УДК: 355.4:004.7:001.8 DOI: **10.33099/2311-7249/2025-53-2-109-119**

ПІОНТКІВСЬКИЙ Петро Миколайович,
кандидат технічних наук, старший науковий співробітник,
Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна,
https://orcid.org/0000-0002-9103-5393

МОДЕЛІ ОРГАНІЗАЦІЇ МЕНЕДЖМЕНТУ НАУКОВО-ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В ОБОРОННОМУ СЕКТОРІ

Стаття присвячена аналізу теоретичних і практичних аспектів розроблення моделей організації менеджменту науково-інформаційної діяльності в оборонному секторі. ***Метою статті*** *є формування моделей організації управління науково-інформаційними процесами в оборонному секторі з урахуванням сучасних викликів інформаційної безпеки, технологічних трендів і особливостей інтеграції інформаційних систем, спрямованих на підвищення ефективності функціонування інноваційних та науково-дослідних установ (підрозділів) оборонного комплексу.*

Методи дослідження. *У статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за тематикою функціонування та застосування інформаційно-комунікаційних систем. Під час проведення дослідження використано підходи методів теорії управління, методів оптимізації рішень та організаційного моделювання складних систем.*

Отримані результати дослідження. *У роботі проведено аналіз та запропоновані рішення, які є основою для створення єдиної національної платформи обміну даними між військовими й цивільними установами, сприятимуть інтеграції оборонного сектору в міжнародні наукові мережі та дадуть змогу підвищити ефективність управлінських процесів завдяки обґрунтуванню структурних вимог до рівнів управління.*

Елементи наукової новизни. *Наукова новизна дослідження зводиться до визначення головних принципів науково-інформаційного обміну в системі менеджменту науково-інформаційної діяльності оборонного сектору, зокрема, інтеграції інформаційних потоків між військовими та цивільними науковими установами, стандартизації протоколів обміну даними.*

Теоретична й практична значущість викладеного у статті. *Запропоновано новий підхід до побудови загальної архітектури системи менеджменту науково-інформаційної діяльності, яка об'єднує сучасні методи обробки великих даних, штучного інтелекту та хмарних обчислень, забезпечуючи високу надійність, адаптивність і стійкість до кіберзагроз. Обґрунтовано функціональне призначення головних елементів системи та їхню взаємодію для покращення моніторингу й управління інформаційними потоками. Практичне значення дослідження визначається його спрямованістю на реалізацію сучасних підходів до управління науково-інформаційною діяльністю.*

Ключові слова: *моделі організації менеджменту науково-інформаційної діяльності, оборонний сектор, архітектура системи менеджменту, інформаційні потоки, принципи обміну даними.*

Вступ

Зростання обсягів інформації та різноманітність джерел її надходження створюють нові виклики для ефективного управління в оборонному секторі (далі – ОС). Основними проблемами є інтеграція різнорідних інформаційних систем, а саме відсутність уніфікованих стандартів обміну даними та розбіжності між платформами, що ускладнює управління інформаційними потоками. Зростаюча кількість кібератак ставить під загрозу конфіденційність і цілісність критично важливої інформації. Умови воєнного часу вимагають зменшення часових затримок у передачі даних, що є критично важливим для прийняття рішень у реальному часі. Відсутність належних механізмів управління науково-інформаційною діяльністю (далі – НІД) ускладнює реалізацію стратегічних завдань ОС, підвищуючи ризики національній безпеці.

Постановка проблеми. Сучасна оборонна сфера зіткнулася з викликами, які обумовлені глобальною цифровізацією, стрімким розвитком технологій та зростаючими кіберзагрозами. У цих умовах ефективний менеджмент НІД стає головним фактором забезпечення функціональної спроможності оборонного комплексу. Зокрема, важливість обґрунтованих рішень у сфері управління інформацією визначається необхідністю своєчасного збору, аналізу та поширення даних. Управління НІД охоплює комплекс процесів, спрямованих на організацію, обробку, зберігання та безпечний обмін інформацією. Воно включає застосування методологій управління знаннями, впровадження автоматизованих систем (далі – АС) та інтеграцію сучасних інформаційно-комунікаційних технологій (далі – ІКТ), які здатні забезпечити відповідність вимогам динамічного інформаційного середовища.

Розроблення науково обґрунтованих підходів до менеджменту НІД є актуальним завданням, результат сприятиме інтеграції сучасних технологій в ОС, що

дасть змогу забезпечити його стійкість і функціональну спроможність в умовах зростаючої складності інформаційного середовища.

Аналіз останніх досліджень і публікацій. Наукові праці сучасних авторів підтверджують значення інформаційних технологій у різних аспектах управління та оптимізації процесів. Так, у роботі [1] підкреслено, що впровадження сучасних інформаційних технологій у логістичні процеси сприяє автоматизації та оптимізації операцій, покращенню обробки великих обсягів даних і зниженню ризиків. Аналіз сучасних технологій кібербезпеки, проведений у дослідженні [2], виявив основні підходи до захисту інформаційних систем у цифровому середовищі. Було наголошено на важливості багаторівневих систем захисту та нових стандартів шифрування.

Стаття [3] досліджує вплив хмарних обчислень і генетичних алгоритмів на стратегічну оптимізацію в бізнесі, окрім того зазначається, що використання штучного інтелекту (далі – ШІ) дає змогу автоматизувати прийняття рішень і покращувати точність прогнозування ризиків. У дослідженні [4] аналізується вплив інформаційних технологій на управління університетськими службами, це завдання актуальне і для закладів вищої освіти (далі – ЗВО), вищих військових навчальних закладів (далі – ВВНЗ), їх наукових підрозділів, наукових установ (далі – НУ) ОС.

У статті [5] Адріан Стельмач демонструє, як «Індустрія 4.0» та цифрові трансформації сприяють інтеграції інформаційних і операційних технологій оптимізації виробничих процесів. У [6–7] автори аналізують, як новітні технології та управлінські методи можуть підвищити ефективність оборонних структур, а у статті [8] розглядається створення інноваційної екосистеми для розвитку безпілотної авіації в Україні, в якій автори наголошують на важливості співпраці між НУ та промисловістю, важливості обміну даними для прискорення технологічного прогресу та впровадження нових бізнес-моделей.

Ці дослідження демонструють актуальність і багатогранність використання інформаційних технологій, а також критичну важливість менеджменту НІД в ОС. У той же час питання особливостей потоків даних, можливі моделі організації НІД, напрями розвитку та особливості формування ефективних моделей організації менеджменту НІД в ОС не розкриті.

Метою статті є розроблення моделей організації управління науково-інформаційними процесами в ОС з урахуванням сучасних викликів інформаційної безпеки, технологічних трендів і особливостей інтеграції інформаційних систем, спрямованих на підвищення ефективності функціонування інноваційних та науково-дослідних установ (підрозділів) ОС.

Виклад основного матеріалу дослідження

Науково-інформаційна діяльність – це сукупність процесів збору, обробки, аналізу, збереження, передачі та використання науково-технічної інформації (далі – НТІ), спрямованих на підтримку досліджень, розробок та інновацій. Вона охоплює організацію інформаційних потоків, управління знаннями та створення інформаційних ресурсів і технологій, що забезпечують доступ до актуальних даних. В ОС НІД має стратегічне значення, забезпечуючи науково-технічний розвиток та обороноздатність держави. Оперативне управління інформаційними процесами дає змогу формувати базу знань для прийняття рішень, впроваджувати передові технології та забезпечувати інформаційну безпеку, включно із захистом конфіденційної інформації від кіберзагроз.

