

# НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

## Командно-штабний факультет

### Кафедра військового зв'язку та інформатизації

ЗАТВЕРДЖУЮ

Начальник кафедри ВЗтаІ

доктор технічних наук, с.н.с., доцент

полковник



Олександр ІОХОВ

30 вересня 2021

## СИЛАБУС

НАУКОВІ ПРОБЛЕМИ (МОДЕЛІ ТА МЕТОДИ) ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ  
ВІЙСЬКОВОГО ЗВ'ЯЗКУ

РІВЕНЬ ВИЩОЇ ОСВІТИ

третій (освітньо-науковий)

ГАЛУЗЬ ЗНАНЬ

25 Воєнні науки, національна безпека, безпека  
державного кордону

СПЕЦІАЛЬНІСТЬ

255 Озброєння та військова техніка

Розглянуто та ухвалено на засіданні  
кафедри військового зв'язку та  
інформатизації

Протокол від 30.08.2021 р. № 1

<b>Інформація про викладача</b>	
<b>Прізвище, ім'я, по батькові</b>	Іохов Олександр Юрійович
<b>Наукова ступінь</b>	Доктор технічних наук
<b>Вчене звання</b>	Доцент
<b>Посада</b>	начальник кафедри
<b>Місце роботи</b>	Національна академія Національної гвардії України, м. Харків, майдан Захисників України, 3
<b>Адреса кафедри</b>	Навчальний корпус №1, кабінет №704
<b>Контакти</b>	тел. +38097-698-1250
<b>E-mail</b>	iohov@ukr.net

### **Примітка**

Консультативну допомогу здобувачі вищої освіти можуть отримати у науково-педагогічних працівників (НПП) кафедри, які безпосередньо проводять заняття або звернувшись з письмовим запитом на електронну пошту НПП.

## 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, рівень вищої освіти	Характеристика навчальної дисципліни	
		Денна форма навчання	
Кількість кредитів – 4	Галузь знань:	Нормативна (за вибором)	
	25 Воєнні науки, національна безпека, безпека державного кордону		
Блоків змістових модулів –	Спеціальність: 255 Озброєння та військова техніка	Рік підготовки	
Змістових модулів – 2		1 - й	
Індивідуальне завдання (Обґрунтування технічних вимог до системи захисту допоміжного пункту управління) – 28		Семестр	
		1- й	2- й
		Лекції	
Загальна кількість годин - 120	Рівень вищої освіти: третій (освітньо-науковий)	8 год.	- год.
		Практичні, групові	
		22 год.	28 год.
		Самостійна робота	
		16 год.	16 год.
		Контрольна робота	
		-	-
		Індивідуальні завдання-	
			28
Вид контролю: екзамен (2 години)			

## 2. Мета та завдання навчальної дисципліни

*Предмет вивчення навчальної дисципліни:* організація зв'язку у формуваннях Національної гвардії України, Основні положення, критерії й поняття організації зв'язку, Наукові основи радіомоніторингу, радіоконтролю та РЕБ.

*Міждисциплінарні зв'язки з дисциплінами:* під час вивчення дисципліни використовуються теоретичні знання та практичні навички, одержані здобувачами вищої освіти у курсах “Застосування інтегрованих середовищ розробки програмного забезпечення для дослідження систем військового зв'язку”, “Методи дослідження сигналів та процесів в засобах військового зв'язку”.

*Метою:* вивчення теоретичних основ організації зв'язку у формуваннях НГУ, основи управління зв'язком, основи радіоелектронної боротьби та організація зв'язку у підрозділах та частинах НГУ з врахуванням досвіду організації та забезпечення зв'язку під час проведення операції об'єднаних сил, порядок застосування основних сучасних засобів зв'язку, що використовуються в підрозділах та частинах НГУ, основи кібернетичного захисту в інформаційно-телекомунікаційних мережах НГУ.

