Методологічні та практичні основи інформаційно-аналітичного забезпечення органів військового управління: Стратегічна рамка розробки та впровадження

Частина I: Теоретико-методологічні основи інформаційно-аналітичного забезпечення (ІАЗ)

Ця частина закладає інтелектуальний фундамент інформаційно-аналітичного забезпечення, визначаючи його не просто як технічну функцію, а як критично важливу управлінську дисципліну, необхідну для досягнення інформаційної переваги в сучасній війні.

Глава 1: Сутність, мета та завдання ІАЗ у військовому управлінні

1.1. Визначення інформаційно-аналітичного забезпечення (ІАЗ)

Інформаційно-аналітичне забезпечення (ІАЗ) є невід'ємною складовою успішного функціонування будь-якої системи управління, особливо у військовій сфері.[1] Його слід визначати як безперервний, циклічний процес перетворення необроблених даних та розрізненої інформації на перевірені, синтезовані та прогностичні розвідувальні дані, призначені для підтримки прийняття рішень на всіх рівнях військового командування. Це

інтелектуальне ядро системи управління та контролю (С2).

ІАЗ є специфічною формою інтелектуальної діяльності, в процесі якої з первинної інформації, шляхом застосування визначеного алгоритму пошуку, накопичення, обробки та аналізу, створюється новий, вторинний аналітичний продукт. Цей продукт може мати форму аналітичної довідки, звіту, огляду, прогнозу чи оцінки.[2] Саме цей процес створення нового знання відрізняє ІАЗ від простого інформаційного забезпечення, яке обмежується лише наданням даних.

Ключова функція ІАЗ полягає в тому, щоб забезпечити особу, яка приймає рішення (командира), необхідною та достатньою кількістю аналітичної інформації для прийняття *єдиного правильного, найбільш ефективного управлінського рішення*, особливо в умовах невизначеності, кризи та браку часу.[2] Таким чином, ІАЗ виступає як інструмент, що цілеспрямовано знижує рівень невизначеності, відомий як "туман війни".

1.2. Стратегічні та тактичні цілі ІАЗ

Цілі інформаційно-аналітичного забезпечення є ієрархічними та взаємопов'язаними, охоплюючи як стратегічний, так і тактичний рівні.

Стратегічна мета ІАЗ полягає у досягненні та утриманні *інформаційної переваги* над противником. Це означає формування всеохопного та динамічного розуміння операційного середовища, що дозволяє командуванню діяти проактивно, а не реагувати на дії ворога. Досягнення цієї мети вимагає збору, обробки та аналізу достатнього обсягу інформації для надання споживачеві (командуванню) повного та якісного інформаційного продукту.[2] Інформаційна перевага, у свою чергу, є ключовою передумовою для захоплення та утримання ініціативи на полі бою.

Основна тактична мета ІАЗ полягає у суттєвому зменшенні "туману війни" та невизначеності для командирів, що призводить до мінімізації ризиків та підвищення ймовірності успішного виконання бойового завдання.[2] Це досягається шляхом надання рекомендацій щодо ефективних рішень та прогнозування їхніх наслідків. Сучасне ІАЗ не просто описує поточну ситуацію, а й активно "убезпечує, захищає керівників від ризиків, небезпек і викликів сьогодення", що перетворює його з пасивної служби підтримки на проактивний інструмент управління ризиками та використання можливостей.[2]

1.3. Основні завдання ІАЗ

Для досягнення поставлених цілей система ІАЗ виконує низку основних завдань, що охоплюють весь цикл управління:

- **Інформаційне забезпечення:** Своєчасне та безперервне надання релевантних даних командирам, штабам та підпорядкованим підрозділам. Це базове завдання, що створює основу для подальшого аналізу.[1]
- **Аналітичне забезпечення:** Проведення поглибленого аналізу операційного середовища, що включає оцінку можливостей та намірів противника, аналіз місцевості, погодних умов, а також стану інформаційного простору. Завдання полягає у виборі оптимальної стратегії з-поміж конкуруючих альтернатив на основі ретельного аналізу умов та наслідків.[2]
- **Прогнозування:** Розробка прогностичних оцінок щодо ймовірних сценаріїв розвитку обстановки та способів дій (СД) противника. Це дозволяє здійснювати випереджувальне планування та готувати контрзаходи.
- **Підтримка повного циклу управління:** ІАЗ є не одноразовим продуктом, а інтегральною частиною всього циклу управління військами, починаючи від аналізу завдання та планування операції (за процедурами, як-от Military Decision Making Process - MDMP) і закінчуючи контролем виконання та оцінкою результатів.[3]

Ефективне ІАЗ створює подвійний ефект. Прямий результат — це обґрунтоване, оптимальне управлінське рішення. Однак існує і непрямий, але не менш важливий результат — зміна уявлення самих управлінців про проблемну ситуацію.[2] Процес взаємодії з якісними аналітичними продуктами фундаментально покращує інтуїцію командира та його ментальну модель конфлікту. Таким чином, добре функціонуюча система ІАЗ постійно підвищує когнітивні здібності всього командного ешелону, перетворюючи військову структуру на організацію, що навчається та адаптується швидше за противника.

Глава 2: Основні принципи організації ІАЗ

Організація та функціонування системи ІАЗ ґрунтується на сукупності фундаментальних принципів, які забезпечують якість, релевантність та своєчасність аналітичних продуктів. Ці принципи можна згрупувати за сферами їх застосування.

2.1. Фундаментальні принципи обробки та аналізу інформації

Ці принципи є основою всього інформаційно-аналітичного процесу та визначають його ефективність.

- **Цілеспрямованість:** Вся діяльність ІАЗ повинна бути орієнтована на досягнення конкретних, чітко визначених цілей та вирішення поставлених завдань. Цей принцип є "базовим фундаментальним фактором" забезпечення результативності управлінської діяльності, оскільки він унеможливлює розпорошення зусиль та ресурсів.[1]
- **Об'єктивність та достовірність:** Інформація повинна базуватися на перевірених фактах, з чітким розмежуванням між фактичними даними та аналітичними оцінками чи припущеннями. Достовірність забезпечується глибоким розумінням реальності, правильним відбором фактів та виявленням причинно-наслідкових зв'язків.[2]
- **Повнота:** Надана інформація має бути достатньою для вирішення поставлених завдань та досягнення намічених цілей. Неповнота даних може призвести до хибних висновків та, як наслідок, до неоптимальних рішень.[1]
- **Своєчасність:** Аналітичні продукти повинні надаватися у такі терміни, щоб вони могли реально вплинути на процес прийняття рішень. Цінність своєчасної інформації може бути настільки великою, що заради неї іноді варто частково поступитися повнотою чи абсолютною достовірністю, за умови, що основний зміст не спотворюється.[2]
- **Альтернативність:** Система ІАЗ повинна забезпечувати можливість формулювання різних, конкуруючих оцінок та гіпотез на основі наявної інформації. Це сприяє критичному мисленню, запобігає "груповому мисленню" ("groupthink") та дозволяє розглядати проблему з різних точок зору.[1]

У практичній діяльності ці принципи часто перебувають у стані динамічної напруги. Наприклад, вимога своєчасності може суперечити вимогам повноти та достовірності. Командиру може знадобитися "достатньо добре" рішення *зараз*, а не ідеальне рішення *завтра*. Зріла система ІАЗ полягає не в догматичному дотриманні всіх принципів одночасно, а в умінні гнучко балансувати між ними залежно від конкретної оперативної обстановки. Система повинна бути здатною надавати швидкі попередні оцінки, коли швидкість є пріоритетом, і більш глибокі, всебічні аналізи, коли дозволяє час.

