезпеки. Країна розробила ряд законів, що регулюють захист даних, кібербезпеку та електронні послуги, забезпечуючи високий рівень захисту інформації та інфраструктури. Це включає комплексні заходи щодо захисту персональних даних, кіберзахисту державних служб та впровадження цифрових ідентифікаторів.

4. Cybersecurity Act 2018. Закон, який встановлює юридичну рамку для кібербезпеки в Сінгапурі, зокрема захист критичної інфраструктури від кібератак. Він передбачає створення національної кібербезпеки агенції, яка координує зусилля з кібербезпеки на національному рівні, а також сприяє міжнародній співпраці.

5. Німеччина: Bundesamt für Sicherheit in der Informationstechnik (BSI) - закон, який регулює діяльність Федерального відомства з безпеки в інформаційних технологіях. Він встановлює рамки для захисту федеральних інформаційних систем і сприяє підвищенню кібербезпеки в приватному секторі.

Ці приклади демонструють, що ефективне інформаційно-аналітичне забезпечення сил безпеки в сучасному світі вимагає комплексного підходу, який включає оновлення законодавства, співпрацю між державним та

приватним секторами, а також міжнародну координацію.

Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є ключовим для підвищення ефективності національної оборони та безпеки. Це передбачає комплексний підхід, що включає законодавчі, технічні, та організаційні заходи. Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України вимагає комплексного підходу, урахуванню багатьох факторів що впливають на безпекову складову.

Виклики сучасності з якими зіткнулась наша держава вимагають більш широкого запровадження інформатизації та цифровізації державних органів управління. Останні роки Україна зробила великі кроки до цифровізації, але цей процес для сил безпеки має малі темпи, а в умовах широкомасштабної агресії рф це є одним з критичних безпекових факторів.

Роботи з інформатизації пов’язані з великими витратами сил і засобів, тому не можуть вестися на рівні місцевих ініціатив і громадських засад, а вимагають єдиного керівництва, єдиних концептуальних підходів, узгодження зусиль у рамках відомчих і загальнодержавних програм, створення штатних структур, відповідальних за розроблення й застосування програмно-апаратних засобів, узгодження з реформами й розвитком сил безпеки, що відбуваються. Цілеспрямовану інформатизацію сил безпеки варто розпочинати з процесів навчання, тим самим вирішити важливі завдання: утворити методологічне ядро майбутньої відомчої інформаційної системи та створити базу підготовки кадрів, які володіють досвідом упровадження інформаційних технологій у службово-бойову діяльність.

4.3 Підходи до застосування геоінформаційних систем в управлінській діяльності сил безпеки України

Геоінформаційні системи (ГІС) займають центральне місце в сучасному державному управлінні, пропонуючи інструменти для аналізу, управління та

візуалізації даних з географічною складовою. Використання ГІС у державному секторі значно підвищує ефективність прийняття рішень, планування та моніторингу в різних галузях, від міського розвитку до екологічного контролю та управління кризовими ситуаціями. Зокрема, ГІС у безпековому секторі України дозволяють збирати, обробляти, аналізувати та візуалізувати просторові дані, що стосуються національної безпеки та оборони. Це сприяє підвищенню ефективності планування, координації та виконання оборонних і безпекових операцій як на національному, так і на міжнародному рівнях [218].

Перші геоінформаційні системи з’явилися ще в 1950-1960-х роках і спочатку були розроблені для вирішення завдань у цивільному секторі. Наприклад, наприкінці 1960-х років Бюро перепису населення США створило формат GBF-DIME (Geographic Base File, Dual Independent Map Encoding), де вперше була реалізована топологічна схема визначення просторових відношень між об’єктами. Ця топологія описувала, як лінійні об’єкти на карті взаємодіють між собою, які площинні об’єкти мають спільні межі та які об’єкти складаються із суміжних елементів.

Активне використання сучасних ГІС-технологій почалося понад 25 років тому в Канаді, спочатку для потреб землевпорядкування. У 1970-1980-х роках у світі з’явилася потужна ГІС-індустрія, з лідерством США в цій сфері [233].

Сьогодні сфери застосування ГІС неймовірно різноманітні: землевпорядкування, управління ресурсами, екологія, муніципальне управління, транспорт, економіка, вирішення соціальних питань тощо. Це один із найбільш динамічно розвиваючих сегментів ринку високих комп'ютерних технологій. На цьому ринку працює велика кількість компаній, таких як Intergraph, ESRI, Autodesk, CalComp, ObjectLand, а також українські ГІС, які базуються на цифрових картах, розроблених за програмою Топографічного управління Генерального штабу Збройних Сил України, та інші [212, 233].

Нові можливості органам управління та військам надає використання геоінформаційних систем – комплексу реалізованих на ЕОМ програм та даних, який дозволяє знаходити та відображати картографічну інформацію

різноманітного призначення, проводити певні топографічні розрахунки. Сучасні геоінформаційні системи дозволяють швидко отримати карту місцевості з потрібною деталізацією та масштабом, уточнити елементи інфраструктури місцевості, особливості її рельєфу, здійснити прив’язку до карт отриманих розвідувальних відомостей, допомагають вести орієнтування під час розвідувальних дій.

ГІС, або Географічні Інформаційні Системи – це комп’ютерні системи, побудовані за сучасною технологією, яка дозволяє ефективно працювати з просторово-розподіленою інформацією для картографування та аналізу об’єктів реального миру, подій та явищ, що прогнозуються або відбуваються [233].

За принципами побудови ГІС є закономірним розширенням концепції Баз Даних, доповнюючи їх наочністю представлення і можливістю вирішувати задачі просторового аналізу.

Є багато визначень ГІС, але у Законі України Про Національну програму інформатизації надано таке визначення ГІС: «геоінформаційні системи – сучасні комп’ютерні технології, що дозволяють поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо)» [70].

Тут треба розуміти, що з точки зору науки ГІС – це засіб моделювання та дослідження природних та соціально-економічних систем, в технологічному аспекті це засіб збору, зберігання, відображення та розповсюдження географічної інформації, а з точки зору виробника – це комплекс апаратних засобів та програмних продуктів для управління та прийняття рішень. Таким чином, ГІС може одночасно розглядатися як інструмент наукового дослідження, технологія та продукт ГІС – індустрії. Це типчина ситуація на сучасному рівні розвитку, що характеризується інтеграцією науки та виробництва.

Практично в будь-якій сфері діяльності зустрічається інформація такого роду, що представлена у виді карт, планів, схем, діаграм тощо. Це може бути

схема метро або план будинку, карта екологічного моніторингу території або схема взаємозв’язків між офісами компанії, атлас земельного кадастру або карта природних ресурсів і багато чого іншого. Все це можна відображати й на паперу, але у геоінформаційних системах ці дані звичайно зберігаються у вигляді цифрового набору тематичних шарів, які об’єднані на основі їх географічного положення.

Такий підхід дає можливість працювати як з векторними, так й з растровими моделями відображення графічних даних, він є ефективним при вирішенні будь-яких просторових задач та проведенні відповідних розрахунків. Це дає можливість накопичувати й аналізувати подібну інформацію, оперативно знаходити потрібні зведення і відображати них у зручному для використання виді.

До складових геоінформаційних систем відносяться [218]:

- апаратні засоби (комп’ютери, периферійні та ввідно-виводні пристрої, засоби дистанційного зондування Землі, глобального позиціонування та ін.);
- програмне забезпечення (функції та інструменти, що дозволяють здійснити зберігання, обробку та аналіз, візуалізацію просторової інформації);
- дані (у вигляді готових цифрових та електронних карт з потрібними тематичними шарами, знімків космічної та аерофоторозвідки тощо).

Операції, що здійснюються геоінформаційними системами:

- автоматизоване введення даних;
- управління даними та їх обробка;
- запит та аналіз даних;
- візуалізація даних.

Завдяки достатньо добре відпрацьованим сучасним комп’ютерним технологіям застосування ГІС дозволяє різко збільшити оперативність і якість роботи з просторово-розподіленою інформацією у порівняння з традиційними паперовими методами і традиційними технологіями баз даних.

Традиційно ГІС-технології застосовуються в земельному кадастрі, кадастрі природних ресурсів, екології, сфері роботи з нерухомістю й іншими

об’єктами, вимагають оперативного керування ресурсами і прийняття рішень. Зараз усе ширше починають упроваджуватися ГІ масового користування, типу електронних планів міста, схем руху транспорту тощо. За оцінками, до 80-90% всієї інформації, може бути представлене у виді ГІС [233].

У силових міністерствах та відомствах ГІС також знайшли широке застосування, наприклад, під час:

- планування, оцінювання та відображення дій служб та сил безпеки та оборони;
- планування аварійно-рятувальних і охоронних заходів;
- моделювання надзвичайних ситуацій;
- стратегічного та тактичного планування воєнних дій та операцій;
- здійснення навігації служб та сил швидкого реагування та інших силових відомств тощо.

Таким чином, крім іншого, ГІС – це закономірний етап на шляху переходу до безпаперової технології обробки інформації, що відкриває нові широкі можливості маніпулювання даними, що мають просторову прив’язку.

За територіальним охопленням розрізнюють:

- глобальні ГІС,
- субконтинентальні ГІС,
- національні або державні ГІС,
- регіональні ГІС,
- субрегіональні ГІС,
- локальні або місцеві ГІС.

За час використання ГІС накопичений значний досвід, однак аж до порівняно недавнього часу їхнє застосування було можливе лише на основі могутніх і дорогих ЕОМ. Удосконалювання обчислювальної техніки привело до того, що усе більш широкі можливості ГІС-технологій стають доступні користувачам звичайних персональних комп’ютерів.

Якщо казати про застосування ГІС у воєнному ділі, то слід враховувати, що для прийняття рішень командир будь-якого рівня так чи інакше

використовує зведення про просторове розташування об’єктів. Історично такі дії підтримувалися паперовими картами, що утворювалися військово-топографічними службами. Але ГІС на сей час дозволяють робити й те, що не вдається за допомогою паперових карт:

- по-перше, крім власне карти з’являється можливість побудувати трьохвимірну модель місцевості, що є більш наочною, за допомогою такої карти можна не тільки оцінювати видимість із різних точок, але й моделювати політ над територією, щоб, наприклад виявляти імовірні місця засад противника;

- по-друге, паперова карта не здатна швидко відобразити зміни ситуації. В ГІС же інформація водночас оновлюється шляхом передачі по каналам зв’язку оверлейних шарів з поточною обстановкою (причому це може бути як список координат, який описує просторове розташування об’єктів, так і елементи, що описують більш складні просторові відношення та структури, наприклад, топології кордонів, маршрути, рух цілей тощо).

Працюючи з ГІС, можливо вивести на екран комп’ютера одну або декілька карт (схем, планів і т.д.). Є можливість змінювати детальність зображення, збільшуючи або зменшуючи окремі елементи карти. Наприклад, вибравши на карті міста потрібний будинок, можна вивести його великим планом і розглянути шляхи під’їзду до будинку.

Існує можливість керувати тематичним складом зображуваної інформації. Наприклад, на карті корисних копалин, відключити видимість непотрібних у даний момент видів викопних ресурсів і річкової мережі, залишивши тим часом видимої дорожню мережу.

Вказавши об’єкт на карті, можна одержати інформацію про нього. Наприклад, вказавши об'єкт нерухомості, довідатися про його вартість, хто є його власником, який стан об’єкта та інше. Вибравши промислове підприємство, що знаходиться поблизу, ви одержите дані про його профіль, вплив на екологію району і т.д. Ряд геометричних характеристик об’єктів (довжину вулиці, відстань між містами, площа лісового масиву) можна

виміpити безпосередньо на екрані, користуючись засобами ГІС.

З іншого боку, можно використовувати ГІС як пошукову систему. У цьому випадку складається запит, у якому перелічуються властивості об’єктів, а система виділяє на карті підходящі об’єкти. Наприклад, працюючи з ГІС кадастру земельних ресурсів, можно зажадати показати на карті земельні ділянки площею не менш 10 соток, розташовані не далі 3 км від залізничної станції й одночасно не далі 1 км від прилеглих водойм.

Спеціальні засоби дозволяють проводити аналітичну обробку даних, а в більш складних випадках – моделювання реальних подій. Результати обробки також можна побачити на екрані комп’ютера. Наприклад, можна оперативно прогнозувати можливі місця розривів на трасі трубопроводу, простежити на карті шляху поширення забруднень і оцінити ймовірний збиток природному середовищу, обчислити обсяг засобів, необхідних для усунення наслідків аварії. Іншим прикладом може служити задача оптимізації вартості перевезень вантажів між населеними пунктами з урахуванням характеристик транспортної мережі, обсягу перевезень і інших умов. Найбільш складні технологічні рішення містять у собі експертну підтримку і дозволяють одержувати на виході обґрунтований висновок, придатний для прийняття конкретних рішень.

Більшість задач ГІС можуть вирішуватися і вирішувалися раніш і без використання ГІС – засобів. Останні, однак, дозволяють з великою ефективністю і зручністю для користувача організувати в єдиний комплекс операції введення і відновлення вихідної інформації, її переробки і відображення результатів, вирішувати задачі так називаного просторового аналізу.

Що стосується практичних розробок та використання геоінформаційних систем, то більш складна система «Аргумент», що використовує цифрові карти вітчизняного виробництва розроблена у Харківському університеті Повітряних Сил.

Вже більш 15 років Топографо-інженерний центр Армії США розробляє воєнну геоінформаційну систему, що отримала назву Combat Terrain

Information Systems (CTIS) – це перекладається як бойова топоінформаційна система. Її ядром є цифрова топографічна система підтримки прийняття рішень Digital Topographic Support System (DTSS), яка об'єднує функції ГІС та системи обробки даних дистанційного зондування поверхні Землі. У якості ГІС – компоненти використовуються продукти виробництва компанії ESRI. Оновлення даних в DTSS входить до обов'язків спеціальних мобільних груп картографів зі складу армії США. Основним джерелом при цьому служить агентство NIMA (National Imagery and Mapping Agency). Потім отриману інформацію уточнюють польові групи [233].

Точна картографічна інформація допомагає військовослужбовцям маневрувати, організовувати засідки, визначати положення вогневих точок противника, знаходити місця безпечних місць нічних стоянок. Карти передаються на мобільні прилади з центральних командних пунктів. Така система вже використовувалася у Боснії, в Афганістані і Іраку. Вона давала можливість дати чітке представлення де знаходяться союзники (але хоч це й не заважало іноді вести по ним вогонь), визначати де знаходиться противник, забезпечувати ефективне та безпечне маневрування та ведення боїв. Інтерфейс системи інтуїтивно зрозумілий, що дає можливість засвоїти її у достатньо стислі строки.

Розвиток подібної системи американські військові бачать у створенні так званої бойової системи майбутнього (Future Combat System, FCS), яка допоможе проводити розрахунки та аналіз обстановки не тільки за допомогою отриманих даних розвідки, але й з врахуванням стратегії доцільної поведінки, що визначається прийнятої воєнною стратегію та тактикою дій за ситуаціями, які складаються.

Таким чином, використовуючи ГІС-технології, отримуємо можливість:

- значно підвищити оперативність всіх етапів роботи з просторово розподіленими даними, починаючи від уведення вхідної інформації, її аналізу і до вироблення конкретного рішення. Причому не буде потрібно розшукувати потрібні зведення серед стосів карт і планів – одержати них на екрані, під час

бою тощо;

- використовувати для введення і відновлення інформації в базі даних сучасні електронні засоби геодезії і системи глобального позиціонування (GPS), а значить – постійно мати саму точну і свіжу інформацію;

- заручитися високою компетенцією фахівців, що розробляють програмне забезпечення для ГІС – систем, й тоді для того, щоб використовувати, наприклад, програми розрахунку поширення забруднень, не потрібно буде мати математичної освіти.

Вартість робіт при створенні ГІС визначається різними складовими: витратами на апаратуру і програмне забезпечення, вартістю вхідної інформації і її якістю, витратами на оплату праці операторів, що проводять оцифрування даних і іншими. Тому для того, щоб оцінити вартість проекту, у кожнім конкретному випадку необхідно проконсультуватися з фахівцями.

Швидкий прогрес у сфері обчислювальних технологій, поява нових викликів для національної безпеки України, недостатнє фінансування внутрішніх програм для створення систем підтримки прийняття рішень, часткова нормативно-правова регуляція інформаційно-аналітичних систем, а також відсутність загальнодержавних програм з модернізації та підтримки геоінформаційних систем в управлінських процесах сил безпеки України – це лише деякі з ключових проблемних аспектів, що перешкоджають ефективному впровадженню та розвитку геоінформаційних технологій у діяльності сил безпеки нашої країни.

Питання державного управління інформаційними ресурсами в Україні, особливо щодо впливу геоінформаційних систем на підвищення ефективності управлінських процесів, детально вивчені в працях таких вітчизняних науковців, як: Дробаха Г.А., Єрмошин М.О., Смірнов Є.Б., Іохов О.Ю., Бєлай С.В., Шипулін В.Д., Пітак І.В., Негадайлов А.А., Масікевич Ю.Г., Пляцук Л.Д., Шапорев В.П., Моісеєв В.Ф. та ін.

Геоінформаційні системи знаходять широке застосування у різних сферах державного управління, включаючи міське планування та управління, розробку

генеральних планів розвитку населених пунктів, планування інфраструктури та комунальних послуг, моніторинг забудови та використання земельних ресурсів [129]. Також ГІС активно застосовуються для екологічного моніторингу та управління, оцінки впливу на навколишнє середовище, моніторингу екосистем і біорізноманіття, контролю за рівнем забруднення повітря, води та ґрунтів, а також для планування зон охорони природи та національних парків [31]. Крім того, ГІС використовуються у сфері управління надзвичайними ситуаціями, аналізу ризиків та вразливостей територій щодо природних і техногенних катастроф, планування заходів з цивільного захисту та евакуації, а також координації дій рятувальних служб під час надзвичайних ситуацій [233]. Також значну роль ГІС відіграють у веденні земельного кадастру та управлінні земельними ресурсами, забезпеченні громадської безпеки та правопорядку шляхом моніторингу громадського порядку, профілактики злочинності, планування розташування органів правопорядку та інфраструктури безпеки, а також аналізу даних про злочинність для розробки стратегій профілактики.

Використання ГІС забезпечує численні переваги, серед яких підвищення ефективності управління через точний аналіз геопросторових даних, оптимізація ресурсів завдяки плануванню та координації на основі актуальних даних, покращення процесу прийняття рішень через візуалізацію та моделювання різних сценаріїв, а також підвищення прозорості та доступності інформації для громадськості та зацікавлених сторін.

Застосування ГІС у державному управлінні відкриває нові перспективи для покращення якості життя громадян, забезпечення сталого розвитку та ефективної відповіді на сучасні виклики. Ключові аспекти використання ГІС включають ситуаційну обізнаність та прийняття рішень у реальному часі, планування та моделювання, логістику та управління ресурсами, моніторинг і аналіз, а також координацію з міжнародними партнерами. ГІС дозволяють інтегрувати різноманітні види даних, такі як супутникові знімки, розвіддані, інформацію про місцевість та інфраструктуру, для створення комплексної картини оперативної обстановки, що сприяє оперативному прийняттю рішень

на основі актуальних даних.

Розвиток та інтеграція ГІС у силові структури України супроводжуються рядом 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 за рахунок автоматизації процесів аналізу даних та прийняття рішень [218].

Крім того, ГІС активно використовуються для планування оборонних операцій, моделювання різних сценаріїв конфліктів, оцінки можливих наслідків та ризиків, що дозволяє оптимізувати розміщення військових сил і засобів, планування евакуації цивільного населення та організації гуманітарних операцій. У сфері логістики та управління ресурсами, ГІС допомагають ефективно керувати логістичними процесами, оптимізувати маршрути переміщення військ і матеріально-технічних ресурсів, а також планувати розташування логістичних центрів.

Застосування ГІС у державному управлінні силами безпеки України має значний вплив на стратегічне планування та оперативне реагування, що сприяє зміцненню обороноздатності держави та захисту її національних інтересів. Геоінформаційні системи стають невід’ємною частиною діяльності національної поліції України. Використання ГІС дозволяє значно підвищити ефективність діяльності правоохоронних органів завдяки здатності швидко обробляти великі обсяги інформації, виявляти закономірності та прогнозувати потенційні ризики.

Серед основних аспектів застосування ГІС у діяльності національної поліції України можна виділити: аналіз місцеположень злочинів, виявлення «гарячих точок» для розробки стратегій профілактики злочинності, а також оптимальний розподіл поліцейських ресурсів на підставі отриманих даних. Використання ГІС для аналізу дорожньо-транспортних пригод дозволяє виявляти небезпечні ділянки доріг та планувати ефективні заходи для

підвищення безпеки дорожнього руху. Крім того, ГІС забезпечують швидке реагування на екстрені виклики, дозволяючи визначати найкоротші шляхи до місця події та координувати дії рятувальних служб, що значно знижує час реагування.

Інші важливі сфери використання ГІС включають моніторинг переміщення підозрюваних, нагляд за громадськими місцями та планування заходів безпеки на масових заходах. Серед ключових переваг використання ГІС для національної поліції можна зазначити здатність оперативно обробляти значні обсяги даних і надавати інформацію в режимі реального часу, високу точність геопросторових даних, що сприяє прийняттю більш ефективних рішень, а також графічне представлення даних, яке допомагає краще зрозуміти складні зв’язки та закономірності.

Втім, попри численні переваги, використання ГІС у діяльності силових структур супроводжується певними труднощами, такими як забезпечення конфіденційності даних, необхідність постійного оновлення геоданих, а також підвищення кваліфікації персоналу. Розвиток новітніх технологій, включаючи штучний інтелект та машинне навчання, відкриває нові горизонти для подальшого підвищення ефективності використання ГІС у правоохоронній діяльності. Використання ГІС на службі національної поліції України продовжуватиме розвиватися, відкриваючи нові можливості для забезпечення громадської безпеки та порядку [218].

Геоінформаційні системи також широко використовуються у діяльності Національної гвардії України, де вони відіграють ключову роль у плануванні, координації та виконанні різноманітних операцій [218]. Використання ГІС дозволяє Національній гвардії ефективніше реагувати на загрози, управляти військовими та спеціальними операціями, а також здійснювати постійний моніторинг важливих об'єктів і територій. Зокрема, ГІС сприяють точному плануванню військових операцій, забезпечуючи візуалізацію місцевості, аналіз маршрутів пересування та визначення оптимальних позицій для розміщення підрозділів.

Крім того, Національна гвардія використовує ГІС для ефективного моніторингу важливих інфраструктурних об'єктів, прикордонних зон та інших стратегічно важливих територій. Це включає спостереження за змінами у місцевості, контроль за переміщенням осіб та транспортних засобів, а також виявлення можливих незаконних дій. ГІС дозволяють проводити комплексний аналіз ризиків та загроз на основі великого масиву даних, що охоплюють природні умови, демографічні показники, інфраструктуру та інші важливі чинники. Це дає змогу своєчасно виявляти потенційні загрози та планувати відповідні заходи.

Ефективне розподілення та управління ресурсами є критично важливим для Національної гвардії, особливо під час проведення операцій. ГІС допомагають оптимізувати логістичні процеси, забезпечуючи аналіз маршрутів, розрахунок часу доставки ресурсів та планування їх розподілу. Розвиток технологій ГІС відкриває нові можливості для підвищення оперативності та ефективності діяльності Національної гвардії України. Інтеграція ГІС з іншими технологічними рішеннями, такими як безпілотні роботизовані системи, сенсорні мережі та системи штучного інтелекту, може значно розширити можливості для аналізу даних, моніторингу та управління в реальному часі. Геоінформаційні системи стають важливою складовою стратегії національної безпеки, дозволяючи Національній гвардії України ефективно виконувати свої завдання та швидко адаптуватися до змінних умов і нових викликів.

Геоінформаційні системи є невід'ємною частиною сучасної інфраструктури державної прикордонної служби України (ДПСУ), забезпечуючи ефективне управління державними кордонами, моніторинг безпеки та координацію оперативних дій. Завдяки використанню ГІС прикордонна служба отримує можливість значно підвищити рівень контролю за кордонами, оптимізувати розподіл ресурсів для патрулювання, оперативно реагувати на інциденти, а також забезпечити детальний аналіз територій з метою планування та реалізації різноманітних оперативних завдань [18, 129].

Геоінформаційні системи у державній прикордонній службі

використовуються у багатьох напрямках, серед яких варто відзначити наступні:

ГІС дозволяють створювати візуалізацію та здійснювати глибокий аналіз геопросторових даних, що забезпечує ефективний моніторинг державних кордонів. Це включає відстеження переміщень осіб і транспортних засобів, виявлення незаконних перетинів кордону та виявлення контрабандних операцій;

Використання ГІС сприяє розробці більш ефективних стратегій патрулювання та розміщення прикордонних постів, що забезпечує оптимальне використання ресурсів і людських сил для підвищення безпеки на кордонах;

Аналітичні можливості ГІС дозволяють ідентифікувати зони підвищеного ризику і вразливості вздовж державного кордону, що сприяє своєчасному розподілу ресурсів для попередження потенційних загроз та уникнення кризових ситуацій;

Для прикордонних територій, які можуть включати заповідні зони або особливо чутливі екосистеми, ГІС допомагають моніторити стан довкілля, виявляти екологічні порушення та розробляти ефективні заходи для їх запобігання або усунення;

ГІС можуть бути інтегровані з іншими системами безпеки, такими як системи відеоспостереження, датчики руху та системи збору розвідувальної інформації, що забезпечує комплексний підхід до управління кордонами і значно підвищує загальну ефективність прикордонного контролю.

Серед ключових переваг використання ГІС для державної прикордонної служби варто відзначити підвищення оперативності реагування на інциденти завдяки точному позиціонуванню об'єктів та швидкому аналізу ситуації; ефективне розподілення ресурсів, що дозволяє забезпечити максимальне покриття та надійний контроль державних кордонів; покращення стратегічного планування і управління ризиками на основі детального аналізу геопросторових даних; а також інтеграцію з іншими системами безпеки для створення єдиної оперативної картини.

Застосування ГІС у державній прикордонній службі демонструє, як

передові технології можуть суттєво сприяти зміцненню національної безпеки і забезпеченню ефективного управління державними кордонами. Геоінформаційні системи відіграють критичну роль також у діяльності державних служб з надзвичайних ситуацій, забезпечуючи ефективне управління ризиками, планування заходів реагування на кризові ситуації та координацію дій під час ліквідації наслідків надзвичайних подій.

Використання ГІС дає можливість збирати, аналізувати, візуалізувати та керувати просторовими даними, що є ключовим для розуміння масштабів загроз і оптимізації процесів прийняття рішень. ГІС застосовуються для ідентифікації та аналізу ризиків, пов'язаних як з природними катастрофами (землетруси, повені, лісові пожежі), так і з техногенними аваріями, що дозволяє планувати заходи зниження ризиків і підвищення стійкості інфраструктури. За допомогою ГІС створюються евакуаційні плани та маршрути, які враховують доступність доріг, розташування безпечних зон та можливі перешкоди, що забезпечує швидку і ефективну евакуацію населення з зон ризику.

Крім того, використання ГІС для моніторингу ситуації в реальному часі дозволяє оперативно реагувати на зміни, координувати дії рятувальних служб та надавати необхідну допомогу постраждалим. ГІС надають можливість візуалізувати великі обсяги даних на карті, що спрощує аналіз ситуації та допомагає в прийнятті обґрунтованих рішень щодо розподілу ресурсів і визначення пріоритетів дій. Після ліквідації надзвичайної ситуації ГІС використовуються для оцінки наслідків, планування відновлювальних робіт та розробки стратегій зменшення наслідків майбутніх катастроф [18, 129].

Переваги використання ГІС для державної служби з надзвичайних ситуацій включають підвищення оперативності реагування на надзвичайні ситуації завдяки швидкому аналізу даних і ефективній координації дій; підвищення ефективності у плануванні та виконанні рятувальних операцій; зниження ризиків для населення і зменшення матеріальних втрат завдяки своєчасному виявленню та реагуванню на загрози; покращення управління ресурсами за рахунок точного розподілу та ефективного використання

необхідних засобів і сил.

Використання ГІС службами з надзвичайних ситуацій відкриває нові можливості для забезпечення безпеки населення та ефективного управління ресурсами під час кризових ситуацій, сприяючи швидкому реагуванню та мінімізації наслідків надзвичайних подій. Геоінформаційні системи для сил безпеки стають потужними інструментами підтримки прийняття рішень. Застосування ГІС у діяльності силових структур дозволяє значно підвищити оперативність реагування на непередбачувані ситуації, що виникають у ході службово-бойової діяльності, та підвищити ефективність роботи правоохоронних органів завдяки здатності швидко аналізувати великі обсяги інформації, виявляти закономірності та прогнозувати можливі ризики.

