

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ



ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

Тетяна ГОВОРУЩЕНКО

Ім'я, ПРІЗВИЩЕ

09 2026 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Завадостійкість та інформаційна безпека інфокомунікацій

Назва дисципліни

Галузь знань – G Інженерія, виробництво та будівництво

Спеціальність – G 5 Електроніка, електронні комунікації, приладобудування та радіотехніка

Рівень вищої освіти – Другий (магістерський)

Освітньо-професійна програма – Електронні системи та мережі комунікацій

Обсяг дисципліни – 5 кредитів ЄКТС, Шифр дисципліни – ОФП.01

Мова навчання – українська

Статус дисципліни: обов'язкова (фахової підготовки)

Факультет – Інформаційних технологій

Кафедра – Телекомунікацій, медійних та інтелектуальних технологій

Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
ДФН	1	1	5,0	150	50	16	16	18	-	100	-	-	-	+
Разом ДФН			5,0	150	50	16	16	18	-	100	-	-	-	1

Робоча програма складена на основі освітньо-професійної програми «Електронні системи та мережі комунікацій» за спеціальністю G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка»

Робоча програма складена

Підпис автора(ів)

д-р. техн. наук, професор Юлія БОЙКО

Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри

Телекомунікацій, медійних та інтелектуальних технологій

Протокол від 27.08 2026 № 1.

Зав. кафедри

Сергій ПІДЧЕНКО

Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету

Підпис

Тетяна ГОВОРУЩЕНКО

Ім'я, ПРІЗВИЩЕ

Хмельницький 2026

ЛИСТ ПОГОДЖЕННЯ

(Підписи завідувача кафедри та гаранта ОП, за якою закріплений
обов'язковий освітній компонент)

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, д-р. техн. н., проф.	Телекомунікацій, медійних та інтелектуальних технологій		Сергій ПІДЧЕНКО
Гарант освітньо-професійної програми, д-р. техн. н., проф.	Телекомунікацій, медійних та інтелектуальних технологій		Юлій БОЙКО

3. Пояснювальна записка

Дисципліна «Завадостійкість та інформаційна безпека інфокомунікацій» є однією з дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів другого (магістерського) рівня вищої освіти очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Електронні системи та мережі комунікацій» у межах спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка».

Пререквізити – вихідна.

Постреквізити – Моделювання і оптимізація радіотехнічних засобів електронних комунікацій (ОФП.03), Моделювання і оптимізація радіотехнічних засобів електронних комунікацій (курсова робота) (ОФП.04), Системний аналіз інформаційно-комунікаційних систем та мереж (ОФП.05), Переддипломна практика (ОФП.07), Кваліфікаційна робота (ОФП.08).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

– компетентностей: здатність розв'язувати задачі дослідницького та/або інноваційного характеру в електроніці, електронних комунікаціях, приладобудуванні та радіотехніці (ІК); здатність застосовувати знання у практичних ситуаціях (ЗК 02); знання та розуміння предметної області та розуміння професійної діяльності (ЗК 03); здатність використовувати інформаційні та комунікаційні технології (ЗК 06); здатність генерувати нові ідеї, креативність (ЗК 08); здатність до реалізації принципів системного підходу під час дослідження та оптимізації процесів, що відбуваються в електронних комунікаціях, інформаційно-комунікаційних мережах, радіотехнічних системах, комплексах і пристроях, з урахуванням їх функціональних властивостей, надійності, енергоефективності та безпеки (ФК 02); здатність розв'язувати задачі забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускну здатності інформаційно-комунікаційних мереж, електронних комунікацій, радіотехнічних систем з урахуванням економічних, правових, безпекових та екологічних аспектів (ФК 04); здатність здійснювати дослідження, розробку і застосування програмно-апаратних засобів інфокомунікацій з елементами штучного інтелекту (ФК 10).