2.2. Принципи формування аналітичних продуктів

Ці принципи стосуються кінцевого продукту аналітичної діяльності та його представлення споживачеві.

- **Ясність та лаконічність:** Аналітичні документи мають бути написані чіткою,

недвозначною мовою, що робить їх доступними для осіб, які приймають рішення. Матеріал має бути викладений стисло, оскільки короткі повідомлення легше сприймаються та запам'ятовуються. Практичним втіленням цього принципу є "правило п'яти сторінок" для аналітичних висновків, що подаються на вищий рівень управління.[2]

- **Законність та прозорість:** Усі процеси збору, обробки та використання інформації повинні суворо відповідати нормам національного та міжнародного права, а також етичним стандартам.[5]
- **Захищеність:** Інформація, особливо та, що становить державну або військову таємницю, повинна бути надійно захищена від несанкціонованого доступу, витоку, модифікації чи знищення на всіх етапах її життєвого циклу.[5]

2.3. Принципи, специфічні для військового контексту

В умовах бойових дій до загальних принципів додаються специфічні вимоги, продиктовані динамікою та характером збройної боротьби.

- **Оперативність та ініціативність:** Підрозділи ІАЗ повинні діяти проактивно, передбачаючи інформаційні потреби командира, а не лише реагуючи на запити. Вони мають працювати у високому темпі, що відповідає динаміці сучасних бойових дій.[6]
- **Безперервність:** Процес ІАЗ має бути безперервним, забезпечуючи постійний потік оновлених розвідувальних даних та аналітичних оцінок для підтримки ситуаційної обізнаності 24/7.
- **Поєднання централізації та децентралізації:** Необхідно знаходити баланс між централізованим аналізом на стратегічному та оперативному рівнях (для формування загальної картини) та децентралізованими аналітичними спроможностями на тактичному рівні (для забезпечення релевантності та швидкості реагування на місцях).

Глава 3: Методологічний апарат інформаційно-аналітичної діяльності

Ефективність ІАЗ залежить не лише від якості вихідних даних, але й від потужності та адекватності методологічного інструментарію, що застосовується для їх обробки та аналізу. Цей інструментарій включає як загальнонаукові підходи, так і

вузькоспеціалізовані методи.

3.1. Системний підхід як ключова методологія

Системний підхід (або системний аналіз) є фундаментальною міждисциплінарною методологією для ІАЗ. Він розглядає складні проблеми — політичні, військові, соціальні — не як набір ізольованих подій, а як взаємопов'язані та взаємозалежні системи.[7]

Основне завдання системного аналізу полягає у підвищенні ступеня обґрунтованості рішень у складних, слабко структурованих проблемних ситуаціях.[8] Він виступає як спосіб мислення про проблему, де математичний апарат та комп'ютери є важливими, але не завжди єдиними інструментами. Ключовими методологічними принципами системного аналізу є органічна єдність суб'єктивного та об'єктивного, розуміння структури системи та декомпозиція цілей.[8]

Системний аналіз виконує роль методологічного моста між теорією та практикою. Він дозволяє перетворити неструктуровану проблему командира ("чому ми програємо на цій ділянці?") на структурований набір вимог, які ІТ-фахівці можуть використати для побудови ефективної інформаційної системи підтримки. Системний аналіз є тією інтелектуальною дисципліною, що транслює операційні потреби у технічні специфікації, поєднуючи абстрактне "чому" з конкретним "як".[8]

3.2. Загальнонаукові та аналітичні методи

На основі системного підходу застосовується широкий спектр загальнонаукових та специфічних аналітичних методів:

- **Аналіз та синтез:** Діалектичний процес, що полягає у розкладанні проблеми на складові частини для їх детального вивчення (аналіз), а потім у поєднанні цих частин у єдине ціле для розуміння системи в цілому та ролі кожного елемента (синтез).[2]
- **Історичний метод:** Дослідження хронологічного розвитку ситуації для виявлення закономірностей, тенденцій та прецедентів, що можуть вплинути на майбутнє.[2]
- **Метод аналогії та порівняння:** Використання історичних або сучасних паралелей для висунення гіпотез та оцінки ситуації. Яскравим військовим прикладом є використання історичних схем оборони моджахедів для прогнозування дій Талібану в Афганістані.[10]
- **Моделювання та симуляція:** Створення абстрактних (математичних, логічних) або

імітаційних моделей операційного середовища для перевірки гіпотез, прогнозування результатів бойових дій та "програвання" різних варіантів рішень. Це є наріжним каменем сучасного військового планування.[8]
- **Екстраполяція та прогнозування:** Поширення виявлених тенденцій та закономірностей на майбутнє для розробки прогнозів розвитку подій.[2]

3.3. Спеціалізовані методи обробки інформації

Для роботи з різними типами даних застосовуються спеціалізовані методики:

- **Контент-аналіз:** Формалізований метод кількісного та якісного аналізу текстових та медійних матеріалів (наприклад, пропагандистських повідомлень противника) для виявлення ключових тем, закономірностей та прихованих смислів.[2]
- **Мережевий аналіз:** Графічне моделювання та аналіз зв'язків між особами, групами та організаціями для розуміння структури мереж противника (наприклад, терористичних осередків або командних структур).[2]
- **Методи експертних оцінок:** Систематичний збір та узагальнення думок кваліфікованих експертів для оцінки складних ситуацій, де кількісні дані відсутні або є ненадійними. До цих методів належать метод Дельфі, "мозковий штурм", панельні дискусії та анкетування.[2]
- **Статистичні методи:** Застосування апарату математичної статистики для аналізу кількісних даних з метою виявлення кореляцій, тенденцій, значущих відхилень та інших закономірностей.

Вибір та комбінація цих методів залежить від конкретного завдання, наявності даних та часових обмежень, що вимагає від аналітика не лише знання самих методів, але й уміння гнучко їх застосовувати.

Частина II: Основи проектування та впровадження систем ІАЗ

Ця частина переходить від абстрактного "чому" інформаційно-аналітичного забезпечення до конкретного "як", розглядаючи архітектурні основи, функціональні компоненти та процеси розробки автоматизованих систем, що надають аналітичну підтримку.

