InterConf
Scientific Publishing Center

ISSN 2709-4685

THE ISSUE CONTAINS:

Proceedings of the 13th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

Rome, Italy
19-20.06.2026

Scientific Collection
InterConf+

№ 70 (299)
June, 2026

OPEN ACCESS

ISSN 2709-4685

InterConf
Scientific Publishing Center

Scientific Collection «InterConf+»

№ 70(299)

June 2026

THE ISSUE CONTAINS:

Proceedings of the 13th International
Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

ROME, ITALY

June 19-20, 2026

ROME
2026

ICV (Index Copernicus Value) = 88.21 / 100

UDC 001.1

S 40 *Scientific Collection «InterConf+»*, 70(299): with the Proceedings of the 13th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (June 19-20, 2026; Rome, Italy) / comp. by LLC SPC «InterConf». Rome: Dana, 2026. 275 p.

ISSN 2709-4685
DOI 10.51582/interconf.19-20.06.2026

Please, cite as shown below:

1. Surname, N. & Surname, N. (2026). Title of an article. *Scientific Collection «InterConf+»*, 70(299), 21-27. https://doi.org/10.1080/interconf...

This issue of Scientific Collection «InterConf+» contains the materials of the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

Scientific Collection «InterConf+» and its content are indexed in:

Index Copernicus; Google Scholar; WorldCat; OUCI (*Open Ukrainian Citation Index*); CrossRef; Semantic Scholar; Mendeley; Scilit; OpenAIRE (*pan-European research information system*), etc.

TABLE OF CONTENTS

MEDICINE AND PHARMACY

CHEMISTRY AND MATERIALS SCIENCE

AGROTECHNOLOGIES AND AGRICULTURAL INDUSTRY

INFORMATION AND WEB TECHNOLOGIES

MILITARY AFFAIRS AND NATIONAL SECURITY

Proceedings of the 13th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects»

(June 19-20, 2026). Rome, Italy

No 299

MILITARY AFFAIRS AND NATIONAL SECURITY

DOI 10.51582/interconf.19-20.06.2026.018

Аналіз комутаційнійних засобів мереж зв'язку Збройних Сил України

Коцюба Василь Петрович[1]

[1] кандидат технічних наук, доцент, доцент кафедри інформаційних систем; *Харківський національний економічний університет імені Семена Кузнеця;* Україна

Анотація.
Представлено результати аналізу кінцевих пристроїв телекомунікаційних мереж та засобів криптографічного захисту інформації ЗС України.

Ключові слова:
електронна комунікаційна мережа
телекомунікаційне обладнання

MILITARY AFFAIRS AND NATIONAL SECURITY

Електронна комунікаційна мережа (ЕКМ) ЗС України – комплекс взаємопов'язаних технічних засобів, програмного забезпечення та мережевої інфраструктури, які призначені для забезпечення електронних інформаційних послуг (сервісів), а також для збору, обробки, зберігання та передачі інформації по каналах зв'язку.

Електронна комунікаційна послуга – процес прийому та передачі інформації через електронні інфокомунікаційні мережі за допомогою телекомунікаційного обладнання та засобів зв'язку [1].

Електронна комунікація (телекомунікація, електрозв'язок) – передавання та приймання інформації (голос, дані, відео тощо) у вигляді електромагнітних сигналів за допомогою апаратних, програмно-апаратних та технічних засобів зв'язку. Засоби зв'язку поділяються на засоби електронних комунікацій, рухомі засоби, фельд'єгерсько-поштовий зв'язок та сигнальні засоби [2].

Засоби електронних комунікацій – технічні пристрої, призначені для перетворення повідомлень, що передаються, в сигнали електрозв'язку, їх оброблення, зберігання та обміну цими повідомленнями з використанням цифрових каналів зв'язку, кабельних, супутникових, радіорелейних й тропосферних ліній зв'язку та кінцевих мережевих пристроїв.

Комунікаційні засоби призначені для утворення ліній електронних комунікацій, комутації ліній, мереж зв'язку, повідомлень, пакетів, блоків комутації різноманітного призначення. До засобів комутації належать ручні та автоматичні телефонні станції (АТС), цифрові автоматичні комутаційні системи, комутатори, маршрутизатори, пристрої передачі мови поверх потоків даних, що працюють за IP-протоколами.

Військовий зв'язок – процес обміну повідомленнями в системах управління військами (силами). Зв'язок є поєднанням електронних комунікацій та інформаційних систем. Зв'язок організовується штабами та забезпечується військовими частинами (підрозділами) зв'язку [3, 4].

Проводовий (дротовий) зв'язок здійснюється за рахунок розповсюдження сигналів по кабелях з металевими або волоконно-оптичними жилами. Засоби проводового зв'язку є однією зі основних складових системи зв'язку та ІС ЗС України,

MILITARY AFFAIRS AND NATIONAL SECURITY

яка є матеріальною основою системи керування ЗС України.

Радіозв'язок – це різновид зв'язку, який здійснюється завдяки передачі електричних сигналів (інформації) за допомогою електромагнітних хвиль (радіохвиль) з використанням технічних засобів – радіостанцій. До засобів радіозв'язку також належать радіопередавачі, радіоприймачі і відповідні антени (антенні системи). Радіозв'язок є одним з основних родів електрозв'язку, що забезпечує безперервне управління військами і єдиним родом зв'язку, здатним забезпечити управління літальними апаратами в повітрі.

Сформувалася та стала невід'ємною частиною системи зв'язку – інформаційна систем (ІС) а, яка виконує такі функції: збирання, передавання, перетворення, накопичення, зберігання, оброблення та використання інформації. Інформаційна система – це складова комунікаційної системи, а комунікація – передача символів, значень знаків, літер шляхом пересилання сигналів [3, 5].

Розвиток систем зв'язку та ІС, впровадження технологій gigabit passive optical network (GPON), next generation network (NGN), збільшення кількості мультисервісних послуг, застосування програмно-орієнтованої архітектури побудови мереж, широке застосування інтерактивного телебачення (IP-TV) та відеоконференцзв'язку, об'єднання традиційних телекомунікаційних послуг (телефон, передача даних, Інтернет) та нових медіа (відео, інтерактивні сервіси) в одній інфраструктурі стало підставою до утворення їх загальної форми та назви – інфокомунікаційні технології.

