УДК: 355.4:004.77 DOI: **10.33099/2311-7249/2025-52-1-46-54**

ПАРАЩУК Лідія Ярославівна,
кандидат технічних наук, доцент,
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна,
https://orcid.org/0000-0002-4049-2033

ПАРАЩУК Сергій Миколайович,
Національний університет оборони України, Київ, Україна
https://orcid.org/0009-0000-2830-7109

РЕКОМЕНДАЦІЇ СТОСОВНО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ПОКРАЩЕННЯ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

Стаття присвячена аналізу теоретичних і практичних аспектів створення та впровадження інформаційних систем для підвищення ситуаційної обізнаності органів військового управління.

***Метою статті** є розроблення рекомендацій щодо використання інформаційних систем для покращення ситуаційної обізнаності органів військового управління.*

***Методи дослідження.** У статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за тематикою функціонування та застосування інформаційно-комунікаційних систем. Для оцінювання ефективності застосування систем, що розглядаються у статті, також були використані такі загальнонаукові методи досліджень, як swot-аналіз.*

***Отримані результати дослідження.** У роботі висвітлено сучасні виклики, з якими стикаються збройні сили в умовах глобалізації, стрімкого розвитку інформаційних технологій і трансформації характеру збройних конфліктів. Розглянуто ключові проблеми, пов'язані з інтеграцією інформаційних систем у військове середовище, забезпеченням кібербезпеки, впливом людського фактору та обмеженою оперативністю обробки великих обсягів даних. Проаналізовано переваги та недоліки таких сучасних рішень, як система «Delta», що забезпечує інтеграцію даних із різних джерел (дрони, супутники, сенсори) та відповідає стандартам НАТО. На основі проведеного SWOT-аналізу визначено сильні й слабкі сторони, можливості та загрози впровадження таких систем. Особливу увагу надано ролі штучного інтелекту та автоматизації процесів аналізу й прийняття рішень. Через призму загроз, що можуть застосовуватися до інформаційно-комунікаційних систем загалом та системи «Delta» зокрема, розглянуто реалізацію можливостей використання системи для покращення ситуаційної обізнаності. Разом із тим, показано вплив недоліків, а саме високу залежність від рівня підготовки користувачів та особливих умов роботи в зоні дії пристроїв радіоелектронної боротьби.*

***Елементи наукової новизини.** Наукова новизна дослідження зводиться до проведення комплексного аналізу використання інформаційних систем у військовому управлінні, визначення їх ефективності та розробки практичних рекомендацій щодо їх удосконалення. Запропоновано підходи до інтеграції технологій штучного інтелекту та кібербезпеки у військові інформаційні системи.*

***Теоретична й практична значущість.** Результати дослідження мають важливе значення для військово-оборонної сфери, оскільки сприяють підвищенню ситуаційної обізнаності, покращенню координації та ефективності прийняття рішень. Перспективами подальших досліджень можуть бути: розробка автономних систем, посилення захисту від кібератак, вдосконалення алгоритмів штучного інтелекту, інтеграція з міжнародними платформи та адаптація для цивільного використання.*

***Ключові слова:** інформаційні системи, ситуаційна обізнаність, військове управління.*

Вступ

Застосування інформаційних систем із метою покращення ситуаційної обізнаності органів військового управління зумовлена сучасними загрозами і викликами, що постають перед військовими формуваннями, підрозділами й організаціями в умовах світового масштабування та інтенсивного розвитку інформаційних технологій і зміни у характері збройних конфліктів. Збройні сили сучасності функціонують у надскладному інформаційному полі, якому властиве значний обсяг даних, висока швидкість їхньої зміни та необхідність оперативного прийняття рішення.

На сьогоднішній день поширення цифрових технологій здійснило революцію майже в кожному аспекті нашого життя: від безперебійного зв'язку, що проводиться з допомогою хмарних обчислень, до Інтернету речей, який складається зі складної мережі взаємопов'язаних пристроїв. Наша адикція від цифрової інфраструктури стала фундаментальною для сучасного існування. Ці технології відкрили безпрецедентні рівні ефективності, продуктивності та зв'язку, змінивши спосіб спілкування один з одним і взаємодії з навколишнім світом. Основне місце в цих

зв'язках посіли інформаційні та інформаційно-комунікативні системи, даючи змогу не тільки збирати дані, але й брати участь у прийнятті рішень.

Постановка проблеми. У сучасних умовах динамічних і складних викликів, що постають перед органами військового управління, ефективність прийняття рішень значною мірою залежить від рівня ситуаційної обізнаності. Ситуаційна обізнаність містить здатність командного складу своєчасно отримувати, аналізувати та інтерпретувати інформацію про поточний стан оперативної обстановки, що впливає на результативність виконання завдань для забезпечення національної безпеки й оборони.

