Наукові перспективи
Видавнича група



MODERNÍ ASPEKTY VĚDY

v rámci publikační skupiny
Scientific Publishing Group

Svazek LXIX mezinárodní kolektivní monografie

Česká republika
2026

International Economic Institute s.r.o. (Czech Republic)
Central European Education Institute (Bratislava, Slovakia)
National Institute for Economic Research (Batumi, Georgia)
Al-Farabi Kazakh National University (Kazakhstan)
Institute of Philosophy and Sociology of Azerbaijan National Academy of Sciences (Baku, Azerbaijan)
Institute of Education of the Republic of Azerbaijan (Baku, Azerbaijan)
Regional Academy of Management (Kazakhstan)
Public Scientific Organization "Ukrainian Assembly of Doctors of Sciences in Public Administration" (Kyiv, Ukraine)
University of New Technologies (Kyiv, Ukraine)
International Consulting company "Sidcon" (Kyiv, Ukraine)
European Lyceum "Scientific Perspectives" (Kyiv, Ukraine)

within the Publishing Group "Scientific Perspectives"

MODERN ASPECTS OF SCIENCE

69-th volume of the international collective monograph

Czech Republic
2026

§10.3 РОЗРАХУНОК ПРОПУСКНОЇ СПРОМОЖНОСТІ ТА КІБЕРЗАХИСТ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДОСТУПУ

(**Коцюба В.П.,** Харківський національний економічний університет імені Семена Кузнеця)

При пошуку оптимального варіанту створення мережі доступу проводиться аналіз та синтез альтернативних структур, розрахунок показників її властивостей та обґрунтування критеріїв оцінки. Структура показників властивостей інформаційно-телекомунікаційної мережі наведена на рис 1.

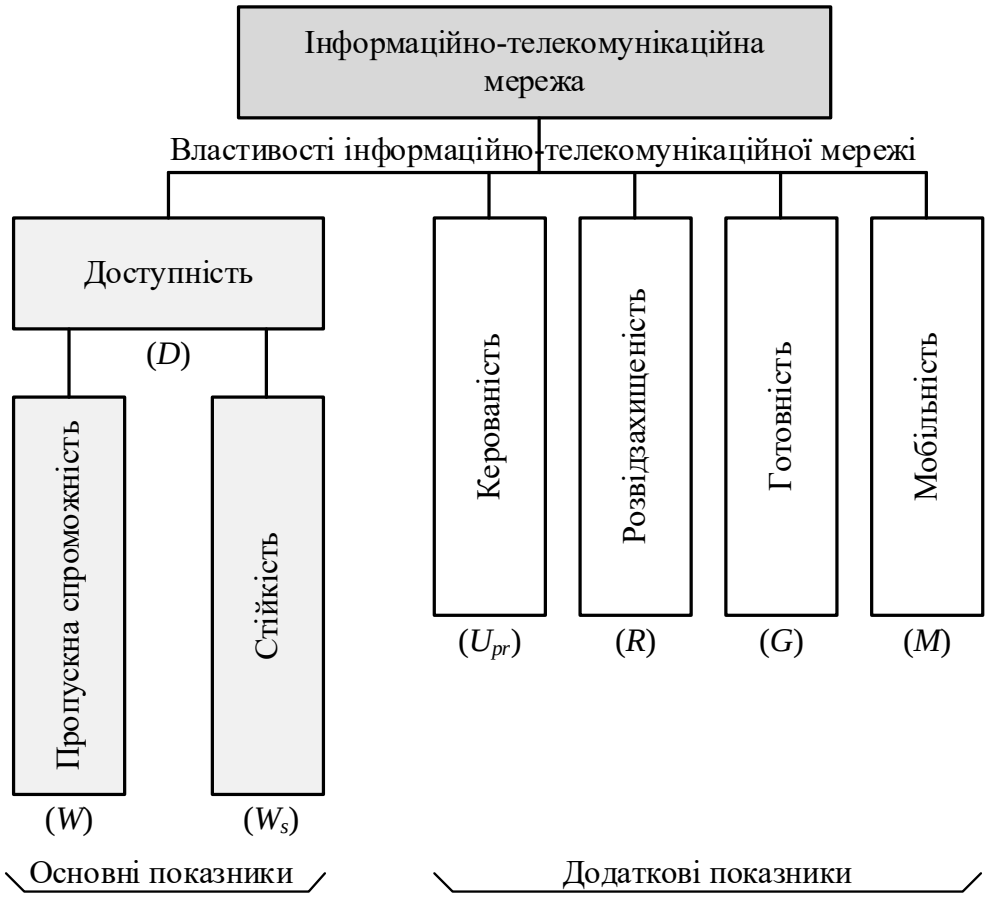


Рис. 1 Структура показників властивостей інформаційно-телекомунікаційних мереж

Основною властивістю телекомунікаційної мережі доступу для проведення оперативних розрахунків є показник “доступність”, який підлягає розрахунку в першу чергу [2, 8].

