Основи збору та зберігання даних для інформаційно-аналітичного забезпечення органів військового управління

Вступ: Інформаційно-керована основа сучасного військового командування

В епоху цифрової трансформації та мережецентричних війн, інформаційно-аналітичне забезпечення (ІАЗ) перестало бути допоміжною функцією і перетворилося на центральну нервову систему сучасних органів військового управління (ОВУ).[1] Ефективність командування, швидкість прийняття рішень та, зрештою, перевага на полі бою сьогодні прямо пропорційні спроможності військової організації керувати своїм інформаційним конвеєром — від моменту збору первинних даних до їх безпечного зберігання та аналітичної обробки. Якість та темп ухвалення управлінських рішень безпосередньо залежать від ефективності цього процесу.[1]

Ця лекція розкриває два фундаментальні стовпи ІАЗ: збір та зберігання даних. Ці процеси не є послідовними чи незалежними; вони утворюють глибоко інтегровану, симбіотичну систему. Методи, що застосовуються для збору інформації, диктують вимоги до архітектури її зберігання. Водночас, можливості систем зберігання відкривають шлях до впровадження більш досконалих технологій збору та аналізу.

Стратегічний контекст цієї дисципліни визначається прагненням до досягнення інформаційної переваги в умовах багатодоменних операцій, що є ключовим принципом сучасної військової доктрини.[3] Кінцева мета ІАЗ полягає у перетворенні потоку необроблених даних на дієву розвідувальну інформацію, яка надає командирам вирішальну бойову перевагу, дозволяючи їм бачити, розуміти та діяти швидше за супротивника.[2]

Частина I: Основи збору даних для ІАЗ ОВУ

Розділ 1: Роль та принципи збору даних у військовому процесі прийняття рішень

1.1. Визначення мети ІАЗ

Інформаційно-аналітичне забезпечення (ІАЗ) визначається як взаємопов'язана логічна система відбору, систематизації, оцінки та діагностики даних, що створена для підтримки своєчасних та ефективних управлінських рішень.[2] Його головна мета — надати особам, що приймають рішення, необхідний та достатній обсяг аналітичної інформації для мінімізації ризиків та вибору оптимального курсу дій, особливо в умовах невизначеності та кризових ситуацій.[1]

Процес ІАЗ не обмежується простою акумуляцією фактів. Його ключова функція полягає у якісно-змістовному перетворенні первинної, "сирої" інформації на вторинний, якісно новий продукт — аналітичне знання.[1] Це знання дозволяє не лише констатувати поточний стан справ, але й виявляти приховані закономірності, прогнозувати розвиток подій та оцінювати наслідки потенційних рішень.

1.2. Збір даних у циклі прийняття рішень (цикл OODA)

Фундаментальною моделлю для розуміння процесу прийняття військових рішень є цикл OODA (Observe-Orient-Decide-Act або Спостереження-Орієнтація-Рішення-Дія).[6] У цій моделі етап "Спостереження" (Observe) є синонімом процесу збору даних. Це початкова і

найважливіша фаза, оскільки якість та повнота зібраної інформації визначають ефективність усіх наступних етапів циклу.[7]

Швидкість та якість етапу "Спостереження" безпосередньо впливають на оперативний темп. Чим швидше та точніше збираються й обробляються дані, тим швидше командир може зорієнтуватися в обстановці, прийняти рішення та діяти, випереджаючи супротивника.[6] Однак цикл OODA є не просто лінійною послідовністю, а системою зі зворотним зв'язком. Кожна "Дія" (Act), наприклад, нанесення вогневого ураження чи здійснення маневру, змінює оперативну обстановку. Ця зміна генерує нову інформацію — реакцію ворога, результати ураження (оцінка бойових втрат), зміну позицій тощо. Ця нова інформація стає вхідним потоком для наступного етапу "Спостереження". Таким чином, збір даних є не статичним процесом отримання заздалегідь визначеної інформації, а динамічним, що вимагає постійної адаптації до наслідків власних дій та дій супротивника. Це створює безперервний, самовдосконалюваний розвідувальний цикл, де дія породжує потребу в нових даних, які, у свою чергу, формують основу для наступної дії.

1.3. Фундаментальні принципи якості даних

Щоб дані були придатними для використання у військовому плануванні та розвідці, вони повинні відповідати низці непорушних принципів якості.

- **Своєчасність:** Дані мають надходити в межах того часового вікна, коли вони ще здатні вплинути на прийняття рішення.[8] Застаріла інформація не просто марна — вона може бути небезпечною, вводячи в оману. У тактичному контексті це вікно може вимірюватися секундами чи хвилинами, наприклад, при виявленні мобільної артилерійської установки противника.[1]
- **Релевантність та Пертинентність:** Зібрані дані повинні безпосередньо відповідати інформаційним потребам командира та конкретній проблемі, що вирішується.[8] Зусилля зі збору мають бути сфокусованими, щоб уникнути марнування ресурсів на несуттєву інформацію.
- **Точність та Достовірність:** Інформація має бути правильною та надійною. Рішення, засновані на неточних даних, можуть призвести до катастрофічних наслідків: від ураження хибних цілей до неправильної оцінки сил противника.[1] Цей принцип є абсолютним пріоритетом у процесах цілеутворення, де точність є ключем до ефективності.[10]
- **Повнота та Достатність:** Хоча ідеалом є повна картина обстановки, практична мета полягає у зборі *достатнього* обсягу даних для прийняття обґрунтованого рішення, не потрапляючи в пастку аналітичного паралічу через пошук абсолютно всіх деталей.[1] Цей принцип вимагає знаходження балансу між ретельністю та швидкістю.