З розвитком інформаційних технологій виникає потреба впровадження існуючих інформаційно-комунікаційних систем в органи військового управління з метою підтримки ситуаційної обізнаності. Однак, імплементація таких технологій зумовлює низку проблем, які вимагають системного аналізу та наукових досліджень. До основних проблем, які найчастіше зустрічаються на практиці та описаних, зокрема, у роботах авторів [1] можна віднести:

складність впровадження інформаційно-комунікаційних систем у мілітарне середовище – переважна більшість існуючих на сьогодні військових систем вже мають власну інфраструктуру, яка може бути несумісною з новими інформаційними технологіями. Інтеграція нових систем вимагає адаптації технічних рішень та навчання персоналу;

проблема забезпечення кібербезпеки – інформаційні системи, які застосовуються у військовому управлінні, мають бути стійкими до кібератак і забезпечувати надійний захист даних. Це вимагає розроблення новітніх криптографічних протоколів, систем контролю (зокрема, й автоматизованого) доступу та методик виявлення загроз;

ризик людського фактору – складність і багатофункціональність інформаційних систем вимагає високої підготовки операторів. Помилки, викликані некомпетентністю чи недостатнім рівнем підготовки персоналу спричиняють зниження ефективності застосування систем і впливають на якість прийнятих рішень;

недостатня швидкість обробки великого обсягу даних – ведення, супроводження та планування військових операцій пов'язана з обробкою значної кількості інформації у реальному часі. У штабах оперативно-стратегічних та оперативно-тактичних угруповань військ з технічних чи кадрових причин часто стикаються з обмеженнями у швидкості обробки даних та її передачі до центру прийняття рішень, що впливає на ситуаційну обізнаність. Тому застосування інформаційних систем у процесі управління, зокрема й військового, є перспективним і актуальним сучасним напрямом розвитку поінформованості і оперативності прийняття рішень.

Аналіз останніх досліджень і публікацій. Останні публікації А. Гавриленко [4] та дослідження A. Nadibaidze, I. Bode, Q. Zhang [5] підкреслюють значний прогрес у використанні інформаційних систем загалом та для підвищення ситуаційної обізнаності органів військового управління, зокрема.

Обробка інформації здійснюється органами військового управління відповідно до вимог чинного законодавства, внутрішніх регламентів та встановлених процедур. Основними визначеними завданнями обробки інформації є: збір, аналіз, узагальнення і подальше поширення актуальних даних. Ці процеси спрямовані на своєчасне інформування командного складу щодо змін, що відбулися в оперативній обстановці, встановлення імовірних потенційних загроз та прогноз можливих шляхів розвитку ситуації. Організація потоків інформації здійснюється через інтеграцію підрозділів шляхом використання сучасних комунікаційних технологій та автоматизованих систем управління.

Збір інформації здійснюється відповідно до завдань і планів, що затверджені командуванням. Джерелами інформації є розвідувальні дані (зокрема, радіоелектронна, агентурна і технічна розвідка), доповіді підрозділів, оперативні звіти, а також інформація, отримана із автоматизованих систем управління, сенсорів та систем моніторингу. Окрім того, важливим джерелом є інформація, отримана від партнерів та союзників. Для її подальшого аналізу та використання особливо детально фіксують місце, час та обставини отримання інформації [2].

Усі дані та інформація проходять етапи, які є уніфікованими як у цивільній, так і військовій сфері і описані у праці [3] авторами М. Поповим, О. Зайцевим, С. Стефанцевим. На стадії первинної обробки здійснюється перевірка достовірності, точності і повноти зібраних даних. Аналіз первинних даних передбачає оцінку їхньої значущості в контексті актуальної ситуації. Отримана інформація співвідноситься з історичними показниками, що дає змогу визначити ключові зміни, тенденції та закономірності. Це, своєю чергою, сприяє побудові прогнозів щодо можливого розвитку подій. Результатом такої аналітичної роботи стають висновки та рекомендації, що мають практичне значення для підтримки процесу ухвалення рішень.

Тому враховуючи проаналізовані джерела літератури та актуальність імплементації інформаційно-комунікаційних технологій у військову сферу **метою статті** обрано розроблення рекомендацій щодо використання інформаційних систем для покращення ситуаційної обізнаності органів військового управління.

Виклад основного матеріалу дослідження

Сьогодні комп'ютерні системи здатні вивчати дані та середовище і самостійно виправляти помилки. Основною і найвагомішою такою системою у сучасному світі є штучний інтелект (далі – ШІ). Він є напрямом у сучасній науці та техніці, що передбачає створення і розробку комп'ютерних систем або алгоритмів, здатних виконувати завдання, які традиційно потребують супроводження людського інтелекту [6]. Впровадження ШІ у всі сфери діяльності людини (рис. 1), включно з оборонною, стає одним із найважливіших досягнень сучасного світу.

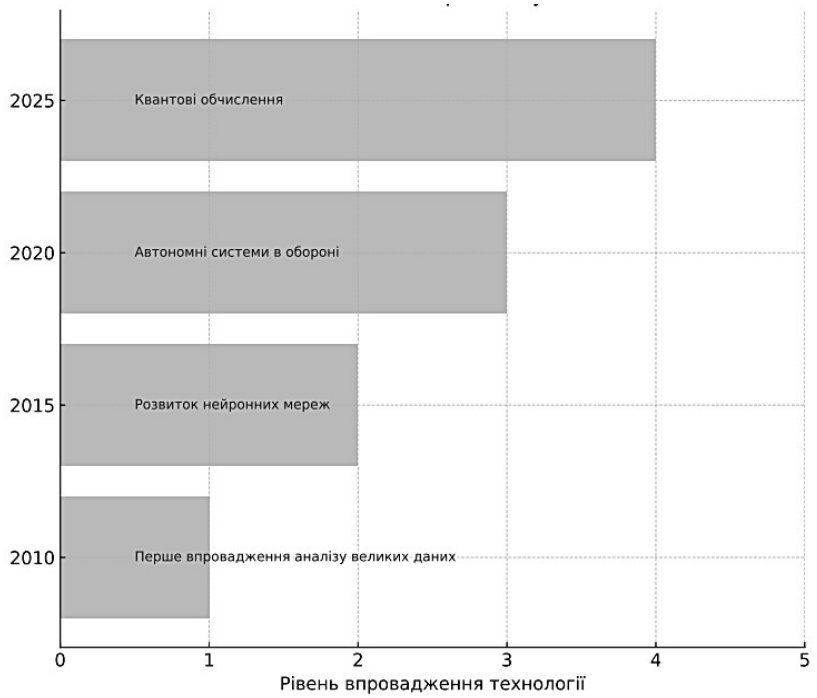

Рисунок 1 – Часова діаграма імплементації інформаційно-комунікаційних технологій у військову сферу

