УДК 355/359:004.7

К. О. Споришев,
к. т. н., доцент, докторант ад'юнктури та докторантури,
Національна академія Національної гвардії України
https://orcid.org/0000-0003-4737-9698

DOI: 10.32702/2306-6814.2024.6.251

МЕТОДОЛОГІЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ТА РОЗВИТКУ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ 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

METHODOLOGICAL PRINCIPLES OF FUNCTIONING AND DEVELOPMENT OF STATE MANAGEMENT MECHANISMS OF THE INFORMATION AND ANALYTICAL SUPPLY SYSTEM SECURITY FORCES OF UKRAINE

У статті розглянуті методологічні засади функціонування та розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Ефективне функціонування та розвиток механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України вимагає комплексного підходу, постійного оновлення технологій та методів аналізу, а також забезпечення високого рівня безпеки та захисту інформації. Інтеграція інформаційних систем та стандартизація процесів обробки даних є фундаментальними аспектами, що забезпечують ефективність, безпеку та надійність управління інформаційними ресурсами в силових структурах. Ці процеси дозволяють синхронізувати діяльність різних підрозділів, забезпечуючи їх здатність оперативно реагувати на змінні умови та загрози.

Розвиток інформаційно-аналітичного забезпечення здійснюється за напрямами — впровадження новітніх інформаційних технологій для прийняття рішень під час виконання службово-бойових завдань, створення нових технічних рішень під час розроблення (модернізації), розроблення і вдосконалення інформаційної інфраструктури сил безпеки з урахуванням національних та міжнародних стандартів, створення інформаційно-аналітичних систем з урахуванням вимог щодо забезпечення взаємодії між наявними та створюваними у силах безпеки інформаційними системами, впровадження автоматичної ідентифікації та автентифікації користувачів інформаційно-аналітичних систем, регламентованого доступу і обміну даними, забезпечення необхідного рівня захисту інформації від зовнішніх та внутрішніх загроз, удосконалення організаційної структури інформаційно-аналітичних систем.

The article examines the methodological principles of the functioning and development of mechanisms of state management of the system of information and analytical support of the security forces of Ukraine. The effective functioning and development of state management mechanisms of the system of information and analytical support of the security forces of Ukraine requires a comprehensive approach, constant updating of technologies and methods of analysis, as well as ensuring a high level of security and information protection. Integration of information systems and standardization of data processing processes are fundamental aspects that ensure efficiency, security and reliability of information resource management in law enforcement agencies. These processes allow to synchronize the activities of various divisions, ensuring their ability to respond quickly to changing conditions and threats.

The development of information and analytical support is carried out along the lines of ? introduction of the latest information technologies for decision-making during service and combat tasks, creation of new technical solutions during development (modernization), development and improvement of the information infrastructure of the security forces taking into account national and international standards, creation of information and analytical systems taking into account the requirements for ensuring interaction between existing and created information systems in the security forces, implementation of automatic identification and authentication of users of information and analytical systems, regulated access and data exchange, ensuring the necessary level of information protection against external and internal threats, improvement organizational structure of information and analytical systems.

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

Key words: state management mechanisms, information and analytical support, security forces, modern challenges to state security.

ПОСТАНОВКА ПРОБЛЕМИ

Аналітичні служби (підрозділи) створювались у всіх вузлах інформаційної інфраструктури, тобто у всіх сферах діяльності, де концентрувалися, перероблялися великі інформаційні потоки з метою прийняття соціально значимих управлінських рішень. Саме тому інформаційно-аналітичні служби (підрозділи) стали створюватися в структурах органів державного і військового управління, у міністерствах і відомствах, в органах ЗМІ, у сфері бізнесу, при політичних партіях і рухах. Загальною відмітною рисою даних служб є органічне входження у відповідні сфери діяльності, функціональний і організаційно-діяльний симбіоз з їхніми соціальними інститутами, конкретними організаціями і органами управління (ОУ).

Стан інформаційно-аналітичної інфраструктури, яка спрямовується для забезпечення потреб керівного складу структурних сил безпеки не відповідає сучасним викликам під час підтримання прийняття рішень на застосування сил. Інтеграція інформаційних систем за окремими напрямами відсутня або здійснюється фрагментарно, й не враховує сучасні вимоги щодо консолідації [1—3], а це призводить до дублювання та недостатньої достовірності і повноти інформації щодо комплексного управління процесами виконання службово-бойових завдань в цілому.

