Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 3.

DOI: http://doi.org/10.32702/2307-2156.2024.3.24

УДК 355/359:004.7

К. О. Споришев,

к. т. н., доцент, докторант ад'юнктури та докторантури,

Національна академія Національної гвардії України

ORCID ID: https://orcid.org/0000-0003-4737-9698

ПЕРСПЕКТИВНІ ШЛЯХИ ПЛАНУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ В СИЛАХ БЕЗПЕКИ УКРАЇНИ

K. Sporyshev,

PhD in Technical Sciences, Associate Professor, Doctoral student of adjunct and doctoral studies, National Academy of the National Guard of Ukraine

PROSPECTIVE WAYS OF PLANNING INFORMATION AND ANALYTICAL ACTIVITIES IN THE SECURITY FORCES OF UKRAINE

У статті досліджені механізми державного управління системою планування інформаційно-аналітичного забезпечення сил безпеки України. Розглянуті існуючі підходи до планування інформаційно-аналітичного забезпечення сил безпеки України. Проведений аналіз поточного стану інформаційно-аналітичної діяльності в силах безпеки України на основі SWOT-аналізу. Наведені основні нормативно-правові акти щодо планування інформаційно-аналітичного забезпечення сил безпеки України.

Ефективне стратегічне планування є ключовим для національної безпеки, а інформаційно-аналітична діяльність забезпечує необхідну інформаційну базу для цього процесу. Аналіз даних допомагає формувати реалістичне розуміння поточного стану безпекового середовища, оцінювати можливі ризики та визначати стратегічні пріоритети. Інформаційно-аналітична діяльність забезпечує керівництво сил безпеки та оборони даними, необхідними для прийняття обґрунтованих рішень. Використання детального аналізу дозволяє уникнути поспішних чи емоційних рішень, спираючись на фактичні дані та оцінки.

Основою подальшого розвитку інформаційно-аналітичної діяльності в силах безпеки України є інтеграція новітніх технологій, зокрема штучного інтелекту та машинного навчання, для автоматизації збору та аналізу даних. Важливим аспектом є також розвиток міжвідомчої координації та співпраці, як внутрішньо, так і з міжнародними партнерами. Ключ до успіху лежить у створенні гнучких інформаційно-аналітичних систем, здатних адаптуватися до швидко змінюваних умов та нових викликів безпекового середовища, а також у підвищенні професійного рівня аналітиків через спеціалізовані програми навчання та міжнародні обміни досвідом. Ефективна координація між різними агенціями та відомствами, що займаються безпекою, забезпечує обмін інформацією та координоване реагування на загрози.

Важливість інформаційно-аналітичної діяльності для національної безпеки не може бути переоцінена. Це фундаментальний елемент у побудові стійкої, ефективної оборонної політики та забезпеченні безпеки держави. Розвиток цієї сфери має бути пріоритетом для України у відповідь на сучасні виклики та загрози.

The article examines the mechanisms of state management of the planning system for information and analytical support of the security forces of Ukraine. The existing approaches to the planning of information and analytical support of the security forces of Ukraine are considered. An analysis of the current state of information and analytical activity in the security forces of Ukraine was carried out

based on a SWOT analysis. The main normative legal acts regarding the planning of information and analytical support of the security forces of Ukraine are given.

Effective strategic planning is key to national security, and information and analytical activities provide the necessary information base for this process. Data analysis helps to form a realistic understanding of the current state of the security environment, assess possible risks and determine strategic priorities. Information and analytical activity provides the leadership of the security and defense forces with data necessary for making informed decisions. Using detailed analysis avoids hasty or emotional decisions by relying on factual data and estimates.

The basis for the further development of information and analytical activities in the security forces of Ukraine is the integration of the latest technologies, in particular artificial intelligence and machine learning, for the automation of data collection and analysis. An important aspect is also the development of interdepartmental coordination and cooperation, both internally and with international partners. The key to success lies in the creation of flexible information and analytical systems capable of adapting to rapidly changing conditions and new challenges of the security environment, as well as in raising the professional level of analysts through specialized training programs and international exchanges of experience. Effective coordination between various security agencies and departments ensures information sharing and a coordinated response to threats.