Доступність інформаційно-телекомунікаційної мережі – здатність мережі забезпечувати отримання органами управління (оперативним складом) необхідних їм інформаційно-телекомунікаційних послуг з заданою якістю.

Для визначення показника доступності (D) мережі доступу, яка використовує цифрові системи передачі, використовують узагальнений показник – коефіцієнт доступності за пропускною спроможністю:

$$K_{\text{дост}}^{\text{проп.спр}} = \min\left\{\frac{V_{\text{пл}}}{V_{\text{потр}}},\ 1\right\}, \qquad (1)$$

де $V_{\text{пл}}$ – швидкість передачі, що планується (повинна бути реалізована);

$V_{\text{потр}}$ – потрібна швидкість передачі.

Якщо значення $K_{\text{дост}}^{\text{проп.спр}}$ за величиною перевищує 1, то проводиться розрахунок резерву інформаційних можливостей мережі за формулою:

$$Q_{\text{рез}} = K_{\text{дост}}^{\text{проп.спр}} - 1. \qquad (2)$$

Швидкість передачі, що запланована, встановлюється старшим органом управління зв’язку в розпорядженні зі зв’язку та ІС. Потрібна швидкість передачі розраховується на підставі потреби посадових осіб пункту управління в інформаційних і телекомунікаційних послугах. Потреба в інформаційних і телекомунікаційних послугах (сервісах) визначається начальником штабу органу військового управління (військової частини).

Для розрахунку пропускної спроможності мережі доступу необхідно узагальнити вихідні дані. На підставі вхідних даних, які отримані від начальника штабу органу військового управління (військової частини), розпорядження зі зв’язку та інформаційних систем старшого штабу й після

з'ясування задачі необхідно розробити логічну схему підключення абонентських пристроїв мережі доступу.

На схемі необхідно відобразити:

– кількість користувачів, поділивши їх за сегментами;

– спосіб підключення користувачів;

– типи з'єднувальних ліній;

– довжину з'єднувальних ліній;

– типи інтерфейсів в точках підключення.

З метою структуризації розрахунків, користувачів мережі необхідно умовно розділити на дві групи: користувачі телефонного зв'язку і користувачі послуг передачі даних, поділивши їх за сегментами (N_i). Варіант логічної схеми підключення абонентських пристроїв наведено на рис. 2.

Для обох груп користувачів необхідно вказати загальні вихідні дані:

1) N_i – кількість сегментів, що обслуговуються системою доступу;

2) n_i – кількість користувачів в сегменті;

3) V_i – швидкість передачі для конкретного виду послуги.

Швидкість передачі в телефонних сегментах визначається швидкістю кодування, що залежить від типу обраного вокодера і алгоритму кодування.

Продуктивність в кожному сегменті мережі розраховується за формулою:

