УДК 681.324

Соболенко С.О., к.т.н., доцент,
Дубина О.Ф., к.т.н., доцент,
Заєць Ю.О., здобувач
Житомирський військовий інститут імені С. П. Корольова
Пивовар О.П., ад'юнкт
Національний університет оборони України

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ КАНАЛІВ ЗВ'ЯЗКУ В ПІДРОЗДІЛАХ SHORAD

Досвід ведення бойових дій в ході широкомасштабного вторгнення рф показав важливість засобів захисту об’єктів від ударів противника з повітря (БПЛА, ракети, КАБи і т.д).

Short Range Air Defense (SHORAD) – це комплекс протиповітряної оборони, призначений для захисту сухопутних військ та об'єктів від повітряних загроз на малих висотах і дальностях. Вони забезпечують безпосереднє прикриття об’єктів, часто будучи мобільними.

Існуючі канали передачі даних в підрозділах SHORAD будуються на сучасних мережевих технологіях із використанням технології захисту інформації (*міжмережеві екрани* (Firewall), *системи виявлення втручань* (Intrusion Detection System), *засоби створення віртуальних приватних мереж* (Virtual Private Network). Цей процес, як правило передбачає додатково виконання значної кількості операцій, в тому числі шифрування, що збільшує сумарний час передачі інформації $\tau_{\Sigma \text{пі}}(t)$. Окрім сталої складової цього часу $\tau_{\Sigma \text{пі}}$, що враховує розповсюдження сигналу по каналам зв'язку, існує змінна складова, яка не піддається точному прогнозуванню, вона враховує пропуски і затримки в роботі цифрової мережі (Jitter) $\tau_{Jet}(t)$ (1):

$$\tau_{\Sigma \text{пі}}(t) = \tau_{\Sigma \text{пі}} + \tau_{\text{J}et}(t). \qquad (1)$$

Час передачі інформації є критично важливим для підрозділів, які виконують завдання щодо виявлення та знищення цілі у реальному часі. Повітряна ціль рухається із швидкістю від сотні до тисяч км/г і чим більше час на передавання інформації, тим більше похибка точності наведення. Методами зменшення часу передачі інформації мають бути, в першу чергу, організаційні заходи, які забезпечать таку побудову мережі, що істотно не збільшуватиме час проходження команд управління.

Класичний підхід до формування захищених мереж зв'язку, прагнення впорядкувати та централізувати інформаційні потоки, зашифрувати, убезпечити тощо призводять до зниження ефективності роботи підрозділів типу SHORAD. Це призводить до певного ряду проблем, пов'язаних із критичною залежністю від якості каналів зв'язку на всьому далеко не близькому шляху до серверів VPN і в зворотному напрямку, якості роботи сервісів VPN тощо.

Тому, засоби кожного тактичного підрозділу ППО з АСУ повинні входити в склад своєї локальної мережі, яка навіть у випадку виходу із ладу глобальної мережі, повинна залишитись функціональною. Система зв'язку повинна бути децентралізованою, само відновлюваною з багатоланковою ретрансляцією з резервуванням фізичних каналів.

Таким вимогам відповідає технологія Mobile Ad hoc Network (MANET). Вона складається з мобільних пристроїв, які самостійно встановлюють з'єднання між собою, передаючи дані один через одного (багато-стрибковий режим), що робить її стійкою та динамічною. Тому поєднання всіх засобів в підрозділі пропонується на основі розгортання автономної високошвидкісної радіомережі шляхом використання комунікаційних засобів Silvus [1], MPU5 [2, 3] або їх аналогів. Практичне випробування таких систем показало їх ефективність в умовах впливу РЕБ та спроможність забезпечити передавання даних в межах підрозділу без затримок інформації, які істотно впливають на точність наведення.

Список використаних джерел:

1. Silvus Technologies : офіційний сайт. URL: https://www.silvustechnologies.com (дата звернення: 12.03.2026).

2. Сайт оборонних технологій та мережевих рішень (Persistent Systems, LLC): Persistent Systems : офіційний сайт. URL: https://persistentsystems.com/ (дата звернення: 12.03.2026).

3. Радіо MPU5: протестовано Rakkasan. Army.mil : веб-сайт. URL: https://www.army.mil/article/222056/mpu5_radio_rakkasan_tested (дата звернення 15.03.2026).