Термін «штучний інтелект» набуває все більшої популярності завдяки його потенціалу змінювати підходи до вирішення складних завдань. З рисунка 1 бачимо, що перший досвід обробки великого обсягу даних було здійснено ще у 2010 році. З розвитком галузі інформаційних технологій (далі – ІТ) сфери все ширшого вжитку зазнають нейронні мережі, що починають застосовуватися і для військової сфери. Пізніше, на їх основі вибудовуються цілі автономні системи, які дають змогу миттєво розпізнавати певні типи інформації, перетворювати їх у рішення та застосовувати в оборонній сфері.

Що стосується квантових обчислень, то дана галузь в обороні та системі прийняття рішень застосовується переважно для аналізу аномалій, які можна виявити під час кібератак, а також використовувати для прогнозування ймовірних сценаріїв розвитку бойових дій. Всі перераховані вище стадії використання інформаційно-комунікаційних технологій (далі – ІКТ) у військовій сфері не є максимальними, тому навіть на сучасному рівні розвитку комп'ютерних технологій ще є ніша, яку можна було б заповнити інноваційними рішеннями.

Однак ці рішення мають бути актуальними, тому для їх вибору оптимальним підходом є проведення аналізу, який дає змогу виявити сильні та слабкі сторони. Для цього найкраще підходить SWOT-аналіз. Здійснивши такий аналіз основних принципів, на яких базується процес обробки інформації, можна стверджувати, що підвищення результативності, а заразом і продуктивності використання інформаційно-комунікаційних систем відбувається у випадках, коли інформація для аналізу перевірена та актуальна (табл. 1).

Таблиця 1

SWOT-аналіз основних принципів процесу обробки інформації

Сильні сторони (Strenghts)	Слабкі сторони (Weaknesses)
1. Достовірність використання перевірених і надійних джерел зменшує ризик поширення хибної інформації; забезпечує високу якість даних для прийняття рішень. *2. Своєчасність* швидка обробка і передача даних забезпечують оперативне реагування на зміну обстановки; мінімізує ризики затримок у прийнятті важливих управлінських рішень. *3. Конфіденційність* надійний захист інформації знижує ймовірність витоку даних; сприяє збереженню стратегічної переваги. *4. Безперервність* постійний моніторинг та оновлення баз даних гарантують актуальність інформації;	*1. Висока залежність від якості джерел інформації* неточності чи помилки у вихідних даних можуть спотворити аналітичні висновки. *2. Часові обмеження* надмірна вимога до швидкості обробки може вплинути на якість аналізу. *3. Складність захисту конфіденційності* уразливість до кіберзагроз під час використання цифрових каналів; потреба в постійних оновленнях систем безпеки. *4. Технологічна залежність* необхідність у сучасному обладнанні та програмному забезпеченні; високі витрати на підтримку технічних ресурсів.

Сильні сторони (Strenghts)	Слабкі сторони (Weaknesses)
виключає можливість втрати даних через технічні або організаційні збої. *5. Інтегрованість* координація між рівнями управління сприяє єдності інформаційних потоків; підвищує ефективність взаємодії між підрозділами.	
Можливості (Opportunities)	**Загрози (Threats)**
1. Розвиток автоматизованих систем управління застосування нових технологій для автоматизації збору, обробки та аналізу даних. *2. Міжнародна співпраця* обмін досвідом та інформацією з союзниками сприяє підвищенню ефективності процесів. *3. Інноваційні методи аналізу даних* використання штучного інтелекту та машинного навчання для точнішого прогнозування ситуацій. *4. Удосконалення законодавчої бази* з процедур обробки інформації відповідно до сучасних умов.	*1. Кіберзагрози* ризик атак на інформаційні системи, які можуть призвести до витоку чи втрати даних. *2. Швидка зміна обстановки* неочікувані зміни можуть ускладнити процеси аналізу та реагування. *3. Технологічна застарілість* використання застарілого обладнання або систем може знизити ефективність інформаційної роботи. *4. Проблеми координації* недоліки у взаємодії між рівнями управління можуть спричинити неефективність інформаційних потоків.

Збільшення швидкості обробки даних може зменшувати кількість гілок розгалуження алгоритму чи здійснення перевірки по циклу недостатньої кількості варіантів. Це призводить до зниження якості аналізу. Подолання слабких сторін у вигляді заміни застарілого обладнання на найсучасніше та постійного захисту від кіберзагроз, створюють нові можливості для розвитку інформаційно-комунікаційних систем, здійснення аналізу ситуації з використанням штучного інтелекту, піднесе ці процеси на новий рівень у очах партнерів у ракурсі міжнародного співробітництва.