*Завданнями:*

освоєння ад'юнктами базових знань в області:

- надбання слухачами знань щодо виявлення та вирішення проблемних питань у процесі вирішення завдань зв'язку, обґрунтування та досягнення вимог, що ставляться до засобів зв'язку і до систем зв'язку; способів та методів організації зв'язку різними родами та видами зв'язку; наукові основи радіоелектронного захисту засобів зв'язку, які забезпечують управління частинами НГУ; наукових основ радіомоніторингу та радіоконтролю у частинах НГУ; правових основ використання інформаційних технологій в процесі управління військами; наукових основ організації, обґрунтування та досягнення основних характеристик та прийоми використання інформаційного забезпечення процесів управління формуваннями Національної гвардії; принципів побудови і використання сучасних моделей спеціальних операцій, геоінформаційних, навігаційних та експертних систем, можливості сучасних телекомунікаційних систем, структурну організацію та можливості комп'ютерної мережі Internet.

- передати розуміння основних положень та проблематики щодо захисту інформації у комп'ютерних мережах і шляхам їх реалізації;

- визначити проблеми щодо використання основних методів криптографічного захисту інформації при експлуатації комп'ютерних систем та мереж;

- надати базові знання, потрібні при вивченні дисциплін предметної галузі їх діяльності;

- ознайомити з перспективними напрямками розвитку теорії і методів захисту інформації у комп'ютерних системах та мережах.

Компетентності, які формує дисципліна: ІК, ЗК-3, ЗК-4, ЗК-5, ЗК-7, ЗК-8, ПК-4, ПК-5, СК-4 ... СК-9, СК-11, СК-12.

### 3. Зміст навчальної дисципліни (анотація навчальної дисципліни)

Згідно з вимогами освітньої програми здобувачі вищої освіти повинні:

**Знати:** - методологічні проблеми процесу організації військового зв'язку; - методику розв'язання прикладних наукових завдань з організації військового зв'язку НГУ; - теоретичні та практичні питання використання засовів військового зв'язку та інформатизації в складних умовах обстановки; - методику розв'язання прикладних наукових завдань з забезпечення військового зв'язку та інформатизації в умовах ведення радіоелектронної боротьби; - методику розв'язання прикладних наукових завдань з забезпечення кібербезпеки, кіберзахисту, кібергігієни інформаційно-телекомунікаційних мереж спеціального призначення.

**Уміти:** - створювати та описувати моделі процесів захисту в системах військового зв'язку; - створювати методи та моделі інформаційно-телекомунікаційних мереж спеціального призначення.

**Володіти:** - технологіями забезпечення безпеки військового зв'язку; - практичними навичками захисту інформаційного простору в інформаційно-телекомунікаційних мережах спеціального призначення.

### 4. Календарно-тематичний план вивчення дисципліни.

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л.	гр.	п.р.	с.р.
1	2	3	4	5	6
<b>Блок змістових модулів 1. Організація зв'язку у формуваннях Національної гвардії України.</b>					
<b>Змістовий модуль 1. Загальні положення з організації зв'язку.</b>					
Заняття 1 Основні положення, критерії й поняття організації зв'язку. 1. Основні положення організації зв'язку відповідно до вимог країн-членів НАТО. 2. Критерії й поняття організації зв'язку в країнах членів НАТО.	2	2			
Самостійне вивчення 1. Роди зв'язку, види зв'язку підрозділів Національної гвардії України.	2				2
Заняття 2. Завдання та характеристики системи зв'язку. 1. Завдання зв'язку відповідно до вимог країн-членів НАТО. 2. Основні проблеми забезпечення	2	2			

