

**НАЦІОНАЛЬНА АКАДЕМІЯ
НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ**

**Навчально-науковий інститут
забезпечення державної безпеки**

**Актуальні проблеми діяльності складових
сектору безпеки і оборони України**

**ІІІ ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ



*08 жовтня 2026 року
м. Золочів*

Актуальні проблеми діяльності складових сектору безпеки і оборони України : тези III Всеукраїнської науково-практичної конференції (08 жовтня 2026 року). Харків: Вид-во НАНГУ, 2026. 901 с.

Видання містить тези доповідей III Всеукраїнської науково-практичної конференції «Актуальні проблеми діяльності складових сектору безпеки і оборони України», яка відбулась 08 жовтня 2026 року. Організатор конференції – Навчально-науковий інститут забезпечення державної безпеки Національної академії Національної гвардії України.

Палевич С.В. ШЛЯХИ ПІДВИЩЕННЯ ЕМОЦІЙНОЇ СТІЙКОСТІ В ПРОЦЕСІ УДОСКОНАЛЕННЯ ФІЗИЧНОЇ ПІДГОТОВКИ КУРСАНТІВ (СТУДЕНТІВ) СЛУЖБИ БЕЗПЕКИ УКРАЇНИ	575
Панасюк В.В., Сахон О.О., Феденко А.В. СТВОРЕННЯ УГРУПУВАНЬ НГУ ЯК НОВИЙ ЕТАП РОЗВИТКУ СПРОМОЖНОСТЕЙ СИЛ ОБОРОНИ В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ	576
Паращук Д.Л., Кузьменко Р.В. ЄДИНИЙ ПІДХІД ДО ОРГАНІЗАЦІЇ ВСТАНОВЛЕННЯ ДОДАТКОВОГО ЗАХИСТУ НА ВІЙСЬКОВУ АВТОМОБІЛЬНУ ТЕХНІКУ	579
Pasichnyk A.V., Protasiuk V.R. CHALLENGES OF ENSURING COMMUNICATIONS AND INFORMATION MANAGEMENT BETWEEN UNITS OF THE DEFENSE FORCES OF UKRAINE AND COMPREHENSIVE SOLUTIONS	580
Pasichnyk A.V., Protasiuk V.R. PECULIARITIES AND CHALLENGES OF DEPLOYING PRIVATE LTE NETWORKS WITHIN THE FIELD COMMUNICATIONS STRUCTURE OF THE SECURITY AND DEFENSE SECTOR UNITS	582
Пащетник О.Д., Петлюк І.В. ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС ПЛАНУВАННЯ ВОГНЕВОГО УРАЖЕННЯ ПРОТИВНИКА	583
Перемибіда Д.О., Перемибіда І.В. ШЛЯХИ ВДОСКОНАЛЕННЯ ТАКТИКИ ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ І БОЙОВОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ	587
Перкатий Р.М., Мазур І.М. ВОГНЕВА ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ У СКЛАДІ ГРУПИ ПРИКРИТТЯ ПІД ЧАС СПІЛЬНИХ ДІЙ ІЗ ПІДРОЗДІЛАМИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ	588
Перкатий Р.М., Парчевська О.О. ВПЛИВ РІВНЯ ФІЗИЧНОЇ ПІДГОТОВЛЕНOSTІ НА ЕФЕКТИВНІСТЬ ВИКОНАННЯ ВПРАВ З ВОНЕВОЇ ПІДГОТОВКИ	591
Перкатий Р.М., Тимчишин П.А. ВОГНЕВЕ ЗАБЕЗПЕЧЕННЯ ЕВАКУАЦІЇ УЧАСНИКІВ СЛІДЧОЇ ДІЇ З НЕБЕЗПЕЧНОЇ ДІЛЯНКИ МІСЦЕВОСТІ	593
Пилипенко В.М., Гулковський Н.М. ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОМУНІКАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ ЦИВІЛЬНОГО ЗАХИСТУ ШЛЯХОМ КОМПЛЕКСНОГО РЕЗЕРВУВАННЯ	596
Пилипенко В.М., Мєзєнцев С.Є. ПІДХІД ДО ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ ТАКТИЧНОГО РІВНЯ НА ОСНОВІ АВТОНОМНИХ КОНТЕЙНЕРИЗОВАНИХ ВУЗЛІВ	598
Піонтківський П.М., Дзюбчук Р.В. ПРОБЛЕМНІ ПИТАННЯ УНІФІКАЦІЇ ТЕРМІНОЛОГІЇ ТА КЛАСИФІКАЦІЇ БЕЗПЛОТНИХ НАЗЕМНИХ КОМПЛЕКСІВ (СИСТЕМ) СИЛ ОБОРОНИ УКРАЇНИ	600
Площик А.С., Бібік А.В. ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ	