Інформаційна система (англ. information system) – це сукупність обладнання, методів, процедур і персоналу, організованого для виконання функцій обробки інформації. Згідно з ДСТУ 2392-94: Інформаційна система – комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації.

Система зв'язку та інформаційні системи (англ. communication and information systems, CIS) є узагальнюючим терміном, що об'єднує сукупність технічних, апаратних і програмних засобів, в поєднанні з організаційними заходами, які спрямовані на впорядкування діяльності персоналу та процесів експлуатації й призначені для формування, передавання, приймання, обробки, зберігання та захисту

MILITARY AFFAIRS AND NATIONAL SECURITY

інформації з метою забезпечення управління й взаємодії між користувачами [4].

Розгортання інформаційних систем здійснюється на інформаційно-комунікаційних вузлах (ІКВ). Доступ до ресурсів ІС здійснюється з автоматизованих робочих місць (АРМ) відповідних службових осіб. Розгортання та обслуговування АРМ та локальних мереж покладається на підрозділи зв'язку та інформаційних систем (автоматизації) ІКВ.

Розподіл потоків повідомлень (цифрових потоків, телефонних каналів) здійснюється на ІТВ і станціях зв'язку різного рівня за допомогою керуючих сигналів відповідних систем кросування і комутації (комутаційних центрів). При цьому вирішуються дві основні мети: доставка кожного повідомлення (IP-пакету) за визначеною адресою і підвищення ефективності використання каналів зв'язку. У зв'язку з цим, на ІТВ (вузлах зв'язку) застосовується відповідне устаткування, що дозволяє автоматично або вручну передавати в потрібному напрямку повідомлення, що поступають на комутаційний вузол [11].

Маршрутизатор (англ. *router*) – програмно-апаратний пристрій, що використовується для поєднання двох або більше локальних мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня між різними сегментами мережі.

Маршрутизатори можуть виконувати додаткові функції, зокрема: захист локальної мережі від зовнішніх загроз; обмеження доступу користувачів локальної мережі до ресурсів зовнішніх мереж (Інтернету); роздача IP-адрес (DHCP-сервер); шифрування трафіку тощо. Приклади маршрутизаторів виробництва компаній Cisco та MikroTik наведено на рис. 1.

Рисунок 1
Маршрутизатори виробництва компаній Cisco та MikroTik

MILITARY AFFAIRS AND NATIONAL SECURITY

Маршрутизатори працюють на 3-му (мережевому) рівні моделі OSI. Для того, щоб надіслати пакети в потрібному напрямку, маршрутизатор використовує таблицю маршрутизації, яка зберігається у його пам'яті. Таблиця маршрутизації наповнюється вручну (статична маршрутизація) та/або за допомогою роботи протоколів динамічної маршрутизації.

Комутатор (англ. *switch*) – апаратний пристрій, що призначений для з'єднання кінцевих пристроїв (комп'ютерів, VoIP-шлюзів тощо) в межах однієї локальної мережі. Для пересилки пакетів від одного вузла мережі до іншого комутатори використовують таблицю комутації (таблицю MAC-адрес), що дозволяє пересилати дані лише до вузла-призначення. Комутатор працює на 2-му (канальному) рівні моделі OSI. Приклад комутаторів виробництва компанії Cisco наведено на рис. 2.

Рисунок 2
Комутатори виробництва компанії Cisco

Телекомунікаційний комплект тип 1 (ТК-1) – польовий маршрутизатор тактичної ланки управління з підтримкою VoIP телефонії, що призначений для забезпечення передачі даних в телекомунікаційній мережі ЗС України та відкритого телефонного зв'язку. Він забезпечує організацію однієї лінії прив'язки до транспортної телекомунікаційної мережі ЗС України, підключення 4-х пристроїв, наприклад персонального комп'ютера, до локальної мережі та 4-х аналогових телефонних апаратів [8].

До складу обладнання ТК-1 входять: маршрутизатор Cisco RV130, комутатор Cisco SF100D, голосовий шлюз Grandstream HT704 та мікрокомп'ютер Raspberry Pi. Зовнішній вигляд телекомунікаційного комплекту ТК-1 наведено на рис. 3.

MILITARY AFFAIRS AND NATIONAL SECURITY

Рисунок 3
Телекомунікаційний комплект ТК-1

Батальйонний телекомунікаційний комплект тип 2 (ТК-2) – призначений для забезпечення службових осіб ПУ відкритим телефонним зв'язком та відкритої передачі даних, а також надання телекомунікаційного ресурсу мережам спеціального зв'язку. Зовнішній вигляд телекомунікаційного комплекту ТК-2 наведено на рис. 4.

Рисунок 4
Телекомунікаційний комплект ТК-2

ТК-2 забезпечує організацію не менше двох ліній прив'язки до телекомунікаційної мережі ЗС України, підключення 6-ти пристроїв до локальної мережі та 20-ти аналогових телефонних апаратів. До складу обладнання ТК-2 входять: маршрутизатор Cisco C891, VoIP-шлюз Grandstream HandyTone 704 на 4 FXS порти; VoIP-шлюз Grandstream GXW4216 на 16 FXS портів та мікрокомп'ютер Intel NUC [2, 8].

Центральний телекомунікаційний комплект тип 3 (ТК-3) – призначений для забезпечення службових осіб ПУ тактичної, оперативної та стратегічної ланок управління послугами відкритого телефонного зв'язку та відкритої передачі даних, а також надання телекомунікаційного ресурсу мережам

MILITARY AFFAIRS AND NATIONAL SECURITY

спеціального зв'язку. ТК-3 забезпечує організацію не менше двох ліній прив'язки до телекомунікаційної мережі ЗС України, однієї DSL-лінії для передачі Ethernet-трафіку по мідним кабелям, підключення до 28-и пристроїв до локальної мережі та 20-ти аналогових телефонних апаратів.

До складу обладнання ТК-3 входять: маршрутизатор Cisco C891, комутатор Cisco 2960-X, G.SHDSL-модем, VoIP-шлюз Grandstream HandyTone 704 на 4 FXS порти, VoIP-шлюз Grandstream GXW4216 на 16 FXS портів та мікрокомп'ютер Intel NUC. Зовнішній вигляд телекомунікаційного комплекту ТК-3 наведено на рис. 5.