Загалом будь-яка інформаційна система виконує певні функції. На рис. 2 авторами наведено основні функції інформаційних систем, які забезпечують ефективну обробку, управління та використання інформації.

Рисунок 2 – Структурна схема функціонування інформаційно-комунікаційних систем ситуаційної обізнаності

Процес одержання даних із різних джерел забезпечується функцією збору інформації. Метою цієї функції є забезпечення актуальності й повноти даних, шо необхідні для подальшого аналізу та прийняття рішень. На стадії обробки даних зібрана інформація перетворюється, очищується, структурується чи проходить інші види аналізу, які дають змогу підготувати її до використання. Обробка поєднує алгоритмічний аналіз, статистичні операції або ж, залежно від призначення системи, створення необхідних моделей прогнозування.

Відповідно до робіт автора [7], процес обробки інформації здійснюється за такими принципами:

забезпечення достовірності – використання надійних і перевірених джерел інформації, уникаючи поширення непідтверджених даних;

організація своєчасності – оброблення та передавання даних виконується у найкоротші терміни для підтримання ефективного прийняття рішень у реальному часі;

дотримання конфіденційності – встановлення правил безпеки, що надають доступ до інформації користувачам відповідно до рівня її таємності;

забезпечення безперервності – процес постійного контролю, оновлення інформаційних баз даних та матеріалів, що не допускає зупинок;

інтегрованість – здійснюється горизонтальна та вертикальна координація рівнів військового управління для отримання уніфікації інформаційних потоків.

З метою подальшого використання необхідно забезпечити організацію та архівацію даних. Використовуються різні типи сховищ – від локальних баз даних до хмарних платформ. Саме цим займається функція зберігання. Основна вимога до цієї функції – надійність і захист даних.

За інтерпретацію інформації у вигляді, зрозумілому для користувачів відповідає функція відображення. Це можуть бути графіки, таблиці, діаграми чи інтерактивні інтерфейси, що полегшують аналіз інформації. Передавання здійснює транспортування інформації між різними складовими системи чи користувачами. Ефективна комунікація досягається завдяки використанню сучасних мережевих технологій та протоколів, які забезпечують швидкість і безпеку передачі даних. Підтримка прийняття рішень – це кінцева мета роботи інформаційних систем, яка передбачає допомогу користувачам у виборі оптимальних рішень. На основі зібраних, оброблених та проаналізованих даних створюються рекомендації, прогнози чи сценарії, які сприяють ефективному управлінню [8].

Інформаційні системи виконують основну роль у здійсненні обробки даних, однак їхня важливість зростає тоді, коли вони перетворюються у засіб досягнення ситуаційної обізнаності. Ситуаційна обізнаність – це усвідомлення свого оточення через різноманітні потенційні небезпеки або загрози. Такий підхід дає змогу оцінювати ризики, виявляти причинно-наслідкові зв'язки, а також формувати багаторівневу стратегію управління. Згідно [9] існує чотири основні характеристики ситуаційної обізнаності: спостереження, орієнтація, рішення та дія. *Спостереження* передбачає постійний моніторинг дій та ситуацій, що відбуваються навколо нас. *Орієнтація* спонукає аналізувати оточуючі обставини і обробляти інформацію на основі власного досвіду. *Рішення* має бути таким, що зважує всі варіанти та знаходить найкращий можливий результат у межах існуючих можливостей. *Дія* – це завершальний крок, в якому необхідно використати всю попередню інформацію, щоб застосувати певні міри або заходи, залежно від обставин та отримання бажаного результату.

На сучасному полі бою ситуаційна обізнаність є одним із ключових чинників прийняття рішень та успішного ведення бойового досвіду Як і будь-яка система з прийняття рішення, вона вимагає ґрунтовного збору, глибокого аналізу та синтезу великих об'ємів інформації, систематизованих з різних джерел, що стає можливим виключно через впровадження інноваційних технологій. У військових операціях НАТО ключовим інструментом для забезпечення ситуаційної обізнаності на оперативному, тактичному та стратегічному рівнях є принципи ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance (розвідка, спостереження, захоплення цілей, рекогносцировка)). Ця система охоплює комплексний збір, обробку та інтеграцію даних з таких різноманітних джерел, як пункти і підрозділи військової розвідки, супутники, дрони.

ISTAR сприяє формуванню точного та актуального уявлення про обстановку на полі бою, забезпечуючи безперервний моніторинг і раннє виявлення загроз. Завдяки цьому принципу, командуванням НАТО може бути ефективно визначено критичні цілі, скоординовано дії військових підрозділів та адаптовано стратегії в режимі реального часу. Такий підхід покращує точність та швидкість у прийнятті рішень, зменшуючи ризики для особового складу та підвищуючи ефективність операцій шляхом покращення динамічності середовища сучасного конфлікту [10].

Принципи ISTAR впроваджені в систему ситуаційної обізнаності «Delta», що спроєктована українськими розробниками національної військової системи, створена для впровадження інформації про розміщення сил противника в реальному часі. Дані, що надходять із різних джерел (супутникові знімки, радари, сенсори та GPS-трекери) відображаються на цифровій мапі. Для прикладу система «Delta» здатна акумулювати дані з різноманітних джерел для аналізу та підтримки прийняття рішень у сферах безпеки, оборони та стратегічного управління. Джерела даних у цій системі є надзвичайно різноманітними й охоплюють традиційні і сучасні технологічні канали, що робить її унікальною. Це забезпечує командирам оперативний доступ до актуальної інформації для прийняття обґрунтованих рішень [11].