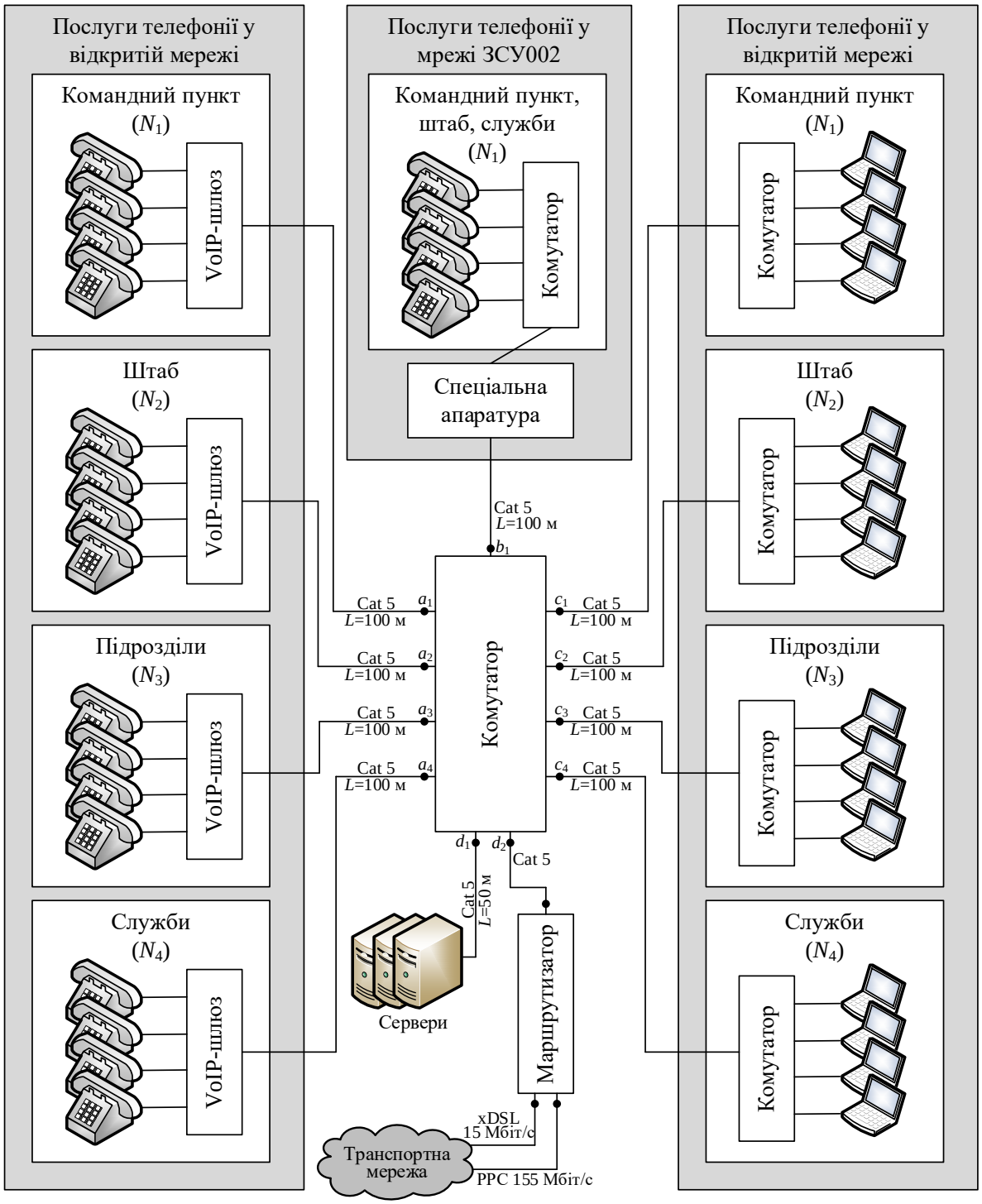
$$C_i = V_i n_j , \tag{3}$$

де C_i – продуктивність сегмента мережі; V_i – швидкість передачі для конкретного виду послуг; n_j – кількість абонентів (користувачів) в сегменті.

Загальна сумарна швидкість передачі інформації в точках включення в транспортну мережу (на вході прикордонного комутатора мережі) визначається за формулою:

$$V_\Sigma = \sum_{i=1}^{N} C_i , \tag{4}$$

де N – кількість сегментів мережі.



Точка включення	Тип інтерфейсу
a_1...a_4	10/100 BASE-TX
b_1	10/100 BASE-TX
c_1...c_4	10/100 BASE-TX
d_1, d_2	100/1000 BASE-TX

Рис. 2. Логічна схема підключення абонентських пристроїв

Вимоги, що висуваються до швидкості передачі даних для інформаційно-телекомунікаційних послуг наведені в табл. 1.

Таблиця 1

Вимоги, що висуваються до швидкості передачі даних
для інформаційно-телекомунікаційних послуг

№ з/п	Вид послуги	Швидкість передачі, кбіт/с
1	Телефонія (визначається типом вокодеру)	2,4…64
2	Відеоконференцзв'язок	1 024
3	Електронна пошта в АСУ ЗС України "СЕДО"	512
4	Електронна пошта в мережі ЗСУ001, ЗСУ002	512
5	WEB-доступ в АСУ ЗС України "СЕДО"	512
6	Захищена система електронного документообігу	2 048
7	"Віраж-планшет"	512
8	"Ореанда ПС"	1 024
9	"Персонал"	1 024
10	"Дельта"	1 024
11	Логістична та медична інформаційні системи	1 024

Для підвищення надійності функціонування (живучості) системи зв'язку здійснюється прив'язка ІКВ до двох і більше опорних вузлів зв'язку (вузлів прив'язки, пунктів виділення цифрових каналів). При цьому забезпечується передача даних з використанням стандартних цифрових каналів та потоків [7]:

- E0 – 64 кбіт/с (базовий цифровий канал);E1 – 2,048 Мбіт/с;
- E2 – 8,448 Мбіт/с;
- E3 – 34,368 Мбіт/с;
- E4 – 139,264 Мбіт/с;
- STM-1 – 155,52 Мбіт/с;

– STM-4 – 622,08 Мбіт/с;
– STM-16 – 2,5 Гбіт/с;
– STM-64 – 10 Гбіт/с [4].