Підвищення ефективності планування спеціальних операцій силовими структурами за допомогою ГІС, з урахуванням поточних загроз, що стоять перед нашою державою, набуває особливої актуальності. Впровадження сучасних інформаційних технологій у діяльність сил безпеки та органів державного управління сприяє посиленню обороноздатності країни та захисту її національних інтересів, що є ключовим аспектом на шляху до забезпечення стабільності і безпеки в умовах сучасних викликів.

4.4 Проблеми формування і суперечності реалізації механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

У сфері державного управління спостерігається значне збільшення обсягів інформаційного обміну, а також зростання динаміки цього процесу. Це супроводжується підвищенням потреби в оперативному і точному реагуванні на різноманітні економічні, соціально-політичні ситуації як в межах країни, так і за її кордонами. Відзначається стійка тенденція до ускладнення існуючих і появи нових організаційних систем, призначених для інформаційно-аналітичного забезпечення діяльності органів державної влади. Ця ситуація

обумовлена швидким розвитком складних технологій виробництва, конструкцій, зростанням обсягів інформаційних потоків, а також створенням автоматизованих систем управління глобального характеру, які є невід'ємною частиною сучасного державного управління. Для того щоб забезпечити належну інформаційно-аналітичну підтримку реалізації державної політики в сфері соціально-економічного та суспільно-політичного розвитку країни, а також для зміцнення національної безпеки, розробляються і впроваджуються нові системи управління.

Військові експерти, що спеціалізуються на інформаційно-аналітичному забезпеченні (ІАЗ) сил безпеки та оборони України [20, 26, 40, 42, 117, 124, 125, 127, 178, 232, 233, 243], серед ключових проблем, що стоять перед цією галуззю на сьогоднішній день, виділяють наступні:

- недостатній рівень розвитку нормативно-правової бази, яка регулює створення інформаційних ресурсів і продуктів, надання інформаційних послуг та функціонування систем інформаційно-аналітичного забезпечення органів управління в цілому;

- відсутність інтегрованої системи інформаційно-аналітичних органів, які б були пов'язані між собою функціонально, технологічно та технічно;

- відсутність єдиної, загальноприйнятої системи класифікації та кодування інформації;

- недостатній рівень розвитку загальних інформаційних ресурсів у силах безпеки України, а також відсутність інтегрованого банку даних, який повинен стати ключовим елементом загальнодержавної інформаційної інфраструктури;

- необхідність впровадження системного сертифікованого програмно-математичного забезпечення, яке вже зарекомендувало себе у практичній діяльності;

- відсутність сертифікованих засобів захисту інформації;

- відсутність чітко визначеного комплексу спеціального програмно-математичного забезпечення для інформаційної діяльності;

- необхідність підготовки висококваліфікованих фахівців для роботи в

сучасних інформаційно-аналітичних системах;

- недостатність фінансування, що ускладнює реалізацію важливих проектів у цій сфері;

- відсутність комплексного підходу до організації досліджень, спрямованих на вирішення проблем створення системи інформаційного забезпечення сил безпеки України.

Проблематика інформаційно-аналітичного забезпечення та створення інформаційно-аналітичних систем (ІАС) розглядається не тільки в Україні, але і за її межами. Цими питаннями займаються як вітчизняні, так і зарубіжні науковці. Серед українських дослідників, що зробили вагомий внесок у розвиток цієї галузі, варто відзначити праці таких науковців, як Мацько О.Й., Микуся С.А., Солоннікова В.Г., Єрмошина М.О., Смірнова Є.Б., Дробахи Г.А., Кириченка І.О., Яковлева М.Ю. Зокрема, значний внесок у розвиток цієї тематики зробили й іноземні дослідники, такі як Cukier K., Mayer-Schönberger V., Gruber T.R., Chandrasekaran B., Josephson John R., Nicolescu B., Klein J. Th., Ayhan A., Aslı A., Guajardo N.R., Dekker A.H., Guarino N.

Аналіз сучасного стану науково-методичних підходів до інформаційно-аналітичного забезпечення сил безпеки під час виконання службово-бойових завдань свідчить про наявність системних недоліків, які значно знижують ефективність цих процесів. Нинішній науково-методичний апарат забезпечує розв’язання лише окремих завдань ІАЗ, залишаючи поза увагою важливі аспекти, що потребують вдосконалення та модернізації [219, 220].

Інформаційно-аналітична система сил безпеки України відіграє ключову роль у забезпеченні національної безпеки та оборони держави. Ефективність цієї системи значною мірою залежить від дієвих механізмів державного управління, які є критично важливими для забезпечення безперебійного та ефективного потоку інформації і розвідданих, необхідних для підтримки процесів прийняття рішень на всіх рівнях. Однак розробка та реалізація таких механізмів супроводжується низкою проблем і протиріч, що вимагають ретельного аналізу та прийняття стратегічних рішень.

Серед основних проблемних питань, які впливають на ефективність механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України, можна виділити наступні:

- відсутність єдиної, цілісної стратегії розвитку ІАЗ, обмежені технологічні ресурси та недостатнє фінансування, що перешкоджає розвитку та оновленню інформаційно-технологічної бази, а також затримує впровадження сучасних стандартів;

- складнощі з обробкою великих обсягів даних, що зумовлені неефективністю наявних методів та інструментів для аналізу цих даних, що ускладнює своєчасне виявлення загроз і ризиків;

- висока залежність від кваліфікації та досвіду фахівців, що створює ризики, пов’язані з людським фактором, які можуть суттєво вплинути на якість інформаційно-аналітичного забезпечення.

Суперечності у реалізації механізмів державного управління виявляються у таких аспектах:

- існує суттєвий розрив між теоретично розробленими науковими підходами та їх практичним впровадженням у діяльність сил безпеки, що призводить до неефективного використання ресурсів та втрати потенційних переваг;

- різні органи безпеки можуть мати різні цілі та завдання, що ускладнює розробку та впровадження єдиної політики в управлінні інформаційними та аналітичними процесами;

- відсутність єдиної інтегрованої системи обробки та аналізу даних призводить до фрагментації інформації, що ускладнює комплексний аналіз та своєчасне реагування на загрози;

- проблеми з оновленням та модернізацією технологічної бази, викликані швидким розвитком технологій, що вимагає постійного оновлення обладнання та програмного забезпечення, часто уповільнюються через бюрократичні процеси та обмеженість бюджету;

- необхідність забезпечення високого рівня інформаційної безпеки, яка

часто обмежується через дефіцит фінансування та обмежені технологічні можливості;

- наявність різних баз даних та систем ускладнює інтеграцію інформації та її єдине використання;

- розбіжності між довгостроковими стратегічними цілями держави в галузі безпеки та поточними оперативними завданнями і потребами, що ускладнює їх гармонізацію та реалізацію.

Ці суперечності значною мірою впливають на ефективність роботи системи інформаційно-аналітичного забезпечення, знижуючи її здатність оперативно та адекватно реагувати на сучасні виклики у сфері безпеки. Вони ускладнюють інтеграцію нових інформаційних потоків, обмежують швидкість обміну даними між різними підрозділами та знижують загальну готовність сил безпеки до адекватної відповіді на потенційні загрози.

Підтвердженням наведеним проблемним аспектам та суперечностям механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України є такі факти [219, 220]:

У 2023 році стався інцидент, коли важлива розвідувальна інформація, що надходила від фронтових підрозділів, затрималася у своєчасній доставці до центрального командування. Причиною цієї проблеми виявилась відсутність сучасних засобів зв’язку, недостатність аналітичних інструментів, а також неефективна структура передачі даних, де кожен рівень додавав додаткову затримку. Це призвело до втрати можливості швидкого реагування на безпекові загрози, що поставило під сумнів ефективність інформаційно-аналітичного забезпечення.

У 2024 році, під час координації між розвідувальним управлінням і військовою поліцією, сталося серйозне непорозуміння через різне трактування даних. Проблема полягала у відсутності чітких протоколів для інтерпретації та обміну інформацією, а також у різних підходах до аналізу даних у різних підрозділах. Це непорозуміння призвело до некоординованих дій, що погіршило ситуацію на місцях і підкреслило необхідність удосконалення

існуючих механізмів інформаційно-аналітичного забезпечення.

Для ефективного вирішення виявлених проблем та суперечностей можуть бути запропоновані наступні заходи [219]:

- розробка та удосконалення законодавчої і нормативної бази для чіткого розмежування повноважень між різними структурами безпеки. Це включає адаптацію нормативно-правової бази до сучасних викликів у сфері інформаційної безпеки та нових технологій. Необхідно встановити чіткі процедури використання даних, що враховують питання конфіденційності та захисту персональних даних;

- створення ефективних механізмів міжвідомчої координації та забезпечення надійного обміну інформацією між різними структурами;

- інтеграція та модернізація технологічної інфраструктури з метою підвищення ефективності обробки та аналізу даних. Це вимагає значних інвестицій в оновлення та розвиток єдиної інтегрованої технологічної платформи;

- розробка та впровадження єдиної інформаційно-аналітичної платформи, яка забезпечить збір, обробку, аналіз та розподіл інформації між усіма зацікавленими структурами безпеки;

- уніфікація форматів даних і забезпечення сумісності різноманітних джерел інформації через стандартизацію форматів даних та протоколів обміну;

- організація регулярних навчальних програм і тренінгів для підвищення кваліфікації аналітиків, інженерів та керівників у галузі обробки та аналізу даних, що є критично важливим для підвищення загальної ефективності;

- формування крос-функціональних команд для обміну досвідом і найкращими практиками у сфері інформаційної безпеки, що дозволить підвищити загальний рівень професійної підготовки;

- залучення інвестицій для впровадження передових технологій обробки великих даних, використання штучного інтелекту та машинного навчання, що дозволить значно підвищити ефективність аналізу даних;

- стимулювання розвитку вітчизняних інноваційних рішень у сфері

інформаційної безпеки та аналітики, що сприятиме створенню власних конкурентоздатних продуктів і рішень.

Цей аналіз демонструє комплексний характер проблематики та підкреслює необхідність інтегрованого підходу для її вирішення. Продовження досліджень у цій галузі дозволить глибше зрозуміти шляхи усунення виявлених суперечностей і підвищення ефективності системи інформаційно-аналітичного забезпечення сил безпеки України.

Імплементація запропонованих механізмів сприятиме не лише оптимізації та вдосконаленню існуючої системи інформаційно-аналітичного забезпечення сил безпеки України, а й значно підвищить загальну ефективність державного управління в цій сфері. Для ефективного впровадження запропонованих заходів необхідний комплексний підхід, що включає забезпечення міжвідомчої координації та постійний моніторинг реалізації прийнятих рішень.

Актуальним питанням залишається необхідність детального аналізу та розвитку напрямків інформаційного забезпечення процесів управління силами безпеки в умовах виконання службово-бойових завдань. У сучасних умовах варто звернути увагу на наступні ключові напрями розвитку інформаційного забезпечення управлінських процесів у силах безпеки України:

– Розробка й удосконалення інформаційно-правової бази, що регулює діяльність, підтримання бойової готовності та застосування сил безпеки у службово-бойових умовах. Це включає приведення нормативних документів, таких як засади, бойові статути, керівництва, настанови, посібники, у відповідність до нових умов і викликів;

– Модернізація форм бойових, плануючих, директивних, інформаційно-довідкових та інших документів з метою підвищення їхньої ефективності та зручності використання;

– Уточнення складу, джерел, форм і порядку передачі інформації, необхідної для управління військовими силами (силами безпеки) під час підготовки та виконання службово-бойових завдань;

– Оптимізація структур і схем взаємодії органів управління під час

підготовки і проведення службово-бойових операцій, забезпечення їх синергізму та адаптації до змін оперативної обстановки та стану сил;

– Систематизація та створення фонду офіційно прийнятих у силах безпеки моделей і задач, розробка програмних комплексів автоматизованих робочих місць (АРМ) для посадових осіб з метою створення єдиної інформаційно-аналітичної системи. Ця система забезпечуватиме розподілену обробку інформації під час підготовки рішень і створення документів для їх впровадження;

– Розвиток моделей і задач, пов'язаних із всебічним забезпеченням діяльності військових підрозділів, що дозволить краще планувати та управляти ресурсами;

– Розробка систем моніторингу, які дозволять контролювати стан військ, озброєння і техніки, а також потенційно небезпечних об’єктів та об'єктів, що знаходяться під охороною;

– Модернізація програмного забезпечення і баз даних у комплексі засобів автоматизації з метою створення сучасної автоматизованої системи управління у силах безпеки України, яка буде використовуватися на всіх етапах: чергування, планування і під час виконання службово-бойових завдань;

– Інтеграція процесів інформаційного забезпечення на етапі планування (збір і підготовка інформації) та на етапі ведення дій (використання зібраної інформації для ухвалення рішень);

– Розробка сучасних багатоцільових автоматизованих пунктів управління, застосування агрегативно-модульного підходу до їх побудови, що забезпечить більшу гнучкість та адаптивність у бойових умовах;

– Вдосконалення концепції єдиного інформаційного простору для силових структур України та інформаційного забезпечення процесів управління ними;

– Підготовка висококваліфікованих фахівців, здатних на сучасному рівні ефективно вирішувати всі зазначені завдання у військових структурах.

Безсумнівно, наведені положення можуть бути додатково розширені й

деталізовані. Однак, на основі проведеного аналізу можна стверджувати, що завжди існує резерв для підвищення ефективності дій військових сил, який можна реалізувати шляхом удосконалення параметрів інформаційного забезпечення процесів управління. Таким чином, навіть без значних додаткових матеріальних витрат на озброєння та військову техніку, за винятком витрат на програмно-технічні комплекси, можна суттєво підвищити ефективність дій сил безпеки.

Структури сил безпеки і оборони, як і інші державні органи, постійно еволюціонують, адаптуються до нових умов і стають дедалі складнішими. Це супроводжується появою нових видів озброєнь, створенням нових військових формувань, виділенням нових завдань, а також зміною підходів і стратегій ведення службово-бойових дій. В контексті виконання бойових операцій, ключовими факторами є швидкість збору, обробки, перетворення, передачі та використання інформації, а також методи її збереження, що є критично важливими для успішного виконання завдань [233].

Процес управління є одним із найскладніших аспектів людської діяльності, що потребує глибокого аналізу та постійного вдосконалення. Ураховуючи подвійний характер управління, який включає як об'єктивні (раціональні), так і суб'єктивні (ірраціональні) складові, цей процес стає ще більш складним через наявність різноманітних проблем. Зі збільшенням складності систем, що підлягають управлінню, зростає і кількість проблем, які потребують вирішення, що, у свою чергу, підвищує вимоги до якості управлінських рішень і ефективності процесів управління[125, 233]. Зазначена Зазначена проблема ускладнюється існуванням ряду суперечностей у самому процесі управління. До них відносяться: зростаюча складність керованих систем та обмежена кількість управлінських кадрів, що ускладнює їх ефективне функціонування; потреба в оперативності процесу управління, яка іноді суперечить необхідності глибокого аналізу для прийняття якісних рішень; конфлікт між спеціалізацією та інтеграцією завдань, що виникають у процесі управління; складність формалізації задач управління при необхідності

використання точних методів оцінки; дисбаланс між складністю управлінських задач і рівнем підготовки управлінських кадрів, а також інші проблеми.

Зазначені фактори в комплексі утворюють суперечність що поглиблюється між існуючим станом процесу реалізації органами управління своїх функцій і необхідним рівнем ефективності реалізації управління. Це протиріччя у чому має прагматичний характер і зумовлює наявність зв'язку між теоретичними і практичними аспектами вирішення проблем управління. Наявність зазначеного протиріччя сприяє формуванню перманентної кризи управління. Особливо криза помітна в системах державного і військового управління, в яких помилки найбільш помітні і мають найбільшу «ціну». У даному зв’язку важливим є виявлення специфіки прояву факторів, що породжують кризу управління в структурі досліджуваної предметної області. Характеру впливу комплексу протиріч управління складає основу для цілеспрямованого розвитку методології вдосконалення системи управління.

Ця система охоплює різні органи державного управління, такі як Міністерство оборони, Служба безпеки України, Міністерство внутрішніх справ та інші спеціалізовані структури. Кожен із цих органів має свої підрозділи інформаційно-аналітичного забезпечення, які взаємодіють для формування єдиної стратегії безпеки. Інформаційно-аналітичне забезпечення базується на використанні сучасних технологій збору, обробки та аналізу даних. Використовуються різні типи інформаційних систем, включаючи геоінформаційні системи, розвідувальні системи та системи електронної розвідки, що дозволяє ефективно обробляти великі обсяги інформації та виявляти потенційні загрози [2, 14, 15]. Сучасні виклики, такі як кіберзагрози, гібридні війни та міжнародний тероризм, вимагають постійного розвитку та адаптації системи інформаційно-аналітичного забезпечення. Акцент робиться на розробці нових методів аналізу, інтеграції штучного інтелекту та машинного навчання для підвищення ефективності аналітичних процесів.

У сучасних умовах, коли на передній план виходять кіберзагрози, гібридні війни та міжнародний тероризм, система інформаційно-аналітичного

забезпечення вимагає постійного розвитку та адаптації. Особливу увагу приділяється розробці нових методів аналізу, інтеграції штучного інтелекту та технологій машинного навчання для підвищення ефективності аналітичних процесів.

Інформаційно-аналітичне забезпечення відіграє вирішальну роль у забезпеченні національної безпеки України. Його значення можна проаналізувати через декілька ключових аспектів:

- Підтримка прийняття рішень: Надання актуальної, точної та вичерпної інформації дозволяє керівництву сил безпеки приймати обґрунтовані рішення в критичний момент, що допомагає вирішувати складні завдання національної безпеки з вищою ефективністю та впевненістю.

Прогнозування та аналітика: Систематичний аналіз зібраних даних сприяє виявленню трендів і прогнозуванню потенційних загроз, що дає змогу розробляти проактивні стратегії для запобігання негативним сценаріям.

Оперативне реагування: Швидкий доступ до інформації та її оперативний аналіз дозволяють ефективно реагувати на надзвичайні ситуації та кризи. Така оперативність є критичною для забезпечення національної безпеки і стабільності в країні.

Координація між відомствами: Ефективна інформаційно-аналітична система сприяє покращенню координації між різними структурами сил безпеки, забезпечуючи створення єдиного оперативного простору для реагування на загрози.

Зміцнення міжнародних позицій: Інформаційно-аналітичне забезпечення сприяє формуванню обґрунтованої зовнішньої політики та зміцненню міжнародних позицій країни, особливо у сферах безпеки та оборони, що є важливим аспектом для України в умовах сучасних глобальних викликів.

Таким чином, інформаційно-аналітичне забезпечення виступає фундаментальною основою для ефективного державного управління в сфері національної безпеки, надаючи Україні можливість адекватно реагувати на внутрішні та зовнішні виклики. Система державного управління інформаційно-

аналітичним забезпеченням сил безпеки України складається з кількох ключових компонентів, кожен з яких відіграє важливу роль у забезпеченні її ефективності та функціональності:

Організаційна структура: Включає різноманітні установи та агентства, які займаються збором, обробкою, аналізом і розповсюдженням інформації. Ці структури можуть охоплювати розвідувальні служби, військові організації, правоохоронні органи та спеціалізовані науково-дослідні центри. Взаємодія між ними забезпечує цілісність інформаційно-аналітичного процесу;

Інформаційні ресурси: Цей компонент охоплює бази даних, аналітичні звіти, статистичні дані, геопросторову інформацію та інші типи даних, що необхідні для детального аналізу ситуації та підтримки прийняття рішень. Ці ресурси є критичними для забезпечення актуальності та повноти інформації;

Технологічне забезпечення: Включає сучасні системи збору даних, обчислювальні мережі, програмне забезпечення для аналізу даних, засоби комунікації, а також системи кібербезпеки. Впровадження новітніх технологій дозволяє підвищити ефективність і швидкість обробки великих обсягів інформації;

Процедурне забезпечення: Охоплює стандарти, протоколи і процедури, які регулюють процеси збору, обробки, аналізу, зберігання та розповсюдження інформації. Дотримання цих процедур забезпечує точність, конфіденційність та безпеку інформації, що є важливим для національної безпеки;

Кадрове забезпечення: Складається з фахівців та аналітиків, які працюють у системі, включаючи розвідників, аналітиків, програмістів, інженерів та інших спеціалістів. Високий рівень кваліфікації цих фахівців є запорукою ефективного функціонування всієї системи;

Механізми координації та контролю: Забезпечують ефективну взаємодію між різними компонентами системи, допомагають контролювати виконання завдань і оцінювати загальну ефективність системи в цілому. Вони також сприяють узгодженості дій між різними органами державної влади.

Інформаційно-аналітичне забезпечення відіграє критичну роль у процесах

прийняття рішень у сфері державного управління, особливо в контексті національної безпеки України [230, 233]. Отже, інформаційно-аналітичне забезпечення є життєво важливим інструментом у руках державного управління, що дозволяє здійснювати виважені, своєчасні та ефективні рішення в інтересах національної безпеки та стабільності країни. Розвиток механізмів у державному управлінні, особливо в контексті інформаційно-аналітичного забезпечення сил безпеки України, є ключовим для підвищення ефективності відповіді на сучасні виклики та загрози. Ось деякі основні напрямки розвитку цих механізмів:

Впровадження новітніх технологій: Інтеграція таких технологій, як штучний інтелект, машинне навчання, обробка великих даних та кібербезпека, дозволить покращити процеси збору, обробки та аналізу інформації;

Створення єдиної інформаційної системи: Інтеграція даних з різних джерел, включаючи міжнародні, дозволить забезпечити комплексний аналіз і підвищити оперативність прийняття рішень;

Навчання та підвищення кваліфікації фахівців: Підготовка та перепідготовка фахівців, залучених до інформаційно-аналітичного забезпечення, з метою забезпечення високого рівня компетентності у використанні сучасних технологій і методик аналізу;

Розробка та вдосконалення механізмів координації: Покращення координації між різними органами державної влади, зокрема в обміні інформацією та спільному використанні ресурсів, сприятиме підвищенню ефективності управлінських процесів;

Оновлення законодавчої бази: Адаптація законодавства до сучасних стандартів інформаційної безпеки, приватності та захисту даних, а також забезпечення правової підтримки нових підходів і технологій у державному управлінні;

Удосконалення методів аналізу даних: Розробка спеціалізованих аналітичних інструментів та моделей для оцінки ризиків і прогнозування розвитку ситуацій.

Розвиток цих механізмів сприятиме підвищенню ефективності державного управління в Україні, особливо у сфері забезпечення національної безпеки, дозволяючи більш прогнозовано, оперативно та ефективно реагувати на сучасні виклики.

Висновки до розділу 4

1. Україна досягла значного прогресу в галузі управління інформаційно-аналітичним забезпеченням (ІАЗ), особливо завдяки впровадженню цифрових ініціатив, які спрямовані на вдосконалення державного управління та підвищення якості надання послуг громадянам. Ці приклади підкреслюють важливість інтеграції сучасних технологій у сферу ІАЗ для досягнення більшої ефективності, прозорості та доступності державних послуг. Оновлений організаційний механізм державного управління системою ІАЗ сил безпеки України включає створення ефективної інформаційної координації між підрозділами та суб'єктами сил безпеки, адаптацію управлінських механізмів до потреб економіки, а також забезпечення високого рівня захисту даних і приватності.

2. Сучасні загрози вимагають постійного оновлення й удосконалення існуючої нормативної бази. Багато чинних нормативно-правових актів були створені ще до масового впровадження цифрових технологій, що робить їх недостатньо адаптованими до актуальних викликів інформаційної безпеки. Це особливо стосується захисту інформаційної інфраструктури, кібербезпеки та регулювання обігу інформації в цифровому середовищі. У деяких випадках чинне законодавство містить прогалини або нечіткі положення, що ускладнює його ефективне застосування на практиці. Удосконалення правового механізму функціонування системи ІАЗ сил безпеки України має базуватися на розробці загальнодержавних підходів до перспектив розвитку ІАЗ, а також на систематизації нормативно-правових актів, що регулюють цю сферу.

3. Процеси інформатизації сил безпеки істотно відрізняються від

ринкових і потребують більш жорсткого управління. У зв'язку з цим необхідно розробити відповідну нормативно-правову базу, а інформатизацію слід розглядати як організований процес створення оптимальних умов для задоволення інформаційних потреб особового складу та керівних кадрів органів управління силами безпеки, з використанням сучасних інформаційних ресурсів у новітньому технологічному середовищі.

4. Аналіз застосування геоінформаційних систем (ГІС) у державному управлінні дозволив виявити основні сфери їх використання: моніторинг забудови та використання земель; екологічний моніторинг і управління; контроль за забрудненням повітря, води та ґрунтів; управління надзвичайними ситуаціями; аналіз ризиків і вразливостей територій щодо природних і техногенних катастроф; планування заходів цивільного захисту та евакуації; координація дій рятувальних служб під час надзвичайних ситуацій; транспортне планування; аналіз трафіку, планування транспортних мереж і маршрутів; земельний кадастр та управління земельними ресурсами; забезпечення громадської безпеки та правопорядку; моніторинг громадського порядку та превенція злочинності; планування розміщення органів правопорядку та інфраструктури безпеки; аналіз даних про злочинність для розробки профілактичних стратегій. У цьому контексті були розвинуті підходи до застосування ГІС у державному управлінні силами безпеки України, що включають розвиток стратегічного планування та оперативного реагування, що сприяє підвищенню обороноздатності країни та захисту національних інтересів. Також було досліджено вплив ГІС на ефективність управління в секторі безпеки та оборони України, з урахуванням особливостей завдань, що вирішуються суб’єктами сил безпеки.

5. До проблемних питань механізмів державного управління системою ІАЗ сил безпеки України належать:

- відсутність єдиної стратегії розвитку, обмежені технологічні ресурси, недостатнє фінансування на розвиток і модернізацію інформаційно-технологічної бази, а також відставання від сучасних стандартів;

- труднощі з обробкою великих обсягів даних. Недоліки існуючих методів та інструментів для аналізу великих даних, що ускладнює виявлення загроз;

- висока залежність від кваліфікації та досвіду фахівців, що призводить до ризиків, пов’язаних із людським фактором.

Суперечності в реалізації механізмів державного управління можна виявити у наступних аспектах:

- існує значний розрив між науково обґрунтованими підходами та їх практичним впровадженням у діяльність сил безпеки;
- різні органи безпеки можуть мати відмінні цілі та завдання, що ускладнює формування єдиної політики управління інформацією та аналітикою;
- відсутність єдиної інтегрованої системи обробки та аналізу даних;
- проблеми з оновленням і модернізацією технологічної бази;
- необхідність забезпечення високого рівня інформаційної безпеки при обмежених бюджетних та технологічних можливостях;
- існування різноманітних баз даних і систем, що ускладнює їх інтеграцію та спільне використання інформації;

Розбіжності між довгостроковими стратегічними цілями держави в галузі безпеки та поточними оперативними завданнями й потребами.

Ці суперечності безпосередньо впливають на ефективність системи ІАЗ, знижуючи її здатність адекватно реагувати на сучасні виклики в сфері безпеки. Вони ускладнюють інтеграцію нових інформаційних потоків, обмежують оперативність обміну даними між різними підрозділами та знижують загальну готовність сил безпеки до викликів.

РОЗДІЛ 5
КОНЦЕПТУАЛЬНІ НАПРЯМИ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ УКРАЇНИ

5.1 Перспективні шляхи планування інформаційно-аналітичної діяльності в силах безпеки України

Серед ключових викликів, з якими стикається інформаційно-аналітична діяльність у силах безпеки України, можна виділити такі аспекти:

- обмежені технологічні ресурси: Незважаючи на значний прогрес у сфері цифровізації, залишається низка прогалин у технологічній інфраструктурі, що обмежує можливості для глибокого аналізу великих даних [185, 184, 260];

- зростання кіберзагроз: Сили безпеки України стикаються з необхідністю підвищення рівня кібербезпеки та захисту інформації. Згідно з прогнозами Cybersecurity Ventures, очікується, що глобальні збитки від кіберзлочинів зростатимуть на 15% щорічно з 2021 по 2025 рік, і можуть досягти 10,5 трильйонів доларів щороку. Такий ріст пояснюється активізацією кіберзлочинних груп, багато з яких отримують підтримку від держав. Збільшення кількості атак також обумовлено процесами цифрової трансформації [185, 184];

- брак висококваліфікованих фахівців: Для ефективної роботи з сучасними інформаційно-аналітичними системами потрібні професіонали високого рівня. У світлі зростаючого попиту на фахівців з кібербезпеки зберігається дефіцит кваліфікованих кадрів. Згідно з дослідженням (ISC) 2 Cybersecurity Workforce Study, глобальний дефіцит кадрів у цій сфері становить 3,4 мільйона, причому 70% організацій мають незаповнені вакансії. Держави та великі корпорації, такі як Google, Microsoft та IBM, активно працюють над

зменшенням цього дефіциту, запроваджуючи різноманітні програми навчання та підвищення кваліфікації у сфері кібербезпеки [185, 184];

- недостатня ефективність державного управління: Існують певні проблеми в управлінні інформаційно-аналітичною діяльністю сил безпеки України, що обмежує їх ефективність [9, 260].