Рисунок 5
Телекомунікаційний комплект ТК-3

Телекомунікаційний комплект розширення тип 4 (ТК-4) призначений для розширення можливостей ТК-1, ТК-2 та ТК-3 при організації відкритої локально-обчислювальної мережі, відкритої абонентської телефонної мережі, локально-обчислювальної мережі ЗСУ002 та абонентської телефонної мережі ЗСУ002. ТК-4 не використовується у якості окремого пристрою. ТК-4 забезпечує підключення 24-х пристроїв до локальної мережі та 16-ти аналогових телефонних апаратів. До складу обладнання ТК-4 входять: комутатор Cisco SF220-24 та VoIP-шлюз Grandstream GXW4216 на 16 FXS портів.

Зовнішній вигляд ТК-4 наведено на рис. 6.

Рисунок 6
Телекомунікаційний комплект ТК-4

MILITARY AFFAIRS AND NATIONAL SECURITY

IP-АТС – автоматична телефонна станція, що працює на основі протоколу IP в системі VoIP-телефонії та призначена для встановлення, підтримання і завершення з'єднання через телекомунікаційні мережі та забезпечує обробку та передачу сигналізації за протоколами SIP або H.323 між телефонними пристроями користувачів та іншими телефонними станціями по різним каналам зв'язку. IP-АТС можуть бути програмні, тобто реалізовані на сервері або комп'ютері, (наприклад, Asterisk, 3CX тощо), або апаратні, які виготовлені у вигляді окремих пристроїв (наприклад, виробництва компаній Grandstream, Cisco, Panasonic та ін.). Приклади IP-АТС виробництва компанії Grandstream наведено на рис. 7.

Рисунок 7
IP-АТС виробництва компанії Grandstream

VoIP-шлюз (голосовий шлюз) – пристрій, що призначений для підключення аналогових телефонних апаратів або цифрових АТС та перетворення голосового трафіку в IP-пакети для його передачі по IP-мережам.

VoIP-шлюзи можуть мати один або декілька портів FXS та/або FXO. FXS-порти призначені для підключення аналогових телефонних апаратів по аналогових телефонних лініях. FXO-порти використовуються для підключення аналогових ліній від аналогових або цифрових АТС. VoIP-шлюз може мати вбудований маршрутизатор (наприклад, серія Grandstream HT8XX), який підтримує технології NAT, DHCP, QoS тощо. Приклад голосових шлюзів виробництва компанії Grandstream наведено на рис. 8.

Рисунок 8
VoIP-шлюзи виробництва компанії Grandstream

MILITARY AFFAIRS AND NATIONAL SECURITY

Цифрова автоматична телефонна станція (ЦАТС) – це сучасна система комутації, яка передає та обробляє телефонні сигнали у вигляді цифрового коду. Вона повністю замінила старі аналогові та координатні АТС. Додаткові функції:

– переадресація: переведення дзвінка на інший номер;

– визначення номера: відображення контактів (англ. caller ID);

– голосова пошта – запис повідомлень, якщо абонент зайнятий;

– конференцзв'язок – одночасна розмова трьох і більше людей;

– голосове меню (IVR): автоматичне розподілення дзвінків за допомогою тонального набору.

Різновиди цифрових АТС:

– залізо (англ. hardware): фізичні сервери, встановлені в офісі компанії;

– віртуальні/хмарні: АТС працює на серверах провайдера через Інтернет;

– програмні (англ. softswitch): спеціальний софт (наприклад Asterisk), встановлений на звичайний персональний комп'ютер.

Цифрова автоматична телефонна станція "Фарлеп-1500" призначена для побудови кінцевих, транзитних і кінцевих – транзитних станцій на міських, відомчих мережах зв'язку в тому числі і військового (спеціального) призначення. Станції системи Ф-1500 взаємодіють з усіма існуючими типами АТС як цифровими, так і аналоговими сигналами по з'єднувальним лініям з усіма стандартними типами сигналізації. Ємність абонентського модуля Ф-1500 складає 512 абонентських портів (абонентських ліній) [8].

Кінцеві пристрої телекомунікаційних мереж

Обмін інформації між абонентами мережі зв'язку здійснюється за допомогою кінцевих пристроїв, які забезпечують перетворення повідомлень, наприклад, телефонних, телеграфних, факсимільних, телекодових тощо до виду придатному до обробки та подальшої передачі по каналу зв'язку.

IP-телефон – пристрій, що забезпечує передачу телефонних голосових повідомлень через IP-мережу. IP-телефони підключаються безпосередньо до комутатора або маршрутизатора

MILITARY AFFAIRS AND NATIONAL SECURITY

за допомогою звитої пари або волоконно-оптичного кабелю. Для роботи в системі VoIP-телефонії IP-телефон повинен бути зареєстрований на IP-АТС.

IP-телефони можуть підтримувати велику кількість додаткових функцій, зокрема аудіоконференції, передавати текстові повідомлення, голосову пошту, виконувати переадресацію викликів, запис телефонних розмов тощо. Приклади IP-телефонів наведено на рис. 9.

Рисунок 9
IP-телефони виробництва компанії Grandstream

Основні характеристики IP-телефона:

– використовувані протоколи SIP, SCCP, H.323, MGCP;

– підтримка аудіокодеків: G.711, G.726, G.729 та ін.;

– інтерфейс 10/100 Мбіт/с, Fast Ethernet (або Wi-Fi) для підключення до IP-мережі, змінне програмне забезпечення;

– додатковий інтерфейс для підключення комп'ютера;

– можливість програмування кнопок для швидкого набору збереженого телефону і перевірки поточного стану лінії.

У багатьох IP-телефонах реалізована функція PoE (англ. Power over Ethernet), що дозволяє здійснювати електроживлення апарату без підключення до електричної мережі через стандартну звиту пару в мережі Ethernet.

Аналоговий телефонний апарат – пристрій, що забезпечує передачу телефонних голосових повідомлень в системі автоматичного телефонного зв'язку. Для роботи аналогових телефонів в системі VoIP-телефонії необхідно використовувати VoIP-шлюзи з FXS-портами (спеціальний порт для підключення аналогових телефонних апаратів з тональним викликом). Приклад аналогового телефонного апарату (ТА) наведено на рис. 10.