Технологія менеджменту в цій сфері визначається як система методів, засобів та процедур для ефективного управління інформаційними процесами, включно з програмно-технічними рішеннями, стандартами та регламентами. Згідно із Законом України «Про наукову і науково-технічну діяльність» [9], вона спрямована на створення, зберігання та поширення інформації, що підвищує ефективність досліджень.

ІКТ та АС управління, регламентовані нормативними актами [10], є основними інструментами оптимізації науково-інформаційних потоків. Ефективні моделі організації менеджменту НІД забезпечать інтеграцію знань, оптимізацію ресурсів та інформаційну безпеку, сприяючи інноваційному розвитку ОС. Умови воєнного стану суттєво трансформують традиційні підходи до менеджменту, особливо у контексті НІД в ОС. Це обумовлено специфічними викликами, що пов’язані з підвищеною невизначеністю, обмеженістю ресурсів та високою динамікою зовнішніх і внутрішніх загроз. Воєнний стан вимагає підвищеної оперативності управлінських рішень і гнучкості організаційних структур. Згідно з теорією ситуаційного менеджменту [11–12], у нестабільних умовах керівництво має адаптуватися до змін, що відбуваються, застосовуючи більш динамічні, «органічні» форми управління. У сфері НІД це означає, що перспективні моделі організації менеджменту мають забезпечувати швидкий збір, обробку та аналіз інформації, мінімізуючи часові затримки, що критично важливо для прийняття стратегічних і тактичних рішень у реальному часі.

Безпека інформації набуває пріоритетного значення. В умовах воєнного стану посилюється загроза кібернападів, інформаційних диверсій та витоку конфіденційних даних, що є критично важливими для оборонного потенціалу держави. Відповідно, менеджмент НІД має інтегрувати комплексні системи кіберзахисту, засновані на багаторівневому контролі доступу, криптографічних методах захисту та регулярному моніторингу інформаційних потоків. Закон України «Про основи національної безпеки України» визначає інформаційну безпеку як складову національної безпеки, що підтверджує необхідність жорстких стандартів управління інформаційними ресурсами в ОС.

Централізація управлінських функцій у воєнний

час є ключовою умовою для ефективної координації дій між численними підрозділами ОС. Централізоване управління інформаційними ресурсами сприяє оптимізації процесів, усуненню дублювання зусиль та уніфікації процедур. Завдяки централізованому підходу забезпечується єдиний інформаційний простір, що критично важливо для швидкої та скоординованої реакції на загрози. Це дає змогу не лише підвищити ефективність використання ресурсів, а й забезпечити належний рівень підготовки та психологічної стійкості військовослужбовців.

Управління кадровими ресурсами набуває особливого значення через необхідність мобілізації, перепрофілювання та навчання спеціалістів. В умовах воєнного стану важливо організувати безперервний процес підвищення кваліфікації та адаптації персоналу до нових технологічних і організаційних вимог. Це підтверджується положеннями Закону України «Про наукову і науково-технічну діяльність» [9], який регламентує розвиток кадрового потенціалу як важливий чинник ефективної НІД. Отже, менеджмент НІД в умовах воєнного стану має специфічні особливості, що містять високу оперативність, посилену інформаційну безпеку, централізовану координацію і гнучке управління людськими ресурсами. Урахування цих факторів є визначальним для забезпечення ефективності функціонування менеджменту НІД ОС в складних кризових умовах.

Науково-інформаційний обмін є базовим процесом, що забезпечує ефективність функціонування науково-дослідних систем та ОС загалом. Його якість та результативність безпосередньо залежать від дотримання головних принципів – *достовірності, доступності та оперативності інформації*.

Достовірність означає гарантію того, що інформація є точною, перевіреною і не містить помилок чи викривлень. У НІД, особливо в ОС, критично важливо мати підтверджені факти, надійні дані та достовірні джерела, адже від цього залежить обґрунтованість рішень та ефективність заходів. Обґрунтування достовірності базується на наукових методах верифікації, стандартах якості даних і використанні багаторівневих процедур контролю інформації (ISO 9001 [13], стандарти управління якістю даних). Закон України «Про наукову і науково-технічну діяльність» [9] підкреслює необхідність забезпечення достовірності НТІ як умови її використання у розробках і впровадженні інновацій.

Доступність характеризує можливість цільових користувачів своєчасно отримати необхідні інформаційні ресурси без технічних чи організаційних бар'єрів. Вона передбачає належну організацію інформаційної інфраструктури, використання уніфікованих стандартів обміну даними, а також забезпечення захищеного доступу з урахуванням рівнів конфіденційності. Особливо в ОС доступність інформації регламентується балансом між відкритістю та захистом даних. Відповідно до діючих наказів технічна підтримка інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем та систем спеціального зв'язку має бути організована так, щоб забезпечити якісний і стійкий доступ користувачів до необхідної інформації.

Оперативність зводиться до забезпечення своєчасності передачі та обробки інформації відповідно до вимог прийняття рішень і реагування на зміни обстановки. У НІД це означає мінімізацію часу від надходження інформації до її використання, що особливо важливо в умовах ОС з огляду на високий темп змін і критичність ситуацій. Цей принцип реалізується через застосування АС, інтегрованих платформ та протоколів швидкого обміну даними, що підтримуються сучасними ІКТ. Відповідно до Закону України «Про інформацію» [14] та нормативних актів щодо інформаційної безпеки, *оперативність* є ключовим фактором забезпечення функціональної готовності ОС.

Дотримання принципів *достовірності*, *доступності* й *оперативності* в науково-інформаційному обміні створює передумови для ефективного управління знаннями та інформаційними ресурсами, підвищення якості наукових досліджень і забезпечення національної безпеки. Ігнорування будь-якого з цих принципів може призвести до втрати критично важливої інформації, уповільнення прийняття рішень або виникнення помилок, що у ОС має особливо серйозні наслідки.

Основним елементом реалізації менеджменту НІД в ОС є *автоматизовані системи управління інформацією* (далі – АСУІ) в обміні НТІ. Обмін НТІ в ОС є критично важливим процесом, що забезпечує інтеграцію наукових досліджень і практичних розробок. АСУІ виступають технологічною базою для організації та оптимізації обміну даними між різними ЗВО, ВВНЗ, НУ, військовими підрозділами та виробничими підприємствами.

Визначимо основні функції АСУІ у контексті обміну інформацією: *централізоване зберігання* (єдині сховища для наукових даних, аналітичних звітів і технологічних розробок); *формалізація даних* (стандартизовані формати, які забезпечують інтероперабельність між системами різних організацій); *інтеграція джерел* (автоматичне агрегування інформації з баз даних, цифрових бібліотек та інших ресурсів).

АСУІ в обміні НТІ мають базуватися на технологіях хмарних платформ, багаторівневого шифрування, мереж із низькою затримкою. Основними викликами на шляху використання АСУІ є висока залежність від якості технологічної інфраструктури, необхідність інтеграції різних форматів і протоколів передачі даних, а також загроза несанкціонованого доступу до конфіденційної інформації.

