

САМУСЕНКО ДАНИЛО ЮРІЙОВИЧ
Київський інститут Національної гвардії України

ОСОБЛИВОСТІ УКРАЇНСЬКИХ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, ПОБУДОВАНИХ ЗА СТАНДАРТАМИ НАТО

Одним з ключових компонентів ефективної системи управління в Силах безпеки та оборони України є Система підтримки прийняття рішень (СППР).

Система підтримки прийняття рішень – це комплекс інформаційних та аналітичних інструментів, які призначені для збору, обробки, аналізу та подання інформації, необхідної для прийняття найкращих рішень в умовах невизначеності, важливості та обмежень [1].

Системне впровадження стандартів НАТО в систему управління є головним інструментом модернізації Сил безпеки та оборони України, завдяки чому перевага на полі бою досягається завдяки кращій обізнаності, оперативності управління та високій професійній автономності командирів.

Стандарти НАТО – це інструмент синхронізації, який перетворює розрізнені національні армії на цілісну коаліційну силу. Вони встановлюють єдині правила гри, що дозволяють військовим із різних країн ефективно взаємодіяти, ігноруючи внутрішні відмінності у методах управління чи програмному забезпеченні.

Одним із головних аспектів впровадження кращих практик Альянсу в управління військами України є перехід до концепції Mission Command (децентралізоване управління). Цей підхід надає молодшим командирам право на ініціативу в межах загального задуму старшого начальника. У контексті виконання бойових завдань цей підхід забезпечує гнучкість і швидкість реакції на динамічну зміну обстановки, що є критично важливим у зіткненнях із переважаючими силами противника.

Можна виокремити такі основні вимоги до українських СППР на основі стандартів НАТО:

- забезпечення сумісності різних систем, зокрема, забезпечення здатності різних систем обмінюватися даними та ефективно працювати разом (стандарти STANAG);
- супроводження та оновлення програмного забезпечення шляхом управління системою на всіх етапах, від розробки до утилізації, з урахуванням тривалого використання;
- забезпечення інформаційної безпеки, а саме – захист даних за стандартами НАТО, що включає кіберзахист та управління доступом;
- створення єдиного інформаційного простору, що забезпечує реальний час та точність даних на у реальному часі на будь-якому етапі проведення бойової операції.

Впровадження цих вимог дозволяє створити єдину екосистему, інтегровану з партнерами НАТО, та підвищити ефективність управління військами.

В умовах ведення бойових дій в Україні набула особливого значення необхідність систем підтримки прийняття тактичного рівня, які дозволяють командирів як оперативної, так і тактичної ланки швидко приймати рішення. Дуже важливим елементом такої СППР є швидкість отримання інформації, бо отримання інформації з певною затримкою стає питанням виживання підрозділу та може коштувати життів та здоров'я особового складу.

На теперішній час в Україні розроблено та впроваджено такі системи підтримки прийняття рішень, як «ОКР Дзвін-АС», ПЗ «Кропива», спеціалізоване програмне забезпечення «Інтеграційна платформа DELTA» (далі – DELTA), «GIS Arta» тощо. Окремо розглянемо систему підтримки прийняття рівень DELTA.

Українська СППР DELTA – це екосистема військових продуктів ситуаційної обізнаності, які складають єдиний робочий простір, в якому підтримується стрімінг відео, є інструменти для планування операцій і розвідки, також розроблений спеціальний мобільний застосунок для роботи в офлайн режимі. Її використання стало основою сучасного підходу до бойового управління, значно підвищивши ефективність і швидкість прийняття рішень на всіх рівнях [2]. Як результат, значно підвищується точність вогневого ураження, покращується взаємодія між різномірними компонентами Сил безпеки та оборони та радикально скорочується час

прийняття рішення. Якісні характеристики СППР DELTA, кіберзахищеність, певна простота використання призвели до масштабування використання цієї системи на всіх рівнях управління та офіційному впровадженні ПЗ DELTA [3].

Слід відмітити, що впровадження спеціального ПЗ DELTA для застосування Силами безпеки та оборони України має на меті забезпечення оперативної сумісності з відповідними структурами держав - членів НАТО [3].

СППР DELTA розроблена з урахуванням стандартів НАТО (таких як ISTAR, C4ISR, Link 16, JChat тощо) і успішно проходить випробування на взаємосумісність, що дозволяє Україні та союзникам бачити спільну картину бою без додаткових перехідників [2].

Проте існують певні аспекти – як технічні, так і процедурні – де повна відповідність стандартам Альянсу або ще не досягнута, або обмежена внутрішніми чинниками. Проте, варто розуміти, що відповідність стандартам НАТО – це не разове отримання сертифіката, а безперервний і складний процес. Він поєднує такі заходи, як вибір технічних профілів та налаштування інтерфейсів, атестацію безпеки та протоколів сумісності, постійну перевірку систем на міжнародних навчаннях.

Отже, на теперішній час системи підтримки прийняття рішень НАТО є стандартизованими та повністю інтегрованими мережами сервісів, тоді як українська СППР перебуває на етапі активної трансформації, поєднуючи передовий бойовий досвід із поступовим переходом на технічні та процедурні платформи Альянсу. Тому для досяжності сумісності українських систем підтримки прийняття рішень є необхідність в створенні певної «мапи досягнення відповідності стандартам НАТО».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Система підтримки прийняття рішень: переваги для ЗСУ / URL: <https://softline.org.ua/news/sistema-pidtrimki-prijnatta-risen-perevagi-dla-zsu.html> (дата звернення: 05.03.2026).

2. Незалежна перевірка засвідчила: після масштабування DELTA зберегла відповідність всім стандартам кібербезпеки / URL: <https://armyinform.com.ua/2026/03/09/nezalezhna-perevirka-zasvidchyla-pislya-masshtabuvannya-delta-zberegla-vidpovidnist-vsime-standartam-kiberbezpeky> (дата звернення: 20.03.2026).

3. Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану. Постанова Кабінету Міністрів України від 4 лютого 2023 р. № 139. URL: <https://zakon.rada.gov.ua/laws/show/139-2023-%D0%BF#Text> (дата звернення: 25.02.2026).

САПУН ВІКТОРІЯ ОЛЕКСАНДРІВНА

курсант навчально-наукового інституту
поліцейської діяльності Національної академії
внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІЙСЬКОВОСЛУЖБОВЦЯ В СОЦМЕРЕЖАХ: ЯК ПРОСТЕ ФОТО МОЖЕ СТАТИ ПРИЧИНОЮ ОБСТРІЛУ (ЦИФРОВА ГІГІЄНА).

У сучасних умовах соціальні мережі перетворилися на наріжний камінь розвідки на основі відкритих джерел відомої, як OSINT. Завдяки величезним обсягам даних у реальному часі такі платформи, як Twitter, Facebook та Instagram, стають для ворога безцінним джерелом інформації. Кожне фото, яке зроблене на місці подій та опубліковане у соцмережі надає противнику безпосередні свідчення, що дозволяє йому не лише відстежувати хронологію подій, а й оперативно приймати рішення в кризових ситуаціях. Також, це дає змогу противнику аналізувати ситуацію на місці вчинення події та розуміти масштаб події, яка була завдана шкода. Ця оперативність є ключовою для термінового збору інформації, яка не