MILITARY AFFAIRS AND NATIONAL SECURITY

Рисунок 10
Аналоговий телефон виробництва компанії Panasonic

Додатковими функціями телефону можуть бути наявність дисплею з можливістю ведення телефонної книги; спікерфон (гучний зв'язок); програмовані кнопки; індикатор виклику (повідомлення) тощо.

Телефонний апарат польовий аналоговий ТА-01 призначений для забезпечення телефонного зв'язку в складі абонентських мереж автоматичних комутаційних систем, у тому числі мереж автоматичного телефонного зв'язку загального користування, ручних комутаційних станцій та дистанційно керувати радіостанціями. Зовнішній вигляд ТА-01 наведено на рис. 11.

Рисунок 11
Телефонний апарат ТА-01

ТА-01 підключається по 2-х дротових лініях зв'язку. Ефективна смуга частот мовного сигналу складає 0,3…3,4 кГц. Телефонний апарат забезпечує дальність зв'язку по легкому польовому кабелю П-274М до 20 км. ТА-01 має пам'ять на 10 номерів. Набір номерів здійснюється в імпульсному, тональному та індукторному режимах. Електроживлення

MILITARY AFFAIRS AND NATIONAL SECURITY

здійснюється від мережі 27 В, автономної батареї 4,5 В або ЦБ АТС.

Телефонний апарат може експлуатуватися в польових умовах, а також у складі стаціонарних або рухомих об'єктів.

Цифровий телефонний апарат (термінал) ЦТА-04 призначений для організації безпосереднього телефонного зв'язку та передачі даних у мережі з однотипним або аналогічним ТА, абонентського доступу до мереж автоматичного телефонного зв'язку, в тому числі до телефонної мережі загального користування, проводового доступу до мережі з цифровим інтерфейсом ISDN S/T та U за протоколом сигналізації DSS1 і ведення переговорів із застосування радіостанцій. Зовнішній вигляд ЦТА-04 наведено на рис. 11.

ЦТА-04 передбачає експлуатацію в польових умовах, а також встановлення та експлуатацію на стаціонарних та рухомих об'єктах. ТА дозволяє виконувати набір номера абонента за допомогою тастатури, набір попередньо заданого номера, повторний набір номера, виклик функцій додаткових видів обслуговування, які забезпечує цифрова автоматична комутаційна система.

Телефонний апарат забезпечує з'єднання підключеного периферійного обладнання до будь-яких абонентів у мережі автоматично або в ручному режимі. Як модуль доступу периферійного аналогового устаткування, телефонний апарат може бути підключений до різноманітного аналогового обладнання, яке використовується у мережі передачі даних. ЦТА-04 передає аналогові дані між аналоговим обладнанням і мережею. Режими роботи: цифровий телефон, периферійне цифрове обладнання, мережевий радіоконтролер, модуль доступу периферійного аналогового устаткування. Набір імпульсний, тональний, індукторний виклик. Ефективна смуга частот 0,3…3,4 кГц, пам'ять на 10 номерів, маса телефонного апарату не більше 3,5 кг. Електроживлення здійснюється від мережі 27 В, від автономної батареї 4,5 В або від цифрової автоматичної комутаційної системи.

Блок гучномовного зв'язку ГЛАС-А – пристрій, що використовується в якості кінцевого абонентського пристрою у складі універсального комплексу гучномовного зв'язку "ГЛАС" або у складі будь-якої іншої системи гучномовного зв'язку. Блок може працювати по 2-х або 4-х дротовим лініям в кінцевому

MILITARY AFFAIRS AND NATIONAL SECURITY

або циркулярному (до 30 блоків) режимі. Зовнішній вигляд блока ГЛАС-А наведено на рис. 12.

Рисунок 12
Блок гучномовного зв'язку ГЛАС-А

Блок гучномовного зв'язку ГЛАС-АТ – пристрій, що призначений для організації гучномовного зв'язку по 2/4-х дротовим лініям та каналам ТЧ (режим А), або сполучення з аналоговим VoIP-шлюзом для організації гучномовного зв'язку у мережі Ethernet, або з цифровою АТС для організації гучномовного зв'язку по телефонній мережі (режим АТ) [16]. Зовнішній вигляд блока ГЛАС-АТ наведено на рис. 13.

Рисунок 13
Блок гучномовного зв'язку ГЛАС-АТ

Абонентський термінал конференцзв'язку (АТКЗ) – пристрій, що призначений для організації гучномовного зв'язку по 2/4-х дротовим лініям або каналам ТЧ. Зовнішній вигляд блоку АТКЗ наведено на рис. 14.

Рисунок 14
Абонентський термінал конференцзв'язку

MILITARY AFFAIRS AND NATIONAL SECURITY

Абонентський термінал конференцзв'язку (АТКЗ-IP) – пристрій, що призначений для організації гучномовного зв'язку по IP-мережі. В АТКЗ-IP використовуються протоколи SIP та IAX2. Термінал може використовуватись в якості SIP-серверу для створення конференцій. Під'єднується до мережі за допомогою звитої пари або волоконно-оптичного кабелю. Зовнішній вигляд блоку АТКЗ-IP наведено на рис. 15.

Рисунок 15
Абонентський термінал конференцзв'язку АТКЗ-IP

Засоби криптографічного захисту інформації.

Безпека системи зв'язку – це стан захищеності системи, при якому унеможливлюється доступ сторонньої особи до інформації (виток інформації), що обробляється, її модифікація, викривлення, порушення режиму **функціонування** системи та виток відомостей про засоби і методи криптографічного захисту, які застосовуються в системі. Безпека системи зв'язку забезпечується шляхом проведення нормативно-правових, організаційних, інженерно-технічних заходів та криптографічних перетворень [8].

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення (засекречення або розсекречення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Криптографічний захист інформації в системах зв'язку реалізовано у вигляді апаратних, програмно-апаратних та програмних засобів.

На сьогодні в Збройних Силах України для побудови комплексних систем захисту інформації використовуються засоби криптографічного захисту серії "Лавина-Е" та серії "Пелена-Е" [11, 18].