Глава 4: Архітектурні основи військових інформаційних систем: від C4ISR до багатодоменних операцій

4.1. Модель C4ISR як фундаментальна архітектура

Фундаментальною концептуальною моделлю для інтегрованих військових інформаційних систем є архітектура C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance — Управління, Контроль, Зв'язок, Комп'ютери, Розвідка, Спостереження та Рекогносцировка). Ця модель описує "нервову систему" сучасних збройних сил, що забезпечує неперевершену ситуаційну обізнаність, точність та ефективність.[15]

Основні компоненти C4ISR:

- **Управління (Command):** Здійснення повноважень та керівництва з боку командира.
- **Контроль (Control):** Процеси та системи, що забезпечують відповідність операцій наміру командира.
- **Зв'язок (Communications):** Захищені, стійкі мережі для обміну даними, такі як тактичні лінії передачі даних (наприклад, Link 16, Link 22), що є основою для взаємодії.[16]
- **Комп'ютери (Computers):** Апаратне та програмне забезпечення для обробки, зберігання та візуалізації інформації.[18]
- **Розвідка (Intelligence):** Продукт, отриманий в результаті аналізу інформації з різних джерел, таких як агентурна (HUMINT), радіоелектронна (SIGINT) та видова (IMINT) розвідка.[15]
- **Спостереження (Surveillance) та Рекогносцировка (Reconnaissance):** Систематичне спостереження за полем бою за допомогою сенсорів, розміщених на різноманітних платформах (безпілотні літальні апарати, супутники, літаки, наземні датчики).[16]

Основна мета архітектури C4ISR — досягнення інформаційної переваги шляхом створення єдиної, спільної для всіх картини обстановки, скорочення циклу "виявлення-ураження" та уможливлення швидких, скоординованих дій.[19]

4.2. Еволюція до багатодоменних операцій (MDO) та JADC2

Сучасне операційне середовище, що яскраво продемонструвала війна в Україні, вимагає інтеграції та синхронізації дій у всіх операційних доменах: на суходолі, на морі, в повітрі, у кіберпросторі та космосі.[17] Це призвело до еволюції концепції C4ISR у напрямку

Об'єднаного вседоменного управління та контролю (Joint All-Domain Command and Control, JADC2). Мета JADC2 — перейти від взаємосумісних, але окремих систем до справді інтегрованої "системи систем", де будь-який сенсор може надавати інформацію для будь-якого засобу ураження (ефектора) у будь-якому домені.

Реалізація такого підходу вимагає чітко визначеної архітектури C4ISR, яка б гармонізувала оборонне планування, дозволила агрегувати спроможності та забезпечила узгодженість у розробці концепцій та можливостей.[17]

4.3. Архітектурні фреймворки НАТО та інтероперабельність

Для гармонізації зусиль різних країн-членів та забезпечення інтероперабельності НАТО адаптувало американський C4ISR Architecture Framework, створивши власний **NATO C3 System Architecture Framework**.[21] Цей фреймворк використовує кілька взаємопов'язаних "поглядів" (Views) для опису системи:

- **Операційний погляд (Operational View):** Описує завдання, операційні елементи та інформаційні потоки, необхідні для виконання місії. Він відповідає на питання "що потрібно зробити?".
- **Системний погляд (System View):** Описує системи та їх взаємозв'язки, що забезпечують виконання операційних вимог. Він відповідає на питання "як це буде зроблено?".
- **Технічний погляд (Technical View):** Визначає стандарти, правила та протоколи, що регулюють реалізацію та функціонування систем. Він відповідає на питання "за якими правилами це буде зроблено?".

Цей підхід дозволяє поєднати вимоги військового користувача з проектом системи розробника та технічними стандартами, необхідними для інтеграції.[21] Досягнення інтероперабельності є найвищою метою, що дозволяє силам з різних країн діяти як єдине ціле.[15]

При цьому важливо розуміти, що C4ISR — це не просто набір технологій, а складна соціотехнічна система. Акцент фреймворків на поєднанні "операційних поглядів" із

"системними" [21] та виклики, визначені у звітах, такі як потреба в нових політиках, планах та цифровій трансформації [17], доводять, що C4ISR стосується доктрини, процедур та людських процесів так само, як і технологій. Систему C4ISR неможливо просто "встановити"; вона вимагає коеволюції технологій, військової доктрини (як воювати), організаційної структури (хто кому підпорядковується) та підготовки особового складу. Нездатність врахувати ці "соціальні" аспекти є однією з головних причин невдач при впровадженні таких систем.

Глава 5: Функціональні компоненти та структура сучасної системи ІАЗ

Сучасна автоматизована система управління військами (АСУВ), що реалізує функції ІАЗ, є складною, багатошаровою системою, компоненти якої тісно інтегровані для забезпечення безперервного циклу обробки інформації та підтримки прийняття рішень.

5.1. Основні підсистеми автоматизованої системи управління військами (АСУВ)

Типова структура АСУВ включає такі функціональні рівні або підсистеми:

- **Рівень збору та агрегації даних:** Цей рівень інтегрує дані з величезної кількості різноманітних джерел: платформ розвідки, спостереження та рекогносцировки (БПЛА, супутники), донесень від підрозділів, даних з відкритих джерел (OSINT), радіоелектронної розвідки (SIGINT) тощо.[15]
- **Рівень комунікацій та мереж:** Це транспортна основа системи, що включає пункти управління, вузли зв'язку, ретранслятори та лінії передачі даних, які забезпечують стійкий та захищений зв'язок між усіма елементами системи.[23]
- **Рівень обробки та зберігання даних:** Включає бази даних, сховища даних та, все частіше, "озера даних" (data lakes) для зберігання як структурованої, так і неструктурованої інформації. На цьому рівні відбувається первинне очищення, злиття (fusion) та підготовка даних для аналізу.[25]
- **Рівень аналітичної обробки:** Це "мозок" системи. Він містить інструменти для статистичного аналізу, моделювання, а також, що є ключовим у сучасних системах, алгоритми штучного інтелекту та машинного навчання (AI/ML) для предиктивного аналізу, розпізнавання образів та виявлення аномалій.[4]
- **Рівень підтримки прийняття рішень та візуалізації:** Цей рівень представляє

аналітичний продукт командиру через інтуїтивно зрозумілі інтерфейси користувача, інформаційні панелі (дашборди), геоінформаційні системи (ГІС-карти) та засоби 3D-візуалізації для створення єдиної оперативної картини.[11]
- **Рівень кібербезпеки:** Цей рівень є наскрізним і пронизує всі інші. Він забезпечує конфіденційність, цілісність та доступність даних і функцій системи через механізми контролю доступу, шифрування, моніторингу загроз та реагування на інциденти.[28]

5.2. Роль математичного та програмного забезпечення

Критично важливим компонентом АСУВ є **математичне забезпечення**, що включає моделі операцій (бойових дій) та тактичних задач. Саме воно дозволяє системі виконувати складні розрахунки, проводити симуляції та здійснювати предиктивний аналіз, надаючи кількісну основу для прийняття рішень.[4]

Програмне забезпечення сучасних АСУВ все частіше будується на основі **сервісно-орієнтованої архітектури (SOA)**. Це означає, що система складається з набору модульних, незалежних, але взаємосумісних сервісів, які побудовані на відкритій, розширюваній платформі. Такий підхід забезпечує гнучкість, масштабованість та полегшує інтеграцію нових компонентів.[29]

Аналіз сучасних систем виявляє фундаментальний архітектурний зсув. Якщо раніше системи будувалися навколо конкретних функцій (наприклад, АСУ артилерією чи АСУ ППО), то сучасні архітектури, керовані потребами AI та MDO, є **датоцентричними**. Центральним архітектурним викликом стає не створення специфічного функціонального додатку, а побудова стійкої, захищеної та доступної екосистеми даних (так званої "тканини даних" або "бойової хмари"). З цієї екосистеми різні аналітичні додатки та сервіси можуть черпати інформацію. Самі дані стають основним, постійним активом, тоді як додатки, що їх використовують, можуть бути більш модульними та адаптивними. Це підтверджується появою таких систем, як "Гризельда", що обробляє дані з найрізноманітніших джерел — від супутників до зламаних баз даних противника.[22]

Глава 6: Життєвий цикл розробки проектів ІАЗ: стандарти та сучасні методології

Процес створення, впровадження та супроводження складних інформаційно-аналітичних систем регулюється певними моделями життєвого циклу та стандартами. У військовій

сфері спостерігається кардинальний перехід від традиційних, послідовних підходів до гнучких, ітеративних методологій.