Розділ 2: Джерела та методи: огляд розвідувальних дисциплін

2.1. Імператив комплексного підходу (Multi-INT)

Жодне окреме джерело розвідувальної інформації не є безпомилковим. Кожне має свої сильні сторони, обмеження та вразливості. Тому для формування всебічної, стійкої та достовірної картини оперативної обстановки необхідний комплексний, багатодисциплінарний підхід, відомий як Multi-INT (Multiple Intelligence). Цей підхід дозволяє різним джерелам верифікувати, доповнювати та підтверджувати інформацію одне одного, підвищуючи загальну надійність аналітичних висновків.[13]

2.2. Розвідка з відкритих джерел (OSINT)

- **Визначення:** Збір та аналіз загальнодоступної інформації.[14] Джерела включають засоби масової інформації, інтернет, наукові публікації, соціальні мережі (що є предметом окремої піддисципліни SOCMINT), комерційні бази даних та урядові звіти.[16]
- **Роль та переваги:** OSINT надає базову розвідувальну інформацію та контекст, часто з низькими витратами та ризиком. Ця дисципліна є ключовою для розуміння соціально-політичної обстановки, ідентифікації ключових осіб та подій, а також для підготовки підґрунтя для інших розвідувальних операцій.[13]
- **Обмеження:** Головними викликами є величезний обсяг даних, що може призвести до інформаційного перевантаження, а також висока ймовірність натрапити на дезінформацію, що вимагає ретельної перевірки та валідації джерел.[16]

2.3. Агентурна розвідка (HUMINT)

- **Визначення:** Отримання розвідувальної інформації від людських джерел через

міжособистісну комунікацію.[14] Методи включають шпигунство, проведення інтерв'ю, допитів та опитувань свідків.[15]

- **Роль та переваги:** HUMINT є найстарішою розвідувальною дисципліною і часто єдиним способом отримати дані про наміри, плани, бойовий дух та внутрішні процеси супротивника — інформацію, недоступну для технічних засобів.[15] Вона забезпечує неперевершену глибину та нюанси.
- **Обмеження:** Це найскладніша та найризикованіша дисципліна. Вона вимагає значних ресурсів, часу та є вразливою до людських помилок, упереджень та навмисного введення в оману.[13]

2.4. Радіоелектронна розвідка (SIGINT)

- **Визначення:** Розвідка, що базується на перехопленні сигналів. Вона поділяється на розвідку комунікацій (COMINT), що займається перехопленням повідомлень, та радіотехнічну розвідку (ELINT), що фокусується на не комунікаційних випромінюваннях (наприклад, від РЛС).[14]
- **Роль та переваги:** SIGINT надає дані в реальному часі про комунікації противника, його командну структуру та електронний бойовий порядок. Перехоплення радіообміну може розкрити місцезнаходження, плани та можливості ворожих підрозділів.[16] ELINT є критично важливою для виявлення та ідентифікації систем ППО та інших радіолокаційних систем.
- **Обмеження:** Високотехнічна дисципліна, що потребує спеціалізованого обладнання та експертизи. Її ефективність знижується через використання супротивником сучасних методів шифрування та процедур радіомаскування.

2.5. Видова розвідка (IMINT) та Геопросторова розвідка (GEOINT)

- **Визначення:** Отримання розвідувальних даних шляхом аналізу зображень та геопросторової інформації.[13] GEOINT є ширшою категорією, що інтегрує зображення (IMINT) з іншими геопросторовими даними (карти, рельєф, інфраструктура) для опису, оцінки та візуального представлення фізичних об'єктів та діяльності на Землі.
- **Роль та переваги:** Надає конкретні візуальні докази щодо місцезнаходження, складу, оснащення та діяльності сил противника. Є незамінною для планування цілеутворення, аналізу місцевості, оцінки бойових ушкоджень та моніторингу змін у часі.
- **Обмеження:** Ефективність може бути обмежена погодними умовами, часом доби та засобами маскування. Статичні зображення не завжди розкривають наміри чи

реальні можливості об'єкта. Вимагає висококваліфікованих аналітиків для правильної інтерпретації.

2.6. Вимірювально-сигнатурна розвідка (MASINT)

- **Визначення:** Технічно отримана розвідувальна інформація, яка виявляє, відстежує, ідентифікує або описує відмінні характеристики (сигнатури) цілей.[14] MASINT відповідає на питання *"що це?"*, * "як воно працює?"* та *"з чого зроблено?"*.
- **Роль та переваги:** MASINT надає унікальні дані, недоступні для інших дисциплін. Приклади включають ідентифікацію типу двигуна за його акустичною сигнатурою, визначення хімічного складу викидів промислового об'єкта або виявлення запуску балістичної ракети за її інфрачервоною сигнатурою.[16] Часто її називають "розвідувальною дисципліною майбутнього" через її здатність ідентифікувати нові та нетрадиційні загрози.[18]
- **Обмеження:** Надзвичайно наукоємна та технічна дисципліна, що вимагає передових сенсорів та глибоких знань у різних галузях науки. Це найменш зрозуміла дисципліна, яку важко практикувати поза професійним середовищем.[13]

Критерій	OSINT	HUMINT	SIGINT	GEOINT/IMINT	MASINT
Основні джерела	Публічні медіа, інтернет, соцмережі, бази даних [16]	Люди (агенти, полонені, біженці, дипломати) [17]	Електронні сигнали (радіо, РЛС, телеметрія) [14]	Супутникові та аерофотознімки, карти [13]	Специфічні сигнатури (акустичні, хімічні, радіологічні) [18]
Тип даних	Переважно неструктуровані (текст, відео), частково структуровані	Переважно неструктуровані (звіти, розмови)	Структуровані (параметри сигналу) та неструктуровані (зміст	Неструктуровані (зображення) та структуровані (координати)	Високоструктуровані (вимірювання, числові дані)

			розмов)		
Ключові можливості	Надання контексту, базової інформації, моніторинг громадської думки [13]	Розкриття намірів, планів, морального стану супротивника [15]	Перехоплення комунікацій в реальному часі, виявлення РЛС [16]	Точне визначення місцезнаходження, ідентифікація техніки, оцінка збитків [13]	Ідентифікація унікальних характеристик зброї, виявлення прихованих об'єктів [18]
Обмеження	Інформаційне перевантаження, дезінформація, потреба у верифікації [16]	Високий ризик, тривалість, суб'єктивність, можливість обману [13]	Шифрування, радіомовчання, складність аналізу [13]	Погодні умови, маскування, статичність зображення [13]	Висока технічна складність, дорожнеча, вузька спеціалізація [18]
Військовий приклад	Аналіз пропагандистських каналів для оцінки інформаційних операцій ворога.	Допит військовополоненого для отримання даних про плани його підрозділу.	Перехоплення радіопереговорів танкового батальйону для визначення його напрямку руху.	Аналіз супутникових знімків для виявлення скупчення ворожої техніки на аеродромі.	Аналіз сейсмічних датчиків для виявлення підземного ядерного випробування.