Не менш важливими аспектами побудови моделей організації менеджменту НІД, для реалізації обміну НТІ, є використання *баз даних, знань і цифрових бібліотек*. Ці інструменти забезпечують зручний доступ до знань, знижуючи часові та організаційні витрати на пошук необхідної інформації. *Бази даних* організують структуру збереження інформації у формі таблиць, що дає змогу швидко отримувати доступ до

технічної документації, креслень, патентів та інших даних. У контексті обміну вони допомагають об'єднати інформацію різних установ у єдиний інфраструктурний комплекс. *Бази знань* призначені для збереження експертних знань у формі правил, сценаріїв або аналітичних моделей. У процесі обміну вони сприяють автоматизації аналізу даних і генерації рекомендацій. Наприклад, в ОС вони можуть використовуватися для оптимізації процесів проєктування нових зразків озброєння. *Цифрові бібліотеки* забезпечують централізований доступ до наукових публікацій, технічних звітів, нормативної документації та інших ресурсів. Цифрові бібліотеки значно прискорюють обмін інформацією завдяки пошуковим системам, які використовують технології ШІ та семантичного аналізу.

Перевагами такого обміну є прозорість завдяки доступу до актуальної інформації для всіх учасників, оперативність у миттєвому оновленні та поширенні даних, а також можливість глобальної інтеграції інформації з урахуванням безпекових обмежень. Основними викликами при цьому є необхідність забезпечення сумісності між різними системами зберігання даних, усунення дублювання або суперечливості інформації через відсутність єдиного стандарту та високі вимоги до підтримки актуальності ресурсів.

Обмін НТІ у сфері досліджень тактики дій підрозділів, тактико-технічних характеристик озброєння та військової техніки (далі – ОВТ) має низку особливостей, які визначаються специфікою галузі. Однією з провідних характеристик є високий рівень секретності й захищеності інформації. Дані, що стосуються тактики, технічних характеристик ОВТ, здебільшого класифікуються як державна таємниця. Для забезпечення безпеки пропонуємо використовувати багаторівневі криптографічні механізми, протоколи захищеного з'єднання та спеціалізовані апаратні рішення. Інформація у цій сфері є високо спеціалізованою. Це можуть бути технічні параметри озброєння, результати випробувань або тактичні сценарії. Усі дані мають бути наведені у стандартизованих форматах і з використанням уніфікованої термінології, що дасть змогу забезпечити точність їхнього сприйняття та інтерпретації між різними учасниками процесу.

Окреме місце в обміні НТІ займають *інформаційно-аналітичні матеріали вивчення та впровадження досвіду* (далі – ІАМ ВВД), включно з ідентифікованими бойовими прикладами [15]. Їх значення у системі НІД зводиться до інтеграції отриманого досвіду в поточні й майбутні операції, а також у підготовці тактичних і стратегічних рішень. Основною особливістю ІАМ ВВД є їхня висока практична цінність, зокрема, можливість застосування конкретних бойових сценаріїв для навчання та адаптації підрозділів до реальних умов, а також для аналізу й удосконалення існуючих методів ведення бойових дій і покращання тактико-технічних характеристик ОВТ. Накопичення матеріалів ВВД і забезпечення до них доступу авторизованим користувачам системи є важливим для формування бази знань і підвищення рівня обізнаності фахівців.

Оперативність передачі інформації є ще однією критично важливою вимогою. У дослідженнях військової тактики швидкий доступ до результатів моделювань чи експериментів може суттєво впливати на ухвалення рішень щодо модернізації техніки або розробки нових тактичних прийомів. Інтеграція міжвідомчих структур до системи менеджменту НІД в ОС є важливою особливістю. Обмін інформацією часто відбувається між різними установами (цивільними та військовими), такими як ЗВО, ВВНЗ, науково-дослідні інститути, виробники оборонної техніки чи військові штаби, органи військового управління (далі – ОВУ). Це вимагає створення інтегрованих мереж, які дають змогу учасникам ефективно співпрацювати, дотримуючись при цьому вимог захищеності інформації.

Актуальність інформації також відіграє важливу роль. Дані про технічні характеристики, результати випробувань чи аналіз тактичних сценаріїв мають постійно оновлюватися. Для цього пропонуємо використовувати АС синхронізації, що забезпечать доступ до найсвіжіших результатів. Отже, обмін НТІ у сфері досліджень тактики, ОВТ передбачає поєднання високої оперативності, захищеності, стандартизації та актуальності даних.

Управління НІД в ОС потребує ефективної роботи з великими обсягами даних, які генеруються з різноманітних джерел. Це можуть бути розвіддані, результати наукових досліджень, дані про розробки та випробування ОВТ, інноваційні проєкти, а також геополітична інформація. Аналіз великих даних (Big Data) дає змогу створювати прогностичні моделі, які визначають потенційні загрози, оцінюють розвиток технологій та тенденції у військовій (військово-технічній) сфері.

В ОС великі дані, інтегровані за принципами стандартизації, автоматизації та централізованої обробки, пропонуємо використати для прогнозного моделювання тактичних сценаріїв, оптимізації логістичних ресурсів і стратегічного планування із застосуванням машинного навчання та адаптивної аналітики. ШІ забезпечить автоматизацію визначення пріоритетності запитів, раціональний розподіл ресурсів, підтримку стратегічного менеджменту через аналіз трендів і прогнозування, а також кібербезпеку шляхом виявлення загроз і ініціації захисних заходів. Інтеграція ШІ у процеси прийняття рішень може підвищити адаптивність і ефективність управління.

Геоінформаційні системи (далі – ГІС) є невід'ємною складовою науково-інформаційного менеджменту в ОС, забезпечуючи збір, аналіз і інтеграцію просторових даних для підтримки тактичних і стратегічних рішень. Вони використовуються для моделювання оперативних сценаріїв, прогнозування дій противника, оптимізації маршрутів переміщення військ та розробки озброєння з урахуванням географічних і кліматичних умов. Крім того, ГІС сприяють підвищенню ефективності логістичних процесів через визначення оптимальних

шляхів постачання ресурсів. Інтеграція ГІС у менеджмент НІД базується на створенні централізованих баз даних, що постійно оновлюються, включно з інформацією про інфраструктурні об'єкти, зони бойових дій і природні особливості територій.

Сучасний менеджмент НІД поєднує великі дані, штучний інтелект і геоінформаційні технології, забезпечуючи стандартизацію інформації, оперативний аналіз і прогнозування загроз. Такий підхід дає змогу інтегрувати різні структури, підтримувати стратегічні рішення та значно підвищувати оборонні можливості. НІД в ОС характеризується складною системою інформаційних потоків, які забезпечують взаємодію між НУ, ОВУ та виробниками озброєння. Основні типи інформаційних потоків наведено у табл. 1.