6.1. Традиційна "водоспадна" модель та її обмеження у військовому контексті

Класична, або "водоспадна" (waterfall), модель життєвого циклу є лінійним, послідовним підходом, де кожен етап — визначення вимог, проектування, розробка, тестування, впровадження — має бути повністю завершений перед початком наступного.[30]

Для військової сфери, що характеризується високою динамікою та невизначеністю, цей підхід має критичні недоліки:

- **Повільність:** Жорстка послідовність призводить до багаторічних циклів розробки, що є неприйнятним в умовах швидкої зміни загроз та технологій.[31]
- **Негнучкість:** Модель погано адаптується до змін у вимогах, які неминуче виникають у ході проекту. Будь-яка зміна вимагає повернення на попередні етапи, що є дорогим та складним процесом.
- **Застарівання на момент впровадження:** Через тривалий цикл розробки система, що впроваджується, часто вже не відповідає поточним потребам користувачів (військ) та технологічному рівню.[31]

6.2. Парадигмальний зсув до Agile та DevSecOps

Усвідомлення недоліків водоспадної моделі призвело до переходу на гнучкі (Agile) методології розробки, які є ітеративними та інкрементальними.

- **Agile Development:** Це підхід, за якого розробка ведеться короткими циклами ("спринтами"), кожен з яких завершується створенням робочого фрагмента продукту. Ключовим елементом є постійна тісна співпраця між розробниками та кінцевими користувачами, що дозволяє оперативно вносити зміни та гарантувати, що кінцевий продукт відповідає реальним потребам.[31]
- **DevSecOps (Development, Security, and Operations):** Це подальший розвиток Agile, що інтегрує питання безпеки (Security) та експлуатації (Operations) у кожен етап життєвого циклу. Такий підхід гарантує, що програмне забезпечення розробляється не лише швидко, але й є безпечним та надійним з самого початку ("Secure by Design").[32]

Цей перехід є не просто технічною модою, а стратегічним імперативом. Міністерство

оборони США та Збройні Сили України активно впроваджують ці практики. Наприклад, директива армії США 2024-02 та пріоритетне використання шляху закупівель програмного забезпечення (Software Acquisition Pathway, SWP) офіційно закріплюють цей зсув, відмовляючись від поділу на фази "закупівлі" та "супроводження" на користь моделі безперервної інтеграції та поставки (CI/CD).[31]

Критерій	Водоспадна модель (Waterfall)	Гнучка модель (Agile/DevSecOps)
Основна філософія	Лінійна, послідовна	Ітеративна, інкрементальна
Обробка вимог	Фіксуються на початку, зміни ускладнені	Динамічні, уточнюються протягом усього циклу
Цикл розробки	Довгий, монолітний (місяці, роки)	Короткі ітерації ("спринти", 1-4 тижні)
Залучення користувача	На початку (вимоги) та в кінці (прийомка)	Постійна співпраця протягом усього життєвого циклу
Тестування	Окрема фаза наприкінці розробки	Безперервне, інтегроване в кожен спринт
Управління ризиками	Ризики виявляються пізно, вартість виправлення висока	Ризики виявляються та усуваються на ранніх стадіях
Придатність для ІАЗ	Низька, через нездатність адаптуватися до мінливої обстановки	Висока, забезпечує швидку поставку та еволюцію спроможностей

6.3. Ключові етапи сучасного життєвого циклу

Сучасний життєвий цикл розробки ІАЗ є не лінійним процесом, а безперервним циклом

еволюції спроможностей:

1. **Фаза 1: Визначення вимог та планування:** Це безперервний процес співпраці з користувачами (військовослужбовцями) для визначення, пріоритезації та уточнення вимог до функціоналу. Це не одноразовий етап, а постійна діяльність.[31]
2. **Фаза 2: Проектування, розробка, тестування (ітеративні цикли):** Швидкі, повторювані цикли кодування, автоматизованого тестування та сканування безпеки. Результатом кожної ітерації є мінімально життєздатний продукт (Minimum Viable Product, MVP) або мінімально життєздатна спроможність (Minimum Viable Capability Release, MVCR).[32]
3. **Фаза 3: Розгортання та впровадження:** Безперервна поставка (Continuous Delivery) нових функцій та оновлень в операційне середовище, що дозволяє військам швидко отримувати нові можливості.[31]
4. **Фаза 4: Експлуатація та супроводження (безперервна еволюція):** Програмне забезпечення ніколи не є "завершеним". Ця фаза включає постійний моніторинг роботи системи, збір зворотного зв'язку від користувачів та подальше ітеративне вдосконалення протягом усього життєвого циклу системи.[31]

6.4. Регулюючі стандарти для забезпечення інтероперабельності

Розробка військових систем ІАЗ суворо регулюється національними та міжнародними стандартами для забезпечення якості, надійності та, що найважливіше, інтероперабельності.

- **Національні стандарти (ДСТУ):** В Україні діє система державних стандартів оборонного призначення (серія ДСТУ В), яка регламентує всі етапи життєвого циклу озброєння та військової техніки, включаючи програмне забезпечення (наприклад, ДСТУ В 15.003, ДСТУ В 15.004). Ці стандарти активно гармонізуються зі стандартами НАТО.[34]
- **Стандарти НАТО (STANAGs):** Дотримання Угод зі стандартизації НАТО (Standardization Agreements, STANAGs) є критично важливим для забезпечення технічної, процедурної та доктринальної інтероперабельності з силами Альянсу. Це стосується стандартів на формати даних, протоколи зв'язку, процедури планування та системи гарантування якості (наприклад, STANAG 4107).[34]

Частина III: Ключові технології та майбутні траєкторії розвитку ІАЗ

Ця частина досліджує трансформаційні технології, які переосмислюють можливості ІАЗ, переводячи його від простої обробки даних до інтелектуальної автоматизації та прогностичного аналізу.

Глава 7: Роль штучного інтелекту та великих даних у трансформації військового аналізу

7.1. Великі дані (Big Data) як основа

Сучасні військові операції генерують величезні за обсягом, швидкістю та різноманітністю масиви даних, відомі як "великі дані" (Big Data). Джерелами цих даних є соціальні мережі, супутникові знімки, потоки даних із сенсорів, результати кібероперацій та багато іншого.[38]

Основний виклик і водночас можливість полягає в здатності об'єднувати та аналізувати ці масивні, різнорідні потоки даних для створення високодеталізованої та гранулярної картини операційного середовища.[39] Аналітика великих даних дозволяє виявляти раніше приховані закономірності, кореляції та аномалії, які неможливо виявити людським аналітикам через обмеженість когнітивних можливостей.[10]

7.2. Штучний інтелект (ШІ) та машинне навчання (МН) як аналітичний рушій

Алгоритми штучного інтелекту та машинного навчання є необхідним інструментом для обробки великих даних зі швидкістю та в масштабах, яких вимагає сучасна війна.[41]

Ключові сфери застосування AI/ML в ІАЗ:

- **Предиктивний аналіз:** Прогнозування маневрів противника, потенційних загроз та логістичних потреб шляхом аналізу історичних та поточних даних. Це дозволяє перейти від реактивного до проактивного управління.[42]
- **Автоматичне розпізнавання цілей (ATR):** Використання комп'ютерного зору для автоматичної ідентифікації та класифікації цілей на зображеннях та у відеопотоках.

