

**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
Перкати́й Р.М., Мазур І.М. ВОГНЕВА ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ У СКЛАДІ ГРУПИ ПРИКРИТТЯ ПІД ЧАС СПІЛЬНИХ ДІЙ ІЗ ПІДРОЗДІЛАМИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ	588
Перкати́й Р.М., Парчевська О.О. ВПЛИВ РІВНЯ ФІЗИЧНОЇ ПІДГОТОВЛЕНOSTІ НА ЕФЕКТИВНІСТЬ ВИКОНАННЯ ВПРАВ З ВОНЕВОЇ ПІДГОТОВКИ	591
Перкати́й 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	

або припинення, організовує фіксацію обстановки та повинен розуміти порядок безпечного виходу учасників із місця події. Тому під час підготовки слідчих, оперативних працівників і поліцейських, які забезпечують прикриття, мають відпрацьовуватися узгоджені алгоритми припинення слідчої дії, вибору маршруту виходу, збереження доказової інформації, надання невідкладної медичної допомоги та документування причин евакуації. За таких умов вогневе забезпечення евакуації включається в законну і керовану роботу поліції, де безпека учасників, збереження доказів і правомірність дій поліцейських оцінюються разом.

УДК 621.39

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

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОМУНІКАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ ЦИВІЛЬНОГО ЗАХИСТУ ШЛЯХОМ КОМПЛЕКСНОГО РЕЗЕРВУВАННЯ

Під час виконання завдань підрозділи цивільного захисту значною мірою залежать від надійної роботи систем зв'язку. Відмова мережевого обладнання, пошкодження каналів передавання даних або тривале знеструмлення можуть призвести до часткової чи повної втрати зв'язку та ускладнити оперативне управління підрозділами. Тому важливо передбачити резервування, яке дозволить скоротити перерви у зв'язку та швидко відновити роботу критичних елементів системи.

Метою роботи є визначення підходів до підвищення стійкості комунікаційних систем підрозділів цивільного захисту шляхом резервування обладнання, каналів передавання даних та джерел живлення. Основну увагу приділено рішенням, спрямованим на збереження критичних функцій зв'язку та скорочення часу їх відновлення в умовах відмов окремих елементів комунікаційної інфраструктури.

У роботі резервування розглядається за трьома основними напрямками: резервне обладнання, альтернативні канали передавання даних та автономне електроживлення. Самої наявності запасного обладнання недостатньо. Воно має бути справним, налаштованим і готовим до швидкого введення в роботу, а персонал повинен знати порядок перемикання.

Планування резервування варто починати з визначення елементів, відмова яких найбільше вплине на роботу системи. Для кожного критичного елемента слід визначити, скільки часу система може працювати без нього, і який резерв потрібно передбачити запасний пристрій, альтернативний канал

або незалежне живлення. Такий підхід дає змогу спрямувати ресурси на компоненти, резервування яких безпосередньо підвищує стійкість системи.

Одним із базових способів підвищити стійкість системи це передбачити резерв для критичного обладнання: маршрутизаторів, комутаторів, радіостанцій, блоків живлення та акумуляторів. Водночас резервувати лише один пристрій недостатньо. Якщо в схемі залишається спільний комутатор або єдине джерело живлення, саме вони можуть стати причиною втрати зв'язку.

Резервування може передбачати ручне підключення запасного пристрою після відмови основного або автоматичне перемикання на попередньо налаштоване обладнання. Можлива також паралельна робота кількох пристроїв із розподілом навантаження за умови збереження достатньої продуктивності системи після відмови одного з них. Вибір способу залежить від можливостей обладнання та допустимої тривалості перерви у зв'язку.

Для автоматичного резервування мережевого шлюзу можна використовувати VRRP (Virtual Router Redundancy Protocol). У такій схемі декілька маршрутизаторів працюють зі спільною віртуальною IP-адресою, а у разі відмови основного пристрою його роль переходить до резервного.

Окремо потрібно передбачити резервний канал зв'язку. Наприклад, основний дротовий канал може доповнюватися каналами 4G/LTE через резервні модеми з використанням спрямованих антен для стабілізації сигналу, бажано з використанням іншого оператора та, за можливості, фізично незалежної комунікаційної інфраструктури. Такий канал потрібно перевіряти саме там, де він буде використовуватися, оскільки його робота залежить від покриття, завантаження мережі та стану інфраструктури оператора.

Не менш важливим є резервне електроживлення. Джерела безперебійного живлення забезпечують роботу обладнання протягом обмеженого часу після зникнення електроенергії, а для триваліших відключень можуть застосовуватися генератори. Автономність системи залежить від ємності акумуляторів, їхнього технічного стану та енергоспоживання обладнання.

Резервне обладнання потрібно зберігати так, щоб його можна було швидко використати, водночас захистивши від вологи, перегріву та механічних пошкоджень. Для запасних радіостанцій необхідно перевіряти сумісність із діючою мережею, налаштування робочих каналів, стан антени й акумулятора. Водночас резервування має враховувати характер можливої відмови, оскільки заміна кінцевого пристрою не усуне несправності мережевої інфраструктури.

На практиці для рятувального підрозділу це може означати наявність запасної радіостанції, альтернативного доступу до службової мережі та резервного живлення для критичного обладнання. Персонал повинен знати місце розташування резервних засобів і порядок їх використання, а вибір резерву має відповідати призначенню конкретного виду зв'язку.

Резервне обладнання потрібно регулярно перевіряти: контролювати його справність, актуальність конфігурації та фактичний час перемикання. Під час планових тестувань доцільно імітувати відмову основного пристрою або каналу та контролювати відновлення зв'язку. Порядок дій персоналу необхідно

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