Таблиця 1

Основні типи інформаційних потоків науково-інформаційної діяльності в оборонному секторі

Тип інформаційних потоків	Зміст	Особливості	Інструменти
Тактичні інформаційні потоки. Тактична наукова інформація забезпечує оперативну підтримку рішень на полі бою, що вимагає швидкого обміну даними. Наприклад, використання ОВУ наукових розробок для аналізу в часі близькому до реального, таких як моделювання бойових сценаріїв або оцінка ефективності застосування озброєння	Технологічні інструкції, алгоритми управління озброєнням, розвіддані	Висока швидкість передачі, захист даних від втручання	АС управління, сенсорні мережі та аналітичні алгоритми
Стратегічні інформаційні потоки. Цей тип потоків обслуговує довгострокове планування у сфері оборонних наукових досліджень, таких як розробка перспективних зразків військової техніки чи технологій подвійного призначення	Прогнози науково-технічних трендів, стратегічні звіти, результати випробувань	Висока точність даних, інтеграція з геополітичними факторами	Спеціалізовані бази даних, системи підтримки рішень, аналітика великих даних
Наукові інформаційні потоки. Об'єднують результати наукових досліджень і розробок, обмін знаннями між ОВУ, науковими центрами та оборонними установами. Вони є основою для впровадження інновацій у військову сферу	Наукові статті, технічні звіти, дані випробувань, патенти	Довгострокове збереження, доступність для різних структур	Цифрові бібліотеки, платформи відкритих даних, системи управління знаннями

Організація НІД в ОС має стратегічне значення для забезпечення технологічної переваги, підтримки національної безпеки та впровадження інновацій у військову справу. Вибір відповідної моделі організації НІД залежить від вимог до обміну, зберігання та захисту даних, а також від особливостей функціонування оборонної інфраструктури.

Централізована модель НІД в ОС є підходом, що забезпечує інтеграцію всієї НТІ в одному центрі управління, створюючи основу для стратегічного планування, стандартизації та уніфікації даних [16]. Основними характеристиками такої моделі є централізоване сховище з високим рівнем захисту, єдина система управління інформаційними потоками, яка інтегрує дані з різних наукових і військових джерел, жорстка ієрархія доступу до інформації.

Ця модель має значні переваги, включно з уніфікованими стандартами обробки і зберігання даних, що сприяє ефективності моніторингу інформаційних потоків і прийняття рішень. Однак, вона не позбавлена недоліків, таких як вразливість до атак на центральний вузол і менша адаптивність до швидких змін у тактичній ситуації. Прикладом застосування централізованої моделі є оборонні інформаційно-аналітичні центри, які об'єднують дані, зокрема, від розвідувальних супутників, для стратегічного прогнозування. Це доводить її ефективність у довгостроковому плануванні й забезпеченні безперервності інформаційних процесів.

Децентралізована модель НІД в ОС передбачає розподіл інформації між регіональними або функціональними вузлами, кожен з яких спеціалізується на окремих аспектах діяльності. Такий підхід є особливо актуальним в умовах воєнного стану, коли централізовані вузли можуть стати недоступними через пошкодження або загрози.

Основними характеристиками моделі є розподіл даних між різними вузлами, які функціонують автономно, та локалізоване управління інформацією і прийняттям рішень. Її перевагами є стійкість до втрати окремих вузлів або каналів зв'язку, а також висока адаптивність до швидко змінюваних умов. Однак децентралізована модель має й недоліки, такі як ускладнена інтеграція даних і зростання витрат на координацію інформаційних потоків. Прикладом реалізації такої моделі є розподілені бази даних, які використовуються локальними науково-дослідними центрами і військовими підрозділами. Як зазначено в роботі [17], децентралізація сприяє ефективному обміну інформацією між мобільними підрозділами

навіть в умовах бойових дій, забезпечуючи їх автономність і оперативність.

Гібридна модель управління НІД в ОС поєднує централізоване стратегічне управління із децентралізованою оперативною підтримкою, забезпечуючи гнучкість та баланс між безпекою і доступністю даних. Центральний вузол координує довгострокові завдання, тоді як локальні вузли обробляють тактичну інформацію та обмінюються даними через захищені канали. Такий підхід потребує потужної технічної інфраструктури для інтеграції різнорідних даних, проте він сприяє стійкості інформаційної системи та адаптивності до змін. Прикладом реалізації цієї моделі є NATO Information Exchange System («NIES»), де централізоване керування поєднується із децентралізованими механізмами обміну даними, що, згідно з дослідженням [18], забезпечує ефективну співпрацю між оборонними структурами.

Централізація забезпечує стратегічне зберігання та довгострокову безпеку наукових даних, тоді як децентралізація дає змогу створювати автономні вузли інформаційного обміну, що є критично важливим у ситуаціях воєнного часу. Гібридна модель поєднує ці підходи, оптимізуючи інтеграцію та ефективний обмін даними в умовах складного й динамічного інформаційного середовища. Для формування уявлення про склад і конфігурацію системи менеджменту НІД в ОС автором розроблено її загальну архітектуру, наведену на рис. 1.

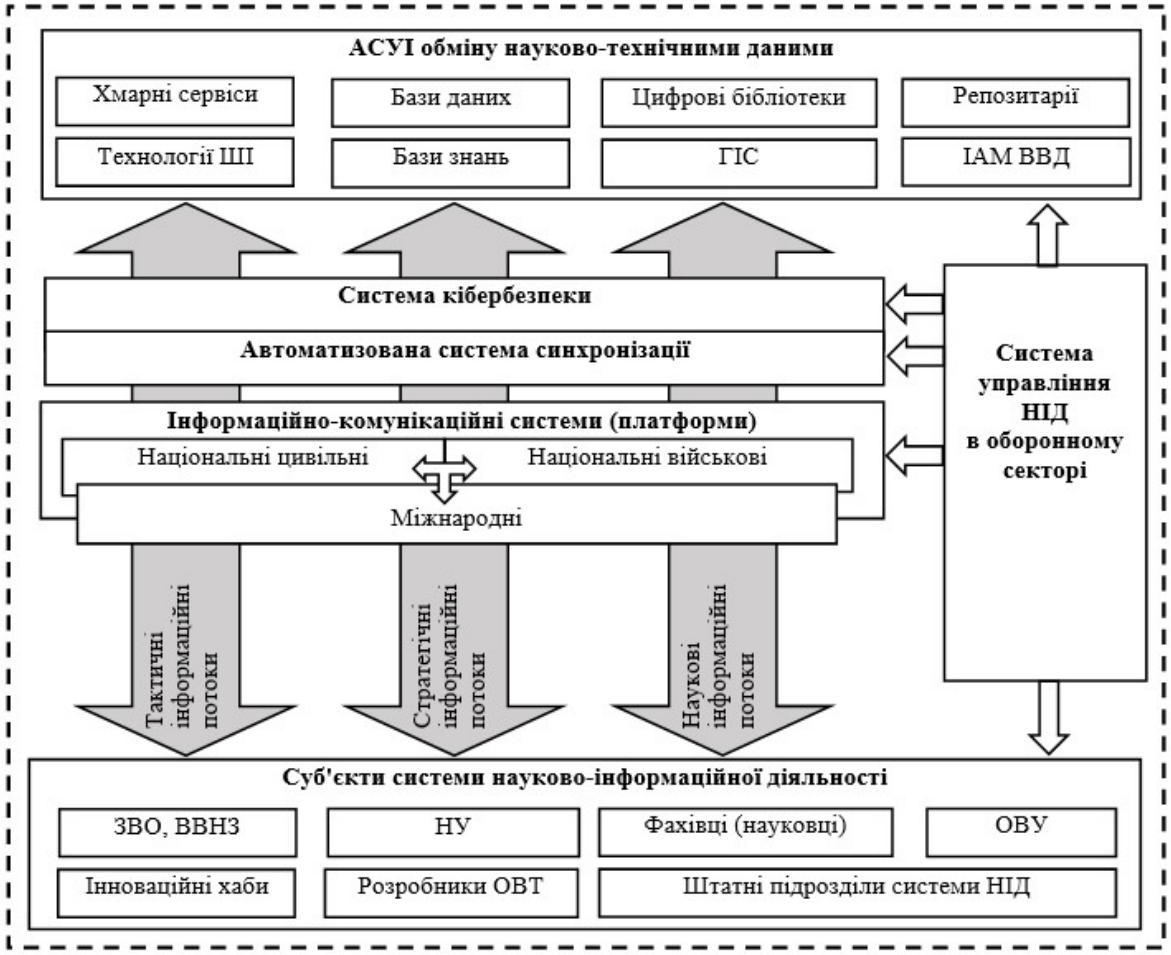

Рисунок 1 – Загальна архітектура системи менеджменту науково-інформаційної діяльності в оборонному секторі