Характеристики вокодерів для цифрових каналів наведено в табл. 2.

Таблиця 2

Характеристики вокодерів для цифрових каналів

Стандарт	Вокодер	Використання	Швидкість кодування, кбіт/с	Довжина кадру	Затримка, мс	MOS, середня
G.711	PCM	Телефонія	64	0,125	0,125/ 0,75/5	4,15
G.722	SB-ADPCM	Телефонія	66	40	5	–
			56	35	5	–
			48	30	5	–
G.726	ADPCM	Телефонія	40	25	5	–
			32	0,125/20	1/5	3,91
			24	15	5	–
			16	10	5	–
G.728	LD-CELP	Телефонія	16	0,625/10	2,5/3…5	3,69
G.729	CS-ACELP	Телефонія	8	10	10	3,96
G.729a	CS-ACELP	Телефонія	8	10	10	3,71
G.723.1	MP-MLQ	Телефонія	6,3	20/24	30/37,5	3,93
G.723	ACELP	Телефонія	5,3	30/20	30/37,5	3,66
ETSIGSM	RTP-PLE	GSM	13	20	–	3,3
ETSI TETRA	ACELP	Транкінг	4,8	–	–	3,4
США	MELP	Телефонія	2,4	–	45	3,5
TETRA	ACELP	Транкінг	4,57	–	–	3,4

Примітка. MOS (Mean Opinion Score) – нормована оцінка розбірливості мови. MOS дає кількісне (числове) уявлення про якість переданої медіа-інформації після стиснення за допомогою кодеків і передачі по каналах зв’язку. MOS приймає значення від 1 до 5.

Вибір варіанту структури мережі доступу (англ. Subscriber access network) визначає надійність, пропускну здатність та вартість розгортання всієї телекомунікаційної інфраструктури. основна мета цього процесу – знайти оптимальний баланс між капітальними витратами (Capex), операційними витратами (Opex) та технічними вимогами користувачів.

Основні варіанти архітектури мереж доступу. Сучасні мережі доступу класифікують за типом середовища передачі даних та топологією:

– оптичні мережі (англ. fiber to the home/passive optical network);

– бездротові мережі (англ. Wireless);

– Wi-Fi / кампусні мережі, використовуються точки доступу (wap) для локального покриття радіусом до 100 метрів;

– FWA (англ. fixed wireless access): фіксований бездротовий доступ через мережі 4g/5g або Wimax для віддалених об’єктів;

– гібридні та мідні мережі;

– Ethernet-мережі, що побудовані на базі керованих комутаторів (топології “зірка” або “кільце”).

Для визначення потрібної швидкості передачі інформації в мережі необхідно використовувати коефіцієнт використання ресурсу мережі (k), що враховує затримку доступу до середовища передачі даних. Для сімейства технологій Ethernet k = 1,4. Отже, потрібна швидкість передачі інформації з урахуванням внутрішніх дестабілізуючих факторів буде визначатися за формулою:

$$V_{\text{потр}} = V_{\sum} k \,, \tag{5}$$

де $V_{\text{потр}}$ – потрібна швидкість передачі;

k – коефіцієнт показника використання ресурсу мережі.

Критерієм позитивного розрахунку пропускної спроможності мережі є вираз:

$$V_{\text{потр}} > V_{\text{пл}}, \tag{6}$$

де $V_{\text{пл}}$ – швидкість передачі, що планується використовувати.

У період з 2022 року та до сьогоднішнього часу під час збройної агресії російської федерації здійснюються постійні масовані кібернетичні атаки на елементи критичної інформаційної інфраструктури як держави в цілому, так і на інформаційні ресурси Сил оборони України.

Під час бойових кібернетичних атак спеціальні служби реалізують концепції інформаційних та кібернетичних операцій, які направленні на систему управління та особовий склад ЗС України. Система управління ЗС використовує інформаційно-телекомунікаційні системи для передачі команд бойового управління та здійснення заходів повсякденної діяльності військ. Реалізація атак в кібернетичному просторі проти ЗС України може привести до витоку інформації, несанкціонованого доступу та порушення керованості елементами ІТС, відмови в доступі до ресурсів та систем, дезінформації особового складу частин (підрозділів) ЗС тощо.