Розділ 3: Технологічне посилення збору даних

3.1. Великі дані (Big Data) та Штучний інтелект (AI) як

мультиплікатори сили

Сучасні військові операції генерують величезні обсяги даних (Big Data), які значно перевищують можливості людського аналізу.[19] Штучний інтелект (AI) та машинне навчання (ML) стають незамінними інструментами для обробки цих даних у необхідному масштабі та з потрібною швидкістю. Застосування AI включає автоматичне розпізнавання цілей на зображеннях, виявлення аномалій у мережевому трафіку, аналіз великих масивів текстової інформації та прогнозування дій супротивника.[19] Використання AI дозволяє військовим значно скоротити цикл OODA, автоматизуючи частини етапів "Спостереження" та "Орієнтація", що дає змогу командирам приймати швидші та більш обґрунтовані рішення.[19]

3.2. Всеохопна сенсорна мережа

Сучасне поле бою насичене сенсорами — від індивідуальних пристроїв на бійцях до автономних наземних датчиків та космічних апаратів.[21] Це призводить до появи концепції "Інтернету військових речей" (IoMT), де кожен елемент — від зброї та транспортного засобу до безпілотника — є потенційним джерелом даних, створюючи багаторівневу, щільну сенсорну мережу.[23] Безпілотні літальні апарати (БпЛА) відіграють ключову роль у цій мережі, забезпечуючи можливість ведення тривалого спостереження та несучи на борту різноманітні сенсори (IMINT, SIGINT, MASINT), що робить їх універсальними платформами для збору даних.[7]

3.3. Периферійні обчислення (Edge Computing) для тактичної обробки даних

Одним із головних викликів є обробка даних у тактичній зоні, яка часто характеризується нестабільним, низькошвидкісним або відсутнім зв'язком (DIL — Disconnected, Intermittent, Low-bandwidth).[24] Периферійні обчислення (Edge Computing) пропонують рішення шляхом розгортання обчислювальних потужностей та алгоритмів AI безпосередньо на тактичних платформах (наприклад, на борту БпЛА чи бронемашини).[24] Це дозволяє аналізувати дані в реальному часі на місці їх збору, не пересилаючи величезні обсяги "сирої" інформації до віддаленого командного центру, що є критично важливим для

чутливих до часу завдань, таких як цілеутворення.

Конвергенція AI, всеохопних сенсорних мереж та периферійних обчислень фундаментально змінює саму природу збору розвідувальних даних. Історично, збір інформації був реактивним, цілеспрямованим процесом: відправка розвідника, виліт літака-розвідника, моніторинг конкретної радіочастоти. Сьогодні, завдяки IoMT, дані збираються *безперервно* та *пасивно* з тисяч джерел, створюючи проблему Big Data.[19] AI та ML автоматизують аналіз цього постійного потоку, а Edge Computing дозволяє робити це в реальному часі на тактичному рівні.[24] Це призводить до парадигматичного зсуву: замість того, щоб аналітик "витягував" інформацію за запитом, система тепер здатна "виштовхувати" попередження та висновки командиру автоматично, як тільки виявляє щось значуще. Розвідка стає проактивною та миттєво реагуючою.

Розділ 4: Навігація на сучасному інформаційному полі бою

4.1. Виклик інформаційного перевантаження

Прямим наслідком феномену Big Data є інформаційне перевантаження. Надлишок даних може призвести до аналітичного паралічу, стресу, втоми та, як наслідок, до прийняття неоптимальних рішень.[26] Проблема полягає не у відсутності інформації, а в браку ефективних інструментів та навичок для фільтрації, пріоритезації та синтезу релевантних даних з інформаційного "шуму".[27]

4.2. Загроза дезінформації та пропаганди

Дезінформація — це навмисне поширення неправдивої або маніпулятивної інформації з метою впливу на громадську думку та прийняття рішень.[28] В умовах сучасної гібридної війни вона є потужною зброєю, що використовується для підриву довіри, поширення паніки, дезорієнтації особового складу та дискредитації військово-політичного керівництва.[27] Легкість поширення дезінформації через відкриті джерела (OSINT) робить

навички верифікації джерел та інформаційної гігієни критично важливими.[29]

4.3. Контрзаходи: валідація джерел та критичне мислення

Технології самі по собі не можуть вирішити проблему дезінформації. Найефективнішим захистом є добре підготовлений аналітик та командир. Розвиток навичок критичного мислення є ключовою вимогою для військовослужбовців, особливо для офіцерів оперативного рівня.[27] Це включає здатність ставити під сумнів припущення, виявляти когнітивні упередження, оцінювати надійність джерел та розпізнавати маніпулятивні наративи. Жорсткі протоколи валідації джерел та перехресної перевірки інформації з кількох незалежних розвідувальних дисциплін (підхід Multi-INT) є основою протидії інформаційним загрозам.[27]

Існує технологічний парадокс: ті самі технології, що посилюють збір даних (AI, Big Data), одночасно посилюють і головні виклики інформаційного середовища (перевантаження та дезінформація). Технології AI дозволяють збирати та обробляти безпрецедентні обсяги інформації, що є перевагою.[19] Проте, саме цей обсяг є причиною інформаційного перевантаження, яке погіршує когнітивні здібності людини.[26] Більше того, супротивник може використовувати ті ж самі технології AI для генерації та поширення високоякісної, переконливої дезінформації в масштабах, які раніше були неможливими. Відкриті джерела, ключовий ресурс для Big Data, водночас є головним каналом для цієї дезінформації.[29] Отже, технологічне "рішення" (більше даних, швидша обробка) нерозривно пов'язане з "проблемою" (забагато даних, недостовірні дані). Це означає, що суто технологічний підхід до досягнення інформаційної переваги є недостатнім. Він має бути збалансований з акцентом на розвиток людських когнітивних навичок, зокрема критичного мислення, для управління негативними наслідками самих технологій.