MILITARY AFFAIRS AND NATIONAL SECURITY

Серія "Лавина-Е" призначена для криптографічного захисту трафіку IP-мереж високого рівня безпеки. Функціональність виробів серії "Лавина-Е" охоплює наступні складові:

1. Прохідне шифрування трафіку IP-мереж. Шифрування трафіку здійснюється на периметрі локальної мережі. Криптографічна обробка в режимі on-line забезпечує "прозору" роботу мережевих додатків обробки даних, IP-телефонії, відеоконференцзв'язку.

2. Віртуальні канали шифрованого зв'язку. Під час обміну шифрованою інформацією створюються віртуальні канали шифрованого зв'язку за схемою, яка задається адміністратором комплексу.

3. Резервування каналів. Для кожного напрямку зв'язку можуть бути визначені декілька віртуальних каналів з різними маршрутами, що забезпечує резервування каналів зв'язку.

4. Ключова система. Ключова система забезпечує централізоване підготування та розподілення ключових даних. Під час генерації ключових даних пристроєм О372-Е використовуються фізичні сенсори, що відповідають стандарту безпеки з обробки інформації FIPS 140-2.

5. Розподілення ключів здійснюється двома методами: передача мережею шифрованого зв'язку та/або на носіях ключових даних.

6. Апаратна реалізація криптомодуля. Функції криптографічного перетворення здійснюються спеціалізованими мікросхемами із дублюванням, що забезпечує високу пропускну здатність та надійність шифрування.

7. Балансування завантаження каналів. Віртуальні канали можуть об'єднуватися в групи, з метою балансування завантаження та збільшення пропускної здатності вузлів мережі.

8. Резервування обладнання. Обладнання може дублюватися з метою "гарячого" резервування та аґреґування пропускної здатності.

9. Моніторинг та керування. Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, за допомогою централізованої системи керування (ЦСК).

Програмне забезпечення ЦСК встановлюється на комп'ютері під керуванням операційної системи Windows та дозволяє керувати режимами роботи обладнання, змінювати параметри

MILITARY AFFAIRS AND NATIONAL SECURITY

конфігурації, переглядати статистичну інформацію, протоколювати та обробляти повідомлення про події в мережі шифрованого зв'язку.

Захист від несанкціонованого доступу до керування обладнанням забезпечується за допомогою двофакторної аутентифікації.

Серія "Лавина-Е" складається з комплексів криптографічного захисту "Лавина-Е", "Тритон-Е" та "Скат-Е" [23].

До складу комплексу криптографічного захисту "Лавина-Е" входять:

- шифратор О371-Е(РЕ);
- пристрій генерації ключових даних О372-Е;
- централізована система керування – ЦСК.

Шифратор О371-Е(РЕ) призначений для криптографічного захисту трафіку IP-мереж високого рівня безпеки (рис. 16).

Рисунок 16
Шифратор О371-Е

Шифратор використовується для захисту каналів проводового, супутникового, радіорелейного та стільникового (3G, 4G) зв'язку. Виготовляється у варіантах для використання на стаціонарних (О371-Е) та рухомих (О371-РЕ) об'єктах.

Пристрій генерації ключових даних О372-Е призначений для генерації, зберігання та розподілу ключових даних. Централізована система керування призначена для віддаленого керування мережею шифрованого зв'язку.

Шифратор з інтегрованим модулем комутації "Тритон-Е (О271-Е(РЕ))" призначений для криптографічного захисту трафіку IP-мереж високого рівня безпеки (рис. 17).

Використовується для захисту каналів проводового, супутникового, радіорелейного, тропосферного та стільникового (3G, 4G) зв'язку. Вбудований керований комутатор дозволяє підключати абонентське обладнання безпосередньо до шифратора

MILITARY AFFAIRS AND NATIONAL SECURITY

[18].

Виробляється у варіантах для використання на стаціонарних (О271-Е) та рухомих (О271-РЕ) об'єктах. Сумісний із шифраторами О371-Е(РЕ) та О171-Е.

Рисунок 17
Шифратор О271-Е

Шифратор з інтегрованим модулем перетворення мовної інформації "Скат-Е (О171-Е)" забезпечує криптографічний захист мовної інформації та трафіку IP-мереж високого рівня безпеки (рис. 18).

Рисунок 18
Шифратор О171-Е

Забезпечує можливість роботи з обладнанням проводового, супутникового, радіорелейного, стільникового (3G, 4G) та КХ/УКХ зв'язку. Вбудований модуль перетворення мовної інформації дозволяє підключити телефонну трубку або гарнітуру безпосередньо до шифратора [16].

Призначений для використання на стаціонарних та рухомих об'єктах. Сумісний із шифраторами О371-Е(РЕ) та О271-Е(РЕ).

Серія "Пелена-Е" призначена для криптографічного захисту трафіку IP-мереж середнього рівня безпеки. Ключова система забезпечує централізоване генерування та розподілення ключових даних. Під час генерації ключових даних пристроєм

MILITARY AFFAIRS AND NATIONAL SECURITY

В364-Е використовуються фізичні сенсори, що відповідають FIPS 140-2. Розподілення здійснюється двома методами: передача мережею шифрованого зв'язку та/або на носіях ключових даних.

Серія "Пелена-Е" складається з комплексів криптографічного захисту "Пелена-Е" та "Гном-Е" [23]. До складу комплексу криптографічного захисту інформації "Пелена-Е" входять:

- шифратор В371-Е;
- пристрій генерації ключових даних В364-Е;
- централізована система керування.

Шифратор В371-Е призначений для криптографічного захисту трафіку IP-мереж середнього рівня безпеки (рис. 19). Використовується для захисту каналів проводового, супутникового, радіорелейного та стільникового (4G, 5G) зв'язку. Виготовляється у варіантах для використання на стаціонарних об'єктах.

Рисунок 19
Шифратор В371-Е

Пристрій генерації ключових даних В364-Е призначений для генерації, зберігання та розподілу ключових даних.

Централізована система керування призначена для віддаленого керування мережею шифрованого зв'язку.

Шифратор з інтегрованим модулем комутації "Гном-Е (В271-Е(РЕ))" призначений для криптографічного захисту трафіку IP-мереж середнього рівня безпеки (рис. 20).