Яскравим прикладом є американський проект Maven, спрямований на аналіз відео з БПЛА.[44]

- **Автоматизація розвідки:** Автоматизація рутинних, інтенсивних за даними завдань, таких як обробка документів, автоматичне реферування та розпізнавання іменованих сутностей (люди, організації, місця). Це звільняє час аналітиків для виконання завдань вищого когнітивного рівня.[45]
- **Підтримка прийняття рішень:** Системи підтримки прийняття рішень на основі ШІ (AI-DSS) можуть генерувати та оцінювати численні варіанти дій, надаючи командирам обґрунтовані рекомендації.[42]

Український контекст: Такі системи, як "Гризельда", "Дельта" та "Кропива", демонструють практичне застосування ШІ у Збройних Силах України для швидкої обробки розвідданих та наведення засобів ураження, що значно скорочує цикл "виявлення-ураження".[22]

Ці технології створюють стратегічний імператив, що виходить за межі розробки кращих алгоритмів. Виникає так звана "гонка озброєнь за даними", де дані живлять системи ШІ, які, у свою чергу, використовуються для націлювання та збору нових даних.[38] Це означає, що військова перевага все більше залежить не лише від переваги у зброї, але й від переваги у "ланцюгу постачання даних". Для України це створює стратегічну необхідність розбудови та захисту суверенної екосистеми даних, розглядаючи дані як стратегічний національний ресурс, нарівні з боєприпасами чи паливом.

7.3. Виклики та відповідальне впровадження

Впровадження ШІ пов'язане з низкою серйозних викликів. Системи ШІ не є "оракулами"; їхня ефективність прямо залежить від якості, повноти та релевантності даних, на яких вони навчалися. Вони схильні до помилок при застосуванні в умовах, що суттєво відрізняються від їхнього тренувального середовища.[47]

Тому критично важливим є принцип "людина в контурі" (human-in-the-loop) або "людина над контуром" (human-on-the-loop). ШІ слід розглядати як інструмент для співпраці, що доповнює, а не замінює людських аналітиків та командирів, які забезпечують необхідний контекст, критичне мислення та остаточне судження.[43] Усвідомлюючи ці ризики, НАТО розробило шість принципів відповідального використання ШІ: законність, відповідальність та підзвітність, пояснюваність та відстежуваність, надійність, керованість та пом'якшення упередженості.[49]

Глава 8: Геопросторова розвідка (GEOINT) та симуляція в оперативному плануванні

8.1. Геоінформаційні системи (ГІС) як основа єдиної оперативної картини

Геоінформаційні системи (ГІС) відіграють ключову роль у сучасних військових операціях, надаючи просторовий контекст для всієї іншої інформації. Вони є візуальною основою для ситуаційної обізнаності.[27]

ГІС дозволяють інтегрувати та візуалізувати на єдиній цифровій карті різноманітні шари даних: позиції противника, розташування своїх військ, аналіз рельєфу місцевості, стан інфраструктури, зони ураження тощо.[27] Це має вирішальне значення для планування стратегічних операцій, моделювання обстановки та підтримки прийняття рішень на всіх рівнях.[27]

8.2. Моделювання та симуляція для планування та воєнних ігор

Системи моделювання та симуляції є незамінними інструментами для підтримки процесу прийняття військових рішень (MDMP).[3] Вони дозволяють командирам та штабам моделювати та "програвати" (wargaming) різні варіанти дій (як своїх, так і противника) для аналізу потенційних наслідків ще до віддання наказу військам.[12]

Такі системи, як TOPFAS, що використовується в НАТО, допомагають автоматизувати підготовку планувальних документів та виконувати розрахунки для моделювання бойових дій.[12] Сучасні технології 3D-візуалізації та комп'ютерної анімації використовуються для детального моделювання поля бою, що значно підвищує якість планування та обґрунтованість рішень.[11]

Спостерігається конвергенція цих технологій в єдину потужну екосистему планування. ГІС надає базову карту та просторові дані.[27] Системи на основі ШІ, такі як "Гризельда", обробляють розвіддані та наносять їх на цю карту, інтегруючись із ГІС-системами, як-от "Дельта" та "Кропива".[22] Потім інструменти симуляції [12] використовують цю, наповнену даними за допомогою ШІ, ГІС-картину як вихідну точку для моделювання майбутніх сценаріїв. В результаті створюється безперервний робочий процес: надходять необроблені дані, обробляються та локалізуються у просторі за допомогою ШІ/ГІС, а

потім використовуються для моделювання майбутнього за допомогою симуляційних рушіїв. Це створює потужний "цифровий двійник" поля бою, який командири можуть аналізувати та використовувати для прийняття рішень.

Частина IV: Виклики та стратегічні рекомендації для Збройних Сил України

Ця заключна частина синтезує попередній аналіз для визначення найбільш нагальних викликів, що стоять перед ЗСУ у сфері ІАЗ, та пропонує конкретні, дієві рекомендації.

Глава 9: Оцінка ефективності ІАЗ

9.1. Виклик вимірювання

Оцінка ефективності ІАЗ є складним завданням. Прості показники, такі як час безвідмовної роботи системи або кількість підготовлених звітів, є недостатніми. Кінцевим критерієм ефективності ІАЗ є його вплив на результати операцій — чи допомагає він перемагати у боях.[52] Ефективність повинна оцінюватися з точки зору кінцевого користувача (командира) та корисності (utility) аналітичного продукту для його процесу прийняття рішень.[53]

9.2. Рамка оцінювання: Показники виконання та ефективності

Для структурованої оцінки доцільно використовувати двокомпонентну рамку, що поєднує показники виконання та показники ефективності.

- **Показники виконання (Measures of Performance, MoPs):** Це критерії, що використовуються для оцінки виконання поставлених завдань. Вони відповідають на питання: "Чи правильно ми робимо речі?". Приклади: своєчасність надання звітів, кількість виконаних інформаційних запитів, точність наданих даних.[52]

- **Показники ефективності (Measures of Effectiveness, MoEs):** Це критерії, що використовуються для оцінки змін в операційному середовищі, пов'язаних із досягненням мети. Вони відповідають на питання: "Чи робимо ми правильні речі?". Приклади: зменшення втрат серед своїх військ, збільшення кількості успішних уражень важливих цілей, зниження оперативного темпу противника.[52]

Надійна система оцінки вимагає поєднання як кількісних MoPs (що вимірюють "вихід" системи), так і якісних MoEs (що вимірюють "результат" діяльності).[55] При цьому не існує єдиного універсального набору метрик. Ефективність є контекстно-залежною та динамічною. Правильний набір показників залежить від конкретної місії, рівня командування та поточної фази операції.[52] Тому ефективна рамка оцінювання не може бути статичним чек-листом. Це має бути адаптивний процес, у якому командири та розвідувальні штаби

перед початком операції спільно визначають, як виглядатиме "успіх", і встановлюють відповідні MoPs та MoEs для даного конкретного контексту.

9.3. Ключові показники ефективності (KPIs) для ІАЗ

На основі вищезазначеної рамки можна визначити набір ключових показників:

- **Своєчасність:** Час від моменту збору інформації до розповсюдження готового аналітичного продукту.
- **Точність:** Відсоток прогностичних оцінок, що підтвердилися у реальності.
- **Релевантність:** Ступінь, до якого аналітичні продукти відповідають пріоритетним вимогам командира до розвідки (Priority Intelligence Requirements, PIRs).
- **Вплив:** Задокументовані випадки, коли аналітичний продукт безпосередньо призвів до успішного операційного рішення та позитивного результату.