Частина II: Основи зберігання даних для ІАЗ ОВУ

Розділ 5: Характеристики даних та сучасні

архітектури зберігання

5.1. Класифікація військових даних

Ефективне зберігання даних починається з розуміння їх типів. У військовому контексті дані можна класифікувати на три основні категорії:

- **Структуровані дані:** Високоорганізовані дані, що легко вписуються в табличну структуру (рядки та стовпці) з чітко визначеною схемою. Вони легко піддаються пошуку та аналізу за допомогою стандартних інструментів. Приклади: логістичні бази даних (серійні номери техніки, кількість, місцезнаходження), дані про особовий склад, таблиці для артилерійської стрільби, фінансові звіти.[30]
- **Неструктуровані дані:** Дані, що не мають заздалегідь визначеного формату чи моделі. Вони складають переважну більшість (80-90%) інформації, що генерується. Приклади: відео з БпЛА в реальному часі, аудіозаписи радіоперехоплень (COMINT), текстові розвідувальні доповіді (HUMINT), супутникові знімки (IMINT), повідомлення в соціальних мережах.[31]
- **Напівструктуровані дані:** Дані, що не зберігаються в реляційних базах даних, але мають певні організаційні властивості та метадані, які полегшують їх аналіз. Приклади: електронні листи (з полями "відправник", "тема", "дата"), файли у форматі XML, журнали роботи сенсорів з часовими мітками та ідентифікаторами.[33]

5.2. Традиційний підхід: Сховище даних (Data Warehouse)

- **Визначення:** Централізоване сховище інтегрованих, структурованих даних, отриманих з різних джерел. Воно використовує підхід "схема при записі" (schema-on-write): дані очищуються, трансформуються та структурують *перед* тим, як потрапити до сховища.[35]
- **Військове застосування:** Ідеально підходить для бізнес-аналітики (BI) та звітності на основі добре зрозумілих, передбачуваних даних. Наприклад, для аналізу історичних показників споживання пального, статистики бойової готовності особового складу або фінансових витрат.
- **Обмеження:** Негнучкість через жорстку схему. Погано пристосоване для обробки неструктурованих даних. Масштабування є дорогим та складним процесом.[38]

5.3. Сучасний підхід: Озеро даних (Data Lake)

- **Визначення:** Велике сховище, що зберігає величезні обсяги "сирих" даних у їхньому вихідному форматі. Використовує підхід "схема при читанні" (schema-on-read): дані зберігаються "як є", а структура застосовується лише тоді, коли вони потрібні для аналізу.[35]
- **Військове застосування:** Незамінне для сучасного розвідувального аналізу, AI та ML. Дозволяє зберігати всі типи даних з усіх розвідувальних дисциплін (відео, аудіо, текст, дані сенсорів) в одному місці, надаючи аналітикам можливість досліджувати їх та знаходити нові, неочевидні закономірності.[35]
- **Обмеження:** Без належного управління може перетворитися на "болото даних" (data swamp) — дезорганізовану та непридатну для використання колекцію файлів. Вимагає використання зовнішніх інструментів для обробки та аналізу.[35]

5.4. Гібридне рішення: Озерний дім даних (Data Lakehouse)

- **Визначення:** Новітня архітектура, що поєднує гнучкість та низьку вартість зберігання "озера даних" з можливостями управління даними та аналітики "сховища даних".[35]
- **Військове застосування:** Пропонує найкраще з обох світів. Може зберігати всі "сирі" розвідувальні дані (як озеро), одночасно забезпечуючи надійні, високопродуктивні запити та управління для структурованої аналітики (як сховище). Це підтримує як аналітиків, що досліджують необроблені дані для виявлення нових загроз, так і командирів, яким потрібні надійні панелі моніторингу поточної обстановки.[35]

Характеристика	**Сховище даних (Data Warehouse)**	**Озеро даних (Data Lake)**	**Озерний дім (Data Lakehouse)**
Структура даних	Лише структуровані [39]	Структуровані, напівструктуровані, неструктуровані [35]	Всі типи даних [35]

Схема	Schema-on-Write (схема при записі) [36]	Schema-on-Read (схема при читанні) [39]	Гібридна, підтримує обидва підходи [35]
Основні користувачі	Бізнес-аналітики, штабні офіцери [39]	Аналітики даних, спеціалісти з AI/ML [40]	Всі типи користувачів [36]
Модель обробки	ETL (Extract, Transform, Load) [39]	ELT (Extract, Load, Transform) [38]	Підтримує обидві моделі [35]
Вартість	Висока [38]	Низька [38]	Низька вартість зберігання, гнучкі витрати на обробку [35]
Масштабованість	Складна та дорога [38]	Легка та відносно дешева [38]	Легка та відносно дешева [38]
Ключовий військовий сценарій	Створення звітів по логістиці та готовності військ за встановленими формами.	Пошук аномальної активності противника шляхом аналізу необроблених даних з різних сенсорів.	Створення єдиної оперативної картини, що поєднує дані розвідки в реальному часі та історичні аналітичні звіти.

Розділ 6: Інфраструктура зберігання: від централізованого командування до тактичної ланки

6.1. Локальні сервери (On-Premise)

- **Опис:** Дані зберігаються на фізичних серверах, що належать військовій організації та знаходяться під її повним контролем у власних приміщеннях.