1	2	3	4	5	6
характеристик системи зв'язку, заходи по їх виконанню та їх основні показники.					
Самостійне вивчення. 1. Проблемні питання з підготовки системи зв'язку до виконання завдань за призначенням відповідно до вимог країн-членів НАТО. 2. Основні проблеми забезпечення зв'язку у повсякденній діяльності та в особливий період.	2				2
Заняття 3. Система зв'язку та інформатизації НГУ. 1. Основні проблеми управління системою зв'язку, органи та пункти управління зв'язком НГУ. 2. Порядок перевірки стану зв'язку в частинах та підрозділах НГУ. 3. Плануючі, робочі та розпорядчі документи зі зв'язку у частинах НГУ.	2		2		
Самостійне вивчення. 1. Елементи системи зв'язку НГУ. 2. Основні проблеми організації зв'язку в оперативно-тактичній ланці управління і військових частинах іноземних країн. 3. Наукові основи організації зв'язку.	2				2
Заняття 4. Безпека зв'язку. 1. Вимоги та заходи щодо забезпечення безпеки зв'язку. 2. Документи прихованого управління військами.	2		2		
Самостійне вивчення 1. Порядок розробки документів прихованого управління військами в тактичній ланці управління	2				2
Заняття 5. Визначення характеристик радіозв'язку. 1. Розрахунок характеристик радіозв'язку, способи організації радіозв'язку. 2. Розрахунок характеристик радіорелейного (тропосферного) зв'язку і способи його організації. 3. Підготовка командирів і штабів до управління по радіо.	2			2	



1	2	3	4	5	6
Самостійне вивчення. 1. Розрахунок параметрів траси радіорелейного зв'язку	2				2
Заняття 6. Визначення характеристик проводового зв'язку і способи його організації. 1. Розрахунок характеристик проводового зв'язку та способи організації проводового зв'язку. 2. Визначення стану проводового зв'язку.	4			4	
Самостійне вивчення 1. Загальна характеристика сигнального зв'язку і способи його організації	2				2
Заняття 7. Використання автоматизованих систем управління у силових структурах України та світу. 1. Вимоги до систем управління військами. 2. Шляхи удосконалення сучасних інформаційних системах управління в збройних силах країн-членів НАТО. 3. Основні проблеми автоматизації систем управління у силових структурах України. 4. Модульний контроль.	4			4	
<b>Разом за змістовим модулем 1</b>	<b>30</b>	<b>4</b>	<b>4</b>	<b>10</b>	<b>12</b>
<b>Змістовий модуль 2. . Наукові основи радіомоніторингу, радіоконтролю та РЕБ.</b>					
Заняття 1. Загальні положення щодо РЕБ. 1. Радіoeлектронна та радіотехнічна розвідка, основні поняття та визначення. 2. Захист зв'язку та інформації. 3. Перспективи розвитку засобів РЕБ.	2	2			
Самостійне вивчення 1. Вимоги нормативно-правових документів держави щодо створення КСЗІ в ІТС. Принципи створення комплексних систем захисту інформації. Концепція забезпечення захисту інформації в ІТС організацій, підприємств, установ.	1				1
Заняття 2. Наукові проблеми захисту зв'язку на пунктах управління від впливу засобів РЕБ під час виконання службово – бойових завдань. 1. Наукові основи радіoeлектронного захисту вузлів зв'язку пунктів управління.	2	2			

1	2	3	4	5	6
2. Наукові основи захисту зв'язку на пунктах управління від технічних засобів розвідки.					
Самостійне вивчення 1. Протоколи керування мережею. Безпека DNS. Можливі атаки. Протокол ICMP. Можливі атаки. Рекомендації із застосування. Використання ICMP для здійснення атак. Атаки Smurf, TFN, IP Spoofing	1				1
Заняття 3. Математичні методи та симетричні криптографічні перетворення 1. Теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії. 2. Еліптичні та гіпереліптичні групи, основи застосування в криптографії 3. Криптографічні перетворення на основі обчислень алгебри зрізаних поліномів	4		4		
Самостійне вивчення 1. Асиметричні крипто перетворення в групах точок еліптичних кривих	1				1
Заняття 4. Блокове симетричне криптографічне перетворення. 1. Використання блокових симетричних шифрів. 2. Джерела ключів та ключової інформації, вимоги до них.	4			4	
Самостійне вивчення 1. Джерела ключів асиметричних криптосистем та вимоги до них.	1				0,5
Заняття 5. Криптографічні механізми та протоколи. 1. Методи формування цифрового підпису та його властивості. 2. Властивості та основи застосування електронних цифрових підписів. 3. Криптографічні механізми та протоколи управління ключами.	2		2		
Самостійне вивчення. 1. Методи та механізми захисту від несанкціонованого доступу	2				0,5
Заняття 6. Криптографічний аналіз асиметричних криптосистем. 1. Вступ в теорію та практику крипто аналізу.	4		4		