The importance of information and analytical activities for national security cannot be overestimated. This is a fundamental element in building a stable, effective defense policy and ensuring the security of the state. The development of this area should be a priority for Ukraine in response to modern challenges and threats.

Ключові слова: *механізми державного управління, інформаційно-аналітичне забезпечення, сили безпеки, сучасні виклики державній безпеці.*

Keywords: *state management mechanisms, information and analytical support, security forces, modern challenges to state security.*

Постановка проблеми. Серед основних викликів для інформаційно-аналітичної діяльності в силах безпеки України можна виділити:

- обмежені технологічні ресурси, а саме незважаючи на значний прогрес у цифровізації, існують прогалини в технологічній інфраструктурі, які обмежують можливості глибокого аналізу великих даних [1-3];

- зростання кіберзагроз вимагає від сил безпеки України підвищення рівня кібербезпеки та захисту інформації. Відповідно до звіту Cybersecurity Ventures, очікується, що глобальні збитки, спричинені кіберзлочинною діяльністю зростатимуть на 15% на рік з 2021 до 2025 року та можуть досягти 10,5 трильйонів доларів щорічно. Причинами такого зростання є значний ріст активності груп кіберзлочинців та зловмисників, діяльність яких спонсорується державою. У той же час кількість атак зростає внаслідок процесів цифрової трансформації [1, 2];

- необхідність у висококваліфікованих фахівцях, здатних ефективно працювати з сучасними інформаційно-аналітичними системами. В умовах підвищеного попиту на професіоналів у галузі кібербезпеки продовжує зростати дефіцит кваліфікованих кадрів. Згідно з дослідженням (ISC)2 Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 мільйона, при цьому 70% організацій мають незакриті вакансії. Багато держав працюють над зменшенням цього дефіциту, а великі компанії, такі як Google, Microsoft або IBM, запроваджують різні ініціативи, спрямовані на навчання та підвищення кваліфікації людей у сфері кібербезпеки [1, 2];

- недостатня ефективність заходів державного управління інформаційно-аналітичної діяльності в силах безпеки України [3, 4].

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).

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження проблемних питань інформаційно-аналітичної діяльності 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., Бєлай С.В., Горєлишев С. А., Шипілова Л.М., Примуш Р.Б. та ін.

Мета. Дослідження механізмів державного управління системою планування інформаційно-аналітичної діяльності сил безпеки України.

Виклад основного матеріалу дослідження. Україна стикається з унікальним набором безпекових викликів, що включають зовнішню агресію, гібридні загрози та внутрішні виклики, такі як корупція та політична нестабільність. Геополітичне положення України, її стратегічне значення в Європі, а також збройна агресія рф створюють складну безпекову обстановку, в якій ефективне інформаційно-аналітичне забезпечення відіграє ключову роль. Інформаційно-аналітична діяльність дозволяє силам безпеки України виявляти, аналізувати та прогнозувати потенційні загрози на основі збору даних та їх подальшого аналізу. Це включає аналіз великих обсягів інформації з різних джерел, включаючи відкриті джерела, технічну розвідку, та інші спеціалізовані методи збору інформації. Ефективна ІАД не лише підвищує оперативну готовність та стратегічне реагування на загрози, але й сприяє розробці довгострокових стратегій забезпечення національної безпеки. ІАД розглядається як методика підвищення ефективності дій сил безпеки через планування, прогнозування та створення сценаріїв дій.

Ефективне стратегічне планування є ключовим для національної безпеки, а інформаційно-аналітична діяльність забезпечує необхідну інформаційну базу для цього процесу. Аналіз даних допомагає формувати реалістичне розуміння поточного стану безпекового середовища, оцінювати можливі ризики та визначати стратегічні пріоритети. ІАД забезпечує керівництво сил безпеки та оборони даними, необхідними для прийняття обґрунтованих рішень. Використання детального аналізу дозволяє уникнути поспішних чи емоційних рішень, спираючись на фактичні дані та оцінки.