Основними функціями системи менеджменту НІД в ОС вважаємо *управління*, *моніторинг*, *інформаційний супровід та автоматизацію процесів*, *аналітичну обробку даних, інтеграцію з іншими системами, забезпечення безпеки даних*. Запропонована архітектура системи менеджменту НІД в ОС інтегрує мережу технічних засобів, які забезпечують взаємодію з користувачами та джерелами наукових чи технічних даних (суб'єктами) через різноманітні інтерфейси та способи комунікації, включно із пасивними та активними режимами роботи. Засоби комунікаційної інфраструктури, що містять стандарти та протоколи передачі даних, забезпечують інтеграцію пристроїв фізичного рівня в єдине інформаційне середовище, створюючи умови для ефективної обробки та аналізу даних. Така архітектура дає змогу на кожному рівні, від фізичного до стратегічного, використовувати інструменти обчислювальних технологій для впорядкування, обробки та аналізу інформації. Застосування хмарних обчислень і

високопродуктивних обчислювальних систем, включно із системами ШІ, значно підвищує ефективність менеджменту НІД, забезпечуючи швидку обробку великих обсягів даних, адаптацію до змін середовища та інтеграцію різнорідних інформаційних потоків.

Перевагою інтегрованого підходу до НІД є його масштабованість і розподіленість, що забезпечує попередню аналітику даних безпосередньо на місцях збору з можливістю централізованого аналізу в хмарних сервісах. Така архітектура сприяє оперативності прийняття рішень, знижує затримки передачі даних і підвищує рівень інформаційної безпеки. Застосування систем ШІ в цій структурі допомагає автоматизувати обробку даних, виявлення загроз і підтримку прийняття рішень, що є особливо важливим у сучасних умовах високої динамічності загроз і технологічної конкуренції.

НІД в ОС вимагає адаптивних моделей організації, які враховують специфіку військових операцій, рівень ризиків і наявні технологічні ресурси. Розробка таких моделей має базуватися на сучасних наукових підходах, інтеграції міжнародного досвіду та передових технологій. Це дає змогу забезпечити ефективний обмін інформацією, мінімізувати ризики та створити технологічну перевагу в ОС.

Методи забезпечення доступу до критично важливої НТІ в ОС мають враховувати потребу в конфіденційності, оперативності та ефективному управлінні інформаційними потоками. Впровадження багаторівневого доступу допоможе створити оптимальний баланс між захистом інформації та її доступністю. Така модель базується на чіткому розподілі відповідальності між категоріями користувачів, автоматизації регулювання потоків даних і мінімізації бюрократичних процедур, що забезпечить швидкий і безпечний доступ до потрібної інформації. Інтегровані платформи для обміну НТІ є основним інструментом стратегічного менеджменту. Вони забезпечать гнучкість інформаційних систем, можливість адаптації до технологічних змін та автоматизацію аналізу великих масивів даних через впровадження механізмів ШІ. Це сприятиме прийняттю своєчасних і обґрунтованих рішень, підвищуючи ефективність функціонування ОС.

Захищені канали зв’язку є критичним компонентом управління кіберризиками, що впливають на цілісність інформаційних потоків. Для їх ефективного функціонування необхідно проводити регулярну оцінку загроз, впроваджувати міжнародні стандарти кіберзахисту (ISO 27001, NIST Cybersecurity Framework) та оптимізувати логістику передачі інформації, враховуючи швидкість обміну даними та захист критичних вузлів.

Інтелектуальні системи безпеки автоматизують виявлення загроз, прогнозують ризики та адаптивно оновлюють захист у реальному часі, мінімізуючи вразливості. Аудит і контроль доступу забезпечують стратегічне управління безпекою через аналітику великих даних, головні показники ефективності та навчальні програми, знижуючи людські ризики. Ефективне управління НІД вимагає інтегрованого підходу, що поєднує аналітику, прогнозування загроз і стратегічний розподіл ресурсів для забезпечення безперервності функціонування наукових систем. Чітко структуровані інформаційні потоки та сучасні методи захисту сприяють прийняттю рішень, розвитку військових інновацій і посиленню науково-технічного потенціалу ОС.

Захист даних у процесі НІД базується на принципах *конфіденційності, цілісності та доступності*. Основними методами є криптографічне шифрування, системи резервного копіювання та моніторинг мережевих загроз, що дає змогу запобігти витокам даних та атакувальним діям у кіберпросторі. Дослідження І. Килимника розглядає сучасні виклики інформаційної безпеки та механізми їх подолання [19].

Криптографічні технології відіграють провідну роль у захисті НТІ. Використання асиметричного шифрування (RSA, ECC – elliptic curve cryptography) та квантово-стійких алгоритмів підвищує стійкість оборонних систем до атак із використанням квантових обчислень. Ефективне управління доступом передбачає ролеві моделі доступу («RBAC» – role-based access control), що допомагають чітко розмежовувати права користувачів. Біометричні методи автентифікації сприяють підвищенню рівня безпеки, а аудит та контроль доступу допомагають виявляти несанкціоновані дії. Згідно з дослідженням С. Легомінової, впровадження SIEM-систем (security information and event management) дає змогу здійснювати комплексний аналіз поведінкових факторів користувачів та забезпечувати динамічний контроль інцидентів інформаційної безпеки [20]. Інтеграція сучасних технологій кіберзахисту в НІД ОС забезпечить стійкість до атак, захист критичних даних та підвищення загальної ефективності безпекових заходів, що має головне значення в умовах високих інформаційних ризиків.

Міжнародне науково-технічне співробітництво є фундаментальним чинником розвитку глобальних наукових мереж. Воно прискорює науковий прогрес через обмін знаннями та технологіями між країнами, сприяє формуванню спільних дослідницьких програм, які ефективно об'єднують ресурси й експертний потенціал, і забезпечує доступ до міжнародних баз даних та наукової інфраструктури. Це співробітництво інтегрує наукові досягнення у глобальні інноваційні процеси, посилюючи конкурентоспроможність національних систем.

Інтеграція даних між військовими та цивільними НУ є критично важливою для забезпечення інформаційної безпеки та підвищення ефективності досліджень. Основними механізмами інтеграції виступають захищені платформи обміну даними з криптографічними методами захисту, автоматизовані системи аналізу великих масивів інформації, що забезпечують оперативність обробки, та спільні дослідницькі центри, які залучають експертів з обох секторів для розробки передових технологій.