1	2	3	4	5	6
2. Методи крипто аналізу асиметричних криптосистем.					
Самостійне вивчення. 1. Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих. 2. Квантова криптографія та крипто аналіз.	3				3
Заняття 7. Скалярне множення в групі точок еліптичних кривих, афінне подання точок еліптичних кривих. 1. Скалярне множення в групі точок еліптичних кривих, проєктивне подання точок еліптичних кривих, порівняльний аналіз складності операцій додавання та подвоєння точок еліптичних кривих для різних подань. 2. Складений оператор.	4			4	
Самостійне вивчення. 1. Симетричні криптоалгоритми, критерії та показники оцінки якості крипто перетворень, умови реалізації безумовно стійких, обчислювально стійких та ймовірно стійких шифрів.	3				3
Заняття 8. Використання несиметричного крипто перетворення. 1. Несиметричні криптоалгоритми. Синтез крипто перетворень в скінченних полях та кільцях. Направлені шифри та їх реалізація. 2. Несиметричні криптоалгоритми в групах точок еліптичних кривих над скінченними полями	4			4	
Самостійне вивчення 1. Формування та аналіз властивостей псевдо випадкових та випадкових послідовностей. 2. Елементарні шифри та їх властивості	3				3
Заняття 9. Криптографічні механізми та протоколи. 1. Шляхи удосконалення криптографічних механізмів та протоколи управління ключами. 2. Проблеми впровадження криптографічних механізмів та протоколів автентифікації.	2		2		
Самостійне вивчення 1. Порядок встановлення та налаштування	3				3

1	2	3	4	5	6
OpenVPN,					
Заняття 10. Організації захищеного віддаленого доступу 1. Протокол SOCKS. Списки контролю доступу ACL. Протоколи автентифікації PPP та S/Key 2. Використання віртуальних приватних мереж (VPN)	4			4	
Самостійне вивчення 1. Протокол SSL. Призначення, архітектура	2				2
Заняття 11. Використання методів дослідження ZBF з елементами DMZ 1. Списки контролю доступу ACL 2. VPN за допомогою IPSec	4			4	
Самостійне вивчення 1. Використання OpenSSL системи захисту	2				2
Заняття 12. Організація кіберзахисту підрозділів НГУ відповідно до вимог країн-членів НАТО. 1. Сучасні загрози безпеки інформації в системі НГУ. 2. Застосування методів і засобів захисту інформації. 3. Модульний контроль.	4			4	
Разом за змістовим модулем 2	82	4	12	24	20
<b>Усього годин</b>	<b>118</b>	<b>8</b>	<b>16</b>	<b>34</b>	<b>32</b>
<b>Екзамен</b>	<b>2</b>				
<b>Індивідуальне завдання (Обґрунтування технічних вимог до системи захисту допоміжного пункту управління)</b>					28
<b>Разом за дисципліну</b>	<b>120</b>	<b>8</b>	<b>16</b>	<b>34</b>	<b>60</b>

## 5. Самостійна робота.

Самостійна робота здобувачів вищої освіти є основним засобом оволодіння навчальним матеріалом у час, вільний від навчальних занять за розкладом. Без систематичної, безперервної самостійної роботи здобувачів вищої освіти протягом всього періоду навчання неможливо засвоєння ними програмного матеріалу. Час для самостійної роботи відводиться розпорядком дня.