Наявність вразливості ІТС, систем захисту інформації та не достатня підготовка особового складу ЗС призводить до суттєвих ризиків інформаційної безпеки, а успішна реалізація кібернетичних атак призводить до зниження боєготовності військ. З огляду на викладене актуальним та невідкладним є захист кіберпростору ЗС України [8].

Кібернетичний простір – це електронне інформаційне середовище, яке створене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем.

Захист кіберпростору повинен здійснюватися безперервно на землі, в повітрі, на морі та в космосі. Реалізація захисту повинна враховувати середовища розповсюдження інформаційних потоків й включаючи також електромагнітний спектр. Заходи захисту кіберпростору ЗС України повинні реалізовуватись на організаційному, технічному та правовому рівнях.

Організаційні заходи захисту кіберпростору в ЗС передбачають розробку правил доступу та роботи особового складу в ІТС, порядку обробки інформації та навчання основам інформаційної та кібернетичної безпеки. Крім того, особовий склад ЗС повинен бути навчений основам протистояння розвідці противника в інформаційному просторі – соціальній інженерії.

Технічні заходи захисту кіберпростору передбачають захист електронного середовища ІТС Збройних Сил України. З урахуванням особливостей побудови ІТС та сучасних систем захисту інформації можна виділити наступні функціональні рівні кіберпростору:

– рівень інформаційних систем (програмного забезпечення);

– рівень кінцевого телекомунікаційного обладнання;

– рівень мережного телекомунікаційного обладнання;

– рівень транспортної телекомунікаційної мережі.

Під час управління військами вказані функціональні рівні кіберпростору взаємодіють з рівнями, які об’єднують особовий склад та фізичне середовище (стаціонарні та польові об’єкти). Впровадження захисту кіберпростору не повинно обмежуватись стаціонарною компонентою. Реалізація захисту польових елементів обумовлюється їх критичністю внаслідок функціонування за межами контрольованої зони впритул до засобів технічної розвідки проводових, супутникових та радіоліній зв’язку.

Для забезпечення безпеки кіберпростору ЗС України необхідно впровадження комплексу систем та механізмів захисту ІТС на різних функціональних рівнях кіберпростору. До таких систем та механізмів відносяться:

– системи розмежування доступу користувачів до елементів ІТС;

– системи міжмережного екранування на основі фаєрволів (англ. Firewall);

– системи та механізми криптографічного захисту інформації при обміні та зберіганні інформації;

– віртуальні приватні мережі (VPN);

– системи антивірусного захисту елементів ІТС;

– системи виявлення та запобігання вторгненням (IDS/IPS);

– механізми автентифікації, авторизації та аудиту (AAA);

– системи попередження втрати даних – DLP (англ. data loss prevention).

Застосування даних систем та механізмів захисту інформації передбачається на відповідних функціональних рівнях кіберпростору, як зображено на рис. 3.