Систематичний аналіз загроз, можливостей та вразливостей дозволяє зміцнити обороноздатність держави, оптимізувати розподіл ресурсів та підвищити ефективність оборонних стратегій. ІАД сприяє адаптації до змінюваних умов та викликів, що стоять перед національною безпекою. У сучасному світі інформаційна перевага часто стає вирішальним фактором у конфліктах. Здатність швидко збирати, аналізувати та використовувати інформацію може забезпечити перевагу над противником, дозволяючи ефективніше контролювати ситуацію та випереджати дії опонента [5-7].

Стратегічне планування в контексті сил безпеки охоплює розробку довготривалих планів та стратегій для досягнення поставлених цілей у сфері національної безпеки. Це передбачає 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 різноманітних джерел, та її інтеграція в координовані стратегічні рішення [5, 6].

Для деталізації дослідження механізмів державного управління системою планування інформаційно-аналітичної діяльності сил безпеки України розглянемо нормативно-правову базу.

Основні нормативно-правові акти:

- Закон «Про національну безпеку» [8] - визначає основні засади державної політики у сфері національної безпеки, правові та організаційні основи створення та функціонування сил безпеки. Згідно статті 25 цього закону метою планування у сферах національної безпеки і оборони є забезпечення реалізації державної політики у цих сферах шляхом розроблення стратегій, концепцій, програм, планів розвитку органів сектору безпеки і оборони, управління ресурсами та ефективного їх розподілу [8]. Планування у сферах національної безпеки і оборони поділяється на довгострокове (понад п’ять років), середньострокове (до п’яти років) та короткострокове (до трьох років). Документами довгострокового планування є Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія громадської

безпеки та цивільного захисту України, Стратегія розвитку оборонно-промислового комплексу України, Стратегія кібербезпеки України, Національна розвідувальна програма. Документами середньострокового планування є інші стратегічні документи, програми щодо розвитку складових сектору безпеки і оборони, зокрема оснащення їх сучасним озброєнням і військовою технікою, створення необхідних запасів матеріально-технічних засобів та необхідних для цього потужностей оборонно-промислового комплексу, реалізація інших заходів з посилення обороноздатності держави. Короткострокове планування передбачає щорічне розроблення планів утримання та розвитку (діяльності) складових сектору безпеки і оборони, основних показників здійснення закупівель товарів, робіт і послуг оборонного призначення за закритими закупівлями (на трирічний період), у яких визначаються завдання щодо реалізації документів довгострокового і середньострокового планування [8].

- Закон «Про оборону України» - регламентує питання оборонної діяльності та військової служби, включаючи аспекти ІАД. Одним з аспектів є здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії [9].

- Закон «Про розвідку» - встановлює правові основи діяльності розвідувальних органів, що входять до складу сил безпеки, включаючи положення про збір та аналіз інформації [10].

- Закон «Про боротьбу з тероризмом» - окреслює правові та організаційні засади протидії тероризму, в тому числі через ІАД [11].

- Закон «Про основні засади забезпечення кібербезпеки України» - визначає основи захисту національного інформаційного простору, важливу роль у якому відіграє ІАД [12]. 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 [12].

Гібридні загрози, які комбінують військові, не військові, конвенційні та неконвенційні методи ведення війни, вимагають від сил безпеки особливого підходу до планування та аналізу. Інформаційний аналіз дозволяє ідентифікувати, оцінити та прогнозувати такі загрози, об'єднуючи дані з відкритих джерел, розвідданих та інших спеціалізованих джерел інформації. Ефективне використання інформаційного аналізу сприяє розробці стратегічних планів, які враховують широкий спектр потенційних загроз та забезпечують гнучке реагування на динамічну безпекову обстановку.

Сили безпеки України використовують інформаційно-аналітичну діяльність для ідентифікації та аналізу внутрішніх та зовнішніх загроз національній безпеці. Ця діяльність включає збір інформації з різноманітних джерел, включаючи відкриті джерела даних, соціальні мережі, розвідувальні дані, а також інформацію отриману від міжнародних партнерів.

Розглянемо існуючі підходи до планування ІАД сил безпеки [6].

Стратегічне планування. Встановлення довгострокових цілей та визначення напрямків розвитку інформаційно-аналітичної діяльності.