Викладач організує методичне керівництво та забезпечення самостійної роботи здобувачів вищої освіти:

- подає рекомендації з методики вивчення дисципліни та окремих питань, видає завдання та контролює їх виконання;
- застосовує такі методичні прийоми викладення навчального матеріалу, які орієнтують здобувачів вищої освіти на роботу з літературою та самостійне здобування знань;
- аналізує та узагальнює досвід самостійної роботи здобувачів вищої освіти щодо вивчення матеріалу і вносить корективи у завдання.

При самостійному відпрацюванні питань по дисциплінам, що вивчаються, здобувачі вищої освіти повинні враховувати методичні рекомендації по опрацюванню питань тематики дисципліни, відведений час на самостійне опрацювання та дотримуватися контрольних питань, що дають змогу економити час і оволодіти знаннями відповідно до фахової підготовки.

## 6. Політика курсу та оцінювання.

### Політика курсу.

- Курс передбачає роботу в команді.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо слухач відсутній з поважної причини, він/вона презентують виконані завдання під час самостійної підготовки та консультації викладача.
- Під час виконання завдань на заняттях не допустимо порушення академічної доброчесності.

Оцінювання знань (контрольні заходи) здійснюється відповідно до “Положення про оцінювання знань слухачів в Національній академії Національної гвардії України”.

Основними видами контрольних заходів є:

- вхідний (попередній) контроль;
- поточний контроль;
- самоконтроль;
- проміжний модульний контроль;
- рубіжний контроль;
- підсумковий (семестровий контроль, підсумкова атестація).

*Вхідний (попередній) контроль* проводиться перед вивченням навчальної дисципліни з метою визначення рівня підготовки здобувачів вищої освіти з навчальних дисциплін, які забезпечують цю дисципліну.

*Поточний контроль* проводиться викладачами на всіх видах навчальних занять. Основна мета поточного контролю – забезпечення зворотного зв'язку між викладачами та здобувачами вищої освіти у процесі навчання, перевірка їх готовності до виконання наступних навчальних завдань, а також забезпечення управління навчальною мотивацією здобувачів вищої освіти. Інформація, одержана під час поточного контролю, використовується для коригування методів і засобів навчання, а також для самостійної роботи здобувачів вищої освіти.

Поточний контроль може проводитися у формі усного опитування або письмового експрес-контролю (летючки) під час проведення навчальних занять, виступів здобувачів вищої освіти при обговоренні питань на семінарських заняттях, а також у формі комп'ютерного тестування.

Поточний контроль успішності слухачів (курсантів, студентів) здійснюється за національною чотирибальною (5, 4, 3, 2 бали) шкалою оцінювання.

*Самоконтроль* призначений для самооцінки здобувачами вищої освіти якості засвоєння навчального матеріалу з конкретної дисципліни, змістового модуля або заняття. З цією метою в навчальних посібниках, а також у методичних розробках до занять передбачаються питання для самоконтролю.

*Проміжний модульний контроль* – це контроль знань здобувачів вищої освіти після вивчення логічно завершеної частини (модуля) програми навчальної дисципліни. Проміжний модульний контроль може проводитися у формі контрольної роботи, тестування, виконання контрольних завдань тощо.

Оцінку за проміжний модульний контроль записують у журналі обліку навчальних занять за національною чотирибальною шкалою оцінювання.

*Рубіжний контроль* – підсумовує результати поточного та проміжного модульного контролів, можливих поточних перездач, проводиться з метою реалізації безсесійної накопичувальної технології оцінювання навчальних досягнень здобувачів вищої освіти з окремої навчальної дисципліни.

Знання слухачів оцінюються за шкалою ECTS, національною чотирибальною шкалою, та за 100-бальною шкалою академії (див. табл. 1).