Також невирішеними є такі питання: відсутність єдиних методологічних, науково-технічних та організаційних принципів і обгрунтованих підходів щодо створення ІАС та впровадження сучасних когнітивних інформаційних технологій; відсутність єдиних стандартів обміну даними між інформаційними системами для забезпечення взаємосумісності (інтероперабельності); недостатня розробленість питань захисту інформації (інформаційних ресурсів); недостатня розгалуженість інформаційно-телекомунікаційних мереж та швидких каналів передавання даних; організаційна розпорошеність та функціональна роз'єднаність існуючих інформаційних систем; недосконалість та неповнота 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 реалізують семантичну операціональність взаємодії із інформаційними ресурсами [4, 5].

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Значний внесок у дослідження проблемних питань інформаційно-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., Бєлай С.В., Горєлишев С. А. та ін.

МЕТА

Проведення аналізу розвитку механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Методологічні засади 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 забезпечують збір, аналіз, зберігання та передачу інформації необхідної для підтримки діяльності сил безпеки [6]. Розглянемо ключові аспекти механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України.

Ефективне функціонування та розвиток механізмів державного управління системою інформаційно-аналітичного забезпечення сил безпеки України вимагає комплексного підходу, постійного оновлення технологій та методів аналізу, а також забезпечення високого рівня безпеки та захисту інформації. Інтеграція інформаційних систем та стандартизація процесів обробки даних є фундаментальними аспектами, що забезпечують ефективність, безпеку та надійність управління інформаційними ресурсами в силових структурах. Ці процеси дозволяють синхронізувати діяльність різних підрозділів, забезпечуючи їх здатність оперативно реагувати на змінні умови та загрози.

Інтеграція інформаційних систем вимагає узгодження технічних та програмних компонентів, щоб забезпечити безперебійний обмін даними між різними платформами та базами даних. Це включає:

Сумісність форматів даних, усі системи могли "читати" та "розуміти" дані одна одної, використовуючи загальноприйняті формати. Встановлення стандартних протоколів для безпечного обміну даними між системами.

API (Application Programming Interface). Розробка та використання API для забезпечення взаємодії між різними програмними додатками.

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

Важливо забезпечити сумісність та інтеграцію різних інформаційних систем та баз даних, які використовуються в силових структурах, для забезпечення безперервного доступу до актуальної інформації.

Стандартизація процесів обробки даних. Розробка та впровадження стандартів для обробки, зберігання та передачі інформації дозволяють оптимізувати роботу з даними, підвищити їх надійність та захищеність. Стандартизація визначає єдині правила та методики обробки, зберігання та передачі інформації. Ключові елементи включають:

Розробка стандартів даних. Визначення структури даних, форматів зберігання та методів їх обробки. Встановлення правил та процедур для захисту інформації від несанкціонованого доступу, модифікації чи втрати. Аудит та контроль якості даних. Регулярний перегляд та аналіз даних та систем їх обробки для забезпечення відповідності встановленим стандартам. Впровадження політик керування доступом для регулювання хто, коли та як може доступати до певних даних.

Розвиток аналітичних засобів та створення ефективних систем підтримки прийняття рішень є вирішальними для підвищення ефективності управлінських процесів в контексті національної безпеки та оборони. Особливо це стосується сил безпеки України, де швидкі та обгрунтовані рішення можуть мати стратегічне значення.

Використання сучасних методів аналітики, включаючи машинне навчання та штучний інтелект, для обробки великих обсягів даних та виявлення потенційних загроз. Сучасні аналітичні засоби, особливо ті, що базуються на машинному навчанні (МН) та штучному інтелекті (ШІ), здатні ефективно обробляти великі обсяги даних, виділяючи корисну інформацію та виявляючи потенційні загрози. Це включає:

Прогнозування та виявлення загроз. МН та ШІ можуть аналізувати патерни поведінки та історичні дані для прогнозування потенційних загроз, надаючи силам безпеки можливість діяти проактивно. Обробка природної мови (NLP). Це дозволяє автоматично аналізувати текстові дані, такі як звіти розвідки, новини та соціальні медіа, для виявлення корисної інформації. Аналіз візуальних даних. Використання алгоритмів комп'ютерного зору для аналізу зображень та відео може допомогти у виявленні загроз, моніторингу об'єктів тощо.