– програмних результатів навчання: планувати та виконувати наукові й прикладні дослідження у сфері інформаційно-комунікаційних мереж, електронних комунікацій, радіотехнічних систем, технологій, приладів і їх компонентів, застосовувати методи математичного і фізичного моделювання, обробки інформації, інтерпретувати результати досліджень та обґрунтовувати висновки (ПРН 04); аналізувати напрями розвитку та новітні стандарти у сферах інформаційно-комунікаційних мереж, електронних комунікацій, радіотехнічних систем, технологій, приладів і їх компонентів (ПРН 06); застосовувати мови програмування загального та спеціалізованого призначення, пакети аналітичного та імітаційного моделювання, а також інструменти розробки програмного та апаратного забезпечення для розв'язання складних задач у зазначених сферах (ПРН 08); забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність інформаційно-комунікаційних мереж, електронних комунікацій, радіотехнічних систем, технологій, приладів і їх компонентів (ПРН 10); розробляти і реалізовувати інженерні проекти, враховуючи цілі, обмеження, соціальні, економічні, правові та екологічні аспекти (ПРН 11); керувати складними виробничими, експлуатаційними процесами, забезпечувати професійний розвиток персоналу (ПРН 12); здійснювати пошук інформації у науково-технічній та довідковій літературі, патентах, базах даних, інших джерелах, аналізувати і оцінювати цю інформацію (ПРН 14).

Мета дисципліни. Метою навчальної дисципліни є формування у здобувачів загальних і фахових компетентностей та програмних результатів навчання, визначених освітньою програмою, шляхом набуття знань, умінь і навичок щодо методик забезпечення завадостійкості та технологій інформаційного захисту електронних комунікацій, засад інформаційної безпеки, методів технічного захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах, підсистем комплексу засобів захисту, таксономії функцій систем захисту та криптографічних методів захисту інформації.

Предмет дисципліни. Поняття та загальні принципи застосування технологій завадостійкості, інформаційного захисту та методів технічного захисту інформації телекомунікаційних систем.

Завдання дисципліни. Формування загальних і фахових компетентностей щодо безпекових та інших аспектів функціонування телекомунікаційних та інформаційно-комунікаційних систем; методи підвищення завадостійкості електронних комунікацій; технології інформаційного захисту та програмно-апаратне забезпечення телекомунікаційних систем; методи технічного захисту інформації; принципи криптографічних методів захисту інформації; типові вразливості систем і аналіз причин їх появи; шкідливе програмне забезпечення; нормативні документи з оцінювання захищеності інформації; апаратне забезпечення засобів захисту; передавання інформації через захищені мережі; створення, введення в дію та супроводження захищених систем.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: розуміти загальні принципи організації безпекових та інших аспектів функціонування телекомунікаційних та інформаційно-комунікаційних систем, локалізувати та оцінювати стан проблемної ситуації на етапах дослідження інформаційної безпеки телекомунікаційних систем, їх проектування, модернізації, впровадження та експлуатації, а також формулювати пропозиції щодо її вирішення з усуненням виявлених недоліків; забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних та радіотехнічних систем в умовах інформаційних загроз; розуміти концептуальні засади та таксономію функцій щодо методів технічного захисту інформації та криптографічних методів захисту інформації; володіти навичками застосування нормативних вітчизняних і міжнародних документів (стандартів) з оцінювання захищеності інформації; опанувати апаратні та програмні засоби захисту і принципи супроводження комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.

4. Структура залікових кредитів дисципліни

Назва теми	Лекції	Лабораторні роботи	Практичні	СРС
Тема 1. Забезпечення захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах	2	2	–	14
Тема 2. Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях	4	2	2	14
Тема 3. Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах	2	2	8	15
Тема 4. Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних систем	2	2	4	14
Тема 5. Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах	2	2	–	15
Тема 6. Методи та засоби блокування технічних каналів витоку інформації	2	2	2	14
Тема 7. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій	2	4	2	14
Разом за семестр	16	16	18	100