*Підсумковий контроль* є семестровим та забезпечує оцінку результатів навчання здобувачів вищої освіти на проміжних або заключному етапах їх навчання і проводиться у формі заліку або екзамену в термін, встановлений графіком навчального процесу та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Знання слухачів оцінюються за шкалою ECTS, національною чотирибальною шкалою, та за 100-бальною шкалою академії (див. табл. 1).

Під час визначення оцінки необхідно орієнтуватися на такі загальні рекомендації:

– оцінка “відмінно” ставиться, якщо здобувач вищої освіти демонструє повні й міцні знання навчального матеріалу в заданому обсязі, необхідний

рівень умінь і навичок, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях;

- оцінка “добре” – здобувач вищої освіти допускає несуттєві неточності при застосуванні знань та умінь;

- оцінка “задовільно” – здобувач вищої освіти засвоїв основний теоретичний матеріал, але допускає окремі помилки, що не є перешкодою до подальшого навчання. Уміє використовувати знання для вирішення стандартних завдань;

- оцінка “незадовільно” – незасвоєння окремих розділів, нездатність застосовувати знання на практиці, що робить неможливим подальше навчання.



## 7. Критерії оцінювання знань здобувачів вищої освіти.

Оцінювання знань здобувачів вищої освіти здійснюється відповідно до “Положення про оцінювання знань слухачів (курсантів, студентів) у Національній академії Національної гвардії України”.

**Табл. 1 Загальні критерії оцінювання знань слухачів (курсантів, студентів)**

Сума балів за всі види навчальної діяльності / Amount of points for all types of educational activities	Оцінка ЄКТС / ECTS rating	Оцінка за національною шкалою / National grade	Критерії
		для екзамену, заліку, курсового проекту (роботи), стажування, практики / for an exam, a score, a course project (work), internship, practical	
90-100	A	Відмінно / Excellent	Слухач (курсант, студент) виявив всебічні, систематичні та глибокі знання навчального матеріалу дисципліни, передбаченого програмою; опрацював основну та додаткову літературу, рекомендовану програмою; проявив творчі здібності у розумінні, логічному, стислому та ясному трактуванні навчального матеріалу; засвоїв взаємозв'язок основних понять дисципліни, їх значення для подальшої професійної діяльності.
82-89	B	Добре / Good	Слухач (курсант, студент) виявив систематичні та глибокі знання вище середнього рівня навчального матеріалу дисципліни; продемонстрував уміння легко виконувати завдання, передбачені програмою; опрацював літературу, рекомендовану програмою; засвоїв взаємозв'язок основних понять дисципліни, їх значення для подальшої професійної діяльності.
75-81	C		Слухач (курсант, студент) виявив у цілому добрі знання навчального матеріалу дисципліни при виконанні передбачених програмою завдань, але припустив низку незначних помилок; опрацював основну літературу, рекомендовану програмою; показав систематичні знання з дисципліни; здатний самостійно використовувати та поповнювати знання у процесі подальшого навчання та професійної



			діяльності.
66-74	D	Задовільно / Satisfactory	Слухач (курсант, студент) виявив знання навчального матеріалу дисципліни в обсязі, необхідному для подальшого навчання та майбутньої професійної діяльності; виконав завдання, передбачені програмою; ознайомився з основною літературою, що зазначена у програмі; припустив значну кількість помилок або недоліків у відповідях на запитання співбесіди, тестування, при виконанні завдань тощо, які може усунути самостійно.
60-65	E		Слухач (курсант, студент) виявив мінімальні знання основного навчального матеріалу дисципліни в обсязі, необхідному для подальшого навчання та майбутньої професійної діяльності; в основному виконував завдання, передбачені програмою; ознайомився з основною літературою, що зазначена у програмі; припустив значні помилки у відповідях на запитання співбесіди, тестування, при виконанні завдань тощо, які може усунути лише під керівництвом та за допомогою викладача.
35-59	FX	незадовільно з можливістю повторного складання / Fail with possible retake	Слухач (курсант, студент) має значні прогалини в знаннях основного навчального матеріалу дисципліни; припускає принципові помилки при виконанні передбачених програмою завдань.
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни/ Fail with mandatory re-learning discipline	Слухач (курсант, студент) не має знань зі значної частини навчального матеріалу; припускає принципові помилки при виконанні більшості передбачених програмою завдань; не спроможний самостійно засвоїти програмний матеріал.