Розробка інформаційно-аналітичних систем, які надають оперативну інформацію та рекомендації для прийняття рішень на різних рівнях управління. Системи підтримки прийняття рішень (СППР) відіграють ключову роль у покращенні процесу управління, надаючи керівництву сил безпеки актуальну інформацію та аналітичні рекомендації. Такі системи можуть включати:

Інтерактивні дашборди. Надають швидкий доступ до ключових показників ефективності (KPI), аналітики в реальному часі та інших важливих даних. Моделювання та симуляція. Використовуються для оцінки різних сценаріїв та їх потенційного впливу на безпеку, допомагаючи керівництву розуміти можливі наслідки рішень. Системи експертних оцінок. Забезпечують аналіз ситуації на основі даних та досвіду експертів, пропонуючи рекомендації щодо прийняття рішень.

Інтеграція з іншими системами. СППР ефективно інтегруються з іншими інформаційними системами для забезпечення безперервного доступу до даних та аналітики. Застосування цих технологій та підходів може значно підвищити ефективність управління, а також допомогти силам безпеки України швидко реагувати на змінні умови та виклики, забезпечуючи національну безпеку на високому рівні.

Впровадження комплексних заходів щодо захисту інформаційних систем та даних від несанкціонованого доступу, зловмисного втручання або витоку інформації.

Використання сучасних криптографічних методів для шифрування інформації, що передається або збе-

рігається в інформаційних системах сил безпеки. Забезпечення інформаційної безпеки та криптографічний захист даних є критично важливими аспектами для гарантування цілісності, конфіденційності та доступності інформаційних ресурсів в силових структурах, особливо у контексті національної безпеки.

Забезпечення інформаційної безпеки вимагає комплексного підходу, який включає заходи адміністративного, технічного та фізичного характеру для захисту інформаційних систем та даних. Основні складові включають:

Політики безпеки. Розробка та впровадження політик безпеки, що визначають правила поводження з інформацією та інформаційними системами. Контроль доступу. Встановлення строгих процедур контролю доступу до інформаційних систем і даних, використання механізмів аутентифікації та авторизації. Захист від вірусів та шкідливого ПЗ. Використання антивірусного програмного забезпечення та інших засобів захисту від шкідливих програм та вірусів. Впровадження заходів для захисту мережевої інфраструктури, включаючи файрволи, системи виявлення та запобігання вторгнень. Регулярне резервне копіювання важливих даних та розробка планів відновлення після збоїв для забезпечення доступності інформації.

Криптографія є ключовим елементом захисту інформації, що передається через мережі, або зберігається в інформаційних системах. Основні заходи включають: Використання сильних алгоритмів шифрування для захисту конфіденційності даних під час їх зберігання та передачі. Застосування цифрових підписів для забезпечення цілісності та автентичності електронних документів та повідомлень. Впровадження надійних процесів управління криптографічними ключами для запобігання їх неправомірному використанню або втраті. Сертифікація та інфраструктура відкритих ключів (PKI). Розробка та впровадження інфраструктури відкритих ключів для управління цифровими сертифікатами та ключами.

Застосування цих комплексних заходів забезпечує захист інформаційних систем та даних від різноманітних загроз, забезпечуючи конфіденційність, цілісність та доступність інформації, що є критично важливим для ефективного функціонування сил безпеки.

Створення та постійне оновлення нормативно-правових актів, які регулюють діяльність системи інформаційно-аналітичного забезпечення, важливо для забезпечення її законності та ефективності. Розробка законодавчої та нормативної бази є фундаментальною для забезпечення законності, прозорості та ефективності функціонування систем інформаційно-аналітичного забезпечення, особливо у сфері національної безпеки та оборони. Цей процес включає кілька ключових етапів та аспектів:

Визначення правових, технічних та оперативних вимог, які необхідні для ефективного функціонування системи інформаційно-аналітичного забезпечення.Підготовка законопроектів та нормативних актів, які регулюють збір, обробку, зберігання, передачу та захист інформації в системах національної безпеки. Залучення фахівців, громадськості та зацікавлених сторін до обговорення проектів законів та нормативних актів для забезпечення їх комплексності та відповідності реальним потребам. Офіційне прийняття законів та нормативних актів, їх публікація та введення в дію. Організація навчання та інформування співробітників, які працюють у сфері національної безпеки, про нові вимоги та процедури. Постійний моніторинг впливу нового законодавства на діяльність інформаційно-аналітичних систем та їх ефективність. Оцінка потреби в подальших змінах або доповненнях. Законодавство має гарантувати захист прав та основних свобод громадян, включаючи право на приватність. Забезпечення високого рівня безпеки інформації та конфіденційності особистих даних. Гармонізація національного законодавства з міжнародними стандартами та нормами. Забезпечення прозорості процесів збору та обробки інформації, доступності інформації про діяльність системи для громадськості, за умови дотримання вимог національної безпеки.