Незважаючи на виклики, Україна демонструє успіхи в певних аспектах інформаційно-аналітичної діяльності. По-перше це міжнародне співробітництво – активне використання міжнародних партнерств для обміну інформацією та кращих практик забезпечує Україні доступ до новітніх методів аналізу та розвідувальних даних. По-друге це розвиток спеціалізованих програм навчання –впровадження програм навчання та підвищення кваліфікації для аналітиків сприяє підвищенню рівня експертизи в області інформаційно-аналітичної діяльності (ІАД).

Незважаючи на ці виклики, Україна демонструє певні успіхи в окремих аспектах інформаційно-аналітичної діяльності. Зокрема, активне використання міжнародного співробітництва сприяє обміну інформацією та впровадженню передових практик, що дозволяє Україні отримувати доступ до новітніх методів аналізу та розвідувальних даних. Важливим аспектом є також розвиток спеціалізованих програм навчання, що підвищує рівень експертності аналітиків у сфері ІАД.

Значний внесок у дослідження проблем інформаційно-аналітичної діяльності сил безпеки та оборони України зробили такі науковці, як Мацько О. Й., Микусь С. А., Солонніков В. Г., Дробаха Г.А., Єрмошин М.О., Смірнов Є.Б., Шипілова Л.М., Примуш Р.Б. та інші.

Україна стикається з унікальним набором безпекових викликів, серед яких зовнішня агресія, гібридні загрози, а також внутрішні проблеми, такі як корупція та політична нестабільність. Геополітичне розташування України та її стратегічне значення для Європи, разом зі збройною агресією з боку рф, створюють складну безпекову ситуацію, в якій ефективне інформаційно-аналітичне забезпечення має вирішальне значення. ІАД дозволяє силам безпеки

України виявляти, аналізувати та прогнозувати потенційні загрози на основі збору й аналізу даних із різних джерел, включаючи відкриті джерела, технічну розвідку та інші спеціалізовані методи. Ефективна ІАД не тільки підвищує оперативну готовність і стратегічне реагування на загрози, але й сприяє розробці довгострокових стратегій для забезпечення національної безпеки.

ІАД розглядається як метод підвищення ефективності дій сил безпеки через планування, прогнозування та створення сценаріїв дій. Ефективне стратегічне планування є основою для національної безпеки, а ІАД забезпечує необхідну інформаційну базу для цього процесу. Аналіз даних допомагає формувати реалістичне розуміння поточної безпекової ситуації, оцінювати можливі ризики та визначати стратегічні пріоритети.

ІАД забезпечує керівництво сил безпеки та оборони даними, необхідними для ухвалення обґрунтованих рішень. Використання детального аналізу дозволяє уникнути поспішних чи емоційних рішень, спираючись на фактичні дані та об'єктивні оцінки. Систематичний аналіз загроз, можливостей та вразливостей дозволяє посилити обороноздатність держави, оптимізувати розподіл ресурсів і підвищити ефективність оборонних стратегій. ІАД сприяє адаптації до динамічних умов та викликів, що постають перед національною безпекою [146, 252, 233].

Стратегічне планування в контексті сил безпеки охоплює розробку довгострокових планів і стратегій для досягнення цілей у сфері національної безпеки. Це включає аналіз поточної безпекової обстановки, визначення потенційних загроз, розробку стратегій реагування та планів дій для запобігання або нейтралізації цих загроз. Основою стратегічного планування є комплексний аналіз інформації, отриманої з різних джерел, і її інтеграція у злагоджені стратегічні рішення [146, 252].

Для більш детального аналізу механізмів державного управління системою планування інформаційно-аналітичної діяльності сил безпеки України необхідно звернути увагу на нормативно-правову базу, яка регулює цю сферу.

Основні нормативно-правові акти:

- Закон «Про національну безпеку» [66] - визначає ключові принципи державної політики у сфері національної безпеки, а також правові та організаційні основи створення і функціонування сил безпеки. Відповідно до статті 25 цього закону, метою планування в сферах національної безпеки та оборони є забезпечення ефективної реалізації державної політики шляхом розробки стратегій, концепцій, програм і планів розвитку органів сектору безпеки та оборони, управління ресурсами та їх оптимального розподілу [66]. Планування в цих сферах поділяється на довгострокове (понад п’ять років), середньострокове (до п’яти років) та короткострокове (до трьох років). Довгострокове планування включає такі документи, як Стратегія національної безпеки України, Стратегія воєнної безпеки, Стратегія громадської безпеки та цивільного захисту, Стратегія розвитку оборонно-промислового комплексу, Стратегія кібербезпеки та Національна розвідувальна програма. Середньострокове планування охоплює інші стратегічні документи і програми розвитку складових сектору безпеки та оборони, включаючи оснащення їх сучасним озброєнням та військовою технікою, створення необхідних запасів і потужностей оборонно-промислового комплексу. Короткострокове планування передбачає щорічне розроблення планів утримання та розвитку складових сектору безпеки й оборони, включаючи основні показники закупівель товарів, робіт і послуг оборонного призначення на трирічний період [66].

- Закон «Про оборону України» - регулює питання оборонної діяльності та військової служби, включаючи аспекти інформаційно-аналітичної діяльності (ІАД). Один із ключових аспектів – здійснення заходів з кібероборони, що спрямовані на захист державного суверенітету та підвищення обороноздатності, а також запобігання збройному конфлікту і відсіч збройній агресії [67].

- Закон «Про розвідку» - встановлює правові основи діяльності розвідувальних органів, що входять до складу сил безпеки, включаючи положення щодо збору та аналізу інформації [69].

- Закон «Про боротьбу з тероризмом» - окреслює правові та організаційні засади протидії тероризму, в тому числі через ІАД [62].

- Закон «Про основні засади забезпечення кібербезпеки України» - визначає основи захисту національного інформаційного простору, важливу роль у якому відіграє ІАД [68]. Одним з аспектів функціонування національної системи кібербезпеки є стратегічне планування та програмно-цільове забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту [68].

У світлі сучасних викликів, пов'язаних з гібридними загрозами, які поєднують військові та невійськові методи ведення війни, сили безпеки повинні особливо ретельно підходити до планування та аналізу. Інформаційний аналіз дозволяє виявляти, оцінювати та прогнозувати такі загрози, об'єднуючи дані з відкритих джерел, розвідданих та інших спеціалізованих джерел інформації. Ефективне використання інформаційного аналізу сприяє розробці стратегічних планів, що враховують широкий спектр потенційних загроз та забезпечують гнучкість і оперативність у реагуванні на динамічну безпекову ситуацію.

Сили безпеки України активно використовують інформаційно-аналітичну діяльність для ідентифікації та аналізу як внутрішніх, так і зовнішніх загроз національній безпеці. Ця діяльність охоплює збір інформації з різноманітних джерел, включаючи відкриті дані, соціальні мережі, розвідувальні дані, а також інформацію, отриману від міжнародних партнерів.

Розглянемо існуючі підходи до планування ІАД сил безпеки [252].

Стратегічне планування. Встановлення довгострокових цілей і визначення напрямків розвитку інформаційно-аналітичної діяльності.

Оперативне планування. Розробка короткострокових планів дій для досягнення стратегічних цілей.

Сценарне планування. Створення різних сценаріїв майбутнього для кращої підготовки до можливих змін у середовищі.

Ризик-орієнтоване планування. Оцінка потенційних ризиків і розробка стратегій для їх мінімізації.

Застосування цих підходів дозволяє ефективно керувати ресурсами, адаптуватися до змін у середовищі, а також забезпечити високий рівень готовності сил безпеки до різних викликів.

Стратегічне планування є ключовим процесом для визначення довгострокових цілей та напрямків розвитку інформаційно-аналітичної системи, особливо в умовах динамічних змін та нових викликів. Ефективне стратегічне планування забезпечує узгодженість дій, оптимальне використання ресурсів та підвищення стійкості системи..

Інформаційно-аналітичні системи є невід'ємною частиною суб'єктів сил безпеки, частин та підрозділів, забезпечуючи своєчасний аналіз та обробку інформації для прийняття раціональних управлінських рішень. У сфері забезпечення державної безпеки такі системи відіграють ключову роль у попередженні та реагуванні на загрози. Стратегічне планування дозволяє визначити пріоритети розвитку інформаційно-аналітичних систем та забезпечити їх ефективне впровадження.

Розглянемо етапи стратегічного планування для інформаційно-аналітичного забезпечення сил безпеки.

Місія інформаційно-аналітичного забезпечення має чітко відображати головну мету та роль цієї діяльності в межах сил безпеки. Візія, або бачення, є ідеальним уявленням про майбутній стан системи, до якого варто прагнути. Формування місії та бачення дозволяє встановлювати стратегічні цілі та забезпечує узгодженість дій на всіх рівнях організації сил безпеки.

Наступним етапом є аналіз зовнішнього середовища, який включає оцінку політичних, економічних, соціальних, технологічних, екологічних та правових факторів, що можуть вплинути на інформаційно-аналітичне забезпечення. Внутрішній аналіз охоплює оцінку ресурсів, компетенцій, процесів і технологій, що використовуються в системі, а також виявлення сильних і слабких сторін.

SWOT-аналіз є ефективним інструментом для виявлення сильних та слабких сторін інформаційно-аналітичної системи, а також можливостей і

загроз, що перед нею постають. Це дозволяє розробити стратегії, які будуть спрямовані на використання сильних сторін і можливостей, а також на мінімізацію слабких сторін і потенційних загроз.

На основі проведеного аналізу встановлюються стратегічні цілі, які мають бути досягнуті у довгостроковій перспективі. Ці цілі повинні бути конкретними, вимірюваними, досяжними, релевантними та обмеженими у часі (SMART). Прикладами таких цілей можуть бути підвищення рівня кібербезпеки, впровадження передових технологій аналізу даних, підвищення кваліфікації персоналу тощо.

Для досягнення стратегічних цілей розробляються конкретні стратегії. Вони можуть включати інноваційний розвиток, управління ризиками, підвищення ефективності використання ресурсів, навчання та розвиток персоналу. Кожна стратегія повинна мати чіткий план дій, визначені ресурси та відповідальних осіб за виконання.

На етапі впровадження стратегій здійснюється реалізація запланованих дій. Важливо забезпечити належний контроль за виконанням планів, своєчасно вносити корективи та адаптувати стратегії до змін зовнішнього і внутрішнього середовища. Ефективна комунікація між усіма залученими сторонами є ключовим чинником успіху в цьому процесі.

Постійний моніторинг та оцінка результатів є необхідними для забезпечення успішного виконання стратегічних планів. Це дозволяє своєчасно виявляти відхилення від плану, оцінювати ефективність впроваджених заходів та вносити необхідні корективи. Використання індикаторів ефективності (KPI) допомагає об'єктивно оцінювати досягнення стратегічних цілей.

Приклад стратегічного планування може включати:

Місія: Забезпечення високоякісної інформаційної підтримки для прийняття рішень у сфері національної безпеки.

Бачення: Створення передової інформаційно-аналітичної системи, яка здатна оперативно реагувати на виклики та забезпечувати надійну підтримку безпекових структур.

Стратегічні цілі: Підвищення рівня кібербезпеки; впровадження новітніх технологій для аналізу даних; підвищення кваліфікації персоналу; оптимізація процесів обробки інформації.

Стратегії: Розробка та впровадження системи управління ризиками у сфері кібербезпеки; інвестиції в нові технології, такі як штучний інтелект та машинне навчання; проведення регулярних тренінгів і навчальних програм для персоналу; оптимізація процесів збору, обробки та аналізу даних для підвищення їх ефективності.

Стратегічне планування є важливим інструментом, який забезпечує довгостроковий успіх і стійкість інформаційно-аналітичних систем. Воно дозволяє визначити чіткі цілі, розробити ефективні стратегії та забезпечити їх успішне впровадження. У сфері безпеки стратегічне планування сприяє готовності до реагування на виклики та загрози, підвищуючи ефективність і надійність інформаційно-аналітичних систем.

Для проведення оцінки поточного стану інформаційно-аналітичної діяльності в силових структурах України застосуємо метод SWOT-аналізу.

Сильні сторони: Високий рівень професіоналізму аналітичного персоналу: у складі сил безпеки працюють досвідчені аналітики, які мають здатність ефективно обробляти та аналізувати інформацію; багаторічний досвід участі в оборонних операціях і антитерористичних заходах, що надав цінні знання в інформаційно-аналітичній сфері; активна співпраця з міжнародними партнерами та організаціями, що розширює можливості обміну інформацією та накопиченим досвідом.

Слабкі сторони: Обмеженість фінансових, технічних і людських ресурсів, що ускладнює впровадження сучасних інформаційних технологій; використання застарілих систем, які потребують оновлення або повної заміни; труднощі з інтеграцією нових технологій у наявні системи через несумісність або високу вартість впровадження.

Можливості: Стрімкий розвиток інформаційних технологій надає нові можливості для підвищення ефективності аналітичної роботи; можливість

отримання міжнародної допомоги, що сприятиме подоланню фінансових і технологічних бар'єрів; зростаюча увага до кібербезпеки може підвищити рівень захисту інформаційних систем.

Загрози: Постійна загроза кібератак з боку ворожих держав або терористичних угруповань; спроби зовнішнього впливу через дезінформаційні кампанії, що можуть підривати довіру до інформаційно-аналітичної діяльності; ризик витоку таємної інформації, що може мати серйозні наслідки для національної безпеки, як у випадку ненавмисного, так і умисного витоку.

На основі проведеного аналізу можна визначити основні напрями для покращення інформаційно-аналітичної діяльності:

- інвестиції в новітні технології та системи для підвищення ефективності обробки та аналізу даних;
- організація програм навчання та обміну досвідом з міжнародними партнерами;
- розробка та впровадження передових рішень у сфері кібербезпеки для посилення захисту інформаційних ресурсів;
- визначення вимог до технологічного оснащення та програмного забезпечення для підвищення ефективності аналітики;
- розробка програм підготовки та підвищення кваліфікації персоналу з акцентом на сучасні технології та методи аналізу;
- запровадження системи моніторингу для відстеження виконання плану впровадження та оцінки ефективності заходів;
- регулярний перегляд стратегічного плану для внесення необхідних коректив на основі аналізу досягнутих результатів і змін у зовнішньому середовищі.

Стратегічне планування та ефективне втілення виявлених перспективних напрямків здатні значно підвищити якість і результативність інформаційно-аналітичної діяльності в силових структурах України. Це вимагає комплексного підходу, що охоплює технологічне оновлення, підвищення кваліфікації персоналу та посилення кібербезпеки. Реалізація таких заходів потребуватиме

співпраці на всіх рівнях управління, а також належного фінансування.

Оперативне планування є етапом у функціонуванні інформаційно-аналітичних систем, особливо в безпекових структурах. Воно передбачає короткострокове планування дій для забезпечення ефективного виконання щоденних завдань та негайного реагування на поточні виклики і загрози.

Оперативне планування в інформаційно-аналітичних системах орієнтоване на досягнення конкретних результатів у короткостроковій перспективі. Воно включає визначення завдань, розподіл ресурсів, моніторинг виконання та адаптацію планів відповідно до поточних умов. Це дозволяє забезпечити безперебійну роботу системи та своєчасне реагування на події.

Основні етапи оперативного планування:

Перший етап включає визначення конкретних завдань, які необхідно виконати у короткостроковій перспективі. Це можуть бути завдання з аналізу даних, моніторингу ситуації, підготовки звітів, забезпечення кібербезпеки тощо. Важливо, щоб ці завдання були чітко сформульовані та мали конкретні терміни виконання.

Для виконання оперативних завдань необхідно ефективно розподілити наявні ресурси. Це включає призначення відповідальних осіб, розподіл часу, технічних засобів та фінансових ресурсів. Розподіл ресурсів повинен бути оптимальним для забезпечення виконання завдань у встановлені терміни.

Моніторинг виконання – на цьому етапі здійснюється постійний моніторинг виконання оперативних завдань. Це дозволяє своєчасно виявляти відхилення від плану та вживати коригуючих заходів. Моніторинг може включати регулярні наради, звіти, аналіз даних та використання систем управління проєктами.

У процесі виконання оперативних завдань можуть виникати непередбачені обставини, які вимагають адаптації планів. Це може бути зміна пріоритетів, виникнення нових загроз або зміна зовнішніх умов. Адаптація планів дозволяє швидко реагувати на ці зміни та забезпечити безперервність роботи інформаційно-аналітичних систем.

Після виконання оперативних завдань необхідно провести оцінку результатів. Це включає аналіз досягнутих цілей, виявлення проблем та недоліків, а також розробку рекомендацій для покращення процесів. Оцінка результатів дозволяє підвищити ефективність оперативного планування в майбутньому.

Інструменти оперативного планування:

Сучасні системи управління проектами, такі як Microsoft Project, Trello, Asana, дозволяють ефективно планувати, розподіляти завдання, контролювати їх виконання та адаптувати плани в режимі реального часу. Використання таких систем забезпечує прозорість процесів та підвищує ефективність управління.

Інструменти моніторингу та звітності, такі як Power B.I, Tableau, дозволяють здійснювати аналіз даних у режимі реального часу, виявляти відхилення від плану та генерувати звіти для прийняття управлінських рішень. Це сприяє своєчасному виявленню проблем та прийняттю коригуючих заходів.

Інструменти кібербезпеки, такі як системи виявлення загроз, антивірусні програми, фаєрволи, забезпечують захист інформаційно-аналітичної системи від кіберзагроз. Використання таких інструментів дозволяє своєчасно виявляти та реагувати на загрози, забезпечуючи безперебійну роботу інформаційно-аналітичних систем.

Приклад оперативного планування.

Завдання: Моніторинг кіберзагроз та реагування на інциденти.

Етапи:

Визначення завдань: Постійний моніторинг мережевої активності, аналіз логів, виявлення підозрілих дій.

Розподіл ресурсів: Призначення команди кібербезпеки, виділення програмних ресурсів для моніторингу.

Моніторинг виконання: Використання системи SIEM для моніторингу та аналізу даних у режимі реального часу.

Адаптація планів: У разі виявлення інцидентів коригування планів

реагування, призначення додаткових ресурсів.

Оцінка результатів: Після завершення реагування аналіз ефективності дій, виявлення недоліків та розробка рекомендацій.

Оперативне планування є ключовим елементом ефективного управління інформаційно-аналітичною системою. Воно забезпечує своєчасне виконання завдань, оптимальне використання ресурсів та готовність до реагування на непередбачені обставини. Використання сучасних інструментів управління проектами, моніторингу та кібербезпеки дозволяє підвищити ефективність оперативного планування та забезпечити безперебійну роботу інформаційно-аналітичних систем.

Сценарне планування є інструментом стратегічного управління, який дозволяє передбачити різноманітні варіанти розвитку подій та їх вплив на інформаційно-аналітичну систему. Це дає можливість підготуватися до різних майбутніх сценаріїв і розробити відповідні стратегії реагування.

Інформаційно-аналітичні системи відіграють ключову роль у забезпеченні ефективного управління в різних сферах, особливо у силах безпеки. В умовах швидкозмінного світу та невизначеності, сценарне планування стає важливим інструментом для підготовки до можливих майбутніх подій та ризиків.

Сценарне планування включає кілька етапів, кожен з яких є критично важливим для створення реалістичних та корисних сценаріїв:

1. Визначення ключових факторів. Першим кроком є визначення ключових факторів, які можуть вплинути на функціонування інформаційно-аналітичної системи. Це можуть бути політичні, економічні, соціальні, технологічні, екологічні та правові фактори. Важливо враховувати як внутрішні, так і зовнішні чинники.

2. Виявлення невизначеностей. На цьому етапі визначаються основні невизначеності, які можуть суттєво вплинути на систему. Це можуть бути зміни у законодавстві, технологічні прориви, політична нестабільність, економічні кризи тощо. Виявлення таких невизначеностей допомагає сформувати базу для

створення сценаріїв.

3. Розробка сценаріїв. Розробка сценаріїв включає створення декількох альтернативних майбутніх картин розвитку подій. Кожен сценарій повинен бути логічно обґрунтованим і базуватися на виявлених ключових факторах та невизначеностях. Зазвичай створюють 3-5 сценаріїв, що відображають різні можливі траєкторії розвитку подій.

4. Аналіз впливу. Кожен сценарій аналізується на предмет його впливу на інформаційно-аналітичну систему. Визначаються можливі ризики та можливості для кожного сценарію, а також їхній вплив на ключові аспекти системи, такі як надійність, безпека, ефективність та адаптивність.

5. Розробка стратегій реагування. На основі аналізу впливу розробляються стратегії реагування для кожного сценарію. Це включає визначення конкретних дій, які необхідно вжити для мінімізації ризиків та використання можливостей у кожному з можливих майбутніх сценаріїв. Важливо також розробити плани резервного копіювання даних, підвищення кібербезпеки, навчання персоналу тощо.

6. Впровадження та моніторинг. Останнім етапом є впровадження розроблених стратегій та постійний моніторинг ситуації. Необхідно регулярно переглядати та коригувати сценарії та стратегії на основі нової інформації та змін у зовнішньому середовищі. Постійний моніторинг дозволяє своєчасно вносити корективи у плани та забезпечувати актуальність та ефективність інформаційно-аналітичної системи.

Розглянемо приклад сценарного планування для інформаційно-аналітичної системи сил безпеки:

Сценарій 1: Політична стабільність та економічне зростання. У цьому сценарії передбачається, що політична ситуація стабільна, економіка зростає, що дозволяє інвестувати в новітні технології та підвищувати рівень безпеки. Інформаційно-аналітична система розвивається, впроваджуються нові методи аналізу даних та забезпечується висока надійність.

Сценарій 2: Політична нестабільність та економічний спад. Цей сценарій

передбачає політичну нестабільність та економічні труднощі. В таких умовах можливе зменшення фінансування, що вплине на здатність системи до оновлення та підтримки високого рівня безпеки. Потрібно розробити стратегії щодо оптимізації ресурсів та підвищення ефективності використання наявних технологій.

Сценарій 3: Технологічний прорив. У цьому сценарії передбачається швидкий розвиток нових технологій, які кардинально змінюють інформаційно-аналітичні системи. Необхідно адаптувати існуючу систему до нових умов, впроваджувати нові технології та забезпечувати постійне навчання персоналу.

Сценарне планування є потужним інструментом для підготовки до різноманітних майбутніх подій та забезпечення стійкості інформаційно-аналітичних систем. Воно дозволяє ідентифікувати можливі ризики та можливості, розробляти відповідні стратегії реагування та забезпечувати готовність до змін. Це особливо важливо для сил безпеки, де надійність та ефективність інформаційно-аналітичних систем є критично важливими для виконання завдань та забезпечення безпеки.

Одним з підходів для забезпечення ефективності та надійності інформаційно-аналітичних систем, особливо для сил безпеки є ризик-орієнтоване планування. Цей підхід дозволяє ідентифікувати, оцінювати та управляти потенційними ризиками, які можуть вплинути на функціонування системи, що, у свою чергу, сприяє підвищенню її стійкості та надійності.

Першим кроком у ризик-орієнтованому плануванні є ідентифікація можливих ризиків. Це включає аналіз зовнішніх та внутрішніх загроз, таких як кібератаки, технічні збої, людський фактор, природні катастрофи та інші потенційні небезпеки. Важливо залучати експертів з різних галузей для комплексного оцінювання можливих ризиків.

Оцінка ризиків. Після ідентифікації ризиків необхідно провести їх оцінку. Цей етап включає визначення ймовірності настання кожного ризику та потенційного впливу на інформаційно-аналітичну систему. Використовуються кількісні та якісні методи оцінки ризиків, такі як аналіз сценаріїв, методи

Делфі, SWOT-аналіз тощо.

Управління ризиками. Наступним кроком є розробка та впровадження заходів з управління ризиками. Це може включати заходи з попередження ризиків, мінімізації їх впливу, планування дій у випадку настання ризикових подій та моніторинг ефективності вжитих заходів. До управління ризиками також належить створення резервних копій даних, розробка планів відновлення після збоїв, навчання персоналу щодо реагування на надзвичайні ситуації тощо.

Ризик-орієнтоване планування не є статичним процесом. Необхідно постійно моніторити стан ризиків та ефективність заходів з управління ними. Це дозволяє своєчасно вносити корективи у планування та забезпечувати актуальність і надійність інформаційно-аналітичної системи. Регулярний перегляд ризиків та оцінка нових загроз є ключовими елементами безперервного покращення системи. Ризик-орієнтоване планування є необхідним компонентом для забезпечення стійкості та ефективності інформаційно-аналітичних систем сил безпеки. Впровадження цього підходу дозволяє не лише мінімізувати вплив можливих ризиків, але й забезпечити готовність до реагування на надзвичайні ситуації, що є критично важливим у сучасних умовах. Завдяки систематичному підходу до ідентифікації, оцінки та управління ризиками, інформаційно-аналітичні системи можуть функціонувати надійно та ефективно, забезпечуючи необхідну підтримку для прийняття рішень та виконання безпекових завдань.

5.2. Розвиток менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України

На думку авторів Концепції військової кадрової політики [99], однією з ключових проблем, що негативно впливає на укомплектованість сил безпеки та оборони України належно підготовленим і вмотивованим персоналом, є тенденція скорочення кількості громадян з відповідними морально-діловими та професійними якостями, які бажають служити за контрактом. Крім того,

зберігається динаміка плинності кадрів, що виражається у відтоку кваліфікованих та досвідчених військовослужбовців, які не бачать перспективи тривалого проходження служби.

Незважаючи на введення за останні роки комплексу мотиваційних заходів (збільшення грошового забезпечення, компенсація за піднайом житла для рядового та сержантського складу, підвищення додаткових виплат за виконання завдань в зоні ООС на лінії розмежування та за особливі умови служби), відтік військовослужбовців продовжується.

Основні причини проблеми [99]:

- недостатній рівень патріотичного виховання та військово-професійної орієнтації громадян, відсутність масштабної рекламної кампанії на державному рівні для підвищення престижу військової служби;

- існуюча система управління кар'єрою військовослужбовців не забезпечує чіткого розуміння кар'єрного зростання та перспективи для кожного військовослужбовця;

- система підготовки кадрів та військової освіти недостатньо сприяє самовдосконаленню та професійному розвитку військовослужбовців;

- грошове забезпечення військовослужбовців не відповідає сучасним вимогам і не є конкурентоспроможним на ринку праці України;

- низький рівень забезпеченості житлом та соціально-побутовими об'єктами в військових містечках, де компенсація за піднайом житла не покриває реальних витрат, а будівництво нових гуртожитків триває надто довго;

- відсутність ефективних змін у соціальних відносинах "командир - підлеглий", включаючи порушення розпорядку дня та залучення військових до непритаманних завдань;

- значна частина пільг та соціальних гарантій військовослужбовців є декларативними, а система охорони здоров'я для них потребує удосконалення відповідно до стандартів НАТО.

Невизначеність у перспективах кар'єрного зростання, недостатній рівень

соціального та правового захисту, відсутність дієвих механізмів утримання кадрів призводять до низької мотивації громадян щодо вступу на військову службу за контрактом та тривалого перебування на службі. Це негативно впливає на здатність сил безпеки виконувати свої завдання в умовах складної воєнно-політичної, оперативно-стратегічної та економічної ситуації, спричиненої збройною агресією рф проти України.

Висококваліфікований та досвідчений персонал здатний досягати значних результатів в інформаційно-аналітичній діяльності, навіть за умов недостатнього фінансування та матеріально-технічної бази, або ж недосконалого правового забезпечення [233]. Отже, кадрове забезпечення стає одним із ключових чинників ефективності ІАС. Ця проблема стає особливо актуальною в умовах сьогодення, коли результативність роботи ІАС будь-якого підрозділу сил безпеки може визначати успішність виконання службово-бойових завдань.

Однією з проблемних аспектів механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України є нестача кваліфікованих фахівців у галузі інформаційних технологій та аналітики, що обмежує здатність сил безпеки ефективно обробляти та аналізувати дані.

Згідно з даними Державної служби статистики України [188] кількість студентів, які обирають навчання в галузі інформаційних технологій, зростає, проте кількість фахівців у суміжних галузях, таких як природничі науки, автоматизація та приладобудування, електроніка та телекомунікації, виробництво і технології, зменшується. Цю тенденцію ілюструє рисунок 5.1.

Для вирішення цієї проблеми необхідно зосередитися на кількох напрямках. По-перше, слід стимулювати зацікавленість у навчанні за спеціальностями, які відповідають потребам національної безпеки, через стипендії, гранти та інші форми мотивації. Важливим є також підвищення якості освітніх програм, впровадження сучасних курсів, які б включали практичні аспекти використання ІТ у сфері безпеки.