- **Переваги:** Максимальний контроль над безпекою (фізичною та віртуальною), відсутність залежності від зовнішніх провайдерів та інтернет-з'єднання для доступу до локальних даних.[41]
- **Недоліки:** Високі початкові капітальні витрати, значні витрати на обслуговування, складне та повільне масштабування, вразливість до фізичної атаки чи стихійного лиха в одному місці.[41]

6.2. Хмарні обчислювальні моделі (Cloud Computing)

- **Опис:** Дані зберігаються на віддалених серверах, якими керує сторонній провайдер, а доступ до них здійснюється через інтернет.[42] Моделі включають приватні, публічні та гібридні хмари.
- **Переваги:** Висока масштабованість та гнучкість (оплата за фактичне використання), зменшення навантаження на обслуговування, доступ до передових сервісів (платформи AI/ML), вбудована відмовостійкість та механізми аварійного відновлення.[41] Хмарні технології стали критичним компонентом оборони 21-го століття.[23]
- **Недоліки:** Потреба в надійному інтернет-з'єднанні, потенційні ризики безпеки, пов'язані зі зберіганням даних у третьої сторони, питання суверенітету даних.[41]

6.3. Гібридний підхід та тактичні аспекти

- **Опис:** Комбінація локальних та хмарних сховищ, що дозволяє зберігати найбільш чутливі дані на власних серверах, водночас використовуючи хмару для масштабованої обробки та зберігання менш критичних даних.[43]
- **Тактична/Периферійна хмара:** Ця концепція розширює можливості хмари на поле бою. Вона передбачає розгортання невеликих, захищених серверів у тактичних умовах (на транспортних засобах, передових базах), які можуть працювати автономно при втраті зв'язку та синхронізуватися з центральною хмарою при його відновленні.[23] Це є ключовим для забезпечення передовими можливостями підрозділів на "нулі".

Критерій	Локальна інфраструктура	Хмарна інфраструктура (Cloud)

	(On-Premise)	
Контроль безпеки	Повний контроль над фізичним та мережевим доступом.[41]	Спільна відповідальність; провайдер забезпечує інфраструктуру, організація — доступ та дані.[47]
Масштабованість	Обмежена, повільна, вимагає закупівлі обладнання.[41]	Висока, швидка, "еластична" (збільшення/зменшення ресурсів за потребою).[41]
Модель витрат	Високі початкові капітальні витрати (CAPEX).[41]	Операційні витрати (OPEX), оплата за використання.[44]
Доступність	Обмежена локальною мережею, якщо не налаштовано віддалений доступ.[41]	Глобальний доступ за наявності інтернет-з'єднання.[42]
Придатність для тактичної ланки	Висока (у вигляді захищених серверів), оскільки не залежить від зовнішнього зв'язку.	Низька безпосередньо, але висока у вигляді "тактичної хмари" (edge cloud), що синхронізується з основною.[25]
Обслуговування	Повністю лежить на організації (обладнання, ПЗ, охолодження, живлення).[41]	Переважно виконується провайдером.[43]

Розділ 7: Управління даними, безпека та стандартизація

7.1. Тріада CIA: ядро інформаційної безпеки

Фундаментальною моделлю інформаційної безпеки, що застосовується до будь-якої системи зберігання даних, є тріада CIA:

- **Конфіденційність (Confidentiality):** Гарантія того, що дані доступні лише авторизованим особам. Досягається за допомогою механізмів контролю доступу, шифрування та класифікації інформації.[48]
- **Цілісність (Integrity):** Підтримка точності та повноти даних протягом усього їхнього життєвого циклу; захист від несанкціонованої зміни.[48]
- **Доступність (Availability):** Забезпечення того, що авторизовані користувачі мають своєчасний та надійний доступ до даних, коли це необхідно.[48]

7.2. Політики НАТО та Угоди зі стандартизації (STANAG)

- **Стратегічний імператив:** Взаємосумісність (interoperability) є наріжним каменем успішних коаліційних операцій. Стандартизація є механізмом для її досягнення.[51]
- **STANAGs:** Угоди зі стандартизації (Standardization Agreements) є ключовими документами НАТО, що визначають спільні процедури, обладнання та, що найважливіше, формати даних для країн-членів.[53] Приклади, що стосуються даних, включають STANAG 4177 (збір даних), STANAG 5516 (тактична мережа Link 16), STANAG 7023 (формат зображень) та стандарти, що регулюють класифікацію та обмін інформацією.[55]
- **Загальні політики:** НАТО розробляє високорівневі стратегії, такі як Політика використання даних (DEFP) та Стратегія даних для Альянсу (DaSA), які мають на меті перетворити дані на стратегічний актив та створити єдину, безпечну екосистему даних.[57] Ці політики стимулюють потребу в кращому управлінні даними та технологіях на національному рівні.

Стратегічні документи НАТО, такі як DEFP та DaSA, і детальні технічні настанови від країн-членів, як-от "Керівництво з метаданих" Міністерства оборони США, не є паралельними процесами. Вони є причинно-наслідковими компонентами єдиного стратегічного зсуву. Високорівневий політико-військовий *намір* НАТО (досягнення інформаційної переваги) [57] породжує потребу в конкретних, реалізовуваних

технічних стандартах на національному рівні. Щоб різні національні системи могли обмінюватися даними в "єдиному логічному середовищі", вони повинні "розмовляти однією мовою". Це створює вимогу до детальних, обов'язкових стандартів щодо того, як дані форматуються (STANAGs) і, що найважливіше, як вони описуються (метадані). Таким

чином, документ, подібний до "Керівництва з метаданих" [59], є прямим логічним наслідком та необхідним інструментом для реалізації стратегічного бачення НАТО. Для України це означає, що прийняття сумісних з НАТО стандартів даних — це не просто технічна вправа. Це фундаментальна передумова для інтеграції в стратегічні процеси прийняття рішень та операційні цикли Альянсу.