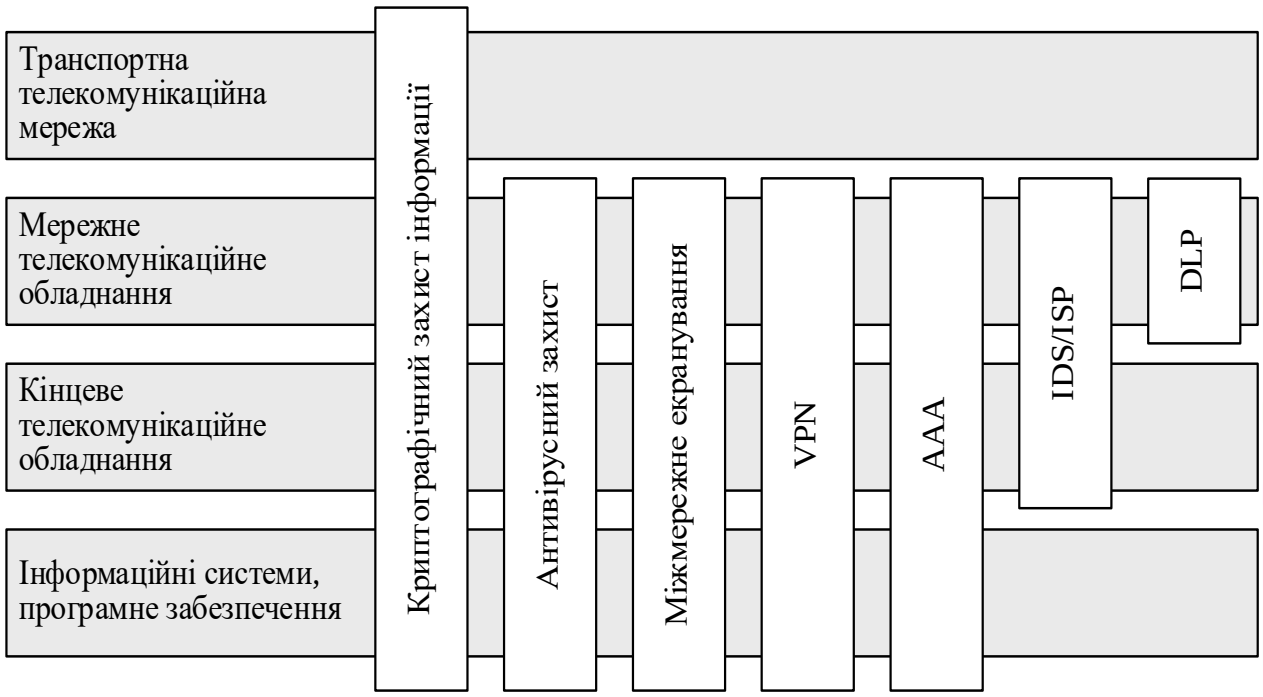


Рис. 3 Системи і механізми захисту інформаційно-телекомунікаційних систем спеціального призначення

Криптографічний захист інформації – один з основних інструментів, що реалізує функції на кожному з функціональних рівнів кіберпростору, включаючи і реалізацію криптографічних функцій в інших системах захисту інформації: VPN, міжмережних екранах (механізм англ. deep packet inspection), автентифікації тощо. Криптографічний захист інформації забезпечує конфіденційність та цілісність інформації [11].

Системи антивірусного захисту є невід'ємною складовою будь-якого елементу ІТС. Антивірусне програмне забезпечення, разом з існуючими методами (сигнатурним, евристичним, виявлення аномалій), впроваджує нові технології та механізми захисту – "пісочниця", емуляція, реалізація декількох антивірусних модулів тощо.

На сьогоднішній час реалізовані основні підходи щодо антивірусного захисту: системи антивірусного захисту шлюзів (англ. gateway antivirus) та захист кінцевих точок (англ. end point security). Для ефективного антивірусного захисту доцільне впровадження обох підходів. Аналогічно до інших програмних засобів існують як комерційні так і умовно безкоштовні антивірусні засоби, але такі засоби можуть мати обмежені функціональні можливості.

Міжмережне екранування здійснюється за допомогою фаєрволів – міжмережних екранів. Міжмережні екрани (МЕ) – комплекс апаратно-програмних чи програмних засобів, що здійснює контроль та фільтрацію інформаційних потоків відповідно до заданих правил політики безпеки.

На сьогоднішній час МЕ реалізуються у наступних виконаннях:

– апаратно-програмні МЕ реалізуються як окремі мережні пристрої. На даний час впроваджена концепція Next Genemtion Firewall (NGFW) – міжмережні екрани, крім функцій фільтрації трафіку, здійснюють антивірусний захист, створення каналів VPN, виявлення та захист від вторгнень та інші;

– програмні МЕ реалізуються у вигляді інтегрованого програмного забезпечення операційних систем, фаєрволів антивірусного програмного забезпечення, окремого спеціалізованого програмного забезпечення.

Сучасні міжмережні екрани дозволяються реалізувати фільтрацію трафіку за IP-адресами, портами відправника та отримувача, протоколами, здійснювати перевірку трафіку за змістом, блокування підозрілого трафіку та інші функції.

Для ефективного захисту інформації в ІТС ЗС України доцільно використовувати МЕ для захисту мереж та автоматизованих робочих місць. В першому випадку використовуються апаратно-програмні МЕ, у другому – програмні МЕ.

Віртуальні приватні мережі (VPN) використовуються для забезпечення захищеного обміну інформацією між мережами (англ. site-to-site) та захищеного доступу віддалених користувачів. Суть VPN полягає в створенні криптографічно-захищеного віртуального тунелю, що забезпечує конфіденційність та цілісність при обміні інформацією. Застосовуються основні схеми організації каналів VPN: мережа-мережа, клієнт-сервер.

До основних протоколів віртуальних приватних мереж відносяться протоколи IPsec, L2TP, GRE, PPTP, TLS. Серверні програмні модулі протоколів VPN реалізуються в серверних операційних системах, маршрутизаторах, NGFW та інших засобах. Функції VPN інтегровані майже в усі сучасні маршрутизатори, що знижує затрати на організацію захищених каналів зв’язку.