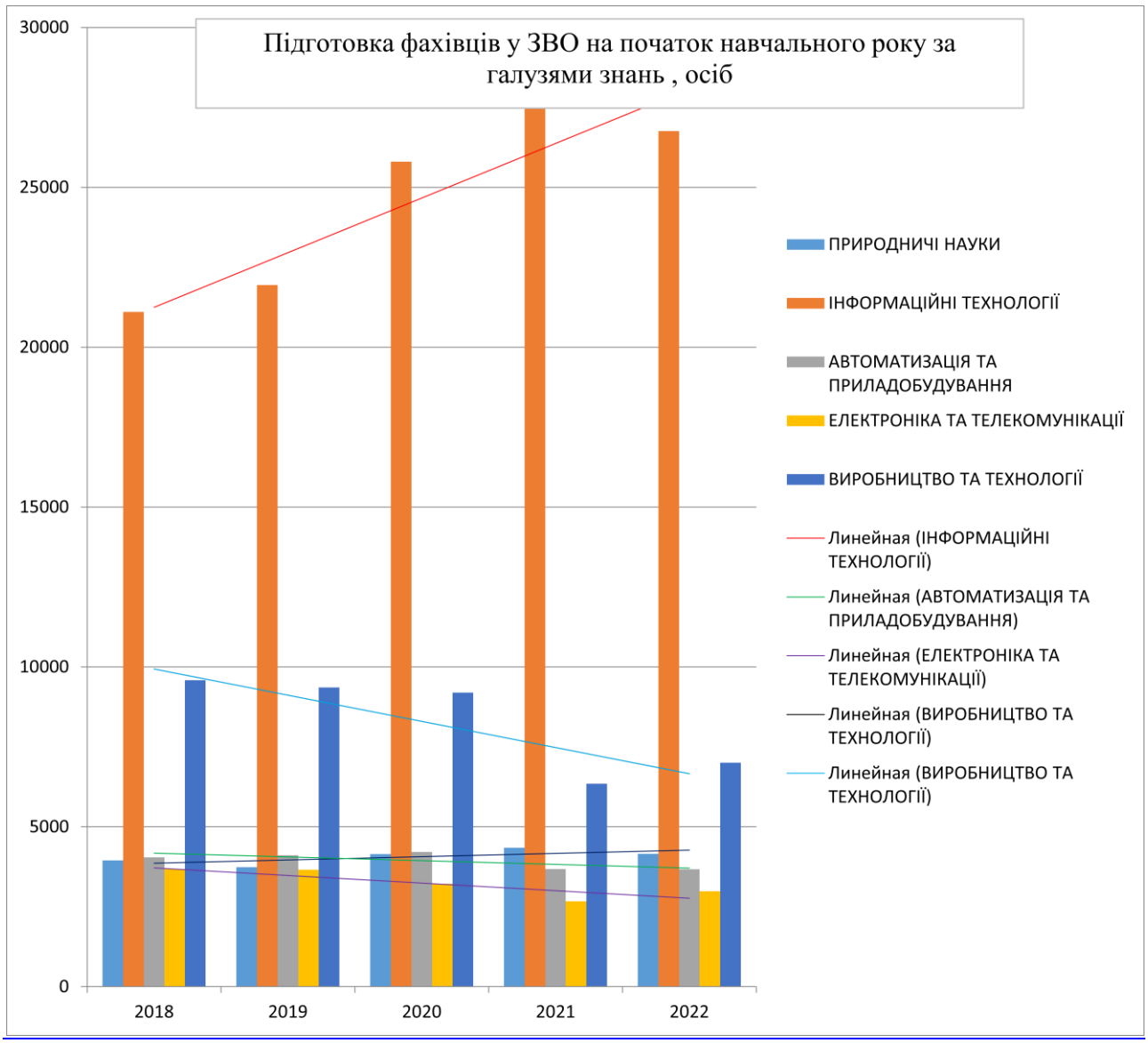

Рисунок 5.1 – Кількість фахівців у ЗВО за галузями знань за 2018-2022 роки, та лінійні тренди їх змін

Крім того, важливою є розвиток співпраці між державою та приватними ІТ-компаніями. Це може включати спільні дослідницькі проекти, стажування для студентів, розробку спеціалізованих ІТ-рішень для потреб сил безпеки. Така співпраця сприятиме підготовці фахівців, здатних ефективно працювати в умовах реальних викликів.

Нестача кваліфікованих фахівців у сфері ІТ та аналітики є серйозною загрозою для національної безпеки України. Вирішення цієї проблеми потребує комплексного підходу, що включає оновлення освітніх програм, підвищення

мотивації серед молоді, розвиток наукових досліджень і зміцнення співпраці між державним і приватним секторами.

Так обмеження фінансування фундаментальних наукових досліджень не дозволяють розробляти нові технології. В таблиці 5.1 наведені дані про витрати на наукові дослідження і розробки за видами робіт за 2010-2022 роки в Україні.

Таблиця 5.1 – Витрати на наукові дослідження і розробки за видами робіт за 2010-2022 роки [188]

Рік	Витрати на виконання наукових досліджень і розробок, млн.грн	У тому числі на виконання			Частка витрат на виконання наукових досліджень і розробок у ВВП, %
		Фундамент-тальних наукових досліджень, млн.грн	Прикладних наукових досліджень, млн.грн	Науково-технічних (експеримент-тальних) розробок, млн.грн	
2010	8107,1	2175,0	1589,4	4342,7	0,75
2011	8513,4	2200,8	1813,9	4498,7	0,65
2012	9419,9	2615,3	2023,2	4781,4	0,67
2013	10248,5	2698,2	2061,4	5488,9	0,70
2014	9487,5	2452,0	1882,7	5152,8	0,60
2015	11003,6	2460,2	1960,6	6582,8	0,55
2016	11530,7	2225,7	2561,2	6743,8	0,48
2017	13379,3	2924,5	3163,2	7291,6	0,45
2018	16773,7	3756,5	3568,3	9448,9	0,47
2019	17254,6	3740,4	3635,7	9878,5	0,43
2020	17022,4	4259,0	3971,4	8792,1	0,41
2021	20923,1	5155,2	4782,9	10985,0	0,38
2022	17117,8	4081,3	4827,6	8208,9	0,33

На рисунку 5.2 наведена динаміка витрат на наукову діяльність в Україні,

як частка ВВП.

Держава повинна збільшити інвестиції в наукові дослідження в галузі інформаційних технологій та кібербезпеки. Це не тільки сприятиме розвитку новітніх технологій, але й забезпечить підготовку висококваліфікованих науковців, здатних розв'язувати складні задачі у сфері безпеки. Обмежені бюджетні ресурси можуть стати суттєвою перешкодою для оновлення технологій, навчання персоналу та підтримки ефективності інформаційно-аналітичної діяльності. У контексті швидко змінюваного безпекового середовища це вимагає постійної адаптації механізмів державного управління та забезпечення здатності сил безпеки оперативно реагувати на нові виклики та загрози.

Рисунок 5.2 – Динаміка витрат на наукову діяльність в Україні, як частка ВВП (розроблена за даними таблиці 4.1)

Ефективність сил безпеки безпосередньо залежить від якості кадрового менеджменту та інформаційно-аналітичного забезпечення. Розвиток менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України зумовлений постійним розвитком технологій та необхідністю адаптації до змінних умов безпекового середовища.

Для того щоб зрозуміти теоретичні основи управління людськими

ресурсами і застосувати їх у контексті сил безпеки України, слід розглянути основні моделі та підходи до кадрового менеджменту, а також їх можливу адаптацію до потреб безпекових структур.

Серед основних моделей управління кадровими ресурсами можна виділити такі [222]:

Модель Гарвардської школи: наголошує на важливості людського фактора в організації та пропонує стратегічний підхід до управління, де співробітники розглядаються як ключові стейкхолдери. Основні компоненти включають взаємодію між співробітниками та менеджментом, мотивацію, корпоративну культуру та системи винагород.

Модель Мічиганської школи: фокусується на процесах відбору, оцінки, мотивації та розвитку персоналу. Ця модель підкреслює важливість забезпечення високої продуктивності через стратегічне управління людськими ресурсами.

Компетентнісний підхід: заснований на необхідності ідентифікації та розвитку ключових компетенцій, необхідних для досягнення цілей організації. Основна увага приділяється розвитку навичок та здібностей співробітників.

На думку Михайлової [116] основними етапами управління персоналом в організації є такі:

– планування персоналу, головною метою якого є розробка плану задоволення майбутніх потреб організації в людських ресурсах;

– залучення персоналу та створення резерву потенційних кандидатів для заміщення усіх посад;

– відбір кадрів, де здійснюється оцінка кандидатів та відбираються найкращі претенденти;

– визначення заробітної плати та додаткових пільг для працівників з метою залучення та збереження кадрів;

– професійна орієнтація та адаптація нових працівників для швидшого їх впровадження в організацію та реалізації їх потенціалу;

– навчання персоналу як безперервний процес, що є необхідною умовою для ефективного виконання робіт;

– оцінка діяльності працівників (атестація кадрів);

– трудове переміщення (підвищення, пониження, переведення, звільнення працівників) з метою більш раціонального їх використання;

– підготовка керівних кадрів як важлива складова всієї системи управління персоналом [116].

Функції управління персоналом – це види діяльності управлінського апарату, що умовно діляться на загальні та специфічні.

До загальних функцій належать [177]: планування, організація, координація, контроль та мотивація. Ці функції виконують усі керівники в межах своїх посадових обов'язків, прав і відповідальності. Специфічні функції управління персоналом визначаються функціональним поділом праці між структурними підрозділами організації та між виконавцями. Ці функції не закріплені в чинних нормативних документах, але їх можна визначити з переліку завдань та обов'язків, зазначених у «Довіднику кваліфікаційних характеристик професій працівників» [177, 196].

До ключових функцій системи управління персоналом, на думку Пожара [137], сьогодні належать: Залучення та відбір персоналу; управління якістю діяльності персоналу, його мотивація; удосконалення системи оплати праці; навчання та підвищення кваліфікації; формування та збереження сприятливого морально-психологічного клімату; удосконалення методів оцінки персоналу; управління внутрішніми переміщеннями і кар'єрою працівників; участь у розробці організаційної стратегії [137].

Методи управління персоналом – це спосіб впливу на колектив або окремого працівника для досягнення поставленої цілі, координації його діяльності в процесі діяльності підприємства [29, 110, 247].

Особливість управління персоналом на відміну від інших, наприклад, технічних систем, полягає в тому, що об'єктом і суб'єктом управління є люди, персонал організації [30, с. 9, 248].

Методи побудови системи управління персоналом наведені в таблиці 5.2, сформованою за джерелом [101].

Таблиця 5.2 – Методи побудови системи управління персоналом [101]

Метод	Суть методу
Метод декомпозиції	Дозволяє розчленувати складні явища на більш прості (наприклад, систему управління персоналом можна розчленувати на підсистеми, підсистеми – на функції, функції – на процедури, процедури – на операції)
Метод послідовної підстановки	Дозволяє дослідити вплив на формування системи управління персоналом окремо кожного фактора, елімінуючи вплив інших факторів. Фактори ранжують та обирають найбільш суттєві
Метод порівнянь	Дозволяє порівняти існуючу систему управління персоналом з подібною системою провідного підприємства, з нормативним станом або станом у минулому періоді
Динамічний метод	Передбачає розташування даних у динамічному ряду та виключення із нього випадкових відхилень (для відображення стійких тенденцій). Метод застосовується під час дослідження кількісних показників, що характеризують систему управління персоналом
Метод структуризації цілей	Передбачає кількісне та якісне обґрунтування цілей підприємства в цілому та цілей системи управління персоналом із точки зору їх відповідності цілям підприємства. Повинні бути забезпечені взаємозв’язка, повнота, співставленість цілей різних рівнів управління персоналом
Експертно-аналітичний метод	Ґрунтується на залученні висококваліфікованих спеціалістів із управління персоналом та управлінського персоналу підприємства до цього процесу. Важливим є опрацювання форм систематизації, запису та чіткого уявлення поглядів та висновків експертів
Нормативний метод	Передбачає застосування системи нормативів, що визначають склад та зміст функцій із управління персоналом, чисельність працівників за функціями, тип організаційної структури, критерії побудови структури апарата управління підприємства в цілому та системи управління персоналом
Параметричний метод	Встановлення функціональних взаємозв’язків між параметрами елементів виробничої системи та системи управління персоналом для встановлення ступеня їх відповідності

продовження таблиці 5.2

Метод функціонально-вартісного аналізу	Дозволяє обрати такий варіант побудови системи управління персоналом або виконання певної функції управління персоналом, який потребує найменших витрат та є найбільш ефективним з точки зору кінцевих результатів. Дозволяє виявити надлишкові або дублюючі функції управління, функції, що з певних причин не виконуються, визначити ступінь централізації та децентралізації функцій управління персоналом тощо. За допомогою цього методу виявляються основні напрямки удосконалення управління персоналом, оцінки результатів аналізу та причини недоліків
Метод головних компонент	Дозволяє відобразити в одному показнику (компоненті) властивості десятків показників. Це дає можливість порівняти не множину показників однієї системи управління персоналом із множиною показників іншої подібної системи, а лише один
Балансовий метод	Дозволяє здійснити балансові співставлення, ув'язки (наприклад, порівнюються результати обробки фотографій робочого дня та технологічних карт виконання управлінських операцій і процедур із діючим фондом робочого часу їх виконання)
Досвідний метод	Базується на досвіді попереднього періоду даної системи управління персоналом та досвіді іншої аналогічної системи
Метод аналогій	Полягає в застосуванні організаційних форм, що виправдали себе в функціонуючих системах управління персоналом зі схожими економіко-організаційними характеристиками, в системі, що розглядається. Його сутність – розробка типових рішень (наприклад, типової оргструктури управління персоналом) та визначення меж і умов їх використання
Метод творчих нарад	Передбачає колективне обговорення напрямків розвитку системи управління персоналом групою спеціалістів та керівників. Ефективність методу полягає в тому, що ідея, висловлена одним працівником, викликає у інших учасників наради нові ідеї, які, в свою чергу, породжують наступні ідеї, в результаті чого виникає потік ідей. Мета творчої наради – виявити найбільше варіантів шляхів удосконалення системи управління персоналом

Методи управління кадровими ресурсами:

- Стратегічний підхід: Акцентується на інтеграції планування людських ресурсів з загальною стратегією організації. Метою є досягнення

довгострокових цілей за допомогою ефективного управління людським капіталом.

- Операційний підхід: Зосереджується на щоденних аспектах управління персоналом, таких як підбір, навчання, оцінка співробітників та вирішення конфліктів. Цей підхід є критично важливим для забезпечення безперебійної роботи організації.

- Розвивальний підхід: Підкреслює важливість постійного розвитку та навчання працівників, що є ключовим елементом у стратегії управління персоналом. Це включає планування кар'єри, навчання та розвиток лідерських навичок.

Особливість сил безпеки полягає в необхідності поєднання високого рівня професіоналізму, стресостійкості та адаптивності до швидко змінюваних умов [105]. Сили безпеки відзначаються необхідністю високого рівня професіоналізму, стресостійкості та здатності адаптуватися до швидко змінюваних умов. Впровадження компетентнісного підходу разом зі стратегічним плануванням та акцентом на розвиток персоналу може підвищити ефективність інформаційно-аналітичного забезпечення та загальну готовність сил безпеки. Стратегії розвитку кадрів відіграють важливу роль у підвищенні ефективності службово-бойової діяльності сил безпеки України.

Ключові стратегії, які можуть бути адаптовані для сил безпеки України:

Стратегічне планування кадрових ресурсів: Передбачає прогнозування потреб у персоналі на основі довгострокових цілей та стратегії організації. Це включає аналіз поточних та майбутніх потреб у кадрах, виявлення прогалин у компетенціях та розробку планів для їх заповнення через підбір, навчання та розвиток персоналу [55].

Управління талантами: Фокусується на ідентифікації, залученні, розвитку та утриманні висококваліфікованих працівників, які можуть забезпечити стратегічну конкурентну перевагу. У контексті сил безпеки це може включати розробку програм лідерства, кар'єрного розвитку та професійного зростання.

Систематичні програми навчання та розвитку: Важливі для підтримки

постійного професійного зростання співробітників. Для сил безпеки такі програми повинні включати спеціалізоване навчання, що охоплює як технічні, так і управлінські навички, включаючи стратегічне мислення, лідерство, управління кризами та міжкультурну комунікацію.

Розвиток позитивної корпоративної культури: Підтримка цінностей організації та сприяння високому рівню задоволення та мотивації співробітників є критичними для успіху стратегії розвитку кадрів. У силах безпеки це може включати заходи для підвищення морального духу, визнання досягнень, а також забезпечення безпеки та добробуту персоналу.

Регулярна оцінка ефективності: Важливий аспект у розвитку персоналу, особливо в силах безпеки, де необхідно мати чіткі критерії оцінки, що базуються на конкретних завданнях та цілях, а також механізми для виявлення та розвитку потенціалу співробітників.

Управління компетенціями та навчанням персоналу [222]:

1. Визначення компетенцій: Основою управління компетенціями є ідентифікація ключових навичок, необхідних для ефективного виконання роботи. У силах безпеки це може включати тактичні навички, стратегічне планування, лідерство, вирішення конфліктів та спеціалізовані технічні знання.

Оцінка компетенцій: Регулярна оцінка навичок співробітників дозволяє визначити рівень їх професійного розвитку та виявити прогалини, які потребують покращення.

Розвиток компетенцій: На основі оцінки компетенцій розробляються індивідуальні або групові програми навчання для заповнення виявлених прогалин. Це може включати тренінги, семінари, менторство, участь у професійних конференціях тощо.

Моніторинг та оновлення компетенцій: Управління компетенціями є постійним процесом. Організації повинні регулярно переглядати та оновлювати набір необхідних компетенцій відповідно до змін у стратегічних цілях, технологіях або зовнішньому середовищі.

Навчання персоналу [222]:

Планування навчання: На основі оцінки компетенцій складається план навчання, що визначає цілі, формати (очне, онлайн, самостійне навчання), вибір тренерів та розклад занять.

Реалізація навчальних програм: Програми навчання повинні бути спеціально адаптовані до потреб працівників та враховувати специфіку роботи в секторі безпеки. Це може включати симуляційні вправи, практичні заняття, кейс-методи та інші інтерактивні підходи.

Оцінка ефективності навчання: Важливою складовою є оцінка результативності навчання, яка допомагає визначити його вплив на професійний розвиток співробітників та їхню продуктивність в роботі.

Корекція навчальних програм: На основі отриманих результатів можуть бути внесені зміни в програми навчання для підвищення їх ефективності або кращої відповідності потребам організації.

Використання інформаційних систем в управлінні кадровими ресурсами:

Застосування інформаційних систем є ключовим фактором для підвищення ефективності та автоматизації управлінських процесів в сфері кадрових ресурсів. Ці системи забезпечують швидкий доступ до даних, покращують комунікацію, спрощують управління навчанням та розвитком, а також сприяють ефективному плануванню та аналізу ресурсів.

Системи управління людськими ресурсами (HRM).

1. Інтеграція даних: HRM-системи дозволяють об’єднувати різноманітну інформацію про співробітників, включаючи особисті дані, інформацію про навчання, оцінки ефективності, вакансії та кар’єрне зростання, що полегшує доступ та управління цією інформацією.

Автоматизація процесів: HRM-системи автоматизують рутинні процеси, такі як ведення табелів робочого часу, нарахування зарплати, облік відпусток та лікарняних, що знижує ризик помилок та підвищує продуктивність HR-відділу.

Підтримка прийняття рішень: Сучасні HRM-системи забезпечують інструменти для аналізу даних та прийняття рішень, що допомагає HR-менеджерам та керівництву ефективно планувати розвиток персоналу,

прогнозувати потреби в наборі та оцінювати ефективність навчальних програм.

Системи управління навчанням (LMS).

Централізоване управління навчанням: LMS дозволяють централізовано керувати навчальними матеріалами, курсами та програмами, забезпечуючи доступ до навчання для всіх співробітників, незалежно від їх місця знаходження.

Моніторинг та звітність: LMS надають інструменти для відстеження прогресу навчання співробітників, оцінки їх успіхів та формування звітів, що сприяє ефективній оцінці та коригуванню навчальних програм.

Персоналізація навчання: LMS дозволяють адаптувати навчальні програми до індивідуальних потреб кожного співробітника, що підвищує мотивацію та ефективність навчання.

Системи аналітики даних у HR.

Прогнозування та оптимізація: Інструменти аналітики даних допомагають прогнозувати тенденції в управлінні персоналом, ідентифікувати ризики, такі як висока плинність кадрів, та оптимізувати стратегії розвитку та утримання талантів.

Глибокий аналіз ефективності: Використання аналітики дозволяє детально аналізувати продуктивність співробітників, оцінювати вплив навчальних програм на продуктивність та визначати ключові фактори успіху організації.

Використання інформаційних систем у менеджменті кадрових ресурсів.

Застосування інформаційних систем не лише підвищує ефективність управління персоналом, але й дозволяє прогнозувати потреби в кадрах, аналізувати тенденції на ринку праці [222].

Автоматизація управління персоналом: Інформаційні системи полегшують процеси набору, відбору, оцінки ефективності, а також управління відпустками та відсутностями, зменшуючи адміністративне навантаження на HR-відділи.

Управління компетенціями та навчанням: Системи дозволяють

створювати детальні профілі співробітників, що містять інформацію про їх навички, кваліфікації та історію навчання, спрощуючи процес виявлення потреб у розвитку та відстеження прогресу навчання.

Планування та аналітика: Інформаційні системи надають інструменти для прогнозування потреб у персоналі, аналізу ринкових тенденцій, оцінки ефективності персоналу та планування навчальних програм.

Самообслуговування співробітників: Модулі самообслуговування дозволяють працівникам самостійно оновлювати свої персональні дані, подавати заявки на відпустки, доступ до навчальних ресурсів, що підвищує їх задоволеність роботою та покращує комунікацію.

Підтримка стратегічного управління та прийняття рішень: Інформаційні системи надають доступ до великого обсягу аналітичної інформації та звітів, сприяючи кращому розумінню організаційних викликів та підтримуючи прийняття стратегічних рішень.

Інструменти та технології:

Системи управління людськими ресурсами (HRM): До прикладу, SAP SuccessFactors, Workday, Oracle HCM Cloud – ці платформи надають потужні можливості для ефективного управління персоналом.

Системи управління навчанням (LMS): Інструменти як Moodle, Cornerstone OnDemand, Blackboard забезпечують централізоване керування навчальними процесами та підвищення кваліфікації співробітників.

Аналітичні та BI-інструменти: Призначені для глибокого аналізу даних, вони допомагають виявити інсайти, що сприяють підвищенню продуктивності та ефективності роботи персоналу.

Роль інформаційних систем в управлінні кадровими ресурсами:

Інформаційні системи є важливою складовою управління персоналом, особливо для організацій, де необхідна висока оперативність і адаптивність, як у випадку сил безпеки. Вони дозволяють оптимізувати управлінські процеси, підвищувати продуктивність співробітників і сприяти розвитку стратегічних переваг організації.

Аналіз успішних практик в менеджменті кадрових ресурсів і інформаційно-аналітичному забезпеченні сил безпеки України може включати дослідження інноваційних підходів, впровадження передових технологій та розробку ефективних стратегій розвитку персоналу. Ось кілька ключових напрямків, на які варто звернути увагу при аналізі таких практик:

Інноваційні методи набору та відбору: Сучасні практики передбачають використання передових технологій для оптимізації процесів набору та відбору, таких як штучний інтелект для аналізу резюме та автоматизації початкових етапів відбору. У сил безпеки це може включати спеціалізовані програмні рішення для оцінки професійних навичок і психологічної відповідності кандидатів.

Розвиток компетенцій та навчання: Ефективні програми навчання включають симуляції, ігрові методи та мобільне навчання, що демонструє високу ефективність у підвищенні кваліфікації персоналу. Використання LMS для відстеження прогресу і адаптації навчальних програм до індивідуальних потреб співробітників є важливим аспектом успішних практик.

Використання інформаційних систем: Успішні приклади впровадження інформаційних систем включають інтеграцію систем управління ресурсами підприємства (ERP) та HRM, що забезпечує ефективне планування, аналіз і управління персоналом на всіх рівнях організації.

Стратегічне управління талантами: Успішні організації часто розробляють стратегії управління талантами, які охоплюють планування кар’єрного розвитку, програми лояльності та резервування кадрів для ключових позицій. Це дозволяє підвищити мотивацію та задоволення співробітників, а також забезпечити довгострокову кадрову стабільність.

Підвищення ефективності роботи: Організації, що успішно впроваджують передові HR-практики, демонструють покращену продуктивність, швидку адаптацію до змін у зовнішньому середовищі та здатність оперативно реагувати на нові виклики.

Рекомендації для сил безпеки України:

На основі аналізу успішних практик у сфері менеджменту кадрових ресурсів та використання інформаційно-аналітичного забезпечення можна розробити наступні рекомендації:

Впровадження інноваційних підходів до набору та відбору персоналу.

Акцент на розвиток компетенцій через сучасні методи навчання.

Інтеграція інформаційних систем для централізованого управління та аналітики.

Розробка стратегій управління талантами для довгострокової стабільності та розвитку.

Адаптація передових HR-практик для підвищення ефективності та оперативності організації.

Ці рекомендації допоможуть підвищити ефективність управління персоналом, оптимізувати процеси навчання та розвитку, а також сприяти кращому використанню інформаційних ресурсів в контексті сил безпеки України.

Рекомендації:

Інтеграція інформаційних систем: Впровадження комплексних HRM-систем, що автоматизують ключові HR-процеси, включаючи підбір, оцінку, навчання та розвиток співробітників.

Цифрове навчання та розвиток: Використання систем управління навчанням (LMS) для організації дистанційного навчання, вебінарів, онлайн-курсів та гнучких програм розвитку.

Стратегічне управління талантами: Розробка програм управління талантами, орієнтованих на виявлення, розвиток і утримання ключових співробітників для досягнення стратегічних цілей організації.

Автоматизація набору та відбору: Використання штучного інтелекту для оптимізації процесів скринінгу резюме та відбору кандидатів, що дозволяє скоротити час на підбір персоналу і підвищити якість нових співробітників.

Культура постійного навчання: Створення умов для безперервного професійного розвитку через регулярне навчання, менторство та самоосвіту, що

сприяє підвищенню загальної кваліфікації персоналу.

Аналітика для ухвалення рішень: Впровадження аналітичних інструментів для збору та аналізу даних про персонал, що забезпечить глибше розуміння потреб організації та допоможе ефективніше планувати розвиток людських ресурсів.

Стратегії впровадження:

Пілотні проекти: Розпочніть впровадження нових систем та процесів з обмеженого масштабування в окремих підрозділах для оцінки ефективності та збору зворотного зв’язку перед їхнім повномасштабним застосуванням.

Тренінги та семінари: Організуйте навчальні заходи для керівників і співробітників HR-відділів, щоб ознайомити їх з новими технологіями та методами управління персоналом.

Залучення стейкхолдерів: Залучайте керівництво та співробітників до процесу планування та реалізації змін, щоб забезпечити підтримку та успішне впровадження нових підходів.

Моніторинг та оцінка: Впровадьте систему моніторингу та оцінки для постійного відстеження прогресу впровадження нових підходів та корекції стратегій на основі отриманих результатів.

Впровадження цих рекомендацій та стратегій допоможе силам безпеки України:

Підвищити ефективність управління кадровими ресурсами.

Оптимізувати процеси навчання та розвитку персоналу.

Зробити краще використання інформаційних ресурсів для підтримки стратегічних цілей.

Для успішного розвитку менеджменту кадрів у силах безпеки України важливо інтегрувати сучасні підходи та технології в усі аспекти управління персоналом. Нижче наведені практичні рекомендації, які допоможуть покращити ефективність і гнучкість кадрової політики:

Впровадження сучасних IT-рішень:

Автоматизація HR-процесів: Застосування HRM-систем для автоматизації

процесів підбору, оцінки, навчання та кар’єрного розвитку.

Використання Big Data та аналітики: Використання інструментів аналітики для аналізу даних про персонал, що дозволить краще розуміти потреби в навчанні, прогнозувати плинність кадрів і планувати їхню кількість.

Розвиток компетенцій та професійне навчання:

Модульні програми навчання: Розробка та впровадження модульних програм, що базуються на конкретних потребах розвитку компетенцій.

Симуляції та тренінги: Використання симуляційних тренінгів для розвитку практичних навичок у віртуальному середовищі, зокрема для підготовки до кризових ситуацій.

Управління талантами:

Розвиток лідерських якостей: Створення програм розвитку лідерства для підготовки майбутніх керівників організації.

Кар’єрне планування та резервування кадрів: Формування системи кар’єрного планування та резервування кадрів для забезпечення неперервності управлінського складу та важливих фахівців.