7.3. Критична роль метаданих

- **Визначення:** Метадані — це "дані про дані". Вони надають контекст, описуючи походження, формат, класифікацію, права доступу та обмеження щодо поводження з інформаційним активом.[59]
- **Функція:** Метадані є ключовими для виявлення даних (пошуку потрібної інформації), контролю доступу (застосування правил безпеки) та автоматизованої обробки. Саме метадані перетворюють хаотичне "болото даних" на корисне та кероване "озеро даних".[59]
- **Приклад стандарту:** "Керівництво з метаданих" Міністерства оборони США є практичним прикладом надійного стандарту. Воно визначає 10 базових обов'язкових полів, таких як унікальний ідентифікатор, організація-творець, організація-зберігач, дата створення, рівень класифікації безпеки та правила розповсюдження.[59]

Розділ 8: Інтеграція та застосування на системному рівні

8.1. Архітектура C4ISR: поєднання сенсора з тим, хто приймає рішення

C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance — Управління, Контроль, Зв'язок, Комп'ютери, Розвідка, Спостереження) — це всеохопна архітектура, що інтегрує військові інформаційні системи.[3] Мета C4ISR — досягнення інформаційної переваги шляхом створення безперебійного потоку даних від сенсорів (збір) через системи обробки та зберігання до командирів та систем озброєння (рішення та дія).[3] Ефективний збір та надійне зберігання даних є фундаментальними

шарами цієї архітектури, без яких вся система не може функціонувати.

8.2. Приклад: українські автоматизовані системи управління військами

Практична реалізація цих концепцій в Збройних Силах України відбувається через розробку та впровадження національних автоматизованих систем управління (АСУ):

- **"Дзвін":** АСУ стратегічного та оперативного рівня, призначена для інтеграції інформаційних потоків від військових та цивільних джерел у єдину мережу для підтримки процесу прийняття рішень на вищих ланках управління.[9]
- **"Простір":** АСУ тактичного рівня для механізованих та танкових підрозділів, що інтегрує дані від сенсорів та засоби управління вогнем безпосередньо на полі бою.[9]
- **"Ореанда":** АСУ для Повітряних Сил та військ ППО, що формує єдину картину повітряної обстановки та автоматизує процеси управління засобами ураження.[9]

Ці системи є прикладами розбудови національного потенціалу C4ISR, який розробляється з урахуванням вимог та стандартів НАТО.[9]

8.3. Приклад: комерційні системи у військовому використанні (Palantir Gotham)

Для ілюстрації зрілої архітектури інтеграції даних доцільно розглянути провідну комерційну платформу, що широко використовується оборонними та розвідувальними структурами по всьому світу.[60]

- **Palantir Gotham** — це програмна платформа, розроблена для інтеграції величезних обсягів різнорідних даних — як структурованих, так і неструктурованих — з ізольованих баз даних у єдине аналітичне середовище.[60] Її архітектура діє як "сполучна тканина" між персоналом, даними та ресурсами, дозволяючи користувачам виявляти критичну інформацію та розуміти складні взаємозв'язки.[24] Використання цієї платформи в таких програмах, як Project Vantage та наземна станція TITAN армії США, демонструє, як комерційне програмне забезпечення може прискорити цифрову трансформацію збройних сил.[24]

Розробка національних систем, таких як "Дзвін", та впровадження комерційних платформ, як Palantir, представляють дві різні, але взаємодоповнюючі стратегії для досягнення

однієї мети — створення ефективної системи C4ISR. Перший шлях забезпечує суверенний контроль та глибоку адаптацію до національних потреб, але може бути тривалим та ресурсозатратним. Другий шлях дозволяє швидко впровадити передові технології, розроблені за рахунок значних приватних інвестицій, але створює залежність від постачальника. Оптимальною стратегією для сучасної армії є гібридний підхід: розбудова власного, суверенного архітектурного "хребта" на основі відкритих стандартів, з можливістю інтегрувати найкращі у своєму класі комерційні компоненти там, де вони надають явну перевагу. Це дозволяє збалансувати національний контроль та технологічну гнучкість.

Висновок: Синтез збору та зберігання для досягнення інформаційної переваги

Ефективне інформаційно-аналітичне забезпечення є основою сучасного військового управління. Цей огляд продемонстрував нерозривний зв'язок між двома його ключовими компонентами: збором та зберіганням даних. Ми простежили еволюцію методів збору від традиційних дисциплін до комплексного підходу Multi-INT, посиленого штучним інтелектом та всеохопними сенсорними мережами. Паралельно, архітектури зберігання даних еволюціонували від жорстких "сховищ" до гнучких "озерних домів", здатних вмістити та обробити будь-які типи інформації.

Критично важливими елементами, що об'єднують ці процеси, є надійне управління даними, безпека, що базується на тріаді CIA, та стандартизація, яка є запорукою взаємосумісності в коаліційних операціях.

Кінцева мета опанування процесів збору та зберігання даних — це досягнення інформаційної переваги. Ця перевага трансформується безпосередньо у швидші та якісніші рішення на полі бою, надаючи командирам вирішальну перевагу над супротивником. Майбутнє військового мистецтва належатиме тим силам, які зможуть найефективніше керувати своїми даними, поєднуючи технологічні інновації з розвитком людських когнітивних навичок для протистояння викликам складного та динамічного інформаційного середовища.