Рисунок 20
Шифратор В271-Е

MILITARY AFFAIRS AND NATIONAL SECURITY

Використовується для захисту каналів проводового, супутникового, радіорелейного та стільникового (3G, 4G) зв'язку. Виробляється у варіантах для використання на стаціонарних (В371-Е) та рухомих (В371-РЕ) об'єктах, наприклад в Р-142Н. Сумісний із шифраторами В371-Е. Пропускна здатність до 70 Мб/с. Режим роботи безперервний, цілодобовий.

Мережевий кабель "звита пара"

Кабель на основі кручених пар ("звита пара", англ. twisted pair) – вид мережевого кабелю з декількома парами (2 або 4) ізольованих провід-ників, скручених між собою в джгути (з визначеною кількістю витків на одиницю довжини для кожної пари) для зменшення взаємних наведень при передачі сигналу та покритих оболонкою полівінілхлориду [13].

Кабель "звита пара" поділяється на кілька категорій (англ. Cat – Category), які визначають його технічні характеристики, такі як швидкість передачі даних, частотний діапазон та пропускна здатність. Чим вища категорія, тим кращі параметри кабелю, й відповідно, складніша конструкція й більша вартість.

Основні категорії мережевого кабелю "звита пара":

– **Cat 5.** Найдешевший варіант використання мережевого кабелю, в першу чергу для побудови домашніх персональних мереж. Підтримує швидкість обміну даними до 100 Мбіт/с (Ethernet) з використання 2-х пар струмопровідних дротів. Частотна смуга пропускання 100 МГц;

– **Cat 5e,** де "е" означає "покращена". Використовується для домашніх та офісних (спеціальних) мереж. Підтримує швидкість передачі до 500 Мбіт/с (Fast Ethernet), при цьому задіяні 1 та 2 лінії (передача) 3 та 6 (прийом). Смуга пропускання 100 МГц;

– **Cat 6.** Забезпечує швидкість передачі даних до 1 Гбіт/с (Gigabit Ethernet) на відстані до 100 метрів, а на коротких відстанях (до 50 м) може передавати дані зі швидкістю до 2…3 Гбіт/с. Смуга пропускання 250 МГц. У кабелів категорії Cat 6 та вище для обміну даними використовуються усі 4 пари струмопровідних дротів. Відповідно 2 пари на "передачу" й 2 на "прийом";

– **Cat 6a,** де "а" – це англ. "augmented", означає "розширена". Покращена версія кабелю Cat 6. Підтримує швидкість обміну даними до 5 Гбіт/с (10 Gigabit Ethernet) на відстані до 100 м. Має частотну смугу 500 МГц;

MILITARY AFFAIRS AND NATIONAL SECURITY

– **Cat 7.** Підтримує швидкість передачі даних до 7 Гбіт/с. Смуга пропускання до 600 МГц. Застосовується для організації високо-швидкісних з'єднань та забезпечує високу якість передачі даних;

– **Cat 7a.** Підтримує швидкість передачі даних до 10 Гбіт/с. Частотний діапазон (смуга пропускання) становить до 1 000 МГц, Використовується для побудови високошвидкісних мереж доступу;

– **Cat 8.** Підтримує швидкість передачі даних до 20 Гбіт/с. Частотна смуга пропускання становить до 2 000 МГц. Найновіша та найшвидша категорія для серверних, дата-центрів тощо.

Для захисту від зовнішніх завад та від перехресних перешкод між парами дротів в кабелях "звита пара" застосовуються різні типи екранування. Екранування застосовується як до окремих кручених пар, які обертаються в алюмінієву фольгу, так й до кабелю в цілому у вигляді загального екрана з фольги або обплетення з мідного дроту.

Для позначення конструкції кабелю використовується комбінація з трьох букв: *U* – неекранований, *S* – металеве обплетення (тільки загальний екран), *F* – металізована стрічка (алюмінієва фольга). З цих букв формується абревіатура виду xx/xTP, що позначає тип загального екрана та тип екрана для окремих пар.

Типи конструкції екрана кабелю "звита пара" поділяються за типом екранування: неекрановані (U/UTP), з індивідуальним екраном для кожної пари (U/FTP), із загальним екраном (F/UTP, S/UTP) та з комбінованим екрануванням (F/FTP, S/FTP). Екрани можуть бути у вигляді фольги, дротяного обплетення або їх комбінації, що впливає на рівень захисту від зовнішніх завад та впливів.

Типи екранування:

– неекранований (U/UTP). Найпростіший і найпоширеніший тип кабелю, який не має жодного екранування;

– індивідуальний екран (U/FTP). Кожна окрема пара проводів має індивідуальне екранування у вигляді алюмінієвої фольги. Це забезпечує захист від перехресних перешкод між парами.

Загальний екран:

– F/UTP (або FTP). Стрічка з фольги обгортає весь пучок пар, але кожна пара індивідуально не екранована;

MILITARY AFFAIRS AND NATIONAL SECURITY

– S/UTP. Замість фольги використовується загальне обплетення з металевих дротів (сітка) для всього кабелю;

– SF/UTP. Комбінований варіант побудови. Загальний екран із алюмінієвої фольги в поєднанні з обплетенням з металевих дротів.

Індивідуальний та загальний екран:

– F/FTP. Кожна пара екранована фольгою, а також є загальний екран з фольги навколо всього пучка пар;

– S/FTP. Кожна пара екранована фольгою, а загальний екран представлений металевим обплетенням;

– SF/FTP. Комбінований тип, що включає індивідуальне екранування кожної пари та загальний екран з фольги й обплетення;

Дальність передачі даних по мережевому кабелю "звита пара" усіх категорій обмежується відстанню до 100 м.

Зовнішній вигляд основних типів та категорії мережевого кабелю "звита пара" наведені на рис. 21.

Кабель "звита пара" підключається до мережевих пристроїв за допомогою роз'єму типу 8P8C, які інколи називають конекторами RJ-45, що використовуються для підключення комп'ютерів, роутерів, комутаторів, відеокамер та іншого телекомунікаційного обладнання. Кабелі усіх категорій випускаються з мідними або біметалевими суцільними жилами [13, 20].