визначити в короткій інструкції із зазначенням відповідальних осіб. Обсяг резервування доцільно визначати з урахуванням критичності конкретних видів зв'язку та допустимого часу їх недоступності.

Перевірка резерву повинна показати, скільки часу займає відновлення зв'язку, чи проходить контрольне повідомлення та чи залишаються доступними критичні інформаційні сервіси. Якщо необхідні функції не відновлюються в межах установленого допустимого часу, резерв не можна вважати готовим до використання.

Таким чином, стійкість комунікаційної системи залежить не від одного резервного пристрою, а від резервування всього критичного ланцюга – обладнання, каналів зв'язку та електроживлення. Запропонований підхід передбачає визначення критичних елементів і єдиних точок відмови, встановлення допустимого часу відновлення їх функцій, вибір відповідного виду резерву та регулярну перевірку його працездатності. Застосування такого підходу сприяє скороченню тривалості перерв у роботі комунікаційної інфраструктури у разі відмов її окремих елементів.

УДК 621.39:004.75

Пилипенко В.М., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, майор служби цивільного захисту, **Мезенцев С.Є.**, курсант навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності, рядовий служби цивільного захисту

ПІДХІД ДО ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ ТАКТИЧНОГО РІВНЯ НА ОСНОВІ АВТОНОМНИХ КОНТЕЙНЕРИЗОВАНИХ ВУЗЛІВ

Під час виконання завдань за призначенням підрозділи сектору безпеки і оборони України, зокрема Державної служби України з надзвичайних ситуацій, значною мірою залежать від стабільної роботи систем зв'язку та інформаційної інфраструктури. Пошкодження каналів зв'язку, перебої електроживлення та радіоелектронні перешкоди можуть суттєво ускладнювати роботу таких систем. Ефективне виконання завдань потребує безперервного збору, передавання, оброблення та використання оперативної інформації навіть за умов часткового або повного порушення зовнішніх каналів зв'язку. Основна проблема полягає в тому, що потреба у постійному обміні даними зберігається навіть тоді, коли доступ до магістральних каналів або центральних серверів порушений. Втрата зв'язку з централізованими центрами обробки даних може суттєво обмежити доступ польових пунктів управління до інформаційних сервісів, ускладнити диспетчеризацію та знизити оперативність управління підрозділами. Тому доцільно передбачити можливість локальної роботи критичних сервісів без постійного доступу до центральної інфраструктури.

Метою роботи є обґрунтування можливості використання автономних

контейнеризованих вузлів для підвищення стійкості систем зв'язку та інформатизації тактичного рівня.

У роботі розглянуто основні чинники, які впливають на стійкість систем зв'язку та інформатизації польових пунктів управління. Комплекси автоматизації залежать від доступності зовнішнього IP-з'єднання з відомчими центрами обробки даних. Централізована клієнт-серверна архітектура, у якій функціонування прикладних сервісів залежить від постійного доступу до віддалених серверів, може втрачати частину функціональних можливостей у разі порушення магістральних каналів зв'язку. У разі втрати зовнішнього IP-з'єднання доступ до окремих логістичних, облікових і диспетчерських сервісів може бути тимчасово обмежений.

Проблеми виникають і під час використання VoIP у нестабільних бездротових мережах. У разі недоступності стаціонарної комунікаційної інфраструктури для організації інформаційного обміну можуть застосовуватися тимчасові локальні Wi-Fi або комірчасті (mesh) мережі. За обмеженої пропускної здатності або наявності перешкод зростають затримка, джиттер і втрати пакетів. Це негативно впливає насамперед на якість передавання голосового трафіку RTP, спричиняючи переривання, затримки або спотворення мовлення. За відсутності налаштованих механізмів Quality of Service (QoS) зростання мережевого навантаження може суттєво погіршувати якість голосового зв'язку.