Глава 10: Подолання ключових викликів: персонал, інтероперабельність та кібербезпека

10.1. Людський фактор: підготовка сучасного військового аналітика

Основна проблема: У ЗСУ існує значний дефіцит професійно підготовлених фахівців-аналітиків, що посилюється відтоком кваліфікованих кадрів. Проблема полягає як у недостатньому рівні теоретичного осмислення аналітичної діяльності, так і у відсутності науково обґрунтованих практичних методик.[1]

Необхідні компетенції: Сучасний аналітик повинен володіти гібридним набором навичок: глибокими військово-оперативними знаннями, володінням методами аналізу даних, навичками критичного мислення та вмінням працювати з сучасними інформаційними системами.[59]

Рекомендації для військової освіти:

- Реформувати навчальні програми у вищих військових навчальних закладах з метою інтеграції в підготовку офіцерів таких дисциплін, як аналіз даних, системний аналіз та критичне мислення.[60]
- Зосередитись на практичному, проблемно-орієнтованому навчанні з використанням реальних кейсів та симуляційних інструментів.[62]
- Створити систему безперервного професійного розвитку для аналітиків, щоб підтримувати їхні знання та навички на рівні сучасних технологічних змін.

10.2. Імператив інтероперабельності

Виклик: Досягнення повної технічної та процедурної інтероперабельності з НАТО є першочерговим стратегічним завданням. Це вимагає не лише використання сумісного обладнання, але й впровадження стандартів НАТО у процеси планування (як-от MDMP), обміну даними та доктрину.[28]

Рекомендації:

- Прискорити впровадження та імплементацію відповідних STANAGs у всі нові та існуючі системи управління та контролю.[65]
- Забезпечити, щоб розробка всіх систем ІАЗ керувалася архітектурним фреймворком НАТО (NATO C3 System Architecture Framework), гарантуючи сумісність з етапу проектування.[21]
- Інтенсифікувати спільні навчання та тренування з партнерами по НАТО для практичного відпрацювання та вдосконалення інтероперабельних процедур.

10.3. Кібернетичне поле бою

Загроза: Військові системи управління та критична інфраструктура, на яку вони спираються, є пріоритетними цілями для кібератак противника. Росія систематично атакує українські військові комунікації (Starlink), енергетичні об'єкти та телекомунікаційні мережі.[67]

Ключові вразливості: Відсутність єдиного стратегічного плану, неузгодженість нормативно-правової бази, дублювання повноважень та дефіцит фахівців з кібербезпеки.[70]

Рекомендації:

- Впровадити архітектуру "нульової довіри" (Zero Trust) для всіх військових мереж, яка виходить з припущення, що жоден користувач або пристрій не є апріорі надійним.[69]
- Застосовувати підхід "безпека через проектування" (Secure by Design), інтегруючи вимоги кібербезпеки на найраніших етапах життєвого циклу розробки систем ІАЗ (в рамках методології DevSecOps).[69]
- Зміцнювати державно-приватне партнерство для залучення цивільних експертів та підвищення національної кіберстійкості.[70]

Ці три ключові виклики — персонал, інтероперабельність та кібербезпека — є не окремими проблемами, а взаємопов'язаною "трилемою". Прогрес в одній сфері обмежується станом справ в інших. Неможливо досягти справжньої інтероперабельності з НАТО без висококваліфікованого персоналу, який розуміє та вміє застосовувати процедури Альянсу. Неможливо розгорнути захищені системи без фахівців, навчених принципам DevSecOps та "нульової довіри". А інтероперабельні системи, що з'єднуються з мережами союзників, створюють ширшу поверхню для атак, що робить надійну кібербезпеку ще більш критичною. Отже, успішна стратегія модернізації вимагає не послідовного, а цілісного, синхронізованого підходу, що одночасно просуває реформу освіти, технічну стандартизацію та посилення безпеки.

Висновок та стратегічний прогноз

Ефективне інформаційно-аналітичне забезпечення в сучасній війні є результатом синергії трьох ключових елементів: обґрунтованої методології, передових технологій та висококваліфікованого персоналу. Всі ці компоненти повинні розвиватися в рамках гнучкої, безпечної та інтероперабельної архітектури. Майбутнє ІАЗ полягає у тісній людино-машинній взаємодії, де штучний інтелект доповнює когнітивні можливості командирів та аналітиків, кардинально прискорюючи цикл OODA (Observe-Orient-Decide-Act) та уможливлюючи прийняття рішень зі швидкістю, що

відповідає динаміці сучасного поля бою.

Для Збройних Сил України, враховуючи набутий бойовий досвід та стратегічний курс на інтеграцію в євроатлантичні структури безпеки, пропонуються наступні фінальні стратегічні рекомендації:

1. **Пріоритезація людського капіталу:** Розпочати комплексну реформу військової освіти для формування нової генерації офіцерів-аналітиків, які однаково добре володіють як тактикою ведення бойових дій, так і методами аналізу даних.
2. **Впровадження датоцентричної доктрини:** Офіційно визнати дані стратегічним активом та переорієнтувати військову доктрину, організаційні структури та процеси на принципи датоцентричної війни та багатодоменних операцій.
3. **Обов'язкове застосування Agile та безпечної розробки:** Запровадити обов'язкове використання методологій Agile/DevSecOps та сумісних з НАТО стандартів для всіх майбутніх проектів у сфері оборонних IT, щоб забезпечити швидкість, адаптивність та безпеку.
4. **Створення єдиного органу з модернізації C4ISR:** Сформувати єдиний, уповноважений орган у структурі Генерального штабу або Міністерства оборони, відповідальний за нагляд за всіма проектами розвитку C4ISR/IA3. Це забезпечить узгодженість зусиль, усуне дублювання функцій та стане рушієм впровадження стандартів інтероперабельності.

Джерела

1. інформаційно-аналітичне забезпечення органів військового управління - Військова освіта, доступ отримано серпня 22, 2025, http://znp-vo.nuou.org.ua/article/view/176001/178684
2. Інформаційно-аналітична діяльність, доступ отримано серпня 22, 2025, https://kjourn.pnu.edu.ua/wp-content/uploads/sites/54/2018/04/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D0%B0-%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C.pdf
3. Військовий процес прийняття рішення (MDMP- Military decision making process), доступ отримано серпня 22, 2025, https://www.psdinfo.pro/post/%D0%B2%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81-%D0%BF%D1%80%D0%B8%D0%B9%D0%BD%D1%8F%D1%82%D1%82%D1%8F-%D1%80%D1%96%D1%88%D0%B5%D0%BD%D0%BD%D1%8F-mdmp-military-decision-making-process
4. Автоматизована система управління військами — ВУЕ, доступ отримано серпня 22, 2025, https://vue.gov.ua/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D