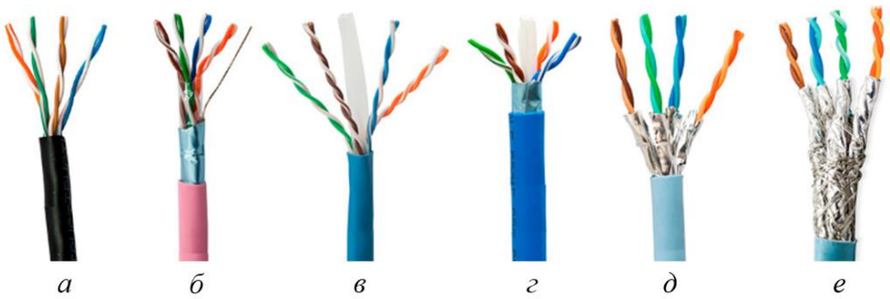

Рисунок 21

Категорії мережевого кабелю "звита пара":
***а* – Cat 5e (U/UTP); *б* – Cat 5e (F/UTP); *в* – Cat 6 (U/UTP);**
***г* – Cat 6 (F/UTP); *д* – Cat 6a (U/UTP); *е* – Cat 7a (S/FTP)**

Мережевий кабель "звита пара" з під'єднаним конектором 8P8C (RJ-45) представлений на рис. 22. Прозорий корпус

MILITARY AFFAIRS AND NATIONAL SECURITY

конектора забезпечує зручний візуальний контроль якості затискання провідників та правильної послідовності чергування кольорових провідників кабелю "звита пара" відповідної категорії (рис. 23).

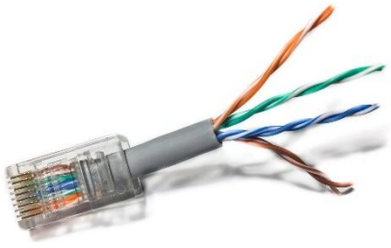

Рисунок 22
"Звита пара" з конектором 8P8C

Рисунок 23
Конектор 8P8C (RJ-45)

Конектор 8P8C дозволяє механічним способом (обтискання) під'єднувати встановленим порядком (8P) струмопровідних жил кабелю та забезпечувати надійний контакт (8C) з відповідними роз'ємами.

Конектор RJ-11 має чотири позиції й два контакти (4P2C) та використовується для підключення двожильних неекранованих телефонних кабелів Cat 1 або Cat 2 аналогового телефонного зв'язку.

Конектор RJ-12 має шість позицій, але може мати чотири або шість контактів (6P4C або 6P6C) й використовується для підключення чотирижильних неекранованих кабелів "звита пара" Cat 3 або Cat 4 та застосовується в телефонних й локальних комп'ютерних мережах з незначними навантаженнями. Максимальна частота, яка придатна для передачі даних по кабелю Cat 3(4), становить 4 МГц, а максимальна пропускна здатність може становити до 5 Мбіт/с.

Для під'єднання конекторів до кабелю типу "звита пара" необхідно дотримуватися використання певної послідовності мідних дротів, які в кабелі позначені різними кольорами відповідно стандарту TIA/EIA-568.

Використовуються два основні варіанти обтискання кабелю "звита пара": за стандартом T-568A (рис. 24) та T-568B (рис. 25).

MILITARY AFFAIRS AND NATIONAL SECURITY

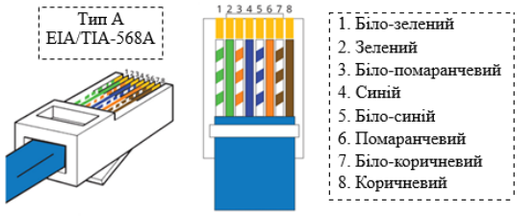

Рисунок 24
Обтискання мережевого кабелю Cat 5e (F/UTP) за стандартом EIA/TIA-568A

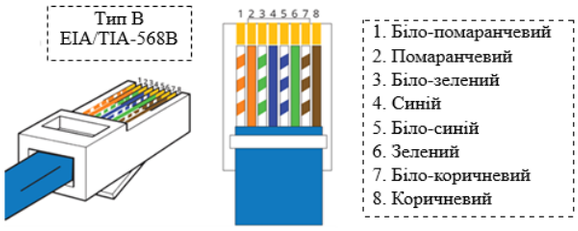

Рисунок 25
Обтискання мережевого кабелю Cat 5e (F/UTP) за стандартом EIA/TIA-568B

Прямий кабель, обтиснутий з обох боків конекторами за однаковим стандартом (568A-568A або 568B-568B), має назву патч-корд та використовується для з'єднання різнотипного телекомунікаційного обладнання (комп'ютер-комутатор, комутатор-маршрутизатор тощо).

Перехресний кабель, обтиснутий з обох боків конекторами за різними стандартами (568A-568B або 568B-568A) використовується для з'єднання однотипного телекомунікаційного обладнання (комп'ютер-комп'ютер, комутатор-комутатор, тощо).

Маркування кабелів "звита пара" містить інформацію про категорію, тип екранування, матеріал оболонки та діаметр провідників. Категорія (наприклад, Cat 5e, Cat 6) вказує на швидкість та частоту передачі даних, а тип екранування (наприклад, UTP, FTP, S/UTP) – на наявність захисту від електромагнітних завад. Маркування кабелю також може включати логотип фірми-виробника, рік випуску, колір оболонки та матеріал з якого виготовлені струмопровідні дроти [5].

Для перевірки цілісності та схеми обтискання кабелю

MILITARY AFFAIRS AND NATIONAL SECURITY

"звита пара" застосовується кабельний (LAN) тестер, який складається з основного та віддаленого модулів. Вони мають світлодіодні LED індикатори, які послідовно загоряються, вказуючи на правильність з'єднання кожної жили.

Висновки

Електронна комунікаційна мережа ЗС України – це комплексна, багаторівнева система, що об'єднує телекомунікаційне обладнання, мережі та інформаційні системи. Її головна мета – забезпечення безперебійного, стійкого та оперативного управління військами в умовах ведення бойових дій.

ЕКМ поділяється на стаціонарні та польові (мобільні) ІКВ, що дозволяє адаптувати систему зв'язку до будь-якої тактичної обстановки на полі бою. Система об'єднує засоби військового зв'язку (радіостанції, супутникові термінали та ін.) та комплекси електрозв'язку. Це гарантує дублювання та високу живучість каналів передачі даних [19].