«Delta» побудована згідно зі стандартами НАТО та розроблена Центром інновацій і розвитку оборонних технологій Міністерства оборони України та 2023 року офіційно впроваджена в Силах оборони. Основним завданням створеної системи є заміна застарілих методів збору та оброблення інформації й створення сучасної платформи, що відповідає потребам сучасного театру бойових дій. Доступ до даних про систему є суворо обмеженим, публічною є невеличка частка інформації про функціонал системи та її переваги. Користувачі системи отримують дані відповідно до рівня доступу, що відповідає рівню доступу до інформації. Повний спектр даних доступний лише на найвищому рівні управління. В умовах сучасних військових конфліктів система «Delta» показує новий рівень оперативного управління, інтегруючи інноваційні технології для посилення обороноздатності України.

Основними джерелами даних у системі «Delta» можна вважати:

спостереження технічними засобами (дані поступають від сучасних пристроїв, таких як супутники, БпЛА та радари. Радари передають інформацію про координати, швидкість і траєкторію об'єктів, в той час як супутники забезпечують високоточні зображення для моніторингу ситуацій на великих територіях. Безпілотниками збагачують деталізовані візуальні та теплові дані);

сховища та бази даних (повна та актуальна інформація забезпечується накопиченням у внутрішніх і зовнішніх базах даних. Вона охоплює оперативні зведення інформацію щодо логістики, демографічні дані та реєстри об'єктів);

діяльність розвідки (важливі дані система отримує через розвідувальні канали. Це можуть бути відкриті джерела (OSINT), дані, зібрані агентами чи свідками (HUMINT), перехоплені радіосигнали (SIGINT) або аналітика супутникових зображень (IMINT). Розвідка є критично важливим джерелом для формування стратегічної картини);

автоматизовані джерела (дані надходять через телекомунікаційні мережі, які забезпечують інформацію про місцеперебування пристроїв або активність у мережах. Веб-скрапінг дає змогу автоматично збирати дані з публічних веб-сайтів і онлайн-ресурсів);

інформація, введена користувачами (визначальну роль відіграє інформація, яка вводиться користувачами системи, зокрема оперативні звіти, коментарі, інтерактивні мітки на картах, що фіксують важливі місця подій або стратегічних об'єктів);

сумісність з іншими інформаційними системами («Delta» має доступ до масиву державних і приватних даних із партнерських джерел та міжнародних організацій через інтерфейси API (Application Programming Interface (програмний інтерфейс додатків));

синтетичні дані та прогнози (окрім збору наявних даних, система генерує прогнози на основі моделювання, аналізуючи існуючі показники та ймовірні сценарії розвитку подій. Це дає змогу їй створювати цілісну й динамічну картину для аналізу та прийняття стратегічних рішень) [12].

Інтелектуальні алгоритми системи забезпечують обробку великих масивів даних, дозволяючи виявляти критичні цілі, оцінювати потенційні загрози та прогнозувати можливі сценарії розвитку бойових дій. Завдяки функціям спостереження та збору даних у реальному часі, «Delta» дає змогу наносити геопросторову інформацію на інтерактивну карту, створюючи чітке уявлення про обстановку на полі бою. Вона також підтримує функції збереження та обміну зображеннями між різними військовими частинами. Завдяки геолокації всі дані в реальному часі відображаються на інтерактивній карті, що забезпечує зручність доступу до інформації та значно скорочує час реакції порівняно з попередніми аналогами. Система також забезпечує передачу релевантної інформації до різних рівнів управління, що відповідає принципу розподіленого доступу ISTAR. Це дає змогу командирам на тактичному рівні отримувати лише необхідні дані для прийняття оперативних рішень, тоді як стратегічне командування має доступ до повної картини бойових дій.

З метою посилення захисту системи від ракетних і кібератак, уряд ухвалив рішення про розміщення «Delta» у хмарних сервісах за межами України. Такий підхід гарантує безперервність її роботи навіть за умов інтенсивного ворожого впливу. Ця платформа дає змогу вести мережевоцентричну війну, забезпечуючи інтеграцію з аналогічними системами союзників. «Delta» сприяє ефективному плануванню операцій та координації між підрозділами, підвищуючи загальну оперативну ефективність [13].

Отже, принципи ISTAR у системі «Delta» допомагають не лише забезпечувати ситуаційну обізнаність, але й оптимізувати процеси управління, роблячи їх більш динамічними та адаптивними до змін у реальному часі. Однак, провівши аналіз самої системи (табл. 2), варто зауважити, що деякі окремі елементи можна віднести одночасно як до переваг, так і до недоліків. Зокрема, такі як розміщення системи в «хмарному середовищі» робить її більш захищеною, водночас прив’язує до залежності від інтернету та коректного функціонування хмарних сервісів.

