прийняття рішення. Якісні характеристики СППР DELTA, кіберзахищеність, певна простота використання призвели до масштабування використання цієї системи на всіх рівня управління та офіційному впроваджені 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-vsim-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

потребують певних зламів сайтів, телеграм каналів чи інших джерел інформації, які перебувають у закритому доступі або мають певний гриф секретності [1].

Опубліковане під час війни «невинне» фото в соцмережах – це потужний інструмент, здатний призвести до загибелі особового складу та знищення техніки. Також завдання шкоди інфраструктурі, навчальним закладам з специфічними умовами навчання і саме головне загибель невинних людей. Це все відбувається тому, що населення мало обізнане в технологіях і на , що здатні їхні телефони. Смартфони автоматично записують GPS-координати в метадані файлів, що дає ворогу точну точку для удару. Публікуючи або роблячи репост, як ми думаємо «невинного» фото ми ворогу допомагаємо оперативно збирати інформацію. Навіть без геолокації ворожі аналітики здатні ідентифікувати місцевість за характерними деревами, лініями електропередач або унікальними географічними об'єктами на фоні. Більше того, відблиски в дзеркалах чи окулярах, специфічний камуфляж та оприлюднення фото в режимі «тут і зараз» дозволяють противнику коригувати вогонь артилерії протягом лічених хвилин [2].

Окрему загрозу становить використання ворогом технологій розпізнавання обличчя для ідентифікації військовослужбовців та створення баз даних для подальшого тиску чи репресій. У зоні бойових дій смартфон фактично перетворюється на радіомаяк. Навіть, якщо телефон просто ввімкнений він випромінює сигнали, які пеленгуються засобами РЕБ противника. У разі втрати пристрою або потрапляння в полон, ворог отримує доступ до особистих повідомлень, контактів та фотографій близьких, що ставить під загрозу безпеку не лише бійця, а й усієї його родини та побратимів [3,4].

Цифрова гігієна – це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий пароль на всіх акаунтах, застосовувати двофакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення застосунків. Цифрова гігієна сьогодні є критично важлива для збереження життя та здоров'я наших бійців і мирного населення. Вона передбачає використання складних унікальних паролів, обов’язкову двофакторну автентифікацію та регулярне оновлення програм для закриття вразливостей. Військовим необхідно дотримуватися суворої дисципліни: встановлювати додатки лише з офіційних магазинів, уникати публічних мереж Wi-Fi та критично аналізувати будь-яку інформацію в мережі. Важливо регулярно створювати резервні копії важливих файлів та робити перерви у використанні гаджетів, щоб уникнути інформаційного перевантаження [5].

Нам варто усвідомити, що смартфон у кишені – це не просто гаджет, а потенційна ціль для ворожої ракети. Успішна цифрова гігієна вимагає не лише технічних налаштувань, а й повної зміни мислення. Кожне селфі чи пост із фронту мають проходити через фільтр безпеки: якщо інформація може допомогти ворогу бодай на один відсоток, вона не повинна потрапити в мережу. Наша приватність і дисциплінованість у цифровому просторі — це броня, яка захищає життя всього підрозділу, тому безпека кожного бійця починається з вимкненої геолокації та критичного ставлення до кожної опублікованої деталі. Фотографуй для історії, але публікуй після перемоги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке OSINT-аналіз? URL: *https://defensetechforukraine.org/ua/volunteer/what-is-osint-analysis/*

2. Як працює OSINT-розвідка та чому небезпечно публікувати інформацію в інтернеті URL: *https://fakty.com.ua/ua/ukraine/suspilstvo/20220429-yak-praczyuye-osint-rozvidka-ta-chomu-nebezpechno-publikuvaty-informacziyu-v-internet/amp/*

3. Чи може фото військового в соцмережах бути використано ворогом, або Що таке OSINT-розвідка URL : *https://armyinform.com.ua/2021/08/06/chy-mozhe-foto-vijskovogo-v-soczmerezhah-buty-vykorystano-vorogom-abo-shho-take-osint-rozvidka/*

4. Як смартфон може стати загрозою на фронті: Сухопутні війська ЗСУ нагадують про правила кібергігієни URL : *https://armyinform.com.ua/2025/02/11/yak-smartfon-mozhe-staty-zagrozoyu-na-fronti-suhoputni-vijska-zsu-nagaduyut-pro-pravyla-kibergigiyeny/*

5. Міністерство цифрової трансформації України URL : *https://thedigital.gov.ua/news/how-tos/tsifrova-gigiena-yakikh-pravil-varto-dotrimuvatisya-v-interneti.*