Розглянемо діючі цифрові платформи, які є провідними інструментами науково-інформаційного

обміну, що сприяють глобальному доступу до досліджень, міжнародній співпраці та інтеграції знань.

«OpenAIRE» (https://www.openaire.eu/), провідна європейська платформа відкритого доступу, забезпечує автоматизовану перевірку індексації наукових статей, інтеграцію з репозиторіями університетів та фінансування відкритих досліджень у межах європейських програм.

«Zenodo» (https://zenodo.org/) слугує репозиторієм для збереження наукових результатів, підтримуючи різні формати даних і забезпечуючи довготривалу архівацію наукових матеріалів. Вона також інтегрується з «ORCID», що дає змогу автоматично прив'язувати публікації до профілю дослідника.

«ResearchGate» (https://www.researchgate.net/), соціальна мережа для науковців, сприяє обміну статтями, публікації препринтів, обговоренню результатів досліджень і автоматичному відстеженню цитувань.

«Academia.edu» (https://www.academia.edu/) надає безкоштовний доступ до наукових матеріалів і дає змогу створювати персональні профілі для представлення досягнень, а також аналізувати вплив досліджень через перегляди та завантаження.

«Mendeley» (https://www.mendeley.com/) є платформою для управління науковими джерелами, яка пропонує інструменти для організації бібліографії, створення дослідницьких груп і синхронізування даних між пристроями.

«COST» (European Cooperation in Science and Technology (https://www.cost.eu/)) це організація, що фінансує дослідницькі та інноваційні мережі й підтримує міжнародну наукову співпрацю, фінансуючи проєкти, організовуючи конференції та надаючи гранти.

Інтеграція міжнародних платформ науково-інформаційного обміну, таких як «ResearchGate», «Academia.edu», «Mendeley» і «COST», в ОС України може значно підвищити ефективність управління науковими даними, сприяти міжнародній співпраці та забезпечити безпеку критично важливої інформації. Ці платформи дають змогу українським військовим науковцям обмінюватися знаннями з міжнародними експертами, аналізувати науковий вплив через відстеження цитувань, організовувати бібліографічні дані та формувати дослідницькі групи для обговорення стратегічних питань. Крім того, вони сприяють залученню грантів для оборонних досліджень і інтеграції українських НУ у європейські наукові мережі. Ці платформи сприятимуть продуктивності наукових досліджень, полегшуючи доступ до даних і обмін інформацією між дослідниками.

Можливими сценаріями співпраці з науково-інформаційними системами України пропонуємо наступні.

1. Інтеграція з «Українським національним грідом». Використання «OpenAIRE» та «Zenodo» для архівування оборонних досліджень. Інтеграція з «ResearchGate» для міжнародного обміну знаннями. Використання «Mendeley» для управління бібліографічними даними.

2. Співпраця з Українською науково-освітньою телекомунікаційною мережею «УРАН». Використання «COST» для фінансування оборонних (подвійного призначення) досліджень. Інтеграція з «Academia.edu» для поширення результатів досліджень. Використання «Zenodo» для довготривалого збереження даних.

3. Впровадження в Національний репозиторій академічних текстів («НРАТ», https://nrat.ukrintei.ua/). Використання «OpenAIRE» для автоматизованої перевірки індексації досліджень. Інтеграція з «ResearchGate» для міжнародної співпраці. Використання «Mendeley» для управління науковими джерелами.

ОС України стикається з низкою викликів у сфері науково-інформаційного менеджменту, що впливають на впровадження інноваційних технологій (створення інноваційних хабів). Основними проблемами є застаріла інформаційна інфраструктура, обмежений доступ до передових технологій через міжнародні санкції та недостатнє фінансування оборонних наукових досліджень. Ці фактори ускладнюють інтеграцію сучасних рішень у практичну діяльність і знижують ефективність інноваційних розробок. Для подолання цих викликів пропонуємо створення національних технологічних кластерів, створення R&D-центрів (research and development) і залучення комерційного сектору до оборонних досліджень.

Ще однією провідною проблемою є сумісність систем різних рівнів. Розрізнені стандарти даних у військових і цивільних НУ, слабка інтеграція між секторами та недостатній рівень кібербезпеки значно обмежують ефективність обміну інформацією. Для вирішення цих питань пропонуємо створити єдину національну платформу обміну даними, запровадити уніфіковані протоколи сумісності та використовувати квантово-стійкі криптографічні алгоритми для захисту інформації. Доцільно розглядати три можливі інноваційні напрями розвитку моделей організації менеджменту НІД в ОС України.

1. *Використання хмарних обчислень для управління НТІ.* Впровадження хмарних технологій дає змогу створити інтегровану інфраструктуру для збереження та обробки оборонних наукових даних. Національна хмарна платформа має включати: захищені канали зв'язку для інтеграції з військовими та цивільними НУ; автоматизоване управління доступом на основі ролевих моделей («RBAC») та поведінкової аналітики; динамічне масштабування ресурсів відповідно до потреб дослідницької діяльності. Перевагами цього підходу є гнучкість (можливість адаптації до змінних обчислювальних вимог), захищене збереження (ізоляція критичних даних у віртуальних приватних хмарах («VPC»)), резервне копіювання (гарантія збереження інформації у випадку технічних збоїв).

2. *Впровадження блокчейн-технологій для забезпечення інформаційної безпеки.* Застосування блокчейн-технологій сприяє посиленню захисту оборонної НТІ шляхом децентралізованого збереження даних, що гарантує їхню автентичність. Введення цифрових паспортів безпеки, забезпечить

унікальний криптографічний підпис кожного документа. Запровадження смарт-контрактів, що регламентують контроль доступу та безпечну передачу інформації. Перевагами цього підходу є незмінність даних (забезпечення цілісності інформації, прозорість (можливість аудиту та відстеження будь-яких змін), захист від кібератак (мінімізація ризиків несанкціонованого доступу).

3. *Інтеграція ШІ для автоматизації управління НТІ*. Використання технологій ШІ дає змогу оптимізувати обробку великих масивів даних у дослідницькій діяльності. Основні напрями впровадження охоплюють застосування нейронних мереж для автоматизованого аналізу інформації, прогнозування загроз на основі аналізу поведінкових патернів користувачів, а також оптимізацію інформаційних потоків через автоматизовану класифікацію наукових результатів. Перевагами цього підходу є висока швидкість обробки даних (автоматизація аналізу великих інформаційних масивів), адаптивність (можливість самонавчання та вдосконалення алгоритмів безпеки), мінімізація людського фактора (зменшення ймовірності помилок під час управління науковими даними).

Зростаюча складність інформаційних систем ОС вимагає відповідної підготовки фахівців. Розробка спеціалізованих освітніх програм сприятиме формуванню компетентного кадрового потенціалу, здатного ефективно управляти великими обсягами НТІ та забезпечувати її кіберзахист. Практичні курси з інформаційної безпеки та кіберзахисту мають стати невід'ємною частиною професійної підготовки. Запропоновані заходи сприятимуть удосконаленню технології менеджменту НІД в ОС України. Їхня реалізація дасть змогу: підвищити ефективність управління науковими даними через впровадження інноваційних технологій; забезпечити надійний рівень інформаційної безпеки, зменшуючи ризики витоку даних; оптимізувати процеси взаємодії НУ та формувати кадровий потенціал для роботи з сучасними інформаційними системами. Комплексний підхід до управління НТІ є стратегічно важливим для забезпечення технологічної переваги ОС та гарантування національної безпеки.