Таблиця 2

SWOT-аналіз системи ситуаційної обізнаності «Delta»

Сильні сторони (Strenghts)	Слабкі сторони (Weaknesses)
1. Інтеграція даних у реальному часі: система здатна об'єднувати інформацію з різних джерел, таких як дрони, супутники, сенсори, що забезпечує повну ситуаційну обізнаність. *2. Сумісність зі стандартами НАТО:* «Delta» відповідає міжнародним стандартам, що спрощує інтеграцію з союзними системами розвідки. *3. Ієрархія доступу:* контрольоване надання інформації залежно від рівня доступу підвищує безпеку даних. *4. Гнучкість і мобільність:* розміщення системи у «хмарі» забезпечує захист від фізичних атак та зберігає працездатність навіть за умов інфраструктурних втрат. *5. Зменшення часу реакції:* швидка передача інформації суттєво скорочує час прийняття рішень.	*1. Залежність від інтернету та хмарних сервісів:* у випадку порушення зв’язку доступ до системи може бути ускладненим. *2. Висока вартість впровадження та підтримки:* технологічна складність і потреба в інфраструктурі потребують значних ресурсів. *3. Потреба в навчанні персоналу:* ефективне використання системи вимагає спеціальної підготовки для операторів. *4. Можливість кібератак:* попри заходи безпеки, система залишається ціллю для складних кібератак з боку противника.
Можливості (Opportunities)	**Загрози (Threats)**
1. Розширення функціоналу: подальший розвиток алгоритмів штучного інтелекту для автоматизації аналізу даних. *2. Міжнародна співпраця:* інтеграція з союзними системами ситуаційної обізнаності для обміну даними в межах спільних операцій НАТО. *3. Використання для цивільних потреб:* адаптація технологій для реагування на надзвичайні ситуації чи гуманітарні місії. *4. Підвищення рівня автономності:* застосування автономних рішень для роботи в умовах тимчасового порушення зв’язку.	*1. Ескалація кібервійни:* зростання кількості та складності кібератак з боку противника. *2. Залежність від іноземних хмарних сервісів:* потенційні ризики доступу до даних через політичні чи економічні фактори. *3. Розкриття інформації через людський фактор:* помилки чи зловмисні дії користувачів можуть поставити під загрозу безпеку даних. *4. Технічні обмеження в екстремальних умовах:* умови війни, такі як радіоелектронна боротьба, можуть ускладнити ефективне функціонування системи.

Сумісність зі стандартами НАТО часто вимагають від користувачів системи додаткових знань протоколів подання інформації та перетворення звичних форм донесень у рапорти за натівськими стандартами. Використання інформаційно-комунікаційних систем нового рівня дає поштовх до розвитку нових підходів до здійснення кібератак, тим самим знижуючи захищеність вищезгаданих систем. Коректне функціонування системи, значною мірою, залежить від умов її експлуатації. Зокрема, якщо це відбувається недалеко від лінії зіткнення, де працюють засоби радіоелектронної боротьби, можна стверджувати, що здатність передачі чи обміну даними можуть сповільнюватися, що впливає на швидкість прийняття рішення.

Отже, система «Delta» є потужним інструментом для збору, обробки та інтеграції даних. Як і в будь-якій інформаційно-комунікаційній системі, у «Delta» можна виділити сильні й слабкі сторони, що підтверджується даними SWOT-аналізу. Однак користь від застосування цієї системи набагато більша від імовірних загроз. Завдяки використанню різноманітних джерел, автоматизації та сучасних аналітичних технологій, вона забезпечує високу точність, актуальність і оперативність інформації, що є критично важливим для прийняття стратегічно виважених рішень у складних умовах.

З метою покращення ситуаційної обізнаності та підтримки прийняття рішень сформульовано *рекомендації* щодо використання інформаційно-комунікаційних систем:

1. Визначити чітко основні цілі використання інформаційно-комунікаційних систем перед впровадженням та обрати необхідний функціонал.
2. Автоматизувати збір даних із доступних джерел та інтерпретувати інформацію у вигляді графіків, зведених таблиць.
3. Визначення тенденцій, прогнозування та аналіз великих об’ємів даних здійснювати з використанням штучного інтелекту.
4. Забезпечити оперативний доступ до інформації з використанням захищених хмарних платформ та їх автоматизацію через API та інтегровані системи повідомлень.
5. Для мінімізації ризиків витоку інформації та кібератак використовувати сучасні засоби шифрування та дворівневу (щонайменше) автентифікацію, а також забезпечити резервне копіювання та відновлення даних.
6. Щомісячно проводити моніторинг ефективності інформаційно-комунікаційної системи використовуючи зворотний зв’язок від користувачів й удосконалення шляхом оновлення програмного забезпечення та впровадження нових технологій, що дасть спроможність відповідати потребам та сучасним викликам.

Висновки й перспективи подальших досліджень

Інформаційно-комунікаційні системи забезпечують виконання широкого спектру функцій, спрямованих на ефективний збір, обробку, зберігання та передачу даних, а також підтримку прийняття рішень. Однак реалізація цих функцій залежить від якості й різноманітності даних, які надходять у систему. Завдяки можливостям сучасних інформаційних систем, дані з різних джерел (розвідувальних дронів, супутників, наземних радарів, сенсорів та інших систем моніторингу) можуть бути зібрані, узгоджені та об'єднані в єдине інформаційне середовище. для формування в реальному часі цілісну картину оперативної обстановки, що критично важливо для прийняття своєчасних управлінських рішень.

Прогнозування можливих сценаріїв розвитку військової операції чи виявлення прихованих загроз (таких як підготовка до кібератаки) відбувається з використанням штучного інтелекту на основі аналізу зібраних даних, встановлення закономірностей, а також виявлення аномалій. Це значно підвищує спроможність командування оперативно реагувати на виклики.