Оперативне планування. Розробка короткострокових планів дій для досягнення стратегічних цілей.

Сценарне планування. Розробка різних сценаріїв майбутнього для кращої адаптації до потенційних змін в середовищі.

Ризик-орієнтоване планування. Оцінка потенційних ризиків та розробка стратегій для їх мінімізації.

Ці підходи дозволяють ефективно управляти ресурсами, адаптуватися до змін у середовищі, та забезпечити високий рівень готовності сил безпеки до різних викликів.

Для проведення аналізу поточного стану інформаційно-аналітичної діяльності в силах безпеки України використаємо SWOT-аналіз.

Сильні сторони: Високий рівень професіоналізму аналітичного персоналу – сили безпеки мають в своєму складі досвідчених аналітиків, які здатні ефективно обробляти та аналізувати інформацію. Багаторічна участь в

оборонних операціях та антитерористичних заходах надала цінний досвід в інформаційно-аналітичній сфері. Активна взаємодія з міжнародними партнерами та організаціями збільшує можливості обміну інформацією та досвідом.

Слабкі сторони: Фінансові, технічні, та людські ресурси залишаються обмеженими, що ускладнює впровадження сучасних інформаційних технологій. Більшість використовуваних систем є застарілими та потребують оновлення або заміни. Складнощі з інтеграцією нових технологій у вже існуючі системи через їх несумісність або високу вартість.

Можливості: Швидкий розвиток інформаційних технологій пропонує нові можливості для покращення ефективності аналітичної роботи. Доступ до міжнародної допомоги може допомогти подолати фінансові та технологічні ба'єри. Зростання уваги до питань кібербезпеки може покращити захист інформаційних систем.

Загрози: Постійна загроза кібератак з боку ворожих держав або терористичних груп. Спроби зовнішнього впливу через дезінформаційні кампанії, які можуть підривати довіру до інформаційно-аналітичної діяльності. Ризик ненавмисного або умисного витоку таємної інформації, що може мати серйозні наслідки для національної безпеки.

На основі проведеного аналізу можна визначити ключові напрямки для покращення інформаційно-аналітичної діяльності: інвестиції в сучасні технології та системи для покращення обробки та аналізу даних; організація навчальних програм та обмінів досвідом з міжнародними партнерами; розробка та впровадження передових рішень у сфері кібербезпеки для захисту інформаційних ресурсів; встановлення вимог до технологічного оснащення та програмного забезпечення для ефективної аналітики; розробка програм навчання та розвитку персоналу з акцентом на новітніх технологіях та методах аналізу; встановлення системи моніторингу для відстеження прогресу у виконанні плану впровадження та оцінки ефективності заходів; регулярний

перегляд стратегічного плану для внесення необхідних коректівів на основі аналізу отриманих результатів і змін у зовнішньому середовищі.

Висновки і перспективи подальших досліджень. Стратегічне планування та ефективне впровадження ідентифікованих перспективних шляхів може значно покращити якість та ефективність інформаційно-аналітичної діяльності в силах безпеки України. Це вимагає комплексного підходу, що включає технологічне оновлення, підвищення кваліфікації персоналу, та посилення заходів кібербезпеки. Реалізація цих заходів вимагатиме співпраці на всіх рівнях управління, а також адекватного фінансування.

Основою подальшого розвитку інформаційно-аналітичної діяльності в силах безпеки України є інтеграція новітніх технологій, зокрема штучного інтелекту та машинного навчання, для автоматизації збору та аналізу даних. Важливим аспектом є також розвиток міжвідомчої координації та співпраці, як внутрішньо, так і з міжнародними партнерами. Ключ до успіху лежить у створенні гнучких інформаційно-аналітичних систем, здатних адаптуватися до швидко змінюваних умов та нових викликів безпекового середовища, а також у підвищенні професійного рівня аналітиків через спеціалізовані програми навчання та міжнародні обміни досвідом. Ефективна координація між різними агенціями та відомствами, що займаються безпекою, забезпечує обмін інформацією та координоване реагування на загрози.