**Примітка:** Підсумкова оцінка формується через розподіл балів між поточним контролем та екзаменом у співвідношенні 60% оцінки за практичні дії, групові вправи, поточний контроль і 40% – результату екзамену.

## 8. Рекомендована література.

### Основна

1. Іохов О. Ю. Захист радіомереж підрозділів Національної гвардії України від радіотехнічної розвідки: монографія. Харків: НАНГУ, 2017. 222 с.

2. Олифер В. Г. Сетевые операционные системы : учеб. пособ. / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2007. – 539 с. : ил. – ISBN 5-272-00120-6. – 39,00
3. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 616 с.
4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.
5. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.
6. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М. : Кудиц – Образ, 2001. – 368 с.
7. 9. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
8. Шеховцов В. А. Захист інформації в інформаційно-комунікаційних системах : підруч. / В. А. Шеховцов. – К. : Вид. група BHV, 2005. – 576 с. : іл. – ISBN 966-552-157-8. – 30,00
9. Бондаренко М. Ф. Захист інформації в інформаційно-комунікаційних системах : навч. посібник / М. Ф. Бондаренко, О. Г. Качко. – Харків : СМІТ, 2008. – 432 с. – ISBN 978-966-2028-02-7. – 45,00
10. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.
11. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.
12. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
13. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
14. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

### Допоміжна

1. ВСТ 01.112.001 – 2006 (01) Військовий зв'язок та інформаційні системи. Військовий зв'язок. Терміни та визначення. — Чинний від 03.05.2006. — Київ: Міністерство оборони України, 2006. — XX с.
2. ВСТ 01.112.002 – 2007 (01) Військовий зв'язок та інформаційні системи. Технічне забезпечення зв'язку та автоматизації. Терміни та визначення. — Чинний від 12.02.2007. — Київ: Міністерство оборони України, 2007. — XX с.