В умовах активної радіоелектронної та кіберборотьби, обов'язковим пріоритетом є кіберзахист інформаційно-телекомунікаційних мереж. Він досягається шляхом використання засобів криптографічного захисту інформації, шифрування та побудови захищених віртуальних приватних мереж (VPN).

Електронна комунікаційна мережа ЗС України є високотехнологічним, захищеним інформаційним комплексом, який постійно удосконалюється. Застосування сучасних технологій та стандартів телекомунікацій у поєднанні з багаторівневою системою кібербезпеки дозволяє ефективно координувати дії підрозділів та виконувати вимоги щодо прихованого управління військами.

References:

[1] Зв'язок та інформаційні системи: Доктрина. Головне управління зв'язку та кібербезпеки ГШ ЗС України. – К. : ГШ ЗС України, 2025. – 36 с.
[2] Інформаційні та автоматизовані системи управління : Настанова, затв. наказом Командувача військ зв'язку та кібербезпеки ЗС України від 24.12.2020 р. № 369. – К. : ГШ ЗС України, 2020. – 40 с.
[3] Військовий зв'язок та інформаційні системи, військовий стандарт ВСТ 01.112.004. Словник НАТО з систем зв'язку та інформаційних систем (AAP-31 (Edition 3), IDT)), – 2017. – 54 с.
[4] Система стандартів НАТО із організації роботи систем зв'язку (C4ISR). Ч. 1 : навч. посіб. / О. Є. Мазулевський, А. О. Зінченко, В. Є. Жуков та ін. – К. : НУОУ ім. Івана Черняховського, 2018. – 94 с.

MILITARY AFFAIRS AND NATIONAL SECURITY

[5] Війська зв'язку та кібербезпеки Збройних Сил України : Доктрина. Командування військ зв'язку та кібербезпеки ЗС України – К. : ГШ ЗС України, 2021. – 64 с.
[6] Воробієнко П. П. Телекомунікаційні та інформаційні мережі : підручник для ВНЗ / П. П. Воробієнко, Л. А. Нікітюк, П. І. Резніченко. – К. : Вид. "САММІТ-Книга", 2010. – 708 с.: іл.
[7] Основи інфокомунікаційних технологій : навч. посіб. / А. П. Бондарчук, Г. С. Срочинська, М. Г. Твердохліб. – К. : ДУТ, 2015. – 76 с.
[8] Основи організації зв'язку та інформаційних систем : навч. посіб. / Д. С. Комін, В. І. Василишин, В. П. Коцюба, В. М. Сухотеплий. – Х. : ХНУПС, 2022. – 224 с.
[9] Поповський В. В. Багатоканальний електрозв'язок та телекомунікаційні технології: підручник / В. В. Поповський, О. В. Лемешко, В. А. Лошаков та ін. – Х. : ХНУРЕ, 2010. – 482 с.
[10] Robert A. Monzingo, Thomas W. Miller Hughes Aircraft Company. Fullerton, California. A Whilley-interscience publication, John Wiley & Sons, New York, Chichester, Brisbance, Toronto, 2011.
[11] Комплекси і засоби військових телекомунікаційних мереж: навч. посіб. / за ред. М. Д. Огороднійчука. – К. : НУОУ, 2010. – 384 с.
[12] Теорія електричного зв'язку : навч. посіб. / О. Ю. Гусєв, Г.Ф. Конахович, В. І. Корнієнко, Г. В. та ін. – К. : КНТУ "КПІ". Вид. "Наукова думка", 2018. – 248 с.
[13] Напрямні системи електричного та оптичного зв'язку : навч. посіб. / В. П. Коцюба, В. І. Василишин, Д. В. Михалевський, В. М. Сухотеплий. – Х. : ХНУПС, 2026. – 144 с.
[14] Високошвидкісні волоконно-оптичні лінії зв'язку : навч. посіб. / Г. М. Розорінов, Д. О. Соловйов. – К. : КНТУ "КПІ", 2012. – 344 с.
[15] Giannakoulas A., Karkanis N., Gavriilidis I., Kaifas T. N. F.. Propagation Models for Wireless Sensor Networks. Electronics. 2026. 15. 925. Pp. 1-45.
[16] Експлуатація короткохвильової радіостанції RF-7800H-MP: метод. рекомен. / В. І. Василишин, В. П. Коцюба, В. М. Сухотеплий. – Х.: ХНУПС, 2025. – 132 с.
[17] Електрозабезпечення систем, комплексів та засобів військового зв'язку: навч. посіб. / В. П. Коцюба, В. І. Василишин, В. М. Сухотеплий, Д. С. Комін. – Х.: ХНУПС, 2024. – 128 с.
[18] Засоби криптографічного захисту інформації. Серія "Лавина-Е" та "Пелена-Е". ТОВ "Трител" – Режим доступу: http://www.tritel.ua.
[19] Коцюба В.П. Оцінювання покриття корпоративних безпровідних мереж на базі модифікованої моделі Окамура-Хата / Д. В. Михалевський, В. І. Василишин, В.П. Коцюба. // Вчені записки Таврійського національного університету. – Вип. № 37 (76), Ч. 2, 2026. С. 47-52. Режим доступу: https://www.tech.vernadskyjournals.in.ua/journals/2026/2_2026/part_2/2-2_2026.pdf

SCIENTIFIC EDITION

SCIENTIFIC COLLECTION «INTERCONF+»

№ 70(299) | June 2026

The issue contains:

Proceedings of the 13th International Scientific and Practical Conference

THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS

Rome, Italy
19-20.06.2026

All materials are reviewed.
The editorial office did not always agree with the position of authors.

Journal's frequency: monthly

Sighed for online publication: June 20, 2026.

Printed: July 19, 2026. Circulation: 200 copies. Format 60×84/8.
Batang & Courier New typefaces. Offset paper 100gsm. Digital color printing.

Contacts of the editorial office:

LLC Scientific Publishing Center «InterConf»
info@interconf.center
https://www.interconf.center

Certificate on the entry of publishing business subject in the State Register of Publishers, Manufacturers and Distributors of Publishing Products of Ukraine: ДК № 7882 of 10.07.2023.