Корпоративна культура та залучення персоналу:

Розвиток корпоративної культури: Підтримка та розвиток корпоративної культури, яка сприяє залученню персоналу та знижує плинність кадрів.

Здоров’я та безпека: Впровадження програм підтримки здоров’я та безпеки на робочому місці, включаючи психологічну підтримку та запобігання професійному вигоранню.

Моніторинг та оцінка ефективності:

Система оцінки ефективності: Створення комплексної системи оцінки ефективності персоналу, яка включає як кількісні, так і якісні показники.

Зворотний зв’язок та адаптація: Регулярний збір зворотного зв’язку від співробітників для адаптації стратегій управління персоналом і вдосконалення робочого середовища.

Впровадження цих рекомендацій забезпечить підвищення ефективності управління кадровими ресурсами, розвиток професіоналізму та готовності

персоналу до виконання поставлених завдань, а також створення основи для постійного розвитку та адаптації до змін.

Перспективи подальших досліджень у сфері розвитку менеджменту кадрових ресурсів, особливо в контексті сил безпеки України, є багатогранними та визначаються як внутрішніми потребами, так і зовнішніми викликами. Ось кілька основних напрямків для майбутніх досліджень:

Технологічні інновації в управлінні кадровими ресурсами:

Дослідження впливу штучного інтелекту та машинного навчання на процеси підбору, оцінки та розвитку персоналу.

Розробка і впровадження автоматизованих систем, що підвищують ефективність HR-процесів і дозволяють адаптуватися до дистанційної роботи.

Стратегії управління талантами та лідерством:

Аналіз ефективності програм управління талантами та розвитку лідерських якостей у силових структурах.

Дослідження міжнародного досвіду в сфері розвитку кадрового потенціалу та його адаптація до українських реалій.

Корпоративна культура та залученість персоналу:

Вивчення впливу корпоративної культури на мотивацію та продуктивність персоналу в силових структурах.

Аналіз стратегій залучення персоналу та їх впливу на зниження плинності кадрів і підвищення лояльності.

Методи оцінки та розвитку компетенцій:

Розробка та перевірка інструментів оцінки компетенцій, здатних точно визначити потреби у навчанні та розвитку.

Впровадження компетентнісного підходу в навчання і розвиток, включаючи симуляції та віртуальні реальності для практичного навчання.

Управління кадровими ресурсами в силових структурах України потребує комплексного підходу, що включає стратегічне планування, оперативне управління та постійний розвиток навичок і компетенцій персоналу. Використання сучасних моделей управління може значно підвищити

ефективність та адаптивність сил безпеки до сучасних викликів.

На сьогоднішній день, згідно з «Концепцією військової кадрової політики в системі Міністерства оборони України на період до 2028 року» [99], розгорнуто автоматизовану інформаційно-телекомунікаційну систему (АІТС) «Оберіг» (Реєстр), яка призначена для збору, зберігання, обробки та використання даних про призовників, військовозобов’язаних та резервістів, що забезпечує військовий облік та комплектування Збройних Сил України та інших військових формувань у мирний час та в особливий період [99]. Реєстр наразі заповнений більш ніж на 90%. Продовжується розгортання стаціонарної інформаційно-аналітичної системи «Персонал» (ІАС «Персонал»), яка покликана підвищити оперативність обліку та управління персоналом, поліпшити обґрунтованість кадрових рішень, скоротити час на підготовку інформаційних матеріалів для керівництва Міністерства оборони та Збройних Сил України, а також зберігати й накопичувати необхідну інформацію про особовий склад. До початку повномасштабного вторгнення рф було розгорнуто 21 захищений автоматизований технологічний комплекс (ЗАТК) ІАС "Персонал" на різних рівнях управління персоналом [99]. Розпочато роботу з інтеграції автоматизованих систем обліку та управління персоналом з державними реєстрами та подальшої цифровізації цих процесів.

Проте, на сьогодні в силових структурах України відсутні діючі автоматизовані бази даних для обліку та управління персоналом, що значно ускладнює процеси прийняття кадрових рішень та зменшує ефективність збору, обробки й використання даних про особовий склад.

Подальші дослідження в галузі розвитку менеджменту кадрових ресурсів у силових структурах України мають значний потенціал для підвищення ефективності та адаптивності організацій до змінних умов зовнішнього середовища.

Це потребує комплексного підходу, який охоплює як впровадження передових технологічних рішень, так і розвиток корпоративної культури, програм навчання та управління компетенціями.

5.3 Загальнодержавна концептуальна модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

Структури безпеки та оборони, аналогічно до інших державних органів, постійно розвиваються, адаптуючись до нових умов та стаючи все більш комплексними. Цей процес супроводжується появою новітніх озброєнь, створенням нових військових підрозділів, постановкою нових завдань і зміною методик та стратегій ведення оперативних дій. У контексті бойових операцій, критично важливою є швидкість збору, обробки, аналізу, передачі та використання інформації, а також методи її збереження і захисту.

Процес управління є одним із найбільш складних видів людської діяльності. Враховуючи двоїсту природу управління, що поєднує об'єктивні (раціональні) та суб'єктивні (ірраціональні) складові, цей процес стає ще більш складним через наявність численних проблем різного характеру. Із зростанням складності керованих систем, кількість і масштаб цих проблем також збільшуються, що викликає необхідність постійного вдосконалення управління та підвищення якості прийняття рішень [1].

Ці проблеми ускладнюються низкою суперечностей у структурі управління, таких як:

- зростаюча складність керованих систем при обмеженій чисельності управлінського апарату;
- дилема між оперативністю процесу управління і якістю прийнятих рішень;
- протиріччя між спеціалізацією і інтеграцією завдань в управлінському процесі;
- потреба в точних методиках оцінки рішень на тлі складності формалізації вирішуваних завдань;
- зростання складності завдань управління та рівня підготовки управлінських кадрів.

Ці фактори створюють загальну суперечність між поточним станом процесу реалізації управлінських функцій і необхідним рівнем ефективності цього управління. Це протиріччя має прагматичний характер, що посилює зв'язок між теоретичними і практичними аспектами вирішення управлінських проблем. Присутність зазначених протиріч сприяє формуванню хронічної кризи в системі управління, що є особливо відчутним у державному та військовому управлінні, де помилки можуть мати особливо високу ціну. У зв’язку з цим важливо виявити специфіку прояву факторів, які провокують кризу управління у даній предметній області, і на основі цього формувати методологію вдосконалення системи управління [1].

Вивчення проблем державного управління в системі інформаційно-аналітичного забезпечення сил безпеки України здійснювалося такими дослідниками, як Мацько О.Й., Микусь С.А., Солонніков В.Г., Андрощук О., Грінченко В., Дробаха Г.А., Єрмошин М.О., Смірнов Є.Б., Іохов О.Ю., Лісіцин В.Е., Горєлишев С.А., Бєлай С.В. та іншими.

Система державного управління інформаційно-аналітичним забезпеченням сил безпеки України є складною та багатокомпонентною структурою, яка об'єднує різноманітні інформаційні потоки, аналітичні інструменти та управлінські рішення. Її основна мета — забезпечення своєчасного і точного аналізу даних для прийняття обґрунтованих рішень у сфері національної безпеки.

Ця система охоплює різні державні органи, такі як Міністерство оборони, Службу безпеки України, Міністерство внутрішніх справ та інші спеціалізовані відомства. Кожен з цих органів має власні підрозділи інформаційно-аналітичного забезпечення, які тісно взаємодіють, формуючи єдину стратегію національної безпеки.

Інформаційно-аналітичне забезпечення ґрунтується на сучасних технологіях збору, обробки та аналізу даних, включаючи геоінформаційні системи, розвідувальні інструменти та системи електронної розвідки. Це дозволяє обробляти великі обсяги інформації та вчасно виявляти потенційні

загрози.

Сучасні виклики, такі як кіберзагрози, гібридні війни та міжнародний тероризм, вимагають постійного вдосконалення та адаптації системи інформаційно-аналітичного забезпечення. Основний акцент робиться на впровадженні нових методів аналізу, інтеграції штучного інтелекту та технологій машинного навчання для підвищення ефективності аналітичних процесів.

Інформаційно-аналітичне забезпечення відіграє критичну роль у забезпеченні національної безпеки України. Його значення можна розкрити через кілька ключових аспектів:

Підтримка прийняття рішень: Надання актуальної та точної інформації дозволяє керівництву сил безпеки ухвалювати обґрунтовані рішення у критичних ситуаціях. Це сприяє більш ефективному вирішенню завдань національної безпеки.

Прогнозування та аналітика: Систематичний аналіз даних дозволяє передбачати потенційні загрози та визначати тренди, що дає можливість розробляти превентивні стратегії.

Оперативне реагування: Швидкий доступ до інформації та її аналіз забезпечують оперативну реакцію на надзвичайні ситуації та кризи, що є вирішальним для національної безпеки.

Міжвідомча координація: Ефективна інформаційно-аналітична система забезпечує кращу координацію між різними структурами сил безпеки, створюючи єдиний оперативний простір для реагування на загрози.

Зміцнення міжнародних позицій: Інформаційно-аналітичне забезпечення сприяє формуванню обґрунтованої зовнішньої політики та посиленню міжнародних позицій країни у сфері безпеки і оборони.

Таким чином, інформаційно-аналітичне забезпечення є основою ефективного державного управління у сфері національної безпеки, що дозволяє Україні успішно відповідати на внутрішні та зовнішні виклики.

Система державного управління інформаційно-аналітичним

забезпеченням сил безпеки України складається з кількох ключових елементів, які забезпечують її ефективність і функціональність:

Організаційна структура: Включає різноманітні установи та агентства, що займаються збором, обробкою, аналізом і поширенням інформації. Це можуть бути розвідувальні служби, військові організації, правоохоронні органи та спеціалізовані дослідницькі центри.

Інформаційні ресурси: Включають бази даних, аналітичні звіти, статистичні матеріали, геопросторові дані та інші види інформації, необхідні для аналізу ситуації та підтримки прийняття рішень.

Технологічне забезпечення: Охоплює системи збору даних, обчислювальні мережі, програмне забезпечення для аналізу, комунікаційні технології та системи забезпечення кібербезпеки.

Процедурне забезпечення: Включає стандарти, протоколи і процедури, що регулюють збір, обробку, аналіз, зберігання та розподіл інформації. Ці процедури гарантують точність, конфіденційність та безпеку інформації.

Кадрове забезпечення: Сюди входять фахівці та аналітики, які працюють у системі, включаючи розвідників, аналітиків, програмістів, інженерів та інших експертів, необхідних для ефективної роботи системи.

Координаційні та контрольні механізми: Забезпечують ефективну взаємодію між різними компонентами системи та дозволяють відслідковувати виконання завдань і загальну ефективність системи.

Ці елементи тісно взаємодіють, утворюючи складну та цілісну систему, яка дозволяє органам державного управління України ефективно розвивати та вдосконалювати інформаційно-аналітичне забезпечення сил безпеки.

Інформаційно-аналітичне забезпечення займає центральне місце в процесі прийняття рішень у сфері державного управління, особливо коли мова йде про національну безпеку України. Його значення проявляється через такі ключові аспекти:

Посилення обізнаності керівництва. Інформаційно-аналітичне забезпечення надає керівним органам та силовим структурам всебічне уявлення

про поточну ситуацію, що допомагає чітко розуміти наявні та можливі загрози і виклики. Це забезпечує більш обґрунтоване та інформоване прийняття управлінських рішень.

Оптимізація стратегічного планування. Аналітичні звіти та прогнози, що генеруються в межах інформаційно-аналітичного забезпечення, створюють можливість для розробки довгострокових стратегій і планів, заснованих на точних даних та глибокому аналізі, а не лише на інтуїції або попередньому досвіді.

Підтримка оперативності прийняття рішень. У критичних ситуаціях або під час надзвичайних подій, оперативний доступ до актуальної та точної інформації дозволяє приймати швидкі рішення, що може бути вирішальним для забезпечення безпеки держави та її громадян.

Управління ризиками. Інформаційно-аналітичне забезпечення сприяє виявленню, оцінці та пріоритизації ризиків, а також розробці ефективних стратегій їхньої мінімізації або повної нейтралізації, що є важливим елементом державного управління.

Підвищення рівня міжвідомчої координації. Використовуючи аналітичні дані, можна значно покращити взаємодію між різними відомствами та організаціями, що займаються забезпеченням національної безпеки, що сприяє більш ефективному об’єднанню зусиль і раціональному використанню наявних ресурсів.

Забезпечення об’єктивності та неупередженості. Аналітичні висновки та інсайти дозволяють ухвалювати рішення, базовані на об'єктивному аналізі фактів і даних, що мінімізує вплив суб’єктивних суджень та особистих упереджень на управлінський процес.

Таким чином, інформаційно-аналітичне забезпечення виступає як життєво важливий інструмент в арсеналі державного управління, що надає можливість приймати зважені, своєчасні та ефективні рішення в інтересах національної безпеки та стабільності України.

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 існуючих владних відносин і суспільних цінностей [221].

Основні аспекти моделі інформаційного механізму:

Інституціонально-правовий аспект: Модель включає 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 дозволяє комплексно підходити до вирішення питань національної безпеки.

Використання математичних методів: Аналіз та моделювання використовують кількісні методи для визначення оптимальних рішень і стратегій. Це включає статистичний аналіз, теорію ігор, оптимізаційні моделі тощо, що дозволяє об'єктивно оцінювати різні сценарії та їх 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 дозволяє 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, враховуючи їхні зв’язки з внутрішнім та зовнішнім середовищами, які служать 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 ряд етапів, де кожен включає специфічні операції по обробці інформації. Ці операції визначають необхідні дії на кожному етапі, а також критерії переходу до наступного. Модель прийняття управлінських рішень у сфері національної безпеки здійснюється відповідно до чітко визначеного алгоритму. У випадку необхідності, весь процес може бути повторений, що робить його ітеративним. Процес триває до моменту знаходження оптимального рішення, відповідного встановленим критеріям, з урахуванням часу, доступного для суб’єктів управління.

Формалізація процесу прийняття управлінських рішень у контексті національної безпеки через модель пропонує наступні переваги:

- розгляд процесу як систему з певними входами та виходами, що сприяє структуруванню підходів;
- мінімізація суб’єктивізму у виборі рішень завдяки заміні неоднозначних формулювань на точніші, дозволяє чітко визначати критерії та процедури оцінювання;
- використання математичних методів для визначення оптимальних рішень залежно від складності та специфіки проблем, що дозволяє ефективніше розв’язувати задачі на кожному етапі.

Діяльність суб’єктів державного управління інтегрована в єдину систему, що включає:

- аналіз стану об’єкту управління;
- розроблення та порівняння альтернатив, узгодження з цілями управління;
- оцінка ефективності досягнення цілей;
- вибір оптимальної альтернативи.

Ці кроки включають ряд операцій, які забезпечують послідовне

опрацювання інформації:

- прийом та аналіз інформації на предмет її достовірності та значущості для прийняття рішень;
- оцінка достатності та придатності інформації для всебічного опису управлінської ситуації;
- розробка відповідей на виклики зовнішнього середовища в контексті національних інтересів;
- вибір та реалізація оптимального управлінського рішення за обраними критеріями.

Особливістю зазначеної моделі є взаємозалежність етапів обробки інформації, де кожен наступний етап розвивається з результатів попереднього. Можливо 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 аналізі надходження інформації, що дозволяє 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 служить як всеохоплюючий алгоритм обробки інформації у сфері державного управління.

Специфіка управління у контексті національних інтересів накладає певні вимоги на організацію процесу розроблення та прийняття управлінських рішень. Ієрархія національних інтересів впливає на процес вибору управлінських альтернатив, акцентуючи на їх значущості для національної безпеки. Стратегія дій суб’єктів державного управління включає оцінку потенційних наслідків впровадження кожної стратегії. Окрім того, значний

вплив на визначення національних інтересів та вибір стратегій реалізації чинять зовнішні фактори, що вимагає від системи управління гнучкості та чутливості до інформації, що надходить.

Ситуативна складова моделі має бути максимально відкритою, щоб ефективно реагувати на змінні умови та потреби. Водночас, концептуальна складова, яка базується на державно-владних вимогах, традиційно є більш закритою та статичною. Проте, в умовах значних суспільних змін та глобальних викликів, абсолютна замкненість концептуальної частини є недоречною. Ця частина моделі має швидко адаптуватися до змінюваних ціннісних орієнтацій суспільства та глобальних змін, забезпечуючи відповідність управлінських рішень актуальним потребам і викликам.

Функціонування інформаційного механізму в процесі прийняття управлінських рішень державними органами включає координацію двох основних типів інформаційних потоків. Перший тип – це потоки, які відображають вимоги, що випливають із національних цілей країни, які конкретизовані в законодавстві з питань забезпечення національної безпеки. Другий тип – це потоки інформації, які надають дані про специфічні потреби та обставини, пов’язані з розв’язанням конкретних проблемних ситуацій.

Ці два потоки взаємодіють, забезпечуючи суб’єктам державного управління необхідну інформацію для прийняття відповідальних та ефективних рішень. Потоки, що стосуються законодавчих вимог, допомагають забезпечити, що усі дії уряду відповідають загальним національним напрямкам і законам. Водночас, інформація про конкретні умови та потреби дозволяє адаптувати ці рішення до реальних обставин і специфіки проблем, що підвищує їхню релевантність та ефективність.

Модель інформаційного механізму у процесі прийняття управлінських рішень враховує специфічні характеристики ситуацій, що вимагають рішень, відповідає національним вимогам і визначає задачі для досягнення національних цілей, а також включає критерії для оцінювання альтернатив. Водночас структура моделі розрізняється на відкриту ситуативну складову та

більш закриту концептуальну складову.

Ситуативна складова динамічна і відкрита, що дозволяє їй адаптуватися до змінюваних умов та вимог сучасності. Концептуальна складова, натомість, включає закріплені правові норми, які виступають як фундамент для взаємодії між різними елементами моделі. Ці правові норми служать не тільки для внутрішньої узгодженості дій у контексті національних інтересів, але і забезпечують зв'язок між потребами суспільного розвитку та держави з зовнішнім середовищем.

Така структура моделі забезпечує цілісне і збалансоване врахування як невідкладних, так і стратегічних аспектів управління, дозволяючи ефективно реагувати на виклики та використовувати можливості, що виникають у зовнішньому та внутрішньому середовищах.

Практика свідчить, що визначення методу прийняття рішення залежить від наявного часу, впливу багатьох факторів, які в тому числі описують умови обстановки і стан суб'єкту сил безпеки. В умовах, наприклад, конкретно визначеної обстановки рішення може прийматися шляхом послідовного прийняття часткових рішень, які за рахунок декомпозиції основної задачі забезпечують досягнення загальної мети. При цьому спрощується довготривалий процес прийняття громіздкого рішення. Можна організувати процес прийняття складного рішення шляхом синтезу кінцевого обрису об'єкта управління, якого (обрису) передбачається досягти в ході діяльності. Шляхи набуття обрису, як окремі складові рішення, поєднуються в одному загальному рішенні, пов'язаному з постановкою часткових задач. Іноді взагалі немає потреби проводити значні спеціальні розрахунки, рішення знаходиться на поверхні. У такому випадку рішення приймається на підставі вимог керівних документів і залежить від знань, інтуїції та досвіду людини-експерта, що приймає рішення [233].

Розвиток механізмів у сфері державного управління, особливо у контексті інформаційно-аналітичного забезпечення сил безпеки України, відіграє вирішальну роль у підвищенні ефективності реагування на сучасні виклики та

загрози. Нижче наведено ключові напрями вдосконалення цих механізмів.

Інтеграція сучасних технологій. Впровадження передових технологій, таких як штучний інтелект, машинне навчання, обробка великих даних і кібербезпека, є основоположним для підвищення точності та швидкості збору, аналізу та обробки інформації. Створення інтегрованої інформаційної системи, яка об’єднує дані з різних джерел, включаючи міжнародні, забезпечує комплексний підхід до аналізу ситуацій і дозволяє приймати оперативні управлінські рішення з більшою ефективністю.

Підвищення кваліфікації фахівців. Навчання та підвищення рівня професійної підготовки працівників, які беруть участь в інформаційно-аналітичному забезпеченні, є важливим кроком для забезпечення високої компетентності в застосуванні новітніх технологій і сучасних методик аналізу. Це сприяє підвищенню якості виконання їхніх завдань та адаптації до нових викликів.

Удосконалення координаційних механізмів. Важливим аспектом є розробка та вдосконалення механізмів координації між різними органами державної влади. Це включає покращення обміну інформацією та спільного використання ресурсів, що дозволяє досягти більшої синергії у забезпеченні національної безпеки.

Адаптація законодавчої бази. Оновлення та адаптація законодавства до сучасних вимог є необхідною умовою для забезпечення відповідності новітнім стандартам інформаційної безпеки, приватності та захисту даних. Це також забезпечує правову підтримку для впровадження нових технологій і підходів у державному управлінні.

Удосконалення методів аналізу. Поглиблення та вдосконалення методів і підходів до аналізу даних, включаючи розробку спеціалізованих аналітичних інструментів та моделей для оцінки ризиків і прогнозування розвитку ситуацій, є важливим для підвищення точності та надійності прийняття рішень.

Ці напрями розвитку механізмів сприяють значному підвищенню ефективності державного управління в Україні, особливо у сфері національної

безпеки, дозволяючи більш оперативно, прогнозовано та результативно реагувати на сучасні виклики.

Розроблена модель функціонування та вдосконалення механізмів державного управління інформаційно-аналітичним забезпеченням сил безпеки України представлена на рисунку 5.3 [208].

Рис. 5.3 – Структурна схема моделі функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

Органи державного управління, відповідальні за керування силами безпеки України, формують механізми, через які здійснюється управлінський вплив на відповідні суб’єкти безпеки. Організаційні механізми державного

управління забезпечують створення та вдосконалення організаційної структури кожного суб'єкта в залежності від його діяльності, завдань та функцій. Правові механізми управління відповідають за формування нормативно-правової бази, яка визначає функції та завдання суб'єктів сил безпеки.

Дотримання законності та виконання поставлених завдань у сфері сил безпеки України забезпечується через механізми контролю. Фінансова підтримка діяльності цих суб'єктів здійснюється за допомогою механізмів фінансового управління. Інформаційно-аналітичне забезпечення підпорядковане цим механізмам, що створюють інформаційні потоки, здійснюють моніторинг та обробку даних, що є ключовим аспектом управління суб'єктами сил безпеки.

Сучасні виклики, з якими стикається Україна, вимагають підвищення ефективності службово-бойової діяльності сил безпеки. Одним з основних шляхів досягнення цього є вдосконалення системи управління. Інформаційно-аналітична підтримка діяльності сил безпеки забезпечує координацію, ефективність та безпеку в процесах обробки і використання інформаційних ресурсів, що має вирішальне значення для досягнення цілей державного управління [205, 216].

Інформаційно-аналітична система сил безпеки України є критичним елементом у забезпеченні національної безпеки та оборони держави. Ефективність цієї системи безпосередньо залежить від якості державного управління, здатного забезпечувати безперервне та надійне функціонування інформаційних та аналітичних потоків, необхідних для ухвалення оперативних і стратегічних рішень.

Проте система стикається з низкою значних проблем та суперечностей, які потребують негайного вирішення. Серед основних викликів варто виділити відсутність цілісної стратегії розвитку, обмежені технологічні та фінансові ресурси, складнощі в обробці великих обсягів даних, залежність від кваліфікації персоналу, а також високі ризики, пов'язані з людським фактором. Додатково, існує значний розрив між теоретичними напрацюваннями в галузі

управління та їх практичним застосуванням, що ускладнює інтеграцію нових технологій та методів аналізу даних у реальну діяльність.

Для подолання цих проблем необхідний комплексний підхід, що включає міжвідомчу координацію та безперервний моніторинг. Такий підхід дозволить не лише оптимізувати роботу системи інформаційно-аналітичного забезпечення сил безпеки України, але й значно підвищити ефективність державного управління в цій сфері, забезпечуючи своєчасну та адекватну відповідь на сучасні виклики безпеки.

Органи державного управління, відповідальні за керування силами безпеки України, розробляють та впроваджують механізми, за допомогою яких здійснюється управлінський вплив на суб'єкти сил безпеки. Організаційні механізми державного управління відповідають за формування структур кожного суб'єкта залежно від його функцій, завдань та призначення. Правові механізми, своєю чергою, забезпечують створення правової бази для виконання функцій та завдань суб'єктів сил безпеки. Дотримання законності та виконання поставлених завдань контролюється через механізми нагляду. Фінансове забезпечення діяльності суб'єктів сил безпеки здійснюється через механізми фінансового управління. Інформаційно-аналітичне забезпечення підпорядковується цим механізмам, створюючи інформаційні потоки, які здійснюють моніторинг та обробку даних, що є критично важливими для ефективного управління суб'єктами сил безпеки.

Сучасні виклики, які стоять перед Україною, підкреслюють необхідність підвищення ефективності службово-бойової діяльності сил безпеки. Одним із шляхів досягнення цього є вдосконалення системи управління. Інформаційно-аналітична підтримка діяльності сил безпеки забезпечує координацію, ефективність та безпеку в обробці та використанні інформаційних ресурсів, що має вирішальне значення для досягнення цілей державного управління.

Організаційні структури та ролі в управлінні інформаційними ресурсами державного управління відіграють ключову роль у забезпеченні ефективної реалізації стратегій інформаційно-аналітичного забезпечення. Вони сприяють

досягненню координації, підвищенню ефективності та забезпеченню безпеки в процесах обробки та використання інформаційних ресурсів, що є критично важливим для досягнення основних цілей державного управління.

5.4 Стратегія розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України

Стратегія розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України передбачає реалізацію кількох ключових напрямків, кожен з яких спрямований на підвищення ефективності та безпеки державних структур у сучасних умовах.

Забезпечення ефективної взаємодії між підрозділами сил безпеки. Це досягається шляхом впровадження інтегрованих інформаційних систем, які дозволяють оперативно обмінюватися даними та аналітичними звітами між різними відомствами. Така взаємодія підвищує координацію дій і сприяє більш злагодженій роботі у сфері національної безпеки.

Впровадження передових технологій обробки даних. Використання штучного інтелекту, машинного навчання та великих даних дозволить значно підвищити ефективність аналітичної роботи. Завдяки цим технологіям стає можливим більш глибокий і точний аналіз великих обсягів інформації, що допомагає приймати обґрунтовані управлінські рішення.

Постійне підвищення кваліфікації персоналу. Особлива увага приділяється організації навчання співробітників сил безпеки, зокрема у сфері новітніх технологій та аналітичних методик. Це забезпечує високу компетентність кадрів та їхню здатність ефективно використовувати сучасні інструменти в роботі.

Розробка та впровадження заходів кібербезпеки. У сучасних умовах захист інформаційних систем від зовнішніх та внутрішніх загроз є пріоритетом. Розробка комплексних заходів кібербезпеки дозволить мінімізувати ризики несанкціонованого доступу до інформаційних ресурсів та забезпечити безпеку

даних.

Актуалізація законодавчої бази. Оновлення нормативно-правової бази у сфері державного управління інформаційно-аналітичним забезпеченням сприятиме підвищенню ефективності управлінських процесів. Це включає встановлення чітких правил обробки, розподілу та захисту інформації відповідно до сучасних стандартів.

Розвиток міжнародного співробітництва та партнерства. Співпраця з міжнародними організаціями та іншими країнами у сфері обміну досвідом, технологіями та інформацією дозволить Україні впроваджувати найкращі світові практики та підвищувати ефективність інформаційно-аналітичного забезпечення.

Впровадження систем моніторингу та оцінки. Для аналізу ефективності роботи інформаційно-аналітичних систем необхідно впровадити системи моніторингу та оцінки, які дозволять оперативно реагувати на виявлені недоліки та приймати своєчасні управлінські рішення.

Реалізація цієї стратегії потребує комплексного підходу, що включає технічні, організаційні, нормативно-правові та освітні аспекти. Важливо враховувати всі ці фактори, щоб забезпечити стійкість та ефективність інформаційно-аналітичного забезпечення сил безпеки України.

Прогнозування розвитку інформаційно-аналітичного забезпечення на наступні десять років вимагає розгляду кількох основних аспектів.

Підвищення ефективності ІАЗ завдяки прогресу в галузі штучного інтелекту, машинного навчання, обробки великих даних та квантових обчислень. Очікується, що ШІ стане ключовим інструментом у роботі з даними, забезпечуючи автоматизацію рутинних процесів, аналіз даних і прогнозування. Це дозволить значно підвищити оперативність і точність інформаційно-аналітичної роботи.

Посилення уваги до кібербезпеки у зв’язку зі зростанням загроз кібератак. Розвиток механізмів виявлення та запобігання вторгненням, а також реагування на інциденти стане пріоритетом для забезпечення надійного захисту

інформаційних ресурсів.