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
1	Тема 1. Забезпечення захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах Завдання захисту інформації. Окреслення загроз захисту інформації та їх класифікації. Типи атак та моделі загроз. Оцінювання, моніторинг та аспекти розробки захищених систем. Особливості архітектури систем захисту інформації. Теоретичні основи захисту інформації. Модель загроз та класифікація атак у середовищі IoT і 5G. Вектори атак на кінцевий пристрій, радіоінтерфейс, вузли периферійних обчислень та хмарну платформу. Класифікація атак на IoT/5G-системи за п'ятьма групами: фізичні (tampering, side-channel, fault injection), мережеві (eavesdropping, MitM, DoS/DDoS), програмні (exploitation, malware, destruction), атаки на конфіденційність (data harvesting, tracking, identity theft, surveillance), атаки на дані (theft, manipulation, destruction). Розширення поверхні атаки внаслідок віртуалізації мережевих функцій (NFV), програмно-конфігурованих мереж (SDN) та багатодоступних периферійних обчислень (MEC). Літ.: [1] с. 6–21; [2] с. 17–31; [5] с. 11–24, 30–58; [9] с. 265–275.	2
	Тема 2. Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях	
2	Лекція 2. Завадостійке кодування в електронних комунікаціях: показники ефективності, дослідження каналу та сигнально-кодові конструкції Методи завадостійкого кодування інформації в електронних комунікаціях. Формування оціночних показників ефективності завадостійкого кодування в електронних комунікаціях. Методика формування та дослідження телекомунікаційного каналу передачі інформації із завадостійким кодуванням. Формування завадостійких сигнально-кодових конструкцій у електронних комунікаціях. Коди з прямим виправленням помилок (FEC). Можливості турбо-кодів, LDPC, полярних кодів у підвищенні завадостійкості електронних комунікацій. Канальне кодування. Літ.: [1] с. 22–50; [3] с. 7–61; [4] с. 143–192; [7] с. 140–205.	2
3	Лекція 3. Завадостійке кодування у мережах 5G NR: архітектура PDSCH та інтелектуальне декодування LDPC і полярних кодів Завадостійке кодування у мережах 5G NR. Структурна схема архітектури фізичного низхідного каналу спільного користування PDSCH: обчислення CRC, сегментація на кодові блоки та буферизація HARQ, кодер LDPC/Polar, узгодження швидкості й вибір версії надлишковості (Rate Matching + RV Selection), модулятор M-QAM, телекомунікаційний канал (AWGN, релеївські замирання), демодулятор з формуванням логарифмічних відношень правдоподібності (LLR), декодер, перевірка цілісності за CRC та формування підтвердження ACK/NACK у механізмі HARQ. Принципи взаємодії фізичних каналів 5G NR: LDPC-кодування транспортних блоків PDSCH (базові граfi BG1, BG2), полярне кодування керуючої інформації PDCCH і PBCH. Інтелектуальне декодування LDPC та полярних кодів: гібридна схема DRL+Soft-Decision за архітектурою Actor-Critic, адаптивне керування кількістю ітерацій BP та списковим декодуванням CA-SCL, оцінювання за BER, BLER, обчислювальною складністю та затримкою декодування. Інтелектуалізація процедур променеформування у 5G як засіб підвищення завадостійкості: beam sweeping, beam measurement, beam determination, beam refinement, beam recovery, вибір оптимальної пари променів за критерієм RSRP, нейромережеве прогнозування пари променів за координатами абонентського обладнання, вплив на час початкового доступу та обсяг сигнального обміну. Літ.: [7] с. 183–202; [8] с. 226–236; [10] с. 509–523; [12] розд. 5, 7.	2
4	Тема 3. Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах Сервісні та функціональні засоби безпеки та механізми їх реалізації. Автентифікація, ідентифікація та керування доступом у контексті забезпечення цілісності системи. Криптографічні системи. Технології шифрування, теорія, алгоритми, криптографічні підсистеми. Криптографічний захист у середовищах IoT та 5G: обмеженість обчислювальних і енергетичних ресурсів, мобільність вузлів, масштабність підключень, стійкість до атак побічними каналами, квантова стійкість. Легкі (lightweight) криптоалгоритми PRESENT, SIMON, SPECK, ZUC, SNOW 3G, компроміс за критеріями Security, Performance, Area. Стек безпеки 5G: NAS Security, AS Security, Transport Security (IPSec, TLS, DTLS на інтерфейсах N2, N3, N6, N9). Алгоритми шифрування та контролю цілісності AES (NEA2/NIA2), ZUC (NEA3/NIA3), SNOW 3G (NEA1/NIA1). Ієрархія ключів 5G. Захист процедур променеформування у 5G: вразливості SSB beam sweeping до перехоплення, глушіння та спуфінгу в діапазоні mmWave, скорочення поверхні атаки керуючої площини, нейромережеве керування променями (secure beam management) як механізм рівня AS. Літ.: [1] с. 51–61; [2] с. 165–173, 186–197; [6] с. 22–31, 43–51; [9] с. 265–275; [11] с. 1–15; [13] розд. 6, 9, дод. D.	2