Висновки й перспективи подальших досліджень

Викладене у дослідженні формує концептуальну основу створення моделей організації менеджменту науково-інформаційної діяльності в оборонному секторі, акцентуючи увагу на централізованих, децентралізованих і гібридних типах організації. Запропоновані підходи дають змогу адаптувати інформаційні процеси до динамічних умов сучасного військового середовища.

Комплексне застосування інформаційно-комунікаційних технологій, автоматизованих систем управління та методів кіберзахисту сприятиме оптимізації обміну науковими даними. Це забезпечить достовірність, оперативність і захищеність інформаційних потоків, що є критично важливим для стратегічного планування та реагування на загрози.

Запропоновані підходи інтеграції штучного інтелекту, великих даних та геоінформаційних систем створюють умови для автоматизації аналітичних процесів, підвищуючи точність прогнозування та ефективність використання наукових ресурсів. Це сприятиме розробці адаптивних моделей управління інформацією, що відповідають вимогам оборонної сфери.

Підвищення інформаційної безпеки на основі використання хмарних обчислень та блокчейн-технологій дасть змогу реалізувати інноваційні механізми захисту даних, мінімізуючи ризики втрати або компрометації критичної інформації. Ці підходи забезпечать стійкість інформаційної інфраструктури та підтримають її безперервне функціонування в умовах кіберзагроз. Розглянуте у статті доводить необхідність системного підходу до реалізації моделей організації управління науково-інформаційної діяльності в оборонному секторі, підкреслюючи значущість стратегічної інтеграції технологій, забезпечення інформаційної безпеки та адаптації до сучасних викликів.

Подальшими напрямами досліджень, що сприятимуть підвищенню ефективності та безпеки науково-інформаційної діяльності в оборонному секторі України, є розроблення інтегрованих платформ обміну науковою інформацією, стандартизація обміну даними в системі і підготовка фахівців, які працюватимуть за спрямуванням.

Список бібліографічних посилань

1. Poberezhna Z., Petrova Y., Slimani K. Information technologies in logistics processes of enterprises in the aviation industry: International workshop on Computational Methods in *Systems Engineering.* 2024. URL: https://www.researchgate.net/publication/383228008_Information_technologies_in_logistics_processes_of_enterprises_in_the_aviation_industry (accessed: 18 March 2025). **2. Chernenko Y., Danchenko O., Mysnyk B., Bielova O., Adamov O.** Optimising Housing and Communal Services Management Through Digital Transformation and Integrated Information Systems. *In E. Faure et al. (Eds.), Information Technology for Education, Science, and Technics: Lecture Notes on Data Engineering and Communications Technologies.* 2024. Vol. 222. Cham: Springer. DOI: 10.1007/978-3-031-71804-5_3. **3. Shanmugapriya M., Venkatramaraju D.** Modern business decisions based on cloud-based genetic algorithms with unleashed strategic optimisation. *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM),* 2024. Noida, India, 1-6. DOI: 10.1109/ICIPTM59628.2024.10563511 4. Wu J. Research on optimising university management service systems based on student needs. *Journal of Modern Education and Culture,* 2024. № 1(1). DOI: 10.70767/jmec.v1i1.77. **5. Stelmach A.** Digital transformation: Impact of modern technologies and project management on optimisation of production processes in the era of Industry 4.0. *Decision Making in Manufacturing and Services,*

2025. P. 39-47. DOI: 10.7494/dmms.2024.si.6650. **6. Suharto P., Mia A.** Defence Management: Integrating strategy, innovation, and leadership in the modern era. *Cv. Aksara global Akademia.* 2025. URL: https://www.researchgate.net/publication/388387686_DEFENSE_MANAGEMENT_Integrating_Strategy_Innovation_and_Leadership_in_the_Modern_Era (accessed: 18 March 2025). **7. Тристан А. В., Ларін В. В., Гмиря В. П., Стріха С. В., Костащук М. М., Піонтківський П. М.** Форсайт як інноваційний інструмент планування та реалізації наукових технологій в оборонно-промисловому комплексі. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем,* 2024. № 1(26 (I). С. 93–106. DOI: 10.46972/2076-1546.2024.26.08. **8. Bugayko D., et al.** Creating an innovative ecosystem for developing unmanned aviation in Ukraine: Synergy between science and industry. *Marketing of Scientific and Research Organisations,* 2024. № 51(1). P. 87–116. DOI: 10.2478/minib-2024-0005. **9. Про наукову і науково-технічну діяльність** : Закон України № 848-VIII від 09.04.2025. URL: https://zakon.rada.gov.ua/laws/show/848-19#Text (дата звернення: 18.03.2025). **10. Аврунін О. Г. та ін.** Інтелектуальні системи автоматизації: монографія. Кременчук : Видавництво «НОВАБУК», 2021. 321 с. DOI: 10.30837/978-617-639-347-4. **11. Kuschnaroff F., Bayma F.** Critical analysis of cyberslacking in organisational structures. *Journal of Human Resource and Sustainability Studies.* 2014. № 2. P. 70–90. DOI: 10.4236/jhrss.2014.22007. **12. Bawa S., Attah P., Agougil A., Harch M.** Impact of knowledge management on firms' innovation performance. *Technology and Investment,* 2023. № 14. P. 293–328. DOI: 10.4236/ti.2023.144018. **13. ISO 9001:2015.** Quality management systems – Requirements. Geneva: International Organization for Standardization. URL: https://www.iso.org/standard/62085.html (accessed: 18 March 2025). **14. Про інформацію:** Закон України № 2657-XII від 02.10.1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 18.03.2025). **15. Інструкція з організації вивчення та впровадження досвіду в навчальних закладах, навчальних частинах (центрах) ЗС України** : Наказ Головнокомандувача ЗС України від 19.02.2025 № 85. ТКП 7-00(162). **16. Smith J., Brown A., Taylor M.** The role of centralised models in strategic data management. *Journal of Defence Studies.* 2020. № 15(2). P. 123–140. DOI: 10.5465/AMR.2011.59330958. **17. Johnson B., Kendall A., Green J., Nagy B., Dogum G.** Blockchain at the tactical edge: Enabling an Internet of Battlefield Things. *American Journal of Computer Science and Technology.* 2023. № 6(4). P. 126–147. DOI: 10.11648/j.ajcst.20230604.12. **18. Johnsen F., Hauge M.** Interoperable, adaptable, information exchange in NATO coalition operations. *Journal of Military Studies.* 2022. № 11. DOI: 10.2478/jms-2022-0005. **19. Килимник І. І.** Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. № 2(76). DOI: 10.24144/2307-3322.2022.76.2.8. **20. Легомінова С., Якименко Ю., Мужанова Т., Капелюшна Т.** Вплив управління інцидентами на функціонування системи управління інформаційною безпекою організації. *Телекомунікаційні та інформаційні технології.* 2025. № 1. DOI: 10.31673/2412-4338.2025.014011.