Впровадження єдиної інформаційної системи, що забезпечує обмін даними між різними відомствами та рівнями влади. Це сприятиме підвищенню ефективності ІАЗ і дозволить забезпечити більш оперативну і злагоджену роботу міжвідомчих структур.

Розширення міжвідомчого та міжнародного співробітництва для обміну досвідом та інформацією. Це сприятиме впровадженню новітніх технологій і методів в Україні, а також дозволить застосовувати найкращі міжнародні практики в ІАЗ.

Посилення акценту на освіту та підготовку фахівців у галузі ІТ, аналітики даних та кібербезпеки. Освіта і постійне підвищення кваліфікації кадрів стане критично важливим для забезпечення якісного ІАЗ. Програми навчання будуть орієнтовані на розвиток відповідних навичок, що дозволить ефективно відповідати на сучасні виклики.

Адаптація законодавства для регулювання питань ІАЗ, зокрема в галузі захисту даних, приватності та використання ШІ. Це має важливе значення для створення збалансованого правового поля, яке буде підтримувати розвиток інформаційно-аналітичних систем.

Зростання важливості етичних аспектів, особливо у контексті використання ШІ та аналітики даних. Прозорість, відповідальність та дотримання прав людини стануть основними принципами, які необхідно враховувати у розвитку ІАЗ.

Загалом, очікується, що інформаційно-аналітичне забезпечення стане більш інтегрованим, автоматизованим і захищеним, з акцентом на співпрацю, освіту та етичні стандарти [73, 125, 233].

Щоб отримати доступ до нових технологій, держава повинна розробити та реалізувати комплексну стратегію, що передбачає такі ключові кроки:

Інвестиції у наукові дослідження та вищу освіту. Необхідно створити міцну базу для технологічних інновацій шляхом фінансування університетів, дослідницьких інститутів та лабораторій. Це дозволить країні розвивати

власний науково-технічний потенціал і забезпечити основу для створення інноваційних технологій.

Підтримка досліджень та розробок (R&D). Держава повинна активно підтримувати підприємства та організації, які займаються дослідженнями та розробками в ключових технологічних сферах. Це може включати надання податкових пільг, грантів, субсидій та інших стимулів для заохочення інновацій як у приватному, так і державному секторах. Важливо створити інноваційне середовище, де університети, дослідницькі інститути, промисловість і уряд зможуть тісно співпрацювати для обміну знаннями та комерціалізації технологій.

Підготовка кваліфікованих фахівців. Важливим аспектом є забезпечення підготовки висококваліфікованих спеціалістів у галузі високих технологій через освітні програми, стажування, майстер-класи та перепідготовку кадрів. Це дозволить формувати людський капітал, здатний підтримувати та розвивати нові технології.

Захист інтелектуальної власності. Створення чіткого та ефективного законодавства для захисту прав на інтелектуальну власність є критично важливим. Це забезпечить інвесторам упевненість у тому, що їхні інновації будуть захищені, що сприятиме залученню інвестицій у дослідження та розробки.

Міжнародне співробітництво у галузі науки та технологій. Держава повинна активно сприяти міжнародній співпраці для обміну знаннями, участі в глобальних дослідницьких проектах та доступу до передових інновацій. Це дозволить прискорити впровадження нових технологій та підвищити рівень технологічного розвитку країни.

Просування цифрової трансформації. Важливо стимулювати цифрову трансформацію в усіх секторах економіки, що сприятиме швидшому впровадженню та поширенню нових технологій. Це створить умови для більш ефективного управління та розвитку технологічного потенціалу.

Підтримка стартапів та технологічних підприємств. Необхідно

створювати сприятливі умови для розвитку стартапів, надаючи їм доступ до фінансування, консультаційних послуг та ринків збуту. Це сприятиме появі нових ідей та їхній успішній реалізації.

Регулярне оцінювання та аналіз ефективності технологічних програм. Важливо здійснювати постійний моніторинг та оцінку ефективності програм з метою їхньої оптимізації. Це дозволить своєчасно коригувати стратегії та політики для досягнення максимального результату.

Реалізація цих заходів надасть державі можливість активно розвивати та впроваджувати новітні технології, що значно зміцнить економіку та підвищить конкурентоспроможність країни на глобальному ринку.

Прогнози щодо отримання нових технологій зосереджуються на кількох ключових напрямках, у яких очікуються значні інноваційні прориви:

Розвиток штучного інтелекту та машинного навчання. Очікується, що алгоритми стануть ще більш досконалими, дозволяючи їм виконувати складніші завдання – від автоматизації виробництв до управління міською інфраструктурою.

Квантові обчислення. Ця технологія обіцяє революційні зміни у сфері обробки даних, забезпечуючи можливість вирішення завдань, які нині недоступні для класичних комп’ютерів, таких як криптографія, матеріалознавство та фармацевтика.

Інтернет речей та цифрові технології. Поглиблення інтеграції цифрових технологій у повсякденне життя та роботу, розвиток інтернету речей дозволить пристроям та системам тісніше взаємодіяти, збираючи та аналізуючи дані в режимі реального часу.

Ці прогнози відображають основні напрями досліджень і можуть змінюватися залежно від технологічного прогресу, ринкових умов та політичних рішень. Успіх у впровадженні нових технологій залежатиме від здатності держави та приватного сектору інвестувати у дослідження, підтримувати інновації та створювати сприятливі умови для комерціалізації технологій.

Фундаментальні дослідження в інформатиці та обчислювальній техніці. Прогрес у цих сферах сприяє створенню потужніших і ефективніших інструментів для обробки великих обсягів інформації. Це дозволяє інформаційно-аналітичним службам працювати з даними більш оперативно та точно. Фундаментальні науки, такі як фізика і хімія, дозволяють краще зрозуміти складні природні та технологічні системи. Це розуміння може бути використане для створення більш точних моделей та інструментів для аналізу складних даних і явищ.

Інтеграція наукових дисциплін. Розвиток фундаментальних наук сприяє інтеграції різних наукових напрямків, що є необхідним для комплексного аналізу складних питань. Міждисциплінарний підхід посилює можливості інформаційно-аналітичних служб у розв’язанні складних завдань.

Освіта та підготовка фахівців. Фундаментальні науки відіграють вирішальну роль у підготовці кваліфікованих кадрів, які володіють знаннями і навичками, необхідними для проведення інформаційно-аналітичної роботи. Глибоке розуміння цих наук дозволяє аналітикам критично оцінювати інформацію, виявляти приховані зв’язки та тренди.

Вплив нових технологій на інформаційно-аналітичні служби. Розвиток нанотехнологій та створення нових матеріалів може призвести до появи нових пристроїв і методів збору, зберігання та передачі даних, що розширить можливості інформаційно-аналітичних служб.

Таким чином, фундаментальні науки є наріжним каменем розвитку інформаційно-аналітичної діяльності, надаючи інструменти, методи та знання, необхідні для ефективного аналізу даних і вирішення складних завдань [222].

Розробка стратегії для вдосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України може базуватися на використанні SWOT-аналізу, який досліджує сильні сторони, слабкості, можливості та загрози [223].

Сильні сторони (Strengths):

Кваліфікований персонал. Наявність досвідчених і висококваліфікованих

фахівців у сфері безпеки та інформаційно-аналітичної роботи є значною перевагою для ефективного функціонування системи; Міжнародне партнерство. Співпраця з міжнародними організаціями та союзниками забезпечує можливість обміну інформацією, доступу до технологічних ресурсів та посилення технічної підтримки; Адаптивність. Система здатна оперативно реагувати на зміни у безпековому середовищі, що дозволяє швидко адаптувати стратегії до нових загроз.

Слабкі сторони (Weaknesses):

Технологічне відставання. Використання застарілого обладнання та програмного забезпечення суттєво обмежує можливості системи щодо ефективної обробки даних та реагування на сучасні загрози; Обмеженість фінансування. Недостатній рівень фінансування не дозволяє проводити своєчасну модернізацію технологічних засобів та забезпечувати належну підготовку персоналу; Координаційні проблеми між відомствами. Відсутність чітко налагодженої координації та ефективної взаємодії між різними відомствами сил безпеки знижує загальну ефективність функціонування системи.

Можливості (Opportunities):

Технологічний прогрес. Впровадження сучасних технологій, таких як штучний інтелект, машинне навчання та засоби кібербезпеки, може суттєво підвищити ефективність аналітичної роботи та забезпечити якісніший захист даних; Міжнародна підтримка та фінансування. Можливість залучення додаткових ресурсів, фінансування та технологічної допомоги від міжнародних партнерів є суттєвим фактором для модернізації системи; Нормативно-правові реформи. Оновлення та удосконалення законодавчої бази дозволить більш точно регулювати діяльність інформаційно-аналітичної системи та забезпечить підтримку сучасних вимог у сфері національної безпеки.

Загрози (Threats):

Кіберзагрози. Зростання кібератак та можливість витоку конфіденційної інформації є серйозною загрозою для функціонування системи; Політична

нестабільність. Внутрішні політичні зміни та міжнародні конфлікти можуть негативно вплинути на стратегію національної безпеки та роботу інформаційно-аналітичних структур; Технологічна залежність. Залежність від іноземних технологій та постачальників може створити додаткові ризики у разі виникнення кризових ситуацій або загострення міжнародних конфліктів.

Стратегія розвитку механізмів державного управління інформаційно-аналітичною системою сил безпеки України повинна включати наступні елементи:

Інвестиції в освіту та науку. Підтримка вищих навчальних закладів та наукових інститутів сприятиме розвитку власного інноваційного потенціалу у сфері технологій та аналітики.

Розвиток технологічної бази. Модернізація апаратного та програмного забезпечення є критично важливою для ефективного функціонування системи.

Міжнародна співпраця. Поглиблення партнерства з міжнародними організаціями дозволить Україні отримати доступ до новітніх технологій та підтримки в обміні інформацією.

Адаптивна організаційна структура. Структура управління повинна бути організована таким чином, щоб забезпечувати можливість оперативного реагування на зміни в безпековому середовищі.

Сучасна нормативно-правова база. Оновлення законодавства повинно враховувати новітні вимоги у сфері інформаційно-аналітичного забезпечення, регулюючи механізми управління з урахуванням сучасних викликів та потреб системи національної безпеки України.

Ця стратегія дозволить зміцнити державні механізми управління та підвищити їхню ефективність в умовах сучасних викликів [212].

Матриця SWOT описує стратегічні заходи, які можуть бути реалізовані шляхом знаходження оптимальної комбінації між сильними та слабкими сторонами як внутрішніми факторами та можливостями і загрозами як зовнішніми факторами. Можливі SWOT-стратегії представлені в таблиці 5.3.

Таблиця 5.3 – Можливі стратегії SWOT

SWOT стратегії	Сильні сторони	Слабкі сторони
Можливості	Стратегія I Сильні сторони – можливості	Стратегія II Слабкі сторони – можливості
Загрози	Стратегія III Сильні сторони – загрози	Стратегія IV Слабкі сторони – загрози

Розроблені стратегії представлені на рисунках 5.4-5.7.

Стратегія I. Стратегія «сильні сторони – можливості» (безпрограшна стратегія) вказує на зовнішні можливості, які підтримують сильні сторони. Це наступальна стратегія, яка застосовується в ситуації, коли суб'єкт ще вибудовує свої позиції і, отже, максимально концентрується на напрямках, де можливості підтримують сильні сторони.

Рисунок 5.4 – Стратегія 1. Порівняльні переваги: співставлення сильних сторін, щоб максимально використати можливості

Рисунок 5.5 – Стратегія 2. Виклики*:* Як подолати слабкі сторони (внутрішні фактори) через використання можливостей (зовнішні фактори).

Стратегія II. Стратегія «слабкі сторони – можливості» вказує на способи, як слабкі сторони можуть бути подолані, щоб розблокувати нові можливості, або як існуючі можливості зможуть ліквідувати/зменшити слабкі сторони суб’єкта. Це більш оборонний стратегічний підхід, при якому, після того, як наявні шанси були використані, ведеться пошук нового місця для участі шляхом усунення власних слабких сторін.

Стратегія III. Стратегія «сильні сторони – загрози» визначає шляхи використання сильних сторін для зменшення або усунення впливу загроз. Ця комбінація також є оборонним варіантом. Вона може бути застосована до розвинених організацій з сильною конкурентною позицією, які працюють над тим, щоб запобігти певним (очікуваним) негативним зовнішнім впливам, використовуючи власні сильні сторони.

Рисунок 5.6 – Стратегія 3. Вплив: визначає способи, як сильні сторони можуть бути використані для того, щоб обмежити або усунути загрози

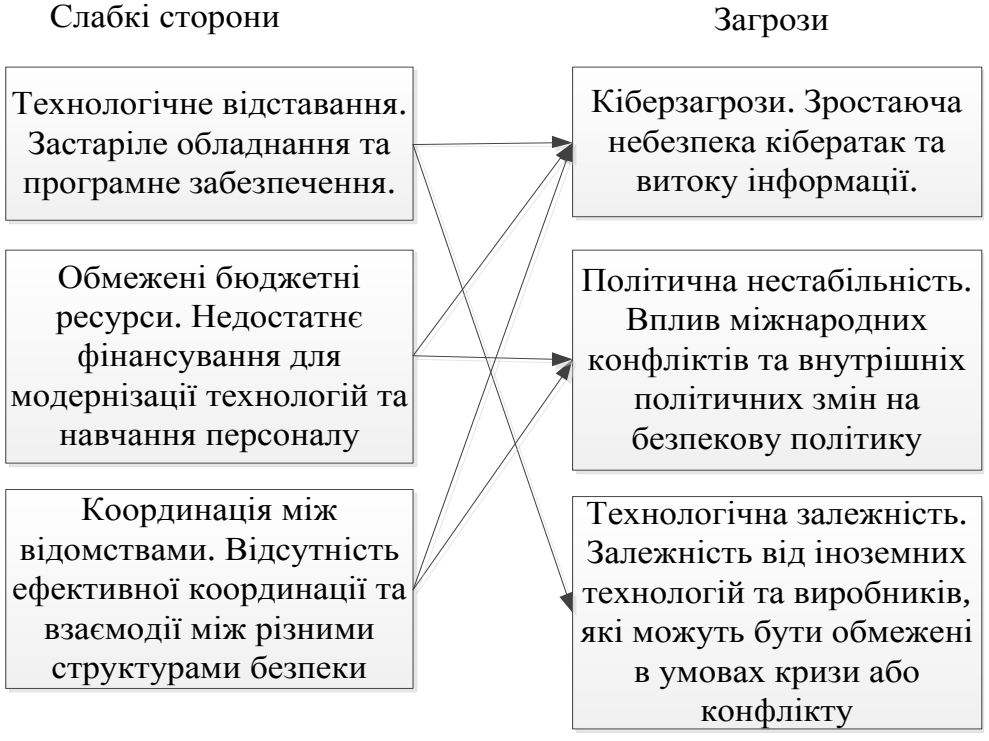

Рисунок 5.7 – Стратегія 4.Ризики: Вплив загроз, які підкріплені слабкими сторонами

Стратегія IV. Стратегія «слабкі сторони – загрози» вказує на план усунення слабких сторін з метою запобігання вразливості організації до зовнішніх загроз. Це повністю оборонна стратегія, яка може бути оптимальною лише для дуже добре розвинених організацій, яким потрібно лише підтримувати свої хороші позиції по відношенню до конкурентів.

Розроблені стратегії та подальші дослідження дозволять визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Ці заходи спрямовані на підвищення ефективності діяльності сил безпеки через покращення процесів збору, аналізу та використання інформації. Важливим аспектом є інтеграція нових технологій та аналітичних методів у повсякденну практику сил безпеки, що забезпечить їхню адаптивність до сучасних викликів і загроз. Реалізація цих заходів може тривати довгий термін, тому для їх успішного втілення у життєдіяльність сил безпеки потрібний довготривалий стабільний політичний курс держави.

Висновки до розділу 5

1. Один з важливих аспектів функціонування національної системи кібербезпеки полягає в стратегічному плануванні та програмно-цільовому забезпеченні розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кібербезпеки. Сили безпеки України активно застосовують інформаційно-аналітичну діяльність для виявлення та аналізу внутрішніх і зовнішніх загроз національній безпеці. Ця діяльність охоплює збір інформації з різноманітних джерел, таких як відкриті дані, соціальні мережі, розвідувальні матеріали, а також інформацію, отриману від міжнародних партнерів.

2. Розглянуто наявні підходи до планування інформаційно-аналітичної діяльності в силових структурах. До цих підходів належать: стратегічне планування, оперативне планування, сценарне планування та ризик-орієнтоване

планування. Використання цих підходів забезпечує ефективне управління ресурсами, адаптацію до змін у середовищі та високу готовність сил безпеки до різноманітних викликів.

3. Визначено ключові напрямки для підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України. Ці напрямки включають обґрунтування теоретичних основ функціонування системи інформаційно-аналітичного забезпечення сил безпеки, розробку методологічних засад розвитку цієї системи з метою забезпечення обороноздатності держави, а також створення механізмів державного управління інтеграцією технологій в інформаційно-аналітичну систему сил безпеки України та розробку інформаційного механізму управління цією системою.

4. Однією з проблем державного управління системою інформаційно-аналітичного забезпечення сил безпеки України є нестача кваліфікованих фахівців у галузі інформаційних технологій та аналітики, що обмежує здатність сил безпеки ефективно обробляти та аналізувати дані. На основі цього, було розвинуто концепцію підготовки кадрів у системі інформаційно-аналітичного забезпечення сил безпеки України. Ця концепція базується на використанні інформаційних технологій для автоматизації управління персоналом, управління компетенціями та планування навчальних потреб, а також застосуванні аналітичних інструментів для прогнозування потреб у персоналі, аналізу тенденцій на ринку праці, оцінки ефективності персоналу та ухвалення обґрунтованих рішень.

Система державного управління інформаційно-аналітичним забезпеченням сил безпеки України складається з кількох ключових компонентів, що забезпечують її ефективність та функціональність. До цих компонентів належать: організаційна структура, інформаційні ресурси, технологічне забезпечення, процедурне забезпечення, кадрове забезпечення, механізми координації та контролю. Ці елементи взаємодіють, утворюючи комплексну систему, яка дозволяє державним органам України ефективно

розвивати інформаційно-аналітичне забезпечення сил безпеки.

5. Обґрунтовано загальнодержавну модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Ця модель передбачає формування організаційної структури інформаційно-аналітичного забезпечення, контроль за функціонуванням системи, вдосконалення нормативно-правової бази, підготовку та перепідготовку кадрів у цій сфері, а також фінансове забезпечення. Ця модель дозволяє оцінювати впливи державного управління на систему інформаційно-аналітичного забезпечення сил безпеки з метою подальшого вдосконалення цієї діяльності.

На основі SWOT-аналізу розроблено стратегії розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Зокрема, було розроблено такі стратегії:

Стратегія 1 «Порівняльні переваги». Орієнтована на використання сильних сторін системи для максимального використання можливостей розвитку інформаційно-аналітичного забезпечення.

Стратегія 2 «Виклики». Спрямована на подолання слабких сторін (внутрішніх факторів) системи через використання можливостей (зовнішніх факторів).

Стратегія 3 «Вплив». Визначає способи, як сильні сторони можуть бути використані для обмеження або усунення загроз функціонуванню системи інформаційно-аналітичного забезпечення.

Стратегія 4 «Ризики». Аналізує вплив загроз, підкріплених слабкими сторонами функціонування системи.

Було проведено комплексне дослідження стратегічних підходів до розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Це дослідження включало розробку комплексних стратегій, базованих на інструментарії SWOT-аналізу, що дозволяє визначити оптимальні шляхи удосконалення управлінських механізмів у цій сфері.

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 поставлені завдання дають підстави сформулюватитакі висновки та практичні рекомендації.

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

2. Досліджені засади функціонування системи підтримки прийняття рішень у державному управлінні силами безпеки України. Для цього визначена роль та місце математичних методів, інформаційних технологій та моделювання процесів та явищ, що характерні для систем державного управління.Встановленішляхи покращення системи підтримки прийняття рішень у державному управлінні силами безпеки України за рахунок

підвищення компетентності та професіоналізму персоналу, застосування сучасних інформаційних технологій таких як штучний інтелект, обробки великих масивів даних та покращення якості прийнятих рішень.Удосконалені механізми державного управління системою підтримки прийняття рішень за рахунок покращення кадрових, організаційних, правових, технічних механізмів державного управління.

3. Визначені аспекти функціонування підсистеми захисту інформації в суб'єктах сил безпеки України. З урахуванням викликів з якими зіткнулась наша держава, були вдосконалені механізми державного управління системами захисту інформації сил безпеки України. Обґрунтовані вимоги до підсистеми захисту інформації та вимоги до захищеностіінформації, що циркулює в системахдержавного управління силами безпеки України. Встановлені фактори,що впливають на ефективність державного управління підсистемами захисту інформації. За рахунок комплексного поєднання організаційних, правових, кадрових механізмів державного управління надані пропозиції з вдосконаленняпідсистеми 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 шляхом оптимізації інформаційних потреб органів управління.Удосконалення організаційних механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України здійснено за рахунок 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.

5. Встановлені шляхи розвитку правового механізму функціонування системи інформаційно-аналітичного забезпечення сил безпеки України за

рахунок комплексного підходу, що включає законодавчі, технічні, та організаційні заходи. З цією метою досліджено міжнародний досвід в сфері нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки, який дозволяє визначити передові практики та інноваційні підходи, які можуть бути адаптовані та впроваджені в Україні. Шляхом 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 удосконалена нормативно-правова база функціонування системи інформаційно-аналітичного забезпечення сил безпеки України, що дозволило надати пропозиції з визначення інформаційних потреб органів управління силами безпеки, узгодження вітчизняних стандартів зі стандартами НАТО, а також здійснити адаптаціюнормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України до стандартів НАТО.

6. Обґрунтовано підходи до застосування геоінформаційних систем в державному управлінні силами безпеки України, які дозволяють підвищити ефективність прийняття рішень та планування у сфері державного управлінні силами безпеки України. Обґрунтування зазначених підходівотримано шляхом подальшого розвитку механізмів стратегічного планування та оперативного реагування, що сприяє підвищенню обороноздатності країни та захисту національних інтересів. Також визначено вплив механізму застосування геоінформаційних систем у державному управлінні силами безпеки України настан забезпечення державної безпеки. Встановлено впливгеоінформаційних систем на ефективність управління в секторі безпеки та оборони України.

7. Надано пропозиції з удосконалення підготовки кадрових ресурсів 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 прийняття обґрунтованих рішень. Надані 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, розробки та імплементації програм управління компетенціями, використанні інструментів на основі штучного інтелекту, впровадженні аналітичних інструментів для збору та аналізу даних про персонал.Створені практичні рекомендаціїдозволяютьпідвищити ефективність та адаптивність кадрової політикиза рахунок впровадження сучасних ІТ-рішень, розвитку компетенцій та професійного навчання, використання зворотного зв'язку з роботодавцями.

8. Сформульовані 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 методологічні засади розвитку системи інформаційно-аналітичного забезпечення сил безпеки щодо забезпечення обороноздатності держави, а також розробленні механізми державного управління системою інтеграції технологій в систему інформаційно-аналітичного забезпечення сил безпеки України та запропоновані інформаційні механізми державного управління інформаційно-аналітичного забезпечення сил безпеки України. Підвищення ефективності планування інформаційно-аналітичної діяльності в силах безпеки України проведено за рахунок удосконалення 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 та технологій; створення механізмів для забезпечення ефективної міжвідомчої координації та обміну інформацією; інтеграція та модернізація технологічної інфраструктури; інвестиції в

оновлення та розвиток єдиної інтегрованої технологічної платформи для обробки та аналізу даних; розробка та впровадження єдиної інформаційно-аналітичної платформи для збору, обробки, аналізу та розподілу інформації між усіма зацікавленими структурами безпеки; уніфікація форматів даних; стимулювання розробки вітчизняних інноваційних рішень в області інформаційної безпеки та аналітики.

9. Обґрунтована загальнодержавна модель функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Модель базується на механізмах: формування організаційної структури кожного суб'єкту 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 в сфері інформаційно-аналітичного забезпечення; фінансового забезпечення. Зазначена модель дозволила 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», та дозволили визначити шляхи удосконалення механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрощук О., Грінченко В. Модель інформаційно-аналітичного забезпечення управлінської діяльності органу охорони державного кордону. *Збірник наукових праць Національної академії державної прикордонної служби України (Серія «Військові науки»)*. 2020. 1(82). С. 5–18.

2. Андрощук О.С., Мисик А. Б. Інформаційно-аналітичне забезпечення інтегрованого управління кордонами. Навчальний посібник. – Хмельницький : Видавництво НАДПСУ, 2016. – 199 с.

3. Антонов В.О. Конституційно-правові засади національної безпеки України: монографія; наук. ред. Ю.С. Шемшученко. К.: ТАЛКОМ, 2017. 576 с.

4. Антонюк В.В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. Електронний журнал «Державне управління: удосконалення та розвиток», № 8, 2014. http://www.dy.nayka.com.ua/?op=1&z=747

5. Бабков Ю. П., Бацамут В. М., Дробаха Г. А. Визначення переліку інформаційно-розрахункових задач і моделей для перспективних комплексів засобів автоматизації різних ланок управління внутрішніх військ. *Честь і закон.* 2012. № 1. С. 64–70.

6. Бабков Ю. П., Горєлишев С. А., Побережний А. А. Комплексний підхід до використання елементів інформаційно-аналітичної системи для підтримки прийняття рішень на застосування угруповань Національної гвардії України. *Збірник наукових праць Національної академії Національної гвардії України*. 2015. Вип. 1 (25). С. 31–39.

7. Бабков Ю.П., Адамчук М.М. Підходи до прийняття рішень при реагуванні на кризові ситуації, що загрожують національній безпеці України. Стан та перспективи реформування сектору безпеки і оборони України: матеріали міжнар. наук.-прак. конф. (м. Київ, 25–26 листопада 2016 р.). К.: ПАЛИВОДА А. В., 2016. С. 24-27.

8. Бандурко О. М. Оперативно-розшукова діяльність: підручник. Харків: Вид-во Нац. Ун-ту внутр. Справ, 2002. Ч. 1. 336 с.

9. Барабаш Ю. Л. Основи теорії оцінювання ефективності складних систем. Барабаш Ю. Л. – К: вид. НАОУ, 1999. – 39 с.

10. Белай С. В. Прогнозирование кризисных ситуаций в современном обществе с помощью использования инновационных информационных технологий //PolitBook. – 2013. – №. 2. – С. 132-141.

11. Бєлай С. В., О. Ю. Іохов, Олещенко О. А. Модель інформаційно-аналітичного забезпечення системи управління військового командування під час дій з охорони правопорядку. *Честь і закон.* 2022. Випуск №2(81). С. 36-41.

12. Бєлай С.В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика: монографія. Х.: Національна акад. НГУ, 2015. 349 с.

13. 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 листопада, 2023р.). Київ:НА СБУ, 2024, Вип.2. с. 36.

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

15. Бєлай С.В., Споришев К.О. Ефективність державного управління у сфері моніторингу та аналізу сучасних викликів державній безпеці України від інформаційних загроз. *Наукові перспективи (Серія «Державне управління»).* 2023. Випуск 12(42). С. 71–79.

16. Бєлай С.В., Споришев К.О. Стан інформаційно-аналітичного забезпечення в суб’єктах сил безпеки. Збірник тез ІІІ Міжнародної науково-практичної конференції «Публічне управління в Україні: виклики сьогодення та

глобальні імперативи». (м. Хмельницький, 8 лютого 2024 року). Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2024. С. 149–151.

17. Бєлай С.В., Споришев К.О., Онопрієнко О.С. Генезіс інформаційно-аналітичного забезпечення службово-бойової діяльності сил безпеки України: сучасні виклики державного управління. *Актуальні питання у сучасній науці (Серія «Державне управління»).* 2024. Вип. № 1(19). С. 105–113.

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

19. Бильчук В.М. Метод определения показателей эффективности и риска принятия решений при проведении операции в условиях нестохастической неопределенности / В.М. Бильчук // Системи обробки інформації. – Х.: ХВУ, 2003. – № 3. – С. 11 – 22.

20. Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів : монографія. Луганськ : Луган. Держ. Ун-т внутр. Справ ім. Е. О. Дідоренка, 2009. 664 с.

21. Богуш В. М., Кривуца В. Г., Кудін А. М., Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В. Г. К., 2004. 508 с.

22. Бочковий О.В. Застосування інформаційно-аналітичних технологій в оперативно-розшуковій діяльності. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск № 4. 2010. С. 272-279.

23. В Днепропетровске создан “Центр безопасности региона”. РИА новости Украина [Електронний ресурс]. Режим доступу: http://rian.com.ua/politics/20150311/364661938.html (дата звернення: 14.07.2021). – Загл. с экрана.

24. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с.