Важливість інформаційно-аналітичної діяльності для національної безпеки не може бути переоцінена. Це фундаментальний елемент у побудові стійкої, ефективної оборонної політики та забезпеченні безпеки держави. Розвиток цієї сфери має бути пріоритетом для України у відповідь на сучасні виклики та загрози.

Література

1. 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

2. 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

3. Яковлев М.Ю., Стрижак О.Є., Семенко Є.Ю. Інформаційно-аналітичне забезпечення Національної гвардії України: сучасний стан та основні напрямки розвитку. *Честь і закон*. 2021. № 3(78). С.11-23.

4. 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.

5. 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

6. Шипілова Л.М. Стратегічне планування у сфері національної безпеки / Л.М.Шипілова. К: ВПЦ "Київський університет". 2023. 143 с.

7. 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.

8. Закон України «Про національну безпеку України» від 21.06. 2018 № 2469-VIII. URL:https://ips.ligazakon.net/document/view/t182469?an=1&ed= 2022_06_15

9. Закон України «Про оборону України» від 6. 12.1991 № 1932-XII. URL:https://zakon.rada.gov.ua/laws/show/1932-12#Text

10. Закон України «Про розвідку» від 17.09.2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text

11. Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text

12. Закон України «Про основні засади забезпечення кібербезпеки України» від 5.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

References

1. The official site UNIAN (2024), “10 cyber security challenges: experts told users and companies what to prepare for”, available at: https://www.unian.ua/science/10-viklikiv-kiberbezpeki-eksperti-rozpovili-do-chogo-gotuvatisya-koristuvacham-ta-kompaniyam-12033828 (Accessed 10 March 2024).

2. The official site of State Service of Special Communications and Information Protection of Ukraine (2023), “The experience of war: what are the challenges facing the state and business in cyberspace”, available at: https://cip.gov.ua/ua/news/dosvid-viini-yaki-vikliki-stoyat-pered-derzhavoyu-ta-biznesom-u-kiberprostori (Accessed 10 March 2024).

3. Yakovlev, M.Yu. Stryzhak, O.E. and Semenko, E.Yu. (2021), “Information and analytical support of the National Guard of Ukraine: current state and main directions of development”, *Chest i zakon*, vol. 3(78), pp. 11–23.

4. Belai, S.V. and Sporyshev, K.O. (2024), “The impact of the state of the system of information and analytical support of the security forces of Ukraine on state security”, *Naukovi innovatsii ta peredovi tekhnolohii (Seriia «Upravlinnia ta administruvannia»)*, vol. 2(30), pp. 29–37.

5. Prymus, R.B. (2018), “Information provision of strategic planning in the field of national security”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, [Online], vol. 7, available at: http://www.dy.nayka.com.ua/pdf/7_2018/41.pdf (Accessed 9 March 2024).

6. Shypilova, L.M. (2023), *Stratehichne planuvannia u sferi natsionalnoi bezpeky* [Strategic planning in the field of national security], VPTs Kyivskyi universytet, Kyiv, Ukraine.

7. Tkachenko, V.I. Smirnov, E.B. Drobakha, G.A. Bilchuk, V.M., and Tristan A.V. (2008), *Teoriia pryiniattia rishen orhanamy viiskovoho upravlinnia* [The theory of decision-making by military administration bodies], KhVU, Kharkiv, Ukraine.

8. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On National Security of Ukraine", available at: https://ips.ligazakon.net/document/ view/t182469?an=1&ed=2022_06_15 (Accessed 9 March 2024).

9. The Verkhovna Rada of Ukraine (1991), The Law of Ukraine "About the defense of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1932-12#Text (Accessed 11 March 2024).

10. The Verkhovna Rada of Ukraine (2020), The Law of Ukraine "About intelligence", available at: https://zakon.rada.gov.ua/laws/show/912-20#Text (Accessed 11 March 2024).

11. The Verkhovna Rada of Ukraine (2003), The Law of Ukraine "About the fight against terrorism", available at: https://zakon.rada.gov.ua/laws/show/638-15#Text (Accessed 11 March 2024).

12. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "About the main principles of ensuring cyber security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show /2163-19#Text (Accessed 11 March 2024).

Стаття надійшла до редакції 13.03.2024 р.