Інформаційні системи дають можливість структурувати та ефективно організовувати інформаційні потоки між підрозділами, військовими органами управління та командними пунктами. Автоматизація процесу передачі даних знижує час, потрібний для прийняття рішень, а також зводить до мінімуму ризики спотворення інформації або її втрати. Впровадження інноваційних технологій і систем, розроблених з урахуванням стандартів НАТО, забезпечує сумісність між національними збройними силами і союзниками у багатонаціональних операціях, що підвищує ефективність спільного командування та є критичним у межах коаліційних операцій або спільних навчань. Разом із тим, виявлено низку викликів, зокрема, значну залежність від дигіталізації, наявність кіберзагроз та необхідність фінансових вкладень для вдосконалення систем.

Перспективи подальших досліджень мають бути зосереджені на вдосконалення інформаційно-комунікаційних систем для підвищення їхньої надійності та ефективності. Пріоритетними завданнями є створення стійких до зовнішніх впливів автономних систем управління, впровадження передових алгоритмів штучного інтелекту для автоматизації аналізу даних та мінімізації впливу людського фактору. Також варто дослідити гармонізацію та інтеграцію інформаційних систем у багатонаціональні військові операції відповідно до стандартів союзників, висвітлити особливості посилення кіберзахисту для забезпечення безпеки інформації, а також охарактеризувати адаптацію цих систем до умов надзвичайних ситуацій і гуманітарних місій. Комплексний підхід до розв'язання цих завдань сприятиме підвищенню оперативності, точності та надійності прийняття рішень у військовій сфері.

Удосконалення та ширше впровадження інформаційних систем дасть змогу суттєво підвищити ефективність військового управління, забезпечивши швидкість і точність у прийнятті рішень.

Список бібліографічних посилань

1. Fay A. Cybersecurity and Information Systems in Military Operations. *Journal of Military and Strategic Studies* .2020. № 22(3). С. 45–63. **2. Лавренчук В. А.** Аналіз інтеграції новітніх технологій в оборонну сферу: теоретичні аспекти та практичні виклики. *Наукові записки Національного університету оборони України*. 2021. № 15(2). С. 78–90. **3. Popov M., Zaitsev O., Stefantsev S.** Innovative approach to reducing cognitive biases in expert evaluation**.** *Social Development and Security***.** 2025. № 15(1). P. 171–179. DOI: 10.33445/sds.2025.15.1.16. **4. Гавриленко А. С.** Аналіз застосування технологій штучного інтелекту в системах військового призначення. *Випробування та сертифікація*. 2024. № 1(3). С. 40-44. DOI: 10.37701/ts.03.2024.6. **5. Nadibaidze A., Bode I., Zhang Q.** AI in Military Decision Support Systems A Review of Developments and Debates. *Center for War Studies*, 2024. 49 p. **6. Костенко О. В.** Аналіз національних стратегій розвитку штучного інтелекту. *Інформація і право*. 2022. № 2(41). С. 58–69. DOI: 10.37750/2616-6798.2022.2(41).270365. **7. Іосіфов Є. А.** Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації: Дис…д-ра філософії: 125. Київський столичний університет імені Бориса Грінченка. Київ, 2024. 214 с. **8. Загорка О. М., Корецький А. А., Загорка І. О., Комолаєва Т. М.** Підтримка вироблення рішень під час ситуаційного управління операцією (боєм): методичне забезпечення. *Воєнно-прикладні питання системного аналізу та математичного моделювання*. 2020. № 1(68). С. 98–109. DOI: /10.33099/2304-2745/2020-0/98-109.
9. Демиденко М. А. Системи підтримки прийняття рішень. Дніпропетровськ : Нац. гірн. ун-т., 2016. 104 с. **10. Joint Intelligence, Surveillance and Reconnaissance**. 2024. URL: https://www.nato.int/cps/en/natohq/topics_ 111830.htm (дата звернення: 29.01.2025). **11. Агентура, супутники, дрони – як «Дельта» поєднує різні дані і допомагає нищити ворога.** 2022. URL: https://texty.org.ua/articles/108967/ahentura-suputnyky-drony-yak-delta-poyednuye-rizni-dani-i-dopomahaye-nyshyty-voroha (дата звернення: 29.01.2025). **12. Миколайчук Р., Старинський І., Миколайчук В.** Аналіз технологічних аспектів реалізації веб-скрапінгу статичних і динамічних сайтів. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 3(51). С. 80–88. DOI: 10.33099/2311-7249/2024-51-3-80-88. **13. Delta для ЗСУ: Що відомо про новітню систему управління української армії.** 2023. URL: https://www.bbc.com/ukrainian/features-64585182 (дата звернення: 29.01.2025).

PROSPECTS OF USING INFORMATION SYSTEMS FOR IMPROVING THE SITUATION AWARENESS OF MILITARY ADMINISTRATION BODIES

PARASHCHUK Lidiia, PhD, associate professor, Hetman Petro Sahaidachny National Army Academy, Lviv, Ukraine, https://orcid.org/0000-0002-4049-2033

PARASHCHUK Serhiy, National Defence University of Ukraine, Kyiv, Ukraine, https://orcid.org/0009-0000-2830-7109

Formulation of the problem in general. *In today's rapid development of information technologies and digitalization of military command, there is a need to ensure a high level of situational awareness. Implementing information and communication systems allows for the rapid analysis of large volumes of data, increasing decision-making efficiency and reducing risks on the battlefield. However, integrating these technologies into the military environment is accompanied by several challenges, such as cybersecurity, interaction between systems, the influence of the human factor, and resource limitations. Accordingly, the problem of developing recommendations for the optimal use of information systems to increase the situational awareness of military command bodies arises.*