25. Вертузаєв М. С., Юрченко О. М., Стрельбицька Л. М. Застосування новітніх технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Боротьба з організованої злочинністю і корупцією (теорія і практика)*. 2006. № 13. С. 165-173.

26. Войтко О. В., Солонніков В. Г. Державна інформаційна політика – основа забезпечення інформаційної безпеки в умовах гібридної війни // XII Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей (Київ, 26.03.2021). URL: https://academy.ssu.gov.ua/uploads/p_ 57_53218641.pdf

27. Войтко О.В., Грозовський Р.І., Кацалап В.О. та ін.. Основи кібербезпеки та кібергігієни: Навч. посібник.- К.: НУОУ ім. І. Черняховського, 2019. - 46 с.

28. Войтко О.В., Кацалап В.О., Цурко Ю.В. Стратегія і тактика інформаційної боротьби**:** курс лекцій. – Київ: НУОУ ім. І. Черняховського, 2021. − 108 с.

29. Волянська-Савчук Л. В. Сучасне поняття системи управління персоналом / Л.В. Волянська-Савчук // Науковий вісник Херсонського державного університету. Сер. : Економічні науки. – 2014. – Вип. 7(2). – С. 149–153.

30. Гавриш О.А. Технології управління персоналом.: монографія / О.А. Гавриш, Л.Є. Довгань, І.М. Крейдич, Н.В. Семенченко – Київ : НТУУ «КПІ імені Ігоря Сікорського», 2017. – 528 с.

31. Геоінформаційні технології в екології : Навчальний посібник / Пітак І.В., Негадайлов А.А., Масікевич Ю.Г., Пляцук Л.Д., Шапорев В.П., Моісеєв В.Ф/.– Чернівці:, 2012.– 273с.

32. Герасимов Б.М. Человеко-машинные системы принятия решений и искусственного интеллекта / Б.М. Герасимов, В.А. Тарасов, И.В. Токарев. – К.: Наук. думка, 1993. – 184 с.

33. Глобальна та національна безпека: підручник / авт. кол. : В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. / за заг. ред. Г.П.Ситника. Київ: НАДУ. 2016. 784 с.

34. Глушков В.М.. Введение в АСУ / В.М. Глушков. Київ: Техніка, 1972. 312с.

35. Горбань О.М., Бахрушин В.Є. Основи теорії систем і системного аналізу: Навчальний посібник. – Запоріжжя: ГУ “ЗІДМУ”, 2004. – 204 с.

36. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України. К.: Євроантлантікінформ. 2007. 592 с.

37. Горбулін В.П., Литвиненко О.В. Національна безпека: український вимір; Інститут проблем національної безпеки Ради національної безпеки і оборони України. К.: Інтертехнологія, 2008. 104 с.

38. Горбунов Е.А. Самоорганизация систем и прогнозирование военно–политических и социальных аспектов / Е.А. Горбунов. – К.: Ника–Центр, 2005. – 320 с.

39. Горєлишев С. А., Іванченко А. О., Башкатов Є. Г.. Програмний комплекс «Кропива» як елемент перспективної автоматизованої системи управління Національної гвардії України. Честь і закон № 4 (87). 2023, С.22-29.

40. Городнов В. П. Моделирование боевых действий частей, соединений и объединений войск ПВО. Харьков : ВИРТА ПВО, 1987. 380 с.

41. Городнов В., Побережний А., Суконько С. Геоінформаційна модель інформаційно-аналітичного забезпечення процесів охорони важливих державних об’єктів у разі нападу озброєних злочинців. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2020. Вип. 79(1). С. 33–46.

42. Городнов В.П. Моделі визначення ефективності та синтезу структури органу інформаційної підтримки рішень у системі управління Збройними Силами / В.П. Городнов, О.П.Михайленко // Наука і оборона. – 2001.– № 2.– С. 39 – 43.

43. Горошко И. Методы и анализы данных в правоохранительной деятельности. АС-траст 2007 г. 224 с.

44. Гриценко А., Кожієл М., Єрмолаєв А., Флурі Ф. Нормативно-правова база в галузі безпеки і оборони України. 2-ге вид., допов. К.: Центр дослідження армії, конверсії та роззброєння. 2012. 820 с.

45. Діджиталізація та права людини: збірник тез Міжнародної науково-практичної інтернет-конференції (м. Хмельницький, 30 березня 2021 року). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова. 2021. 395 с.

46. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України в сфері кібербезпеки. Юридичний часопис НАВС. 2018. №1. С. 141-153.

47. Державне управління: словник-довідник / за заг. ред. В.М. Князева, В. Д. Бакуменка. К.: УАДУ. 2002. 228 с.

48. Довідник НАТО. Брюссель: НАТО, 2001. 600с.

49. Доктрина "Зв'язок та інформаційні системи" затверджена Головнокомандувачем Збройних Сил України від 02.07.2020 №15841/С Центральне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України, 78 с.

50. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту. URL: http://domarev.kiev.ua.

51. Дробаха Г.А. Вплив співвідношення стійкості і безперервності на характеристики управління та шляхи розробки методики розрахунку значень показників процесу безперервності управління з'єднаннями та частинами корпусу ППО під час бойових дій / Г.А. Дробаха, В.П. Варакута // Зб. наук. пр. ХВУ. – Х.: ХВУ, 2002. – № 3 (41). – С. 17–19.

52. Дробаха Г.А., Ткаченко В.І., Смірнов Є.Б. Шляхи формалізації процесів багатокритеріальної оцінки в системі підтримки прийняття рішень //Системи озброєння і військова техніка – 2007. – Випуск 2(10). – С. 2–8.

53. Дума В.В. Правозастосування та форми його здійснения. Правова Інформатика. 2006. №3(11). С. 61-64.

54. Енциклопедія освіти / Акад. пед. наук України ; головний ред. В. Г. Кремень. – К. : Юрінком Інтер, 2008. – 1040 с.

55. Єманов В.В., Бєлай С.В., Тробюк В.І. Обґрунтування пропозицій з удосконалення системи підготовки та перепідготовки персоналу сектору безпеки і оборони України в умовах відсічі збройної агресії. *Вісник Національного університету цивільного захисту. Державне управління*. Харків, 2023. Вип.1(18). С. 271–279.

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

57. Єманов В.В., Споришев К.О., Шаповалов О.І. Проблеми інформатизації процесів управління системою технічного обслуговування та ремонту автобронетанкової техніки Національної гвардії України. *Честь і закон*. 2022. №3(82). С. 108–116.

58. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с.

59. Забезпечення інформаційної безпеки держави: Навчальний посібник /В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

60. Забезпечення інформаційної безпеки держави: підручник. В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; за заг. ред. О.А. Семченка. Київ: ПАТ «Віпол», 2015. 672 с.

61. Загорка О.М., Мосов С.П., Сбитнєв А.І., Стужук П.І. Елементи дослідження складних систем військового призначення. Навчальний посібник. – К.: Видання академії, 2005. – 99с.

62. Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV. URL:https://zakon.rada.gov.ua/laws/show/638-15#Text

63. Закон України «Про державну службу» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/889-19#Text

64. Закон України «Про державну таємницю» від 21.01.1994 року № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 11.02.2024).

65. Закон України «Про засади інформаційної безпеки України»від 28.05.2014 №4949 URL:https://ips.ligazakon.net/document/JG3TH00A?an=3

66. Закон України «Про національну безпеку України» від 21.06.2018 року№ 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text(дата звернення: 12.02.2024).

67. Закон України «Про оборону України» від 6.12.1991№ 1932-XII.URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text

68. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. https://zakon.rada.gov.ua/laws/show/2163-19#Text

69. Закон України «Про розвідку» від 17.09.2020 року № 912-IX. URL:https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 11.02.2024).

70. Закон України. Про засади інформаційної безпеки України. https://ips.ligazakon.net/document/JG3TH00A?an=3

71. Залож В. В., Телелим В. М. Основи стратегічного планування в ДПСУ. Навчальний посібник. Вид. НАДПСУ 2019.

72. Застосування сучасних інформаційних технологій у науковій діяльності : підручник / О. Й. Мацько, С. А. Микусь, В. Г. Солонніков та ін.. К.: НУОУ ім. І. Черняховського, 2021. 340 с.

73. Застосування сучасних інформаційних технологій у науковій діяльності : підручник / [О. Й. Мацько, С. А. Микусь, В. Г. Солонніков, Т. П. Пащенко та ін.].– К. : НУОУ ім. І. Черняховського, 2019. – 368 с.

74. Звіт Національної поліції України про результати роботи у 2022 році https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf

75. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Національний університет "Львівська політехніка" Політичні науки Vol. 2, № 1, 2016. https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf

76. Імітаційне моделювання у практиці підготовки військ: навч. посіб. /колектив авторів; за заг. ред. О. Ю. Пермякова. – К.: НУОУ ім. Івана Черняховського, 2015. – 120 с.

77. Інформаційна безпека держави у контексті протидії інформаційним війнам: навчальний посібник. За ред. В. Б. Толубка. Київ: НАОУ, 2004. 315 с.

78. Інформаційна безпека держави: навчальний посібник. О. К. Юдін, В. М. Богуш. Харків: Консум, 2005. 576 с.

79. Інформаційна безпека: підручник. В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. Під ред. В. В. Остроухова. Київ: Ліра-К, 2021. 412 с.

80. Інформаційна загроза. URL:https:// http://surl.li/tpavi

81. Інформаційно–аналітичне забезпечення діяльності військ: Навчальний посібник. Київ: вид. НАОУ, 2004.

82. Інформаційно-аналітичне забезпечення інтегрованого управління кордонами : навчальний посібник / О. С. Андрощук, В. А. Стрельбіцький, В. С. Кушнір та ін. Хмельницький : Видавництво НАДПСУ, 2016. 200 с.

83. Камінська Н.В. Проблеми імплементації міжнародно-правових стандартів у сфері кібербезпеки. Розвиток науки і практики міжнародного права: матеріали міжнар. науково-практ. конфер., присвяченій 25-річчю УАМП. К., 2018.

84. Капля А.В. Кібербезпека як важливий аспект сьогодення. URL https://conf/ztu.edu.ua/wp-contentuploads 2021-01/29-2.pdf

85. Катеринчук І. С., Литвин М. М., Мисик А. Б. Методики оперативно-тактичних розрахунків : навчальний посібник. Хмельницький : Видавництво

Національної академії Державної прикордонної служби України імені Богдана Хмельницького, 2004. 82 с.

86. Кириленко В. А., Городнов В. П., Литвин М. М., Іщенко Д. В. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (в контексті завдань національної безпеки України в прикордонній сфері) : монографія. Хмельницький : Видавництво НАДПСУ, 2009. 472 с.

87. Кириченко І. О., Горелишев С. А., Побережний А. А. Технологічні основи інформаційно-аналітичного забезпечення службово-бойової діяльності сил охорони правопорядку: монографія. Х.: Акад.ВВ МВС України, 2013. 292 с.

88. Кіберзлочини у 2020 році завдали збитків на трильйон доларів.https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolarıv-doslidzhennia-55857766

89. Кількість хакерских так за місяць війни зросла у тричі, але більшість з них неуспішні, – Держспецзв'язок. URLhttps://espreso.tv/kilkist-khakerskikh-atak-za-misyats-viynı-zrosia-utrichi-ale-bilshist-z-nikh-neuspishni-derzhspetszvyazku

90. Климчук О. О. Забезпечення інформаційної безпеки держави :підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України»,2015. – 672 с.

91. Кобко Є.В. Моніторинг загроз національній безпеці держави; зарубіжний досвід та українські реалії. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 1(106). С.123-134.

92. Ковальов І. В. Волобуєв Р. В.Механізм синтезу інформаційно-аналітичного забезпечення Національної гвардії України в умовах надзвичайних ситуацій. *Науковий вісник: Державне управління*. 2020. № 3(5).С. 3–15.

93. Ковальчук Я. Принципи інформаційно-аналітичного забезпечення діяльності органів Національної поліції України. *Підприємництво, господарство і право*. 2020. № 9. С. 132–136.

94. Коломійцев О. В., Обрядін В. В., Горєлишев С. А., Інформаційно-аналітичні технології забезпечення прийняття військового рішення за стандартами НАТО під час виконання завдань у сфері державної безпеки. Безпека Держави. 2023. Вип. 1 (1) С. 27-39.

95. Конституційне право України: підручник / Під ред. В.Ф. Погорілка. К.: Наукова думка, 2003. 732 с.

96. Конституція України – [Електронний ресурс]. URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-v.

97. Концепція реформування Державної служби спеціального зв'язку та захисту інформації України.Указ Президента Українивід 22 жовтня 2021 року № 544/2021.URL: https://zakon.rada.gov.ua/laws/show/544/2021#Text

98. Концепція розвитку Національної гвардії на період до 2020 року.Розпорядження Кабінета Міністрів України від 1 лютого 2017 р. № 100-р. URL: https://zakon.rada.gov.ua/laws/show/100-2017-%D1%80#Text

99. Концепція військової кадрової політики в системі Міністерства оборони України на період до 2028 року https://www.mil.gov.ua/content/tenders/koncepcia_kadr_29012024.pdf

100. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008. 382 с.

101. Криворучко О. М. Управління персоналом підприємства: навч. посібник / О.М.Криворучко, Т.О.Водолажська – Х. : ХНАДУ, 2016. – 200 с.

102. Криза правоохоронної системи України: монографія/ За загальною редакцією В.В. Євдокімова, Д.О. Грицишина. – Житомир: Видавничий дім «Бук-друк», 2023. – 584 с.

103. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

104. Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І.Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія. Львів : Сполом, 2020. 418 с.

105. Крушельницька О.В., Мельничук Д.П. Управління персоналом: Навчальний посібник. – К., Кондор. – 2006., 308 с.

106. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

107. Лісовська Ю.П. Кібербезпека: ризики та заходи навч. посібник. К. Видавничий дім «Кондор, 2019. 272 с.

108. Маковій В. П., Усата Г. О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави/ *Морська безпека та оборона*, № 1. 2023 С. 62-68.

109. Малиновський В. Я.. Державне управління: Навчальний посібник.- Вид. 2-ге, доп. та перероб. К.: Атіка, 2003. 576 с.

110. Маркова С. В. Управління персоналом: навчально-методичний посібник для студентів освітньо-кваліфікаційного рівня «бакалавр» / С. В. Маркова, О.М. Олійник. – Запоріжжя: ЗНУ, 2013. – 80 с.

111. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу:http://www.dsaua.org/index.php?option=com_

112. Машков О. А., Нижник Н. Р. Системний підхід в організації державного управління: навч. посіб. / за заг. ред. Н. Р. Нижник. К.: УАДУ, 1998. 160 с.

113. Мельник Д. С. Актуальні загрози національній безпеці України в інформаційній сфері: питання визначення та протидії. Інформаційна безпека людини, суспільства, держави. 2021. № 1–3 (31–33). С. 16-27.

114. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: http://www.ua. textreferat.com/referat-7471.html

115. Микусь С.А., Солонніков В.Г., Крайнов В.О., Даник Ю.Г. та ін. Інформаційні технології інформаційно-аналітичного забезпечення органів

управління військами (силами): Підручник.– К.: НУОУ ім. І. Черняховського, 2018. - 352 с.

116. Михайлова Л. І. Управління персоналом : навч. посіб. / Л. І. Михайлова. – К. : ЦНЛ, 2007. – 296 с.

117. Моделювання бойових дій військ (сил) протиповітряної оборони та інформаційне забезпечення процесів управління ними (теорія, практика, історія розвитку): монографія /В.П. Городнов, Г.А. Дробаха, М.О. Єрмошин та ін. Харків: ХВУ, 2004. 410 с.

118. Морозов А.О., Кузьменко Г.Є., Литвинова В.А. Ситуаційні центри. Теорія і практика. Київ. СП «Інтертехнодрук». 2009. 348 с.

119. Мужанова Т.М. Інформаційна безпека держави. Навчальний посібник – К.: ДУТ, ННІЗІ, 2019. – 131 с.

120. Наказ Міністерства оборони Уаїни «Положення про науково-інформаційну діяльність у Збройних Силах України» від 27.07.2016 № 385.URL: https://zakon.rada.gov.ua/laws/show/z1172-16#Text (дата звернення: 12.02.2024).

121. Наказ Міністерства оборони Уаїни «Про затвердження Концепції інформатизації Міністерства оборони України» від 17.09.2014 № 650. URL: https://zakon.rada.gov.ua/rada/show/v0650322-14#Text (дата звернення: 12.02.2024).

122. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім “Гельветика”, 2017. 168 с.

123. Носач А.В. Загрози національній безпеці як обов’язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність Україи. Право і суспільство. 2019. №3. С. 50–56.

124. Організація інформаційно-аналітичного забезпечення органів управління військами (силами): Підручник / Ю.Г. Даник, С. А. Микусь, В. Г. Солонніков, В.О. Крайнов та ін..– К.: НУОУ ім. І. Черняховського, 2019. − 237 с.

125. Основи інформатизації Національної гвардії України: навч. посіб. / Г. А. Дробаха, О. А. Олещенко, О.Ю. Іохов,В. Е. Лісіцин та ін. – Х. : НАНГ України, КП “Міська друкарня”, 2016. – 366 с.

126. Основи інформаційно-аналітичного забезпечення органів управління. Навчальний посібник. Частина перша. Київ: вид. НАОУ, 2004.

127. Основи інформаційно-аналітичної діяльності в Державній прикордонній службі України: підручник / О.М. Шинкарук, Л.М. Артюшин. – Хмельницький: Видавництво НАДПСУ, 2017. – 380 с.

128. Основи моделювання бойових дій військ. підручн. – К: НАОУ,

129. Основні принципи геоінформаційних систем: навч. посібник / В. Д. Шипулін; Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2010. – 313 с.

130. Островський С. О. Поняття та зміст інформаційно-аналітичної діяльності як елемента інформаційно-аналітичного забезпечення взаємодії Національної гвардії України із правоохоронними органами та Збройними Силами України. *Актуальні проблеми вітчизняної юриспруденції.* 2017. № 4. С. 92–96.

131. Павлов В.В. Синтез стратегий в человеко-машинных системах / В.В. Павлов. – К.: Вища шк., 1989. – l62 с.

132. Пащенко Т. П., Микусь С.А., Солонніков В. Г. та ін. Методи моделювання бойових дій військ (сил): навчальний посібник. – К.: НУОУ ім. Івана Черняховського, 2021. − 262 с.

133. Пащенко Т.П. Сучасні методи підтримки прийняття рішень: Курс лекцій. – К.: НУОУ, 2011.

134. Пермяков О. Ю., Рябцев В. В., Вернер І. Є. Інформаційні технології в збройній боротьбі: тенденції та перспективи використання. Наука і оборона. 2004. № 2. С. 23-28.

135. Пермяков О. Ю., Сбітнєв А. І.. Інформаційні технології і сучасна збройна боротьба.– Луганськ: Знання, 2008. – 204 с.

136. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222

137. Пожар О. М. Управління персоналом : навчально-методичний посібник для самостійного вивчення дисципліни / О.М. Пожар, С.В. Зеленський; Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2008. – 199 с.

138. Політологія URL:.https://pidruchniki. com/15341220/politologiya/

139. Положення про порядок надання Державній прикордонній службі та виконання нею доручень правоохоронних і розвідувальних органів щодо осіб, які перетинають державний кордон України. Постанова Кабінету Міністрів України№ 280 від 17 квітня 2013 року. https://zakon.rada.gov.ua/laws/show/280-2013-п#Text

140. Положення про інформаційно-аналітичну систему «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» Наказ Міністерства внутрішніхсправ Українивід 30 березня 2022 року № 207 https://zakon.rada.gov.ua/laws/show/z0425-22#Text

141. Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». Наказ МВСУ від 03.08.2017 № 676 https://zakon.rada.gov.ua/laws/show/z1059-17#Text

142. Постанова Кабінету Міністрів України «Про затвердження Положення про Державне агентство з питань електронного урядування України» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/492-2014-п#Text

143. Постанова Кабінету Міністрів України «Про затвердження Положення про Національне агентство України з питань державної служби» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/500-2014-п#Text

144. Почепцов Г. Г. Інформаційна політика: навчальний посібник. Київ: Знання, 2008. 663 с.

145. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім “Києво-Могилянська академія”, 2015. – 497 с.

146. Примуш Р.Б. Інформаційне забезпечення стратегічного планування в сфері національної безпеки. *Державне управління: удосконалення та розвиток.* 2018. №7.URL: http://www.dy.nayka.com.ua/pdf/7_2018/41.pdf

147. Про Національну програму інформатизації. Закон України № 2807-IX від1 грудня 2022 року https://zakon.rada.gov.ua/laws/show/2807-20#Text

148. Про вищу освіту. Закон України від 01.07.2014р. № 1556. URL:https://zakon.rada.gov.ua/laws/show/1556-18#Text

149. Про внесення змін до Закону України “Про Раду національної безпеки і оборони України” щодо вдосконалення координації і контролю у сфері національної безпеки і оборони. Закон України від 25.12.2014 р. № 43. URL:http://zakon0.rada.gov.ua/laws/show/43-19/paran20?nreg=43-19&find=1& text

150. Про Державну прикордонну службу України. Закон України № 661-IV від 3 квітня 2003 року https://zakon.rada.gov.ua/laws/show/661-15#Text

151. Про Державну прикордонну службу України. Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/ 661-15

152. Про затвердження «Положення про базу даних реєстру атестованих судових експертів Експертної служби МВС». Наказ Міністерства внутрішніх справ України №19 від 15.01.2018 року. https://zakon.rada.gov.ua/laws/show/z0146-18#Text

153. Про затвердження Доктрини інформаційної безпеки України. Указ Президента України від 25.02.2017 № 47/2017. Офіційний вісник України. 2017. № 20. Ст. 554.

154. Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». Наказ Міністерства внутрішніх справ

України № 534 від 28.06.2023 року. https://zakon.rada.gov.ua/laws/show/z1486-23#Text

155. Про затвердження Положення про базу даних «Відомості про осіб, які перетнули державний кордон України» Наказ Адміністрації державної прикордонної служби України № 472 від 25.06.2007. https://zakon.rada.gov.ua/laws/show/z0765-07#Text

156. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів. Постанова КМУ від 14.11.2018 р. № 1024 https://zakon.rada.gov.ua/laws/show/1024-2018-п#Text

157. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України № 80/94-ВР від 5 липня 1994 року. https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

158. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua/laws/show/n0004525-14

159. Про інформацію. Закон України № 2657-XII від 2 жовтня 1992 року https://zakon.rada.gov.ua/laws/show/2657-12#Text

160. Про концепцію Національної програми інформатизації. Закон України №75/98-ВР від 4 лютого 1998 року. https://zakon.rada.gov.ua/laws/show/75/98-вр#Text

161. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/

162. Про Національну поліцію. Закон України. https://zakon.rada.gov.ua/laws/show/580-19#Text

163. Про Національну поліцію: Закон України від 02.07.2015 № 580. URL: URL:https://zakon.rada.gov.ua/laws/show/580-19.

164. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами,

внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.

165. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний вісник України. 2017. № 91. Ст. 2765.

166. Про основні засади забезпечення кібербезпеки України: Закон України https://zakon.rada.gov.ua/laws/show/2163-19/conv@n94

167. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. Закон України від 09 січня 2007 року № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text =%E1%E5% E7%E.

168. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України. https://zakon.rada.gov.ua/laws/show/537-V#Text

169. Про Службу безпеки України. Закон України від 25.03.1992 № 2229. URL: https://zakon.rada.gov.ua/laws/show/ 2229-12.

170. Про Стратегічний оборонний бюлетень України. Указ Президента України від 06.06.2016р. № 240/2016. URL: http://zakon4.rada.gov.ua/laws/show/240/2016.

171. Про Стратегію інформаційної безпеки. Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

172. Про Стратегію національної безпеки України. Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року. Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documen ts/3922020-35037.

173. Проблеми захисту інформаційного простору України: монографія. В. П. Горбулін, М. М. Биченок / Ін-т проблем нац. безпеки. Київ: Інтертехнологія, 2009. 136 с.

174. Пустощі чи прелюдія до війни? Хакерські атаки на Україну. https://www.radiosvoboda.org/a/khakerski-ataky-na-ukrayınu/31709601.html

175. Рахманов В., Ясенко С. Удосконалення освітньої діяльності для кадрового менеджменту в Збройних Силах України. *Військова освіта*. 2021. № 2 (44). С. 194-204.

176. Розроблення пропозицій щодо створення автоматизованої системи управління силами охорони правопорядку із забезпечення громадської безпеки звіт про НДР (“АСТРА”) (заключ.) / Нац. акад. Національної гвардії України; кер. М. Ю. Яковлев, відп. викон. С. А Горєлишев № держреєстрації 0121U100590. Харків, 2021. 169с.

177. Рульєв В.А. Гуткевич С.О. Мостенська Т.Л. Управління персоналом: Навч. посіб. – К.: КОНДОР, 2012. – 324 с.

178. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18 – 23.

179. Саганюк Ф., Павліковський А., Щипанський П., Павленко В. Оборонний огляд: український вимір 2014-2018: монографія. за заг. ред. д. військ. н., проф. І. Руснака. Київ: МО та ГШ ЗС України, НУОУ, 2019. 196 с.

180. Сайт Державної служби України з питань геодезії, картографії та кадастру [Електронний ресурс]. – Режим доступу: https://e.land.gov.ua

181. Сайт Національного агентства з питань державної служби України [Електронний ресурс]. – Режим доступу: https://nads.gov.ua/misiya-nads

182. Сайт «Prozorro» [Електронний ресурс]. – Режим доступу: https://prozorro.gov.ua/uk

183. Сайт «Військовий кур’єр». «Автоматизована система управління військами – зброя перемог». [Електронний ресурс]. – Режим доступу:URL:https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/ (Дата звернення 12.02.2024).

184. Сайт «ДССЗЗІ України». Досвід війни: які виклики стоять перед державою та бізнесом у кіберпросторі. URL: https://cip.gov.ua/ua/news/dosvid-viini-yaki-vikliki-stoyat-pered-derzhavoyu-ta-biznesom-u-kiberprostori

185. Сайт «УНІАН». 10 викликів кібербезпеки: експерти розповіли, до чого готуватися користувачам та компаніям. URL: https://www.unian.ua/science/10-viklikiv-kiberbezpeki-eksperti-rozpovili-do-chogo-gotuvatisya-koristuvacham-ta-kompaniyam-12033828

186. Сайт Equity. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу: https://equity.law/press-center/publications/1169.html

187. Сайт Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/statics/cyber-protection

188. Сайт Державної служби статистики України [Електронний ресурс]. – Режим доступу: https://www.ukrstat.gov.ua/operativ/operativ2021/

189. Сайт електронної платформи «Дія» [Електронний ресурс]. – Режим доступу: https://diia.gov.ua

190. Сайт журналу «Infocity». Cisco Visual Networking Index. [Електроний ресурс]. – Режим доступу: https://infocity.tech/2018/12/cisco-vni-k-2022-polzovateljami-interneta-stanut60-mirovogo-naselenija/.

191. Сайт Міністерства цифрової трансформації України [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/ministry

192. Свідоцтво про авторське право на твір №96078 від 17.02.2020 р. "Комп'ютерна програма "Когнітивна ІТ платформа ПОЛІЕДР" ("КІТ ПОЛІЕДР") ("POLYHEDRON") Автори. Стрижак О. Є., Глоба Л. С., Величко В. Ю., Попова М. А. та ін. Офіційний бюлетень №57 (31.03.2020). С. 402–403.

193. Семенко Є. Ю. Науково-методичні основи формування архітектури інформаційно-аналітичної системи для підтримання та прийняття рішень по застосуванню Національної гвардії України під час супроводження спеціальних вантажів. *Честь і Закон*. 2022. №2. С. 68–77.

194. Семенко Є. Ю. Онтологічне представлення процесів супроводження спеціальних вантажів підрозділами Національної гвардії України. *Честь і Закон*. 2022. № 1(80). С. 20–31.

195. Семенко Є. Ю., Яковлев М. Ю., Стрижак О. Є. Метод ранжування варіантів структури інформаційно-аналітичної системи Національної гвардії України на етапі її створення. Міжнародна науково-технічна конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» зб. тез доп. міжн. наук.-практ. конф. м. Харків: НА НГУ, 15 бер. 2020 р. С. 116–117.

196. Синицина Н. Г., Нові підходи до управління людськими ресурсами в управлінні освітою. *Державне управління: удосконалення та розвиток*. № 11, 2011.

197. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія. О. В. Левченко. Житомир: Вид. «Євро-Волинь», 2021. 172 с.

198. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади). Підручник. К.: НАДУ, 2011. 730 с.

199. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади). Підручник. К.: НАДУ, 2011. 730 с.

200. Сліпченко Т. Кібербезпека як складова системи захиста національної безпеки: европейський досвід. URL: http://dspace.wunu.edu.ua/bitstream/316497/38497/1/Сліпченко.pdf

201. Словник основних термінів та скорочень, які застосовуються в НАТО. – К.: «МП Леся», 2004. – 568 с.