0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B2%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%D0%BC%D0%B8
5. ПРИНЦИПИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ, доступ отримано серпня 22, 2025, http://pgp-journal.kiev.ua/archive/2020/9/24.pdf
6. Роль інформаційно-аналітичних підрозділів Збройних Сил України у відбитті збройної агресії РФ, доступ отримано серпня 22, 2025, http://znp-cvsd.nuou.org.ua/article/view/305574
7. Освітня програма "Системний аналіз" (бакалавр) в Маріупольському університеті - mu.edu.ua, доступ отримано серпня 22, 2025, https://mu.edu.ua/educational-programs/sistemniy-analiz
8. “Системний аналіз”, доступ отримано серпня 22, 2025, https://library.wunu.edu.ua/files/EVD/IV_06/POSIBN_EK.pdf
9. Системний аналіз: необхідна навичка для кожного IT-спеціаліста - DAN IT Education, доступ отримано серпня 22, 2025, https://dan-it.com.ua/uk/blog/sistemnij-analiz-neobhidna-navichka-dlja-kozhnogo-it-specialista/
10. Tactical Data Science - Army University Press, доступ отримано серпня 22, 2025, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Tunnell-Tactical-Data-Science/
11. ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ З ДОСТАТНІМ РІВНЕМ КОРИСНОСТІ РОЗВІДУВАЛЬНО-УПРАВЛІНСЬКОЇ ІНФОРМАЦІЇ ДЛЯ СТВОРЕННЯ ІНТЕРАКТИВНОЇ ТРИВИМІРНОЇ ВІЗУАЛІЗАЦІЇ БОЙОВИХ ЕПІЗОДІВ, доступ отримано серпня 22, 2025, https://dndivsovt.com/index.php/journal/article/view/266
12. ДОСВІД ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ТАКТИЧНИХ (БОЙОВИХ) ДІЙ У ПРОФЕСІЙНІ, доступ отримано серпня 22, 2025, http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Npd_2018_2_11.pdf
13. МОДЕЛЮВАННЯ БОЙОВИХ І СПЕЦІАЛЬНИХ ДІЙ ВІЙСЬКОВИХ ФОРМУВАНЬ ДЕРЖАВНО, доступ отримано серпня 22, 2025, https://periodica.nadpsu.edu.ua/index.php/military_tech/article/download/1662/1578/4545
14. МЕТОДИКА оцінювання рівня авторитету та лідерства командирів (началь - Sprotyv G7, доступ отримано серпня 22, 2025, https://sprotyvg7.com.ua/wp-content/uploads/2023/03/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BA%D0%B0-%D0%BE%D1%86%D1%96%D0%BD%D0%BA%D0%B8-%D0%BB%D1%96%D0%B4%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%B0-%D1%82%D0%B0-%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D1%82%D0%B5%D1%82%D1%83.pdf
15. C4ISR System Ultimate Guide Milrack Command Control, доступ отримано серпня 22, 2025, https://milrack.com/c4isr-system-your-ultimate-guide/
16. Appraising the State of Play of C4ISR Infrastructure within NATO Gaps, Deficiencies and Steps Forward, доступ отримано серпня 22, 2025,

https://hcss.nl/wp-content/uploads/2025/05/Appraising-the-State-of-Play-of-C4ISR-Infrastructure-within-NATO-HCSS-2025-1.pdf
17. The future of NATO C4ISR: Assessment and recommendations after ..., доступ отримано серпня 22, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-future-of-nato-c4isr-assessment-and-recommendations-after-madrid/
18. настанова - “інформаційні та автоматизовані ... - Sprotyv G7, доступ отримано серпня 22, 2025, https://sprotyvg7.com.ua/wp-content/uploads/2024/02/2_%D0%92%D0%9A%D0%94%D0%9F-6-2601.01-%D0%9D%D0%90%D0%A1-%D0%86%D0%9D%D0%A4-%D1%82%D0%B0-%D0%90%D0%A1%D0%A3.pdf
19. C4ISR | Northrop Grumman, доступ отримано серпня 22, 2025, https://www.northropgrumman.com/what-we-do/mission-solutions/c4isr
20. C4ISR як уможливлення спроможності - Військово-Морських Сил, доступ отримано серпня 22, 2025, https://navy.mil.gov.ua/c4isr/
21. Using the C4ISR Architecture Framework as a Tool to Facilitate VV&A for Simulation Systems within the Military Application Domain - arXiv, доступ отримано серпня 22, 2025, https://arxiv.org/pdf/1011.5656
22. В Україні на базі штучного інтелекту розробили систему розвідки - Мілітарний, доступ отримано серпня 22, 2025, https://militarnyi.com/uk/news/v-ukrayini-na-bazi-shtuchnogo-intelektu-rozrobyly-systemu-rozvidky/
23. Система управління військами - Вікіпедія, доступ отримано серпня 22, 2025, https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B2%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%D0%BC%D0%B8
24. Автоматизована система управління військами – зброя перемог - військовий кур’єр, доступ отримано серпня 22, 2025, https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/
25. поняття та зміст інформаційно-аналітичної діяльності - Актуальні проблеми вітчизняної юриспруденції, доступ отримано серпня 22, 2025, http://apnl.dnu.in.ua/4_2017/23.pdf
26. НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ імені Івана Черняховського, доступ отримано серпня 22, 2025, https://nuou.org.ua/assets/documents/slavutychpublic.pdf
27. У сучасних умовах успішне виконання завдань сухопутними військами неможливе без, доступ отримано серпня 22, 2025, https://irbis-nbuv.gov.ua/cgi-bin/opac/search.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Znpviknu%5F2015%5F49%5F29%2Epdf
28. Командний курс тактичного рівня (автоматизовані системи управління військами та озброєнням), L-1C (АСУВ), доступ отримано серпня 22, 2025, https://mitit.mil.gov.ua/api/files/1785

29. Геоінформаційна підсистеми АСУ Збройних Сил України як інструмент інтероперабельності інформаційно-аналітичних систем військового призначення, доступ отримано серпня 22, 2025, https://miljournals.knu.ua/index.php/visnuk/article/view/904
30. КОНСПЕКТ ЛЕКЦІЙ "ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ", доступ отримано серпня 22, 2025, https://www.knuba.edu.ua/wp-content/uploads/2022/10/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC.pdf
31. THE SOFTWARE ADVANTAGE - USAASC, доступ отримано серпня 22, 2025, https://asc.army.mil/web/news-the-software-advantage/
32. Software Life Cycle Management | www.dau.edu, доступ отримано серпня 22, 2025, https://www.dau.edu/acquipedia-article/software-life-cycle-management
33. Software Development Life Cycle - Naval Academy, доступ отримано серпня 22, 2025, https://www.usna.edu/ITSD/software-lc.php
34. ДСТУ В 15.001:2023 Система керування життєвим циклом озброєння та військової техніки. Основні положення - БУДСТАНДАРТ Online, доступ отримано серпня 22, 2025, https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104861
35. ДСТУ В 15.007:2023 Система керування життєвим циклом озброєння та військової техніки. Оцінювання вартості життєвого циклу озброєння та військової техніки. Основні положення - БУДСТАНДАРТ Online, доступ отримано серпня 22, 2025, https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=102510
36. Переваги та виклики впровадження стандартів НАТО в систему військової освіти України, доступ отримано серпня 22, 2025, https://ukrainetonato.com.ua/osvita-ta-boyova-pidhotovka-za-standartamy-nato/perevahy-ta-vyklyky-vprovadzhennia-standartiv-nato-v-systemu-viyskovoi-osvity-ukrainy/
37. ЗАСТОСУВАННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ У КОНФЛІКТАХ СУЧ, доступ отримано серпня 22, 2025, https://dspace.nadpsu.edu.ua/bitstream/123456789/3511/1/zbirnyk_zastosuvannya_%D0%A2%D0%B5%D0%B7%D0%B8%202023_%D1%81%D1%82%D0%BE%D1%80.229.pdf
38. Lieber Studies Big Data Volume - Big Data and Armed Conflict - Legal Issues Above and Below the Armed Conflict Threshold - Lieber Institute, доступ отримано серпня 22, 2025, https://lieber.westpoint.edu/big-data-armed-conflict-legal-issues-above-below-armed-conflict-threshold/
39. Defense Intelligence Analysis in the Age of Big Data, доступ отримано серпня 22, 2025, https://ndupress.ndu.edu/Media/News/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data/