Розробка ефективного законодавчого та нормативного фреймворку для регулювання діяльності систем інформаційно-аналітичного забезпечення є ключовою для забезпечення їх законності, ефективності та відповідності сучасним викликам в сфері національної безпеки. Важливо забезпечити баланс між потребами національної безпеки та захистом прав та свобод громадян.

Програми підготовки та навчання персоналу, залученого до роботи з інформаційно-аналітичними системами, відіграють критичну роль у забезпеченні ефективності та безпеки діяльності організацій, особливо у сфері національної безпеки. Розробка та впровадження цілеспрямованих програм навчання сприяють не тільки підвищенню кваліфікації співробітників, але й зміцненню загальної інформаційної безпеки та оперативності реагування на загрози. Ось кілька ключових аспектів ефективних програм навчання: Перед розробкою програми необхідно провести аналіз навчальних потреб, визначивши специфічні вимоги до навичок та знань для кожної ролі або відділу. Це допоможе виявити прогалини в компетенціях та розробити цілеспрямовані навчальні плани. Навчальні програми мають бути гнучкими та адаптованими до конкретних потреб суб'єкту сил безпеки. Вони можуть включати: Курси, лекції, вебінари для вивчення теоретичних основ. Воркшопи, тренінги на робочому місці, симуляції для розвитку практичних навичок. Онлайн-курси та платформи для самостійного вивчення.

Кваліфіковані інструктори та тренери, які мають глибокі знання та практичний досвід у сфері інформаційних технологій та безпеки, можуть значно підвищити ефективність навчання. Технології та загрози інформаційній безпеці швидко змінюються, тому навчальні програми потребують регулярного перегляду та оновлення. Також важливо проводити оцінку ефективності навчання, збираючи зворотний зв'язок від учасників та аналізуючи результати їх роботи після завершення курсів.

Мотивація співробітників до навчання є ключовим фактором успіху. Використання ігрових елементів, надання сертифікатів та визнання досягнень можуть сприяти залученості та зацікавленості в навчальному процесі.

Забезпечення можливості застосувати отримані знання на практиці в реальних робочих ситуаціях є важливим для закріплення навичок та підвищення загаль-

ної ефективності роботи з інформаційно-аналітичними системами.

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 має безпосередній вплив на національну безпеку.

ВИСНОВКИ

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

Виклики сучасності з якими зіткнулась наша держава потребують негайного вдосконалення системи інформаційно-аналітичного забезпечення сил безпеки України.

Література:

1. 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.

2. 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.

3. 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.

4. Mayer-Schonberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston, MA:Houghton Mifflin Harcourt; 2013. — 252 p.

5. 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.

6. 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.

References:

1. Ostrovskyi, S. O. (2017), "The concept and content of information and analytical activity as an element of information and analytical support for the interaction of the National Guard of Ukraine with law enforcement agencies and the Armed Forces of Ukraine", Aktualni problemy vitchyznianoi yurysprudentsii — Actual problems of domestic jurisprudence, vol. 4, pp. 92—96.

2. Kovalov, I. V. & Volobuiev, R. V. (2020), "Mechanism of synthesis of information and analytical support of the National Guard of Ukraine in emergency situations", Naukovyi visnyk: Derzhavne upravlinnia — Scientific Bulletin: State Administration, vol. 3 (5), pp. 3—15.

3. Dovgyi, S., Stryzhak, O., Ilchenko, M., Uryvsky, L. and Globa, L. (2021), "Transdisciplinary Fundamentals of Information-Analytical Activity. Advances in Information and Communication Technology and Systems. MCT 2019", Lecture Notes in Networks and Systems, Vol 152.

4. Mayer-Schonberger V., Cukier K. (2013), Big Data: A Revolution That Will Transform How We Live, Work, and Think, Houghton Mifflin Harcourt, Boston, USA.

5. Kyrychenko. I. O., Horelyshev. S. A. & Poberezhnyi, A. A. (2013). Tekhnolohichni osnovy informatsiino-analitychnoho zabezpechennia sluzhbovo-boiovoi diialnosti syl okhorony pravoporiadku [Technological bases of information and analytical support of service and combat activities of law enforcement forces], Akad.VV MVS Ukrainy, Kharkiv, Ukraine.

6. Bielai S.V., 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") — Scientific Innovations and Advanced Technologies (Management and Administration Series), vol. 2 (30), pp. 29—37.

Стаття надійшла до редакції 09.03.2024 р.