202. Слово і діло. Аналітичний портал. https://www/slovoidilo.ua /2012/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vinax

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

204. Споришев К.О. Аналіз стану системи інформаційно-аналітичного забезпечення сил безпеки України. Сучасні аспекти модернізації науки: стан,

проблеми, тенденції розвитку: матеріали XLI-ої Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Анкара (Туреччина): ГО «ВАДНД», 07 лютого 2024 р. С. 64–68.

205. 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 XLIV-ої Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Умео (Швеція): ВАДНД, 07 травня 2024 р. С. 20–23.

206. 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 XLII-ої Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Мілан (Італія): ВАДНД, 07 березня 2024 р. С. 39–41.

207. Споришев К.О. Економічна складова механізмів державного управління інформаційно-аналітичним забезпеченням. Публічне управління у сфері цивільного захисту: освіта, наука, практика збірник матеріалів міжнародної науково-практичної інтернет-конференції, м. Харків, 29 березня 2024 р. / за заг. ред. С. М. Домбровської. – Харків : НУЦЗУ, 2024. – с. 245.

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

209. 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://nayka.com.ua/index.php/dy/article/view/2998/3034

210. Споришев К.О. Інформаційні механізми державного управління інформаційно-аналітичним забезпеченням сил безпеки України. Сучасні

аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XLIII-ої Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Пештера (Болгарія): ВАДНД, 07 квітня 2024 р. С. 41–44.

211. Споришев К.О. Інформаційно-аналітичне забезпечення діяльності військових формувань України. Збірник тез доповідей XI міжнародної науково-практичної конференції "Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів" 28жовтня 2022 року м. Харків – Х. : Національна акад. НГУ. – с. 287.

212. Споришев К.О. Інформаційно-аналітичні технології сил безпеки у парадигмі державного управління. *Наукові інновації та передові технології (Серія «Управління та адміністрування»).* 2024. Випуск № 1(29). С. 128–136.

213. Споришев К.О. Математичні моделі системи імітаційного моделювання JCATS. Збірник тез доповідей XII міжнародної науково-практичної конференції "Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів" 27 жовтня 2023 року м. Харків – Х. : Національна акад. НГУ. – с. 314.

214. Споришев 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.

215. Споришев К.О. Організаційні аспекти управління інформаційними ресурсами. *Наукові перспективи (Серія «Державне управління»).* 2024. Випуск 2(44). С. 466–475.

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

217. Споришев К.О. Підсистеми захисту інформації в системі державного управління силами безпеки України. *Інвестиції: практика та досвід.* 2024. Вип. 4. С. 224–228.

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

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

220. 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 XXI століття: збірник тез доповідей Всеукраїнської науково-практичної конференції, 7-8 грудня 2023 року. – Житомир: Житомирська політехніка, 2023. С. 340–344.

221. Споришев К.О. Проблемні питання розвитку інформаційно-аналітичного забезпечення Національної гвардії України // V Всеукраїнська науково-практична конференція кафедри тактики командно-штабного факультету Національної академії Національної гвардії України 26 листопада 2020 року м. Харків – Х. : Національна акад. НГУ, 2020. – с. 134.

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

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

224. 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: Збірник тез доповідей Всеукраїнської науково-практичної конференції (Україна, м. Харків, 09 лютого 2021 року). – Х.: НА НГУ, 2021. – С. 322-323.

225. Споришев К.О., Семенко Є.Ю., Майборода І.М. Тенденції застосування систем управління силами відомств охорони правопорядку провідних країн світу. Інтегровані інтелектуальні робото технічні комплекси (ІІРТК-2020). Збірник тез тринадцятої міжнародної науково-практичної конференції 19-20 травня 2020 р., Київ, Україна. – К.: НАУ, 2020. – С.293–295.

226. Стратегія кібербезпеки України (2021-2025роки) URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

227. Стратегія національної безпеки України: введена у дію Указом Президента від 26.05.2015 р. № 287/2015. Офіційний вісник України, 2015. № 43, Ст. 1353.

228. Стрижак О. Є. Онтологічні інформаційно-аналітичні системи. *Радіоелектронні і комп'ютерні системи.* 2014. № 3 (67). С. 71–76.

229. Стрижак О. Є. Трансдисциплінарна інтеграція інформаційних ресурсів [Текст]: автореф. дис. ... д-ра техн. наук : 05.13.06 / Стрижак Олександр Євгенійович ; Нац. акад. наук України, Ін-т телекомунікацій і глобал. інформ. простору. – Київ, 2014. – 47 с.

230. Субач І. Ю., Рябцев В. В., Голуб А. І. Модель показників ефективності системи інформаційно-аналітичного забезпечення прийняття рішення. Праці Військового Інституту Телекомунікації та Інформатизації. Київ : ВІТІ НТУУ "КПІ", 2005. Вип. 1. С. 27-37.

231. Сурмин Ю.П. Теория систем и системный анализ: учебн. пособие / Ю.П. Сурмин – К.: МАУП, 2003. – 368 с.

232. Теоретичне обґрунтування складу та елементів пунктів управління (основних та допоміжних) Національної гвардії України різних рівнів при виконанні службово-бойових завдань: звіт про НДР (шифр “Едельвейс”) (заключ.). Нац. акад. Національної гвардії України; кер. Г.А. Дробаха, вик. С.А. Горєлишев, О.А.Олещенко, А.А.Побережний та ін. – держ. облік. № 0116U003651. Х., 2018. 336 с.

233. Теорія прийняття рішень органами військового управління: монографія / В.І. Ткаченко, Є.Б. Смірнов та ін.; За ред. В.І. Ткаченка, Є.Б. Смірнова. Х.: ХУ ПС, 2008. 542 с.

234. Теплицька А.О. Програмно-цільове планування у реалізації державних програм розвитку. Інвестиції: практика та досвід. № 22. 2013. С.55-58.

235. Типове Положення Інформаційно-аналітичного підрозділу органу військового управління. – К.: МОУ, 2018. – 12 с.

236. Ткаченко В.І. Аналіз принципів побудови інтелектуальних систем управління ВПС збройних сил іноземних країн/ В.І. Ткаченко, В.І. Карпенко, Є.Б. Смірнов, В.О. Нерубацький // Системи управління, навігації та зв’язку. – К.: ЦНДІ навігації і управління, 2008. – Вип. 2 (6). – С. 79 – 83.

237. Ткаченко В.І. Використання нечітких множин в алгоритмах обробки інформації автоматизованих систем управління військами / В.І. Ткаченко, Є.Б. Смірнов, А.В. Тристан // Перспективи розвитку озброєння і військової техніки в Збройних Силах України: Збірка тез доповідей Першої Всеукраїнської науково-практичної конференції. – Лв.: ЛІСВ «ЛП», 2008. – С. 163.

238. Ткаченко В.І. Метод вибору раціональної за ефективністю стратегії управління в ході збройної боротьби в умовах її нечіткого інформаційного ресурсу / В.І. Ткаченко, В.М. Більчук, Н.І. Літвінець, Є.Б. Смірнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2007. – Вип. 9 (67). – С. 2–10.

239. Ткаченко В.І. Метод поліваріантного аналізу і альтернативного вибору стратегії поведінки військ на етапі завчасної підготовки до бойових дій

// Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2008. – Вип. 5(72). – С. 2 – 5.

240. Ткаченко В.І. Методика визначення раціонального оперативного шикування Військ (сил) ППО на оперативно–стратегічному напрямку / В.І. Ткаченко // Збірник наукових праць ХВУ. – Х.: ХВУ, 2000. – Вип. 3 (29). – С. 3 – 11.

241. Ткаченко В.І. Обґрунтування структури та раціональної побудови системи ППО України.: методичні рекомендації / В.І. Ткаченко. – Х.: ХВУ, 2002. 25 с.

242. Ткаченко В.І. Оцінка ефективності прийняття рішень щодо оперативного управління в умовах нестохастичної невизначеності інформаційного забезпечення / В.І. Ткаченко, В.М. Більчук, Є.Б. Смірнов // Системи озброєння і військова техніка. 2008. № 1 (13). С. 2 – 9.

243. Ткаченко В.І. Рекомендації щодо створення формалізованого середовища процесів підготовки й прийняття рішень як основної складової інформаційно-аналітичної системи забезпечення процесів управління угрупованнями Повітряних Сил // Системи озброєння і військова техніка. 2008. № 2 (14). С. 2 – 6.

244. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Л.: НАСВ, 2015. 265 с.

245. Труш О.О., Кошкіна А.О. Система підтримки прийняття рішень органами державного управління в умовах надзвичайних ситуацій (інцидентів). *Теорія та практика державного управління*. 2013. Вип. 4 (43). С. 1-7.

246. Указ Президента України «Концепція розвитку сектора безпеки і оборони України» від 14.03.2016 року № 92/2016. URL: https://zakon.rada.gov.ua/laws/show/n0002525-16#Text (дата звернення: 13.02.2024).

247. Управління персоналом : навч. посіб. / А. О. Азарова, О. О. Мороз, О.Й. Лесько, І. В. Романець; ВНТУ. – Вінниця : ВНТУ, 2014. – 283 с.

248. Управління персоналом : підручник / О. М. Шубалий, Н. Т. Рудь, А. І. Гордійчук, І. В. Шубала, М. І. Дзямулич, О. В. Потьомкіна, О. В. Середа; за заг. ред. О. М. Шубалого. – Луцьк : ІВВ Луцького НТУ, 2018. – 404 с.

249. Федченко О. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. Journal of Scientific Papers "Social Development and Security", Vol. 12, № 3, 2022,С. 128-134. https://media.neliti.com/media/publications/547667-analysis-of-factors-and-modern-threats-t-7d8ba874.pdf

250. Шахова О., Лозова І., Гнатюк С. Рекомендаці щодо розробки стратегі забезпечения кібербезпеки України. https://dspace.nau.edu.ua/bitstream /NAU/36065/1/10113-26205-1-SM.pdf

251. Шемчук В. В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Парадигми юридичних наук і державного управління*, 1(7), 2020. С. 285-296. https://doi.org/10.32689/2617-9660-2020-1(7)-285-296

252. Шипілова Л.М. Стратегічне планування у сфері національної безпеки / Л.М.Шипілова. К: ВПЦ "Київський університет". 2023. 143 с.

253. Шмаков О.М. Методологічні основи теорії внутрішньої безпеки держави. *Честь і закон*. Х.: Військ. ін-т ВВ МВС України, 2004. №2. С. 3-8.

254. Шорохова Г.М. Інформаційне забезпечення діяльності територіальних органів поліції України. *Юридичний науковий електронний журнал*. 2018. № 6. С. 264–267.

255. Яковлев М.Ю., Герасимов С.В., Семенко Є.Ю. Оцінювання ефективності процесу технічного обслуговування цифрових засобів зв'язку Національної гвардії України. Міжнародна науково-технічна конференція "Перспективи розвитку озброєння та військової техніки", зб. тез доп. наук.-практ. конф. м. Львів, НАСВ 14-15 трав. 2020 р. С. 276–277.

256. Яковлев М.Ю., Горелишев С.А., Семенко Є.Ю. Аналіз військових систем управління військами у формуваннях аналогічних Національній гвардії України. Зб. тез доп. Науково-практичної конференція «Інтегровані

інтелектуальні робототехнічні комплекси», (м. Київ, 19-20 травня 2020 р.). С. 251–252.

257. Яковлев М.Ю., Семенко Є.Ю. Аналіз основних тенденцій застосування та розвитку інформаційно-аналітичних систем при виконанні службово-бойових завдань у провідних країнах світу для формувань аналогічних Національній гвардії України. Науково-практичної конференція «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів» зб. тез доп. наук.-практ. конф. м. Харків: НА НГУ, 29 жовт. 2020 р. С. 352–354.

258. Яковлев М.Ю., Семенко Є.Ю., Герасимов С. В. Онтологічна модель інформаційно-аналітичної системи Національної гвардії України. Науково-практичної конференція «Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів» зб. тез доп. наук.-практ. конф. м. Харків: НА НГУ, 29 жовт. 2021 р. С. 345.

259. Яковлев М.Ю., Семенко Є.Ю., Стрижак О.Є., Аркушенко П.Л. Аналіз методів ранжування альтернатив. Зб. тез доп. Науково-практичної конференція “Створення та модернізація озброєння і військової техніки в сучасних умовах” (м. Чернігів, 3-4 вересня 2020 р.). С. 228–229.

260. Яковлев М.Ю., Стрижак О.Є., Семенко Є.Ю. Інформаційно-аналітичнезабезпечення Національної гвардії України: сучасний стан та основні напрямки розвитку.*Честь і закон*. 2021. № 3(78). С.11-23.

261. AC/322-D(12016) 0017, C3 Taxonomy Baseline 2.0, 14 March 2016

262. Advanced Research Program Agency. – Intelligent Systems. – 23 July 1995.

263. Austrian Cyber Security Strategy. Vienna, 2013. URL: https://www.bka.gv.at/DocView.axd?Cobld-50999

264. Basak I., Saaty Th. Group decision making using the analytic hierarchy process. *Mathl. Compat. Modelling.* Vol. 17, № 415, pp. 101-109, 1993.https://www.sciencedirect.com/science/article/pii/0895717793901793?via%3Dihub

265. Christenson W.M. JCATS Verification and Validation Report / W.M. Christenson, Mary Catherine, Terri J. Walsh, Robert A. Zirkle. – Alexandria, Virginia : Institute for Defense Analyses, October 2002. – 230 p. content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90&lang=uk;

266. Cyber Security Strategy for Germany. Federal Ministry of the Interior, Building and Community. Berlin, 2021. https://www.bmi.bund.de/Shared Docs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4

267. Cyber Security Strategy of Estonia. Ministry of Economic Affairs and Communication. 2022. URL https://www.mkm.ee/media/703/download

268. Cyberspace Protection Policy the Republic of Poland. Ministry of Administration andDigitisation, Internal Security Agency Warsaw, 2013. URL https://www.enisa.curopa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-nesss/copy of PO_NCSS.pdf

269. David S. Alberts, John J. Garstka, Richard E. Hayes,David A. Signori. Understanding Information Age Warfare //Library of Congress Cataloging–in–Publication Data. – August 2001.

270. David S. Alberts. Understanding command and control. The future of command and control / S. David Alberts, E. Richard Hayes. – CCRR Pablication Series,2006. – 249 p.

271. David S. Alberts. Understanding command and control.The future of command and control / S. David Alberts, E. Richard Hayes. – CCRR Pablication Series,2006. – 249 p.

272. David S. Fadok. John Boyd and John Warrden: Air power's quest for strategic paralysi. MAXWELL AIR FORCE BASE, ALABAMA, JUNE 1994.

273. Dewar, James A. "The Importance of 'Wild Card' Scenarios." http://www.cia.gov/nic/PDF_GIF_2020_Support/2003_11_06_papers/dewar_nov6.pdf.

274. Dovgyi S., Stryzhak O., Ilchenko M., Uryvsky L., Globa L. Transdisciplinary Fundamentals of Information-Analytical Activity. *Advances in Information and Communication Technology and Systems.* MCT 2019. Lecture Notes in Networks and Systems. 2021. Vol 152. Springer, Cham.

275. Dovgyi S., Stryzhak O., Ilchenko M., Uryvsky L., Globa L. Transdisciplinary Fundamentals of Information-Analytical Activity. *Advances in Information and Communication Technology and Systems.* MCT 2019. Lecture Notes in Networks and Systems. 2021. Vol 152. Springer, Cham.

276. Dr Sheila E. Widnall, Gen Ronald R. Fogelman, Air Force Executive Guidance (Washington, D.C.: December 1995), 2.

277. Gordon J., Nichiporuk B. Alternative futures implications for army modernization. Santa Monica, 2003. RAND. Arroyo Center. https://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB395.pdf

278. Herbert, A. Simon. The New Science of Management Decision, rev. Ed. Englewood Cliffs, NJ : Prentice-Hall, 1977. 46 p.

279. Hundley, Richard O. Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military? – Santa Monica, CA: RAND. – 1999.

280. Information Operations: A New War–Fighting Capability. A Research Paper Presented To Air Force 2025. – August 1996.

281. ISO/IEC TR 24785:2009(en)/Information technology – Taxonomy of cultural and linguistic adaptability user requirements

282. Інформаційне видання Генерального штабу. Наукова і науково-технічна діяльність у Збройних силах України 2020 рік. К.: «Генеральний штаб». 2020. 178с.

283. Jeffrey McKitrick et al., The Revolution in Military Affairs, Air War College Studies in National Security: Battlefield of the Future. – № 3. – P. 65 – 97. – (Maxwell AFB, Ala.: Air University Press, September 1995).

284. John J. Garstka, Network Centric Warfare: An Overview of Emerging Theory. –PHALANX (December 2000).

285. Klein, J. Th. (2001), “Transdisciplinarity: Joint Problem Solving Among Science, Technology, and Society: An Effective Way for Managing Complexity”, Birkhäuser, 332 p.

286. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston, MA:Houghton Mifflin Harcourt; 2013. – 252 p.

287. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston, MA:Houghton Mifflin Harcourt; 2013. – 252 p.

288. Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, &Kostiantyn Sporyshev. (2024).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. Volume 2(55), 2024.pp.461-473.DOI: https://doi.org/10.55643/fcaptp.2.55.2024.4298. URL: https://fkd.net.ua/index.php/fkd/article/view/4298/4088.

289. National Cyber Secunity Strategy of Hungary. Prime Minister’s Office. Budapest, 2013. URL https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-nesss/HU NCSS.pdf

290. Nicolescu B. Transdisciplinarity - Theory and Practice. Hampton Press, Cresskill, NJ, USA, 2008. 320 p.

291. Oleg Batiuk, Mykhailo Puzyrov, Kostiantyn Sporyshev, Ihor Yevtushenko, GannaVlasova. (2024). Over coming threatsto national security in conditionsofwar. AD ALTA:Journal of interdisciplinary research. VOL.14, ISSUE 1, SPECIAL ISSUE XL. pp.209–214. URL: https://www.magnanimitas.cz/ADALTA/140140/papers/A_34.pdf.

292. Power to the Edge: Command and Control in the Information Age / David S. Alberts, Richard E. Hayes // Information Age Transformation Seriesp. cm. ISBN 1–893723–13–5. –April 2005.

293. Scenario building: The Schwartz / GBN. http://www.infinitefutures.com/tools/sbschwartz.shtml

294. Serhii Bielai, Liudmyla Antonova, Serhii Hololobov, Ihor Yevtushenko, Kostiantyn Sporyshev. The Impact of a Practice-Oriented Paradigm on Public Administration and National Security. International Journal of Sustainable Development and Planning. Vol. 19, No. 1, January, 2024, pp. 277–288. DOI: https://doi.org/10.18280/ijsdp.190126. URL: https://www.iieta.org/journals/ijsdp/paper/10.18280/ijsdp.190126

295. 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. Volume I. Oslo, Kingdom of Norway, 2024. Pp. 379–407.

296. Strategy Cyber Security of Montenegro to 2017. Podgorica. https://www.enisa.europa.eu/securitystrategies-nesss/CyberSecurity StrategyforMontenegro.pdf

297. Stryzhak O., Prychodniuk V., Podlipaiev V. (2019) Model of Transdisciplinary Representation of GEOspatial Information. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham

298. Taylor James G. Support of JCATS Limited Verification and Validation: report / James G. Taylor, Beny Neta. – Monterey, California : Naval postgraduate school, September 2001. – 51 p.

299. Transdisciplinary Engineering: Crossing Boundaries / Editors Milton Borsato, Nel Wognum, Margherita Peruzzini, Josip Stjepandić, Wim J.C. Verhagen // Series Advances in Transdisciplinary Engineering, vol 4, 2016. SBN978-1-61499-702-3 (print) 978-1-61499-703-0 (online)

300. Understanding information age warfare / David S. Alberts, John J. Garstka, Richard E. Hayes, A. David.– Signori p. cm. Includes bibliographical references and index. – ISBN 1–893723–04–6 (pbk.). – August 2001.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ 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/ijsdp.190126
URL: https://www.iieta.org/journals/ijsdp/paper/10.18280/ijsdp.190126 *(Scopus).*

Особистий внесок: визначено підхід до формування інформаційної основи для прийняття та реалізації управлінських рішень.

4. Kryshtanovych 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/fcaptp.2.55.2024.4298
URL: https://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/papers/A_34.pdf. *(Web of Sience).* DOI: https://doi.org/10.33543/j.140140.209214

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

Наукові статті у фахових виданнях

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

Особистий внесок: визначений вплив на ефективність державного управління у сфері державній безпеці України інформаційних загроз.

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

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

9. Бєлай С.В., Споришев 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: визначений вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку.

10. Єманов В.В., Споришев 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: проведений аналіз функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу.

11. Споришев 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: визначена 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://nayka.com.ua/index.php/dy/article/view/2998/3034

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

16. Споришев К.О. Аналіз нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки Україні. *Честь 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 адмініструванн.* 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. 30–309.

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.nayka.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: визначені 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 XLI-ої 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 XLII-ої 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 XLIII-ої 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 XLIV-ої 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 XXI століття*: зб. тез до. 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 JCATS. *Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів:* зб. тез доп. XII 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. XI Міжнар. наук.-практ. конф., м. Харків, 28 жовт. 2022 р. Харків: НА НГУ, 2022. С. 287.

32. Бєлай 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: визначений 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 робото технічні комплекси (ІІРТК-2020)*: зб. тез Тринадцятої міжнар. наук.-практ. конф., м. Київ, 19-20 трав. 2020 р. Київ: НАУ, 2020. С.293–295.

Особистий внесок: визначені 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., Бєлай 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:проведено 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: визначенні шляхи зменшення впливу негативних факторів втрат озброєння і військової техніки на ефективність інформатизації процесів управління.

Додаток Б

ХАРКІВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

ДОВІДКА

про впровадження результатів дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління кандидата технічних наук, доцента Споришева Костянтина Олександровича до практичної діяльності Департаменту з питань оборонної роботи, цивільного захисту та взаємодії з правоохоронними органами Харківської обласної військової адміністрації

Матеріали дисертаційного дослідження кандидата технічних наук, доцента Споришева Костянтина Олександровича на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку на тему: «Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України» використовується в практичній діяльності Департаменту з питань оборонної роботи, цивільного захисту та взаємодії з правоохоронними органами Харківської обласної військової адміністрації під час забезпечення повноважень щодо реалізації державної політики у сфері оборонної роботи, цивільного захисту населення і територій області від надзвичайних ситуацій, а також заходів щодо охорони громадської безпеки, додержання громадського порядку, боротьби зі злочинністю, а саме впроваджено:

- пропозиції з розвитку систем підтримки прийняття рішень у державному управлінні силами безпеки України;
- рекомендації щодо менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України;
- стратегічні засади розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Директор Департаменту по взаємодії з правоохоронними органами, оборонної, мобілізаційної роботи та цивільної оборони Харківської міської ради **Валентин ТОПЧІЙ**

НАЦІОНАЛЬНА ГВАРДІЯ УКРАЇНИ
СХІДНЕ ТЕРИТОРІАЛЬНЕ УПРАВЛІННЯ
вул. Академіка Проскури 1, м. Харків,
61070, тел. (факс): (057) 315-04-00,
e-mail: stu.ngu@ngu.gov.ua
Код ЄДРПОУ 25575782
№ _____
На № _____ від 29.03.2024

ДОВІДКА

Про впровадження у практичну діяльність Східного територіального управління Національної гвардії України результатів дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління кандидата технічних наук, доцента полковника Споришева Костянтина Олександровича

Матеріали дисертаційного дослідження кандидата технічних наук, доцента полковника Споришева Костянтина Олександровича на здобуття наукового ступеня доктора наук з державного управління на тему: «Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України» використовується в практичній діяльності Східного територіального управління Національної гвардії України, а саме впроваджено: системи підтримки прийняття рішень у державному управлінні силами безпеки України, підсистеми захисту інформації в системі державного управління силами безпеки України, геоінформаційні системи в управлінській діяльності сил безпеки України, механізми планування інформаційно-аналітичної діяльності в силах безпеки України, менеджмент кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України, стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Т.в.о. начальника Східного територіального управління
Національної гвардії України
полковник **Антон ВЕРХОВЕНКО**

ОУВ «ХАРКІВ»
ТАКТИЧНА ГРУПА
«СЛОБОДА»
м. Харків,
тел.: 879403
№_____
На № _____ від 15.04.24

ДОВІДКА

Про впровадження у практичну діяльність тактичної групи «Слобода» результатів дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління кандидата технічних наук, доцента полковника Споришева Костянтина Олександровича

На підставі матеріалів дисертаційного дослідження кандидата технічних наук, доцента Споришева Костянтина Олександровича на здобуття наукового ступеня доктора наук з державного управління на тему: «Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України», впроваджено в практичну діяльність тактичної групи «Слобода» наступні результати дослідження:

системи підтримки прийняття рішень у державному управлінні силами безпеки України;

підсистеми захисту інформації в системі державного управління силами безпеки України;

геоінформаційні системи в управлінській діяльності сил безпеки України;

механізми планування інформаційно-аналітичної діяльності в силах безпеки України;

менеджмент кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України,

стратегію розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Командир тактичної групи «Слобода»
полковник **Олексій ЛУНЬОВ**

ДОВІДКА

про впровадження результатів дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління кандидата технічних наук, доцента Спориша Костянтина Олександровича до практичної діяльності Рубіжанської міської військової адміністрації Сєвєродонецького району Луганської області

Матеріали дисертаційного дослідження кандидата технічних наук, доцента Спориша Костянтина Олександровича на здобуття наукового ступеня доктора наук з державного управління на тему: «Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України» використовується в практичній діяльності Рубіжанської міської військової адміністрації Сєвєродонецького району Луганської області під час забезпечення повноважень щодо реалізації державної політики у сфері оборонної роботи, цивільного захисту населення і територій області від надзвичайних ситуацій, а також заходів щодо охорони громадської безпеки, додержання громадського порядку, боротьби зі злочинністю, а саме впроваджено:

- пропозиції з розвитку систем підтримки прийняття рішень у державному управлінні силами безпеки України;
- рекомендації щодо менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України;
- стратегічні засади розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України;
- рекомендації з автоматизації інформаційних систем управлінського призначення сил безпеки України.

Начальник Рубіжанської міської військової адміністрації Сєвєродонецького району Луганської області **Андрій ЮРЧЕНКО**

ЗАТВЕРДЖУЮ
Начальник Національної академії
Національної гвардії України
кандидат технічних наук, доцент
генерал-лейтенант
Сергій СОКОЛОВСЬКИЙ
«17» 05 2024 року

АКТ
про впровадження результатів дисертаційного дослідження
здобувача наукового ступеня доктора наук з державного управління
кандидата технічних наук, доцента
полковника Споришева Костянтина Олександровича
на тему: «Механізми державного управління
системою інформаційно-аналітичного забезпечення
сил безпеки України»

«17» 05 2024 року м. Харків

Про впровадження результатів
дисертаційного дослідження Костянтина Споришева

Комісія у складі:

голови: начальника навчально-наукового центру організації освітнього процесу кандидата військових наук, доцента полковника Володимира Тробюка,

членів: начальника командно-штабного факультету кандидата військових наук, доцента полковника Володимира Антонця,

начальника кафедри забезпечення державної безпеки командно-штабного факультету кандидата військових наук, доцента полковника Олега Голованя,

начальника кафедри військового зв'язку та інформатизації командно-штабного факультету кандидата технічних наук, доцента Віктора Оленченка,

розглянула матеріали дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління Костянтина Споришева

ВСТАНОВИЛА:

основні положення дисертаційного дослідження, а саме питання функціонування систем підтримки прийняття рішень у державному управлінні силами безпеки України та підсистем захисту інформації в системі державного управління складовими сектору безпеки і оборони України, автоматизації інформаційних систем управлінського призначення сектора безпеки та оборони України, застосування геоінформаційних систем в управлінській діяльності сил безпеки України, реалізації механізмів державного управління системою інформаційно-аналітичного забезпечення складових сектора безпеки та оборони України, розвитку менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України використовуються у навчальному процесі та науковій роботі на кафедрі забезпечення державної безпеки, на кафедрі військового зв'язку та інформатизації командно-штабного факультету Національної академії Національної гвардії України при підготовці за навчальними дисциплінами «Тактико-спеціальна підготовка», «Інформаційні технології та електронні комунікаційні системи», а також при проведенні наукових досліджень за напрямом розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення складових сектора безпеки і оборони України.

Результати дисертаційного дослідження здобувача наукового ступеня доктора наук з державного управління кандидата технічних наук, доцента полковника Костянтина Споришева вважати реалізованими.

Голова комісії	полковник	В. Тробюк
Члени комісії	полковник	В. Антонець
	полковник	О. Головань
	полковник	В. Оленченко