40. Five Examples of Big Data Analytics and the Future of ISR - National Defense University Press, доступ отримано серпня 22, 2025, https://ndupress.ndu.edu/Joint-Force-Quarterly/Joint-Force-Quarterly-77/Article/583354/five-examples-of-big-data-analytics-and-the-future-of-isr/
41. Застосування штучного інтелекту у сфері національної безпеки та обороноздатності держави - Сідкон, доступ отримано серпня 22, 2025, https://sidcon.com.ua/tpost/7vuygong71-zastosuvannya-shtuchnogo-ntelektu-u-sfer
42. The Role of AI and Machine Learning in Military Decision-Making Software | Attract Group, доступ отримано серпня 22, 2025, https://attractgroup.com/blog/the-role-of-ai-and-machine-learning-in-military-decision-making-software/
43. Machine Learning for Operational Decisionmaking in Competition and Conflict - RAND, доступ отримано серпня 22, 2025, https://www.rand.org/pubs/research_reports/RRA815-1.html
44. Do AI Decision Support Systems 'Support' Humans in Military Decision-Making on the Use of Force? - Opinio Juris, доступ отримано серпня 22, 2025, http://opiniojuris.org/2024/11/29/do-ai-decision-support-systems-support-humans-in-military-decision-making-on-the-use-of-force/
45. Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation, доступ отримано серпня 22, 2025, https://www.act.nato.int/article/harnessing-artificial-intelligence/
46. The use of artificial intelligence in military intelligence: an experimental investigation of added value in the analysis process - Frontiers, доступ отримано серпня 22, 2025, https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2025.1540450/full
47. AI in Military Decision Support: Balancing Capabilities with Risk, доступ отримано серпня 22, 2025, https://nyudatascience.medium.com/ai-in-military-decision-support-balancing-capabilities-with-risk-d9f83de4baca
48. AI for Military Decision-Making | Center for Security and Emerging Technology - CSET, доступ отримано серпня 22, 2025, https://cset.georgetown.edu/publication/ai-for-military-decision-making/
49. Algorithmic power, NATO and artificial intelligence, доступ отримано серпня 22, 2025, https://www.iiss.org/ar-BH/online-analysis/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence/
50. Summary of NATO's revised Artificial Intelligence (AI) strategy, 10-Jul.-2024, доступ отримано серпня 22, 2025, https://www.nato.int/cps/en/natohq/official_texts_227237.htm
51. (PDF) Оцінка інформативності геоінформаційних систем військового призначення, доступ отримано серпня 22, 2025, https://www.researchgate.net/publication/386572250_Ocinka_informativnosti_geoinformacijnih_sistem_vijskovogo_priznacenna

52. Assessing ISR - Air University, доступ отримано серпня 22, 2025, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-3/F-Hill.pdf
53. Measurement and Evaluation of Military Intelligence Performance - DTIC, доступ отримано серпня 22, 2025, https://apps.dtic.mil/sti/tr/pdf/ADA210690.pdf
54. ІННОВАЦІЙНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЯКОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ІН - Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія, доступ отримано серпня 22, 2025, https://www.pubadm.vernadskyjournals.in.ua/journals/2020/4_2020/9.pdf
55. Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command | RAND, доступ отримано серпня 22, 2025, https://www.rand.org/pubs/research_reports/RR4360.html
56. Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis - RAND, доступ отримано серпня 22, 2025, https://www.rand.org/pubs/research_reports/RRA464-1.html
57. НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОГО УПРАВЛІННЯ ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ, доступ отримано серпня 22, 2025, https://ipa.karazin.ua/wp-content/themes/kbuapa/filesforpages/science/sokol_dis%D0%B5.pdf
58. система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови - Sprotyv G7, доступ отримано серпня 22, 2025, https://sprotyvg7.com.ua/wp-content/uploads/2022/12/inform-bezpeka.pdf
59. Програма фахового вступного екзамену Інформаційно-аналітичне забезпечення у військах (силах), доступ отримано серпня 22, 2025, https://vaodesa.mil.gov.ua/wp-content/uploads/2025/05/Prohrama-vstupnoho-ekzamenu-Informatsiyno-analitychne-zabezpechennia-u-viyskakh-sylakh.pdf
60. Про вдосконалення підготовки офіцерських кадрів тактичного рівня та сержантського (старшинського) складу у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів від 25.04.2016 | LIGA:ZAKON, доступ отримано серпня 22, 2025, https://ips.ligazakon.net/document/MUS27590
61. Щодо підвищення ефективності професійної підготовки майбутніх офіцерів у реаліях війни (українська відповідь - Академічні візії, доступ отримано серпня 22, 2025, https://www.academy-vision.org/index.php/av/article/download/227/201
62. стратегія програми нато з удосконалення військової освіти (deep) - NATO, доступ отримано серпня 22, 2025, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf
63. Assessing Assessments: How Useful is Predictive Intelligence? - Royal Air Force, доступ отримано серпня 22, 2025, https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/apr-vol19-iss3-5-pdf/
64. правові засади запровадження стандартів північноатлантичного альянсу, доступ отримано серпня 22, 2025, http://pgp-journal.kiev.ua/archive/2021/4/28.pdf

65. ДЕЯКІ АСПЕКТИ ВПРОВАДЖЕННЯ СТАНДАРТІВ НАТО У СИСТЕМУ ВИПРОБУВАНЬ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ УКРАЇНИ, доступ отримано серпня 22, 2025, https://dndivsovt.com/index.php/journal/article/view/45
66. для захисту повітряного простору 49 - МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ, доступ отримано серпня 22, 2025, https://www.hups.mil.gov.ua/assets/doc/science/conference/15/8.pdf
67. підтримка дій сил безпеки дозволяє виконувати їх з достатньою, доступ отримано серпня 22, 2025, https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/02.05.03/vsnSporyshev.pdf
68. кіберборотьба у воєнних конфліктах сучасності: передовий досвід, доступ отримано серпня 22, 2025, https://sit.nuou.org.ua/article/download/301405/302376/719334
69. РІЧНИЙ АНАЛІТИЧНИЙ ОГЛЯД - Рада національної безпеки і оборони України, доступ отримано серпня 22, 2025, https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRIeHRuA2FlbQIxMAABHcaZdkgcVIISJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toly6vpuA27mA
70. Правова база української кібербезпеки: - IFES Ukraine, доступ отримано серпня 22, 2025, https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf
71. (PDF) КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ВІЙСЬКОВОЇ ЗАГРОЗИ, доступ отримано серпня 22, 2025, https://www.researchgate.net/publication/387737658_KIBERBEZPEKA_KRITICNOI_INFRASTRUKTURI_PID_CAS_VIJSKOVOI_ZAGROZI