Механізми автентифікації, авторизації та аудиту (англ. AAA – authentication, authorization, accounting) – невід’ємні механізми захисту програмного забезпечення (веб-ресурсу, баз даних та ін.), операційних систем, інформаційних систем, систем захисту тощо. Механізми автентифікації та

авторизації забезпечують санкціонований доступ користувачів до систем (засобів) та надання повноважень відповідно до політики безпеки. Механізми аудиту дозволяють на основі журналів (логів) здійснювати запис подій та інцидентів порушення інформаційної безпеки. Аудит дозволяє проводити розслідування інцидентів та виявлення порушників, які порушують політику інформаційної безпеки.

Для реалізації моніторингу й аудиту подій інформаційної безпеки мережі в цілому використовуються системи SIEM (англ. security lnformation and event management). Ці системи включають у себе засоби автоматизованого збору подій, їх формалізації та узагальнення, відображення у зручному для аналізу вигляді. SIEM дозволяють проводити моніторинг та аудит стану інформаційної безпеки одночасно від багатьох робочих станцій, мережних пристроїв з різними платформами.

Системи виявлення та запобігання вторгненням (IDS/IPS) – це програмно-апаратні чи програмні засоби, які призначені для виявлення фактів несанкціонованого доступу до ІТС чи підозрілої активності. Системи виявлення вторгнення IDS дозволяють виявляти кібернетичні атаки. Системи запобігання вторгненнями IPS реалізують функції захисту, що дозволяють блокувати несанкціонований доступ чи несанкціоновані дії.

Здебільшого виділяється три основні класи IDS: мережні (Network-based IDS, NIDS), вузлові (Host-based IDS, HIDS) та гібридні. Архітектура IDS/IPS, ґрунтується на використанні консольних та сенсорних систем. В системі кібернетичного захисту сенсори збирають інформацію про небезпечну активність та надсилають до консолей, які систематизують, документують та здійснюють управління. Наряду з ефективністю виявлення кібернетичних атак та своєчасної їх нейтралізації, досить важливою є реалізація систематизації несанкціонованих дій та їх візуалізація, що дозволяє адекватно оцінювати стан кібернетичної безпеки.

Системи попередження про втрати даних (англ.data loss prevention, DLP-системи) досить інтенсивно розвиваються останнім часом. В ІТС Збройних Сил України існує велика кількість інформації, яка не відноситься до інформації з обмеженим доступом, але в сукупності розкриває певні відомості.

До такої інформації відносяться: поштові адреси, телефонні номери, особисті ідентифікаційні номери, банківські реквізити установ, технологічна інформація тощо. Окремі з цих відомостей не становлять відносної цінності, але в сукупності втрата вказаних масивів інформації є суттєвим ризиком інформаційної безпеки ЗС України. Системи DLP дозволяють перевіряти вміст трафіку, наявність даних, які задаються при налаштуванні системи, та блокувати передачу небезпечного трафіку [12].

Впровадження складних технологічних систем захисту інформації на кінцеві пристрої – здебільшого АРМ, викликає значні труднощі, тому доцільно впроваджувати мінімальний склад засобів захисту. До такого набору обов'язково повинні входити системи: антивірусного захисту, розмежування доступу та впровадження локальних (групових) політик безпеки, базові налаштування міжмережних екранів та використання, за потреби, VPN-тунелів.

Основним напрямком забезпечення безпеки кіберпростору ЗС України повинен бути направлений на впровадження мережних засобів захисту – шлюзів безпеки (security gateway). На сьогоднішній час шлюзи безпеки являють собою такі засоби захисту, як NGFW, UTM (англ. unified threat management) та NFIPS (англ. Next – generation intrusion prevention system). До основних лідерів в галузі кібернетичної безпеки відносяться: Cisco FireSIGHT, WatchGuard, Check Point, DellSonicWall, Fortinet, McAfee та ін.

Засоби проводового зв’язку

Засоби проводового зв’язку поділяються на [13]:

1) каналоутворення – призначені для утворення каналів передачі та цифрових потоків мереж зв’язку;

2) комутаційні – призначені для комутації каналів, цифрових потоків, повідомлень, пакетів (блоки комутації різного призначення, ручні та автоматичні телефонні станції, цифрові автоматичні комутаційні системи, концентратори, комутатори, маршрутизатори, пристрої передачі мови поверх мереж передачі даних, що працюють за IP-протоколами);

3) кінцеві – призначені для передавання та приймання повідомлень, а також для перетворення їх в зручну для сприйняття форму.

За допомогою кінцевих засобів зв’язку та автоматизованих робочих місць створюються індивідуальні та колективні робочі місця для роботи посадових осіб органів військового управління;

4) спеціальні – призначені для виконання спеціальних функцій щодо засекречування інформації, імітозахисту, підвищення її достовірності, забезпечення контролю і безпеки зв’язку [16].