Джерела

1. Інформаційно-аналітична діяльність, доступ отримано вересня 4, 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
2. Експертні системи та підтримка прийняття рішень - CORE, доступ отримано вересня 4, 2025, https://core.ac.uk/download/pdf/38376998.pdf
3. C4ISR як уможливлення спроможності - Військово-Морських Сил, доступ отримано вересня 4, 2025, https://navy.mil.gov.ua/c4isr/
4. СУТНІСТЬ ТА ЗАВДАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНО, доступ отримано вересня 4, 2025, http://pubadm.vernadskyjournals.in.ua/journals/2024/1_2024/19.pdf
5. ПОНЯТТЯ ТА СКЛАДОВІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІН - Економічний простір, доступ отримано вересня 4, 2025, https://economic-prostir.com.ua/wp-content/uploads/2025/01/196-165-170-grinchenko.pdf
6. «Ми не можемо забрати до себе всіх айтівців зі ЗСУ». Інтерв'ю з командою «Аеророзвідки» — IT-фахівцями, що супроводжують армію на полі бою | DOU, доступ отримано вересня 4, 2025, https://dou.ua/lenta/interviews/how-aerorozvidka-helps-army/
7. II Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та - Державний університет інформаційно-комунікаційних технологій, доступ отримано вересня 4, 2025, https://duikt.edu.ua/uploads/p_2661_99635945.pdf
8. Лекція, доступ отримано вересня 4, 2025, https://learn.ztu.edu.ua/mod/resource/view.php?id=208283
9. Автоматизація за наказом | Defense Express, доступ отримано вересня 4, 2025, https://defence-ua.com/weapon_and_tech/avtomatizatsija_za_nakazom-239.html
10. Firing Data Accuracy and its Impact on the Effectiveness of Artillery Fire - ResearchGate, доступ отримано вересня 4, 2025, https://www.researchgate.net/publication/385650538_Firing_Data_Accuracy_and_its_Impact_on_the_Effectiveness_of_Artillery_Fire
11. Tactics, Techniques, And Procedures for Field Artillery Target Acquisition - GovInfo, доступ отримано вересня 4, 2025, https://www.govinfo.gov/content/pkg/GOVPUB-D214-PURL-gpo130684/pdf/GOVPUB-D214-PURL-gpo130684.pdf
12. Applying the National Training Center Experience: Artillery Targeting Accuracy - DTIC, доступ отримано вересня 4, 2025, https://apps.dtic.mil/sti/tr/pdf/ADA221852.pdf
13. From OSINT to HUMINT: Ranking Intelligence Disciplines by ..., доступ отримано вересня 4, 2025, https://osintteam.blog/from-osint-to-humint-ranking-intelligence-disciplines-by-difficulty-b04bc66b7a52
14. What is Intelligence? - DNI.gov, доступ отримано вересня 4, 2025, https://www.dni.gov/index.php/what-we-do/what-is-intelligence
15. Introduction to intelligence disciplines • #RiskPulse - ACK3, доступ отримано вересня 4, 2025, https://ack3.eu/introduction-to-intelligence-disciplines/
16. Types of Threat Intelligence Gathering - SOCRadar, доступ отримано вересня 4,

2025, https://socradar.io/types-of-threat-intelligence-gathering/
17. Human intelligence (intelligence gathering) - Wikipedia, доступ отримано вересня 4, 2025, https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)
18. VII. MASINT: Measurement and Signatures Intelligence - GovInfo, доступ отримано вересня 4, 2025, https://www.govinfo.gov/content/pkg/GPO-IC21/html/GPO-IC21-7.html
19. Аналіз світових технологічних трендів у військовій сфері, доступ отримано вересня 4, 2025, https://mon.gov.ua/static-objects/mon/sites/1/innovatsii-transfer-tehnologiy/2021/09/30/Analiz.svit.tekhn.trend.viysk.sferi-2021.30.09.pdf
20. український науково-дослідний інститут спеціальної техніки та судових експертиз служби безпеки україни - Львівський НДЕКЦ МВС України, доступ отримано вересня 4, 2025, https://ndekc.lviv.ua/pdf/20.06.2024.pdf
21. Збірник тез доповідей Всеукраїнська науково-практична конференція - НАНГУ, доступ отримано вересня 4, 2025, https://nangu.edu.ua/uploads/files/Zbirnik_tez_APDSSBO.pdf
22. НАУКОВИХ ПРАЦЬ - Репозитарій Національної академії Державної прикордонної служби України імені Богдана Хмельницького, доступ отримано вересня 4, 2025, https://dspace.nadpsu.edu.ua/bitstream/123456789/1884/1/1681-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-4275-1-10-20240514.pdf
23. 'Combat cloud': EDA study shows benefits of cloud computing for EU militaries, доступ отримано вересня 4, 2025, https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows-benefits-of-cloud-computing-for-eu-militaries
24. Palantir Defense Solutions | U.S. Army, доступ отримано вересня 4, 2025, https://www.palantir.com/offerings/defense/army/
25. AWS demonstrates resilient and secure edge-to-cloud at Department of Defense exercise, доступ отримано вересня 4, 2025, https://aws.amazon.com/blogs/publicsector/aws-demonstrates-resilient-and-secure-edge-to-cloud-at-department-of-defense-exercise/
26. 121 ВПЛИВ ВОЄНОГО СТАНУ НА ІНФОРМАЦІЙНЕ НАВАНТАЖЕННЯ ОСОБИ THE IMPACT OF THE WAR - Габітус, доступ отримано вересня 4, 2025, http://habitus.od.ua/journals/2023/47-2023/21.pdf
27. Постановка проблеми. Сьогодні інформаційна зброя стала ..., доступ отримано вересня 4, 2025, http://znp-vo.nuou.org.ua/article/view/336156/324891
28. ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ - Аналітично-порівняльне правознавство, доступ отримано вересня 4, 2025, https://app-journal.in.ua/wp-content/uploads/2025/02/80.pdf
29. Інформаційна гігієна та гібридна безпека: як українці та діаспора в США можуть протидіяти дезінформації? - Вільні Медіа, доступ отримано вересня 4, 2025, https://vilni-media.com/2025/05/17/informatsijna-hihiiena-ta-hibrydna-bezpeka-i