APPROACHES TO IMPLEMENTING MANAGEMENT TECHNOLOGY FOR SCIENTIFIC AND INFORMATIONAL ACTIVITIES IN THE DEFENCE SECTOR

PIONTKIVSKYI Petro, PhD in Engineering, Senior Researcher, Korolyov Zhytomyr Military Institute, Zhytomyr, Ukraine, https://orcid.org/0000-0002-9103-5393

The article analyses the theoretical and practical aspects of developing and shaping approaches to implementing management technology for scientific and informational activities in the defence sector. ***Formulation of the problem in general.*** *The study aims to develop recommendations for managing scientific and informational processes in the defence sector, considering contemporary challenges in information security, technological trends, and the integration of information systems.*

Research methods. *The study employs theoretical methods, particularly analysing studies on the functioning and application of information and communication systems. Approaches from management theory, decision optimisation methods, and complex systems modelling were utilised during the research.*

Literature review. *The analysis of recent scientific publications has confirmed the relevance and multifaceted nature of information technology applications and the critical importance of managing scientific and informational activities in the defence sector. At the same time, issues related to the specifics of data flows, possible models for organising scientific and informational activities, development directions, and the formation of effective management models for scientific and informational activities in the defence sector remain insufficiently addressed.*

Research novelty. *The novelty of the research lies in identifying key principles of scientific and informational exchange within the management system of scientific and informational activities in the defence sector. This includes integrating information flows between military and civilian research institutions and standardising data exchange protocols.*

Theoretical and practical significance. *The article proposes a novel approach to designing the overall architecture of a management system for scientific and informational activities. Functional roles of key system elements and their interactions are substantiated to enhance the monitoring and management of information flows. The practical significance of the research is defined by its focus on implementing modern approaches to managing scientific and informational activities.*

Conclusions and future work. *The study establishes a conceptual framework for management technology in scientific and informational activities within the defence sector, emphasising centralised, decentralised, and hybrid organisation models. Further research directions aimed at improving the efficiency and security of scientific and informational activities in Ukraine's defence sector include the development of integrated information exchange*

platforms, using quantum-resistant data encryption, standardising data exchange within the system, and training specialists in this field.

Keywords: *models of scientific and information management organisation, defence sector, system management architecture, information flows, principles of data exchange.*

References

1. Poberezhna, Z., Petrova, Y., & Slimani, K., (2024). Information technologies in logistics processes of enterprises in the aviation industry [online]. Available at: https://www.researchgate.net/publication/383228008_Information_technologies_in_logistics_processes_of_enterprises_in_the_aviation_industry [Accessed: 18 March 2025]. **2. Chernenko, Y., Danchenko, O., Mysnyk, B., Bielova, O., & Adamov, O.,** (2024). Optimising Housing and Communal Services Management Through Digital Transformation and Integrated Information Systems. In E. Faure et al. (Eds.), *Information Technology for Education, Science, and Technics: Lecture Notes on Data Engineering and Communications Technologies.. 222. Cham: Springer.* DOI: 10.1007/978-3-031-71804-5_3. **3. Shanmugapriya, M. M., & Venkatramaraju, D.,** (2024). Modern business decisions based on cloud-based genetic algorithms unleash strategic optimisation. *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM),* Noida, India, 1-6. DOI: 10.1109/ICIPTM59628.2024.10563511. **4. Wu, J.,** (2024). Research on the optimisation of university management service systems based on student needs. *Journal of Modern Education and Culture,* 1(1). DOI: 10.70767/jmec.v1i1.77. **5. Stelmach, A.,** (2025). Digital transformation: Impact of modern technologies and project management on optimisation of production processes in the era of Industry 4.0. *Decision Making in Manufacturing and Services,* P. 39-47. DOI: 10.7494/dmms.2024.si.6650. **6. Suharto, P., & Mia, A.** (2025). Defence Management: Integrating strategy, innovation, and leadership in the modern era [online].
Available at: https://www.researchgate.net/publication/388387686_DEFENSE_MANAGEMENT_Integrating_Strategy_Innovation_and_Leadership_in_the_Modern_Era [Accessed: 18 March 2025]. **7. Trystan, A. V., Larin, V. V., Gmyrya, V. P., Strikha, S. V., Kostashchuk, M. M., & Piontkivskyi, P. M.,** (2024). Foresight as an innovative tool for planning and implementing scientific technologies in the defence-industrial complex. *Problems of creating, testing, applying and operating complex information systems,* 1(26 (I), 93-106. DOI: 10.46972/2076-1546.2024.26.08. **8. Bugayko, D., et al.** (2024). Creating an innovative ecosystem for developing unmanned aviation in Ukraine: Synergy between science and industry. *Marketing of Scientific and Research Organisations.* 51(1), 87-116. DOI: 10.2478/minib-2024-0005. **9. On Scientific and Scientific-Technical Activities** [online] **:** Law of Ukraine № 848-VIII, 09.04.2025. Available at: https://zakon.rada.gov.ua/laws/show/848-19#Text [Accessed: 18 March 2025]. **10. Avrunin, O. G. et al.,** (2021). Intelligent Automation Systems: *Monograph. Kremenchuk: Publishing House «NOVABUK».* DOI: 10.30837/978-617-639-347-4. **11. Kuschnaroff, F., & Bayma, F.,** (2014). Critical analysis of cyberslacking in organisational structures. *Journal of Human Resource and Sustainability Studies,* 2, 70-90. DOI: 10.4236/jhrss.2014.22007. **12. Bawa, S., Attah, P., Agougil, A., & Harch, M.,** (2023). Impact of knowledge management on firms' innovation performance. *Technology and Investment,* 14, 293-328. DOI: 10.4236/ti.2023.144018. **13. ISO 9001:2015.** Quality management systems – Requirements. Geneva: International Organisation for Standardisation [online]. Available at: https://www.iso.org/standard/62085.html [Accessed: 18 March 2025]. **14. On Information** [online] **:** Law of Ukraine № 2657-XII, 02.10.1992. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Accessed: 18 March 2025). **15. Instructions on the organisation of study and implementation of experience in educational institutions, training units (centres) of the Armed Forces of Ukraine :** Order of the Commander-in-Chief of the Armed Forces of Ukraine No. 85 dated 19.02.2025. TKP 7-00 (162). **16. Smith, J., Brown, A., & Taylor, M.,** (2020). The role of centralised models in strategic data management. *Journal of Defence Studies.* 15(2), 123-140. **17. Johnson, B., Kendall, A., Green, J., Nagy, B., & Dogum, G.** (2023). Blockchain at the tactical edge: Enabling an Internet of Battlefield Things. American *Journal of Computer Science and Technology,* 6(4), 126-147. DOI: 10.11648/j.ajcst.20230604.12. **18. Johnsen, F., & Hauge, M.,** (2022). Interoperable, adaptable, information exchange in NATO coalition operations. *Journal of Military Studies,* 11. DOI: 10.2478/jms-2022-0005. **19. Kilymnyk, I. I.** (2023). Information society and information security. New challenges and ways to overcome information threats. *Scientific Bulletin of Uzhhorod National University. Series: Law,* 2(76). DOI: 10.24144/2307-3322.2022.76.2.8. **20. Legominova, S., Yakymenko, Y., Muzhanova, T., & Kapelyushna, T.,** (2025). The impact of incident management on the functioning of the organisation's information security management system. *Telecommunications and Information Technologies,* 1(2025). DOI: 10.31673/2412-4338.2025.014011.

Рукопис надійшов до редакції 20.06.2025
Рукопис прийнято до друку після рецензування 12.08.2025
Дата публікації 29.08.2025