Purpose (objective) of the article. *The purpose of the article is to analyze the theoretical and practical aspects of the use of information systems in military command, assess their effectiveness, and develop recommendations for increasing the situational awareness of military command bodies.*

Research methods. *When writing the article, analytical research methods were used, particularly the analysis of scientific publications and research in information technology and military management. SWOT analysis was also used to assess the strengths and weaknesses, opportunities, and threats associated with implementing information systems. The methodological approach allows for identifying key problems in integrating systems into the military environment, identifying ways to improve them, and developing recommendations for increasing the effectiveness of their application.*

Analysis of recent research and publications. *Recent research in military information systems indicates significant progress in using automated solutions for situational awareness. In particular, scientific works analyze the impact of artificial intelligence, machine learning, and big data on military decision-making. The main challenges include cyber threats, technological obsolescence, and organizational barriers. The analysis confirms the need for further research in integrating information systems into military structures.*

Presenting the main material. *The article analyzes modern information and communication systems used in military management, particularly the Delta system. Its functional capabilities, advantages, and disadvantages are presented. A SWOT analysis of the system was conducted, which allowed identifying key success factors and potential risks. Recommendations for using information systems to increase situational awareness include introducing artificial intelligence, strengthening cybersecurity measures, and improving personnel training.*

Elements of scientific novelty. *The scientific novelty of the study lies in conducting a comprehensive analysis of the use of information systems in military management, determining their effectiveness, and developing practical*

recommendations for their improvement. Approaches to integrating artificial intelligence and cybersecurity technologies into military information systems are proposed.

Theoretical and practical significance of the article. *The study results are of great importance for the military-defense sphere, as they contribute to increasing situational awareness, improving coordination, and the efficiency of decision-making. The conclusions obtained can be used to develop new information systems, improve existing solutions, and develop standards for their implementation in military management.*

Conclusion and the perspectives of future research. *The article substantiates the feasibility of using information systems to increase situational awareness in military management. The analysis confirms the effectiveness of using such systems, particularly through integrating artificial intelligence and cybersecurity technologies. Further research can be aimed at developing autonomous systems, improving protection against cyberattacks, and integrating information systems into international military platforms.*

Keywords: *information systems, situational awareness, military management.*

References

1. Fay, A., (2020). Cybersecurity and Information Systems in Military Operations. *Journal of Military and Strategic Studies*. 22(3), 45-63. **2. Lavrenchuk, V. A.,** (2021). Analysis of integrating the latest technologies in the defense sphere: theoretical aspects and practical challenges. *Naukovi zapysky Nacionaljnogho universytetu oborony Ukrajiny.* 15(2), 78-90. **3. Popov, M., Zaitsev, O., Stefantsev, S.** (2025). Innovative approach to reducing cognitive biases in expert evaluation. *Social Development and Security*. 15(1). 171-179. DOI: 10.33445/sds.2025.15.1.16 **4. Havrylenko, A.,** (2024). The application of artificial intelligence technologies in military systems analysis. *Testing and certification.* 1(3). 40-44. DOI: 10.37701/ts.03.2024.6 **5. Nadibaidze, A., Bode, I., & Zhang, Q.,** (2024). *AI in Military Decision Support Systems: A Review of Developments and Debates.* Center for War Studies. **6. Kostenko, O. V.,** (2022). Analysis of national strategies for the development of artificial intelligence. *Informacija i pravo.* 2(41), 58-69. DOI: 10.37750/2616-6798.2022.2(41).270365. **7. Iosifov, Je. A.,** (2024). *Methods and means of ensuring safe recognition and parameterization of voice information processing results.* PhD. 125. Kyjivsjkyj stolychnyj universytet imeni Borysa Ghrinchenka. **8. Zaghorka, O., Korecjkyj, A., Zaghorka, I., Komolajeva, T.,** (2020). Support for decision-making during the situational management of an operation (battle): methodical support. *Vojenno-prykladni pytannja systemnogho analizu ta matematychnogho modeljuvannja*. 1(68), 98–109. DOI: /10.33099/2304-2745/2020-0/98-109. **9. Demydenko, M. A.,** (2016). *Decision support systems:* navch. Possible. Nac. ghirn. un-t. Dnipro. **10. Joint Intelligence, Surveillance, and Reconnaissance**. [online], (2024). *E-katalog.* Available at: https://www.nato.int/cps/en/natohq/topics_111830.htm [Accessed: 29 January 2025]. **11. Agents, satellites, drones - how Delta combines various data to help destroy the enemy** [online], (2022). *E-katalog.* Available at: https://texty.org.ua/articles/108967/ahentura-suputnyky-drony-yak-delta-poyednuye-rizni-dani-i-dopomahaye-nyshyty-voroha [Accessed: 29 January 2025]. **12. Mykolajchuk, R., Starynsjkyj, I., Mykolajchuk, V.** (2024). Analysis of technological aspects of implementing web scraping of static and dynamic sites. *Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony.* 3(51), 80-88. DOI: 10.33099/2311-7249/2024-51-3-80-88. **13. Delta for the Armed Forces: What is known about the newest management system of the Ukrainian army.** [online], (2023). *E-katalog.* Available at: https://www.bbc.com/ukrainian/features-64585182 [Accessed: 29 January 2025].

Рукопис надійшов до редакції *04.02.2025*
Рукопис прийнято до друку після рецензування *26.03.2025*
Дата публікації *30.04.2025*