3. ВСТ 01.112.003 – 2009 (01) Військовий зв'язок та інформаційні системи. Зберігання засобів зв'язку і автоматизації ЗСУ. Керівництво. — Чинний від 21.12.2009. — Київ: Міністерство оборони України, 2009. — XX с.
4. ВСТ 01.112.004 – 2017 (01) Військовий зв'язок та інформаційні системи. Словник НАТО систем засобів зв'язку та інформаційних систем (STANAG 5064 Ed. 1 /AAP-31 Ed. 3 (2005), IDT) NATO COMMUNICATION AND INFORMATION SYSTEMS GLOSSARY. — Чинний від 15.08.2017. — Київ: Міністерство оборони України, 2017. — 55 с.
5. ВСТ 01.112.005 – 2017 (01) Військовий зв'язок та інформаційні системи. Військова система зв'язку. Графічні символи (STANAG 5042 (Ed. 1), IDT) MILITARY TELECOMMUNICATIONS-DIAGRAM SYMBOLS. — Чинний від 15.08.2017. — Київ: Міністерство оборони України, 2017. — 28 с.
6. ВСТ 01.112.006 – 2019 (01) Військовий зв'язок та інформаційні системи. Словник НАТО зі зв'язку. Частина 1 (STANAG 5626 Ed: 1 /AcomP-01 (Ed. 3) NATO COMMUNICATION GLOSSARY (Chapters 716-722), MOD). — Чинний від 24.09.2019. — Київ: Міністерство оборони України, 2019. — XX с.
7. ВСТ 01.112.006 – 2018 (01) Військовий зв'язок та інформаційні системи. Словник НАТО зі зв'язку. Частина 2 (STANAG 5626 Ed: 1 /AcomP-01 (Ed. 3) NATO COMMUNICATION GLOSSARY (Chapter 161-703), MOD). — Чинний від 29.12.2018. — Київ: Міністерство оборони України, 2018. — 175 с.
8. ВСТ 01.112.006 – 2019 (01) Військовий зв'язок та інформаційні системи. Словник НАТО зі зв'язку. Частина 3 (STANAG 5626 Ed: 1 /AcomP-01 (Ed. 3) NATO COMMUNICATION GLOSSARY (Chapters 704-712), MOD). — Чинний від 23.10.2019. — Київ: Міністерство оборони України, 2019. — 225 с.
9. ВСТ 01.112.006 – 2020 (01) Військовий зв'язок та інформаційні системи. Словник НАТО зі зв'язку. Частина 4 (STANAG 5626 Ed: 1 /AcomP-01 (Ed. 3) NATO COMMUNICATION GLOSSARY (Chapters 713-715), MOD). — Чинний від 01.04.2020. — Київ: Міністерство оборони України, 2020. — XX с.
10. ВСТ 01.112.006 – 2020 (01) Військовий зв'язок та інформаційні системи. Словник НАТО зі зв'язку. Частина 5 (STANAG 5626 Ed: 1 /AcomP-01 (Ed. 3) NATO COMMUNICATION GLOSSARY (Chapters 723-725), MOD). — Чинний від 03.08.2020. — Київ: Міністерство оборони України, 2020. — XX с.
11. ВСТ 01.112.007 – 2020 (01) Військовий зв'язок та інформаційні системи. Міжнародна система маршрутизації та адресації для тактичних систем зв'язку (STANAG 4214 (Ed. 2) INTERNATIONAL ROUTING AND DIRECTORY FOR TACTICAL COMMUNICATIONS SYSTEMS, IDT). — Чинний від 03.05.2020. — Київ: Міністерство оборони України, 2020. — XX с.
12. ВСТ 01.112.008 – 2020 (01) Військовий зв'язок та інформаційні системи. Міжнародна мережева нумерація для систем зв'язку, що використовуються в НАТО (STANAG 4705 (Ed. 1) INTERNATIONAL NETWORK NUMBERING FOR COMMUNICATIONS SYSTEMS IN USE IN NATO, IDT). — Чинний від 04.01.2021. — Київ: Міністерство оборони України, 2020. — XX с.
13. ВСТ 01.112.009 – 2020 (01) Військовий зв'язок та інформаційні системи. Технічні стандарти для одноканального ВЧ радіообладнання (STANAG 4203 C3 (Ed. 3) TECHNICAL STANDARDS FOR SINGLE CHANNEL

HF RADIO EQUIPMENT, IDT). — Чинний від 01.09.2020. — Київ: Міністерство оборони України, 2020. — XX с.

14. ВСТ 01.112.010 – 2020 (01) Військовий зв'язок та інформаційні системи. Технічні стандарти для одноканального НВЧ радіообладнання (STANAG 4204 (Ed. 3) TECHNICAL STANDARDS FOR SINGLE CHANNEL VHF RADIO EQUIPMENT, IDT). — Чинний від 01.09.2020. — Київ: Міністерство оборони України, 2020. — XX с.

15. ВСТ 01.112.011 – 2020 (01) “Військовий зв'язок та інформаційні системи. Технічні стандарти для одноканального НВЧ радіообладнання (STANAG 4205 (Ed. 4)/AComP 4205 (Edition A Version 1) TECHNICAL STANDARDS FOR SINGLE CHANNEL VHF RADIO EQUIPMENT, IDT)”. — Чинний від 01.10.2020. — Київ: Міністерство оборони України, 2020. — XX с.