ak-ukraintsi-ta-diaspora-v-ssha-mozhut-protydiiaty-dezinformatsii/
30. бойовий статут - “логістика сухопутних військ збройних сил україни” - Sprotyv G7, доступ отримано вересня 4, 2025, https://sprotyvg7.com.ua/wp-content/uploads/2024/02/2_%D0%91%D0%9F-4-3211.01-%D0%91%D0%A1-%D0%9B%D0%9E%D0%93-%D0%A1%D0%92.pdf
31. Structured Data vs Unstructured Data - Difference Between Collectible Data - AWS, доступ отримано вересня 4, 2025, https://aws.amazon.com/compare/the-difference-between-structured-data-and-unstructured-data/
32. Structured vs. Unstructured Data: What's the Difference? - IBM, доступ отримано вересня 4, 2025, https://www.ibm.com/think/topics/structured-vs-unstructured-data
33. Structured vs Unstructured Data: Key Differences - Datamation, доступ отримано вересня 4, 2025, https://www.datamation.com/big-data/structured-vs-unstructured-data/
34. (PDF) From Unstructured to Structured Information in Military ..., доступ отримано вересня 4, 2025, https://www.researchgate.net/publication/228550534_From_Unstructured_to_Structured_Information_in_Military_Intelligence_Some_Steps_to_Improve_Information_Fusion
35. Data Warehouses vs. Data Lakes vs. Data Lakehouses | IBM, доступ отримано вересня 4, 2025, https://www.ibm.com/think/topics/data-warehouse-vs-data-lake-vs-data-lakehouse
36. Data Lakes vs. Data Warehouses - Fivetran, доступ отримано вересня 4, 2025, https://www.fivetran.com/blog/data-lake-vs-data-warehouse
37. Data Lake vs Data Warehouse: 6 Key Differences - Qlik, доступ отримано вересня 4, 2025, https://www.qlik.com/us/data-lake/data-lake-vs-data-warehouse
38. Data Lake vs. Data Warehouse vs. Data Lakehouse: Which One to Choose? - YouTube, доступ отримано вересня 4, 2025, https://www.youtube.com/watch?v=PQFWQmL3fLY
39. Data lakes vs. data warehouses — what's the difference , and which do you need?, доступ отримано вересня 4, 2025, https://business.adobe.com/blog/basics/data-lake-vs-data-warehouse
40. What is a Data Lake? Data Lake vs. Warehouse | Microsoft Azure, доступ отримано вересня 4, 2025, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-data-lake
41. Хмарне сховище чи локальні сервери: дев'ять критеріїв, які слід ..., доступ отримано вересня 4, 2025, https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers
42. Що таке хмарні сховища та навіщо вони потрібні? | Новини - ТОВ Віст+ ІТ, доступ отримано вересня 4, 2025,

https://vistplus.com/novini/shho-take-hmarni-shovishha-ta-navishho-voni-potribni/
43. Хмарне сховище: що це, як працює, його переваги та недоліки - blog.colobridge.net, доступ отримано вересня 4, 2025, https://blog.colobridge.net/uk/2023/12/what-is-cloud-storage-ua/
44. Що таке безпека в хмарі? | Захисний комплекс Microsoft, доступ отримано вересня 4, 2025, https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security
45. NATO's Digital Modernisation: The Case of Cloud Computing - HCSS, доступ отримано вересня 4, 2025, https://hcss.nl/report/natos-digital-modernisation-the-case-of-cloud-computing/
46. Переваги та недоліки хмарних сервісів -.: Ресурсний центр ГУРТ, доступ отримано вересня 4, 2025, https://gurt.org.ua/articles/38359/
47. Безпечне хмарне сховище, в якому файли зберігаються зашифрованими - Dropbox.com, доступ отримано вересня 4, 2025, https://www.dropbox.com/uk_UA/features/cloud-storage/cloud-security
48. Confidentiality, integrity and availability (CIA triad) | Research Starters - EBSCO, доступ отримано вересня 4, 2025, https://www.ebsco.com/research-starters/information-technology/confidentiality-integrity-and-availability-cia-triad
49. What is the CIA Triad and Why is it important? - Fortinet, доступ отримано вересня 4, 2025, https://www.fortinet.com/resources/cyberglossary/cia-triad
50. CIA triad: Confidentiality, integrity, and availability - SailPoint, доступ отримано вересня 4, 2025, https://www.sailpoint.com/identity-library/cia-triad
51. ДОВІДНИК НАТО - NATO, доступ отримано вересня 4, 2025, https://www.nato.int/docu/other/ukr/handbook/2001/pdf/handbook.pdf
52. Topic: Standardization - NATO, доступ отримано вересня 4, 2025, https://www.nato.int/cps/en/natohq/topics_69269.htm
53. STANAG Лабораторія випробувань НАТО - Eurolab, доступ отримано вересня 4, 2025, https://www.eurolab.com.tr/uk/sektorel-test-ve-analizler/spesifik-testler/stanag-test-laboratuvari
54. Standardization agreement - Wikipedia, доступ отримано вересня 4, 2025, https://en.wikipedia.org/wiki/Standardization_agreement
55. Як кодифікують зброю в країнах НАТО та Україні | Пояснюємо МОУ, доступ отримано вересня 4, 2025, https://mod.gov.ua/explanation/yak-kodifikuyut-zbroyu-v-krayinah-nato-ta-ukrayini
56. STANAG 5516 - Вікіпедія, доступ отримано вересня 4, 2025, https://uk.wikipedia.org/wiki/STANAG_5516
57. Official text: Summary of NATO's Data Exploitation ... - NATO, доступ отримано вересня 4, 2025, https://www.nato.int/cps/en/natohq/official_texts_210002.htm
58. Official text: Data Strategy for the Alliance , 05-May.-2025 - NATO, доступ

отримано вересня 4, 2025, https://www.nato.int/cps/en/natohq/official_texts_234937.htm
59. Department of Defense Metadata Guidance - Chief Digital and ..., доступ отримано вересня 4, 2025, https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Metadata%20Guidance.pdf
60. Palantir Technologies - Wikipedia, доступ отримано вересня 4, 2025, https://en.wikipedia.org/wiki/Palantir_Technologies
61. SMC awards $32.5 million to Palantir Technologies Inc for Data-as-a-Service, доступ отримано вересня 4, 2025, https://www.losangeles.spaceforce.mil/News/Article-Display/Article/2592151/smc-awards-325-million-to-palantir-technologies-inc-for-data-as-a-service/
62. TITAN ground station targeting system: a Palantir disruption or a predictable military progress? - MEPEI, доступ отримано вересня 4, 2025, https://mepei.com/titan-ground-station-targeting-system-a-palantir-disruption-or-a-predictable-military-progress/