Засоби каналоутворення

Мультиплексор – пристрій, що дозволяє передавати по одній волоконно-оптичній лінії одночасно декілька різних потоків даних (наприклад, Ethernet-трафік, потоки E1, E2 та ін).

На рис. 4 наведено приклад мультиплексора FG-FOM16-OG, який забезпечує передачу по двох оптичних волокнах трафіка Ethernet зі швидкістю до 1 Гбіт/с та 16 потоків E1.

Рис. 4 Оптичний мультиплексор FG-FOM16-OG

Оптичний модем OM-16E1-Eth призначений для одночасної передачі по волоконно-оптичним лініям до 16 потоків E1 та Ethernet-трафіку зі швидкістю до 100 Мбіт/с [14]. Зовнішній вигляд модему наведено на рис. 5.

Рис. 5. Оптичний модем OM-16E1-Eth

Модем M-4DSL.bis+ призначений для передачі до 4-х потоків E1 та Ethernet-трафіку стандарту 10/100 Base-T по 1 – 4 парах фізичного кабелю зі швидкістю до 15 Мбіт/с по кожній парі. Дозволяє реалізувати агрегацію Ethernet-трафіку по всім 4-м парам з сумарною швидкістю 60 Мбіт/с єдиного потоку. Зовнішній вигляд модему наведено на рис. 6.

Рис. 6. Модем M-4DSL.bis+

Модем M-2E1-Eth-2DSL.bis призначений для передачі двох потоків E1 та Ethernet-трафіку стандарту 10/100 Base-T по одній або двох парах фізичного кабелю зі швидкістю до 15 Мбіт/с по кожній парі. Зовнішній вигляд модему наведено на рис. 7.

Рис. 7. Модем M-2E1-Eth-2DSL.bis

Модем M-Eth-2DSL.bis призначений для передачі Ethernet-трафіку стандарту 10/100 Base-T по одній або двом парах фізичного кабелю зі швидкістю до 15 Мбіт/с по кожній парі. Зовнішній вигляд модему наведено на рис. 8.

Рис. 8. Модем M-Eth-2DSL.bis

Модем “Краб” (рис. 9) призначений для одночасної передачі по одній парі кабелю П-296, П-274М Ethernet-трафіку стандарту 10/100 Base T з максимальною швидкістю 15 Мбіт/с та 4-х каналів ТЧ (2/4-х проводових, з індукторним викликом, абонентів автоматичних телефонних станцій (АТС) або VoIP абонентів) на відстань до 20 км.

Рис. 9. Модем “Краб”

Модем М-8КТЧ-Eth призначений для передачі по мережі Ethernet до 8 2/4-х проводових каналів ТЧ (в т. ч. з індукторним викликом). Зовнішній вигляд модему наведено на рис. 10.

Рис. 10. Модем М-8КТЧ-Eth

Апаратура ІКМ-30-К-ТЧ призначена для організації передачі каналів ТЧ по потоку Е1: 1 – 30 каналів ТЧ з 2/4-х проводовим режимом роботи; 1-30 індукторних телефонних каналів; 1 – 30 каналів прямих абонентів (інтерфейси FXS и FXO); трансляція потоку Ethernet по виділених каналах потоку Е1 [8]. Зовнішній вигляд апаратури ІКМ-30-К-ТЧ наведено на рис. 11.

Рис. 11. Апаратура ІКМ-30-К-ТЧ

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. 12.

Рис. 12 Маршрутизатори виробництва компаній Cisco та MikroTik

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. 13.

Рис. 13. 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. 14.

Рис. 14 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. 15.

Рис. 15. 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 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. 16.

Рис. 16 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. 17.

Рис. 17. Телекомунікаційний комплект ТК-4

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. 18.

Рис.18. 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. 19.

Рис. 19 VoIP-шлюзи виробництва компанії Grandstream

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].

Список використаних джерел:

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.

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

20. https://studfile.net/preview/5366969/page:4/ Електричні процеси в проводових лініях, первинні та вторинні параметри передачі.

21. https://delta.mil.gov.ua/auth/login "Delta" національна військова система ситуаційної обізнаності Сил безпеки та оборони України.

Vydavatel:

Mezinárodní Ekonomický Institut s.r.o.
se sídlem V Lázních 688, Jesenice 252 42
IČO 03562671 Česká republika

MODERNÍ ASPEKTY VĚDY

Svazek LXIX mezinárodní kolektivní monografie

Podepsáno k tisku 11. červen 2026
Formát 60x90/8. Ofsetový papír a tisk
Headset Times New Roman.
Mysl. tisk. oblouk. 8.2. Náklad 100 kopií.