Окрема проблема пов'язана з відновленням інформаційних сервісів і баз даних після аварійного припинення роботи обладнання. За традиційного підходу сервер бази даних розгортається безпосередньо в операційній системі або в окремій віртуальній машині, що може збільшувати час повного відновлення сервісу після аварійного перезавантаження обладнання. У разі аварійного припинення електроживлення після повторного запуску СУБД виконує процедури відновлення узгодженого стану даних із використанням журналу транзакцій, що потребує додаткового часу до моменту повного відновлення доступності сервісу. У такій ситуації важливо, щоб частина сервісів могла продовжувати роботу локально, без постійного з'єднання з центральними ресурсами. Крім того, відмова одного сервісу не повинна призводити до зупинки роботи всього вузла. Саме тому доцільно розділити окремі сервіси та забезпечити можливість їх незалежного запуску і відновлення.

Одним зі способів зменшення залежності від зовнішньої інфраструктури є перенесення критичних сервісів на локальний обчислювальний вузол відповідно до принципів граничних обчислень (edge computing). Для практичної реалізації такого автономного вузла доцільно використовувати програмні платформи віртуалізації, що підтримують як віртуальні машини, так і контейнерні середовища. Для такої реалізації може використовуватися, наприклад, Proxmox Virtual Environment із підтримкою LXC-контейнерів.

У запропонованому варіанті сервер бази даних, веб-сервіси диспетчеризації та SIP-шлюз розміщуються в окремих LXC-контейнерах на базі

Ubuntu. Ізоляція контейнерів за допомогою механізмів ядра Linux дає змогу обмежити взаємний вплив окремих сервісів і підвищити керованість їх розгортання та відновлення. У цьому випадку немає потреби запускати окрему гостьову операційну систему для кожного сервісу, що спрощує їх запуск і зменшує використання ресурсів. Критичні прикладні сервіси можуть працювати з локальною базою даних автономного вузла, а після відновлення зовнішнього каналу зв'язку, за умови реалізації відповідних механізмів синхронізації, накопичені дані можуть передаватися до центральних інформаційних ресурсів.

Для голосового зв'язку доцільно налаштувати QoS із пріоритизацією RTP-трафіку за допомогою DSCP, що зменшує вплив перевантаження мережі на якість передавання голосу. Це особливо важливо, якщо через один канал одночасно передаються голосові повідомлення та інші дані. За великого навантаження голосовий трафік може втрачати якість, тому його пріоритетна обробка дає змогу зменшити вплив перевантаження мережі.

Таким чином, підвищення стійкості систем зв'язку та інформатизації в умовах порушення зовнішніх каналів зв'язку потребує зменшення залежності критичних сервісів від централізованої інфраструктури та забезпечення можливості їх локального автономного функціонування. Застосування автономних вузлів із контейнерною віртуалізацією LXC може скоротити час відновлення програмного середовища та забезпечити локальну доступність критичних інформаційних сервісів після аварійного перезавантаження обладнання. Локальна обробка даних із подальшою синхронізацією з центральними ресурсами та пріоритизація голосового трафіку зменшують залежність системи від стабільності зовнішньої транспортної мережі. Запропонований підхід доцільно надалі перевірити на практиці, зокрема оцінити час запуску і відновлення окремих сервісів, використання ресурсів автономного вузла та роботу голосового зв'язку за різного навантаження на мережу.

УДК 623.4:629.3

Піонтківський П.М., к.т.н., с.н.с., провідний науковий співробітник науково-дослідного відділу розвитку та застосування безпілотних систем науково-дослідного управління розвитку спеціальних систем та інновацій Житомирського військового інституту імені С. П. Корольова, підполковник, **Дзюбчук Р.В.**, к.т.н., с.н.с., професор кафедри бойового забезпечення та повсякденної діяльності факультету професійної військової освіти "Вишкіл Лідерів" Житомирського військового інституту імені С. П. Корольова, полковник

ПРОБЛЕМНІ ПИТАННЯ УНІФІКАЦІЇ ТЕРМІНОЛОГІЇ ТА КЛАСИФІКАЦІЇ БЕЗПІЛОТНИХ НАЗЕМНИХ КОМПЛЕКСІВ (СИСТЕМ) СИЛ ОБОРОНИ УКРАЇНИ