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
5	Тема 4. Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних систем Помилки програмної реалізації систем. Облік вад захисту залежно від їх розміщення в системі. Шкідливе програмне забезпечення. Основні завдання апаратного захисту інформації. Інженерно-технічні та фізичні засоби захисту інформації. Перехоплення даних, канали витоку інформації. Літ.: [1] с. 62–72; [2] с. 112–147.	2
6	Тема 5. Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах Апаратні засоби захисту. Інженерно-технічні та фізичні засоби захисту інформації. Перехоплення даних, канали витоку інформації. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Заходи щодо захисту локальної робочої станції. Літ.: [1] с. 73–83; [2] с. 62–72, 121–127; [6] с. 7–21, 52–63.	2
7	Тема 6. Методи та засоби блокування технічних каналів витоку інформації Технічні канали витоку інформації. Об'єкти та методи технічного захисту інформації. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Методи пошуку радіозакладних пристроїв. Захист інформації від витоку технічними каналами, утвореними допоміжними технічними засобами, звукозаписувальними та оптичними пристроями. Літ.: [1] с. 84–96; [2] с. 124–127; [5] с. 281–292.	2
8	Тема 7. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій Інформаційна безпека як складова національної безпеки. Стандартизація та специфікація вимог захисту інформації в системах. Критеріальні ознаки оцінювання захищеності інфокомунікаційних систем. Концепція профілю захисту. Розгляд напрямів призначення стандартів інформаційної безпеки. Літ.: [1] с. 97–107; [2] с. 6–14; [5] с. 25–29, 66–74.	2
	Разом за семестр	16

5.2 Зміст практичних занять

№ п/п	Теми практичних занять	Кількість годин
1	Практ. роб. № 1. Ознайомлення з методами кодування інформації	2
2	Практ. роб. № 2. Види шифрів. Ознайомлення з методикою шифрування методом заміни	2
3	Практ. роб. № 3. Вивчення асиметричних криптосистем на основі алгоритму RSA	4
4	Практ. роб. № 4. Шифри складної заміни. Багатоалфавітні шифри	2
5	Практ. роб. № 5. Аналіз загроз та методів захисту інформації в інфокомунікаційних системах	4
6	Практ. роб. № 6. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій	2
7	Практ. роб. № 7. Заходи щодо інформаційного захисту локальної робочої телекомунікаційної станції	2
	Разом за семестр	18

5.3 Зміст лабораторних занять

№ п/п	Теми лабораторних занять	Кількість годин
1	Лаб. роб. № 1. Ознайомлення з інструментами захисту інформації у MS Word	2
2	Лаб. роб. № 2. Дослідження завадостійкості широкосмугових телекомунікаційних каналів засобами Matlab/Simulink	2
3	Лаб. роб. № 3. Визначення пропускну здатності каналів передачі інформації	2
4	Лаб. роб. № 4. Ознайомлення з поняттям захисту інформації та інформаційної безпеки. Визначення критеріїв та аспектів захисту при оцінюванні інформаційної безпеки	2
5	Лаб. роб. № 5. Принципи захисту інформації на основі генератора шуму «Базальт-5 ГШ»	2
6	Лаб. роб. № 6. Використання радіолокаційної станції ПСНР-1 для захисту інформації та визначення дальності до цілі	2
7	Лаб. роб. № 7. Ознайомлення із засобами технічного захисту інформації	4
	Разом за семестр	16

5.4 Зміст самостійної роботи здобувача вищої освіти

Самостійна робота здобувачів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до практичних і лабораторних занять, контрольних робіт та тестування. Крім цього, до послуг здобувачів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1, 2	Опрацювання теоретичного матеріалу з Т1. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 1. Опрацювання матеріалу «Загрози та криптографічні вимоги в середовищі IoT і 5G» у Модульному середовищі для навчання	12
3, 4	Опрацювання теоретичного матеріалу з Т2. Підготовка до лабораторного заняття. Опрацювання презентаційного матеріалу «Завадостійке кодування у мережах 5G NR: архітектура PDSCN та інтелектуальне декодування LDPC і полярних кодів» у Модульному середовищі для навчання	12
5, 6	Опрацювання теоретичного матеріалу з Т3. Підготовка до лабораторного заняття, підготовка до практичних занять ПЗ 2, ПЗ 3. Опрацювання матеріалу «Стек безпеки 5G та інтелектуалізоване керування променями» у Модульному середовищі для навчання	12
7, 8	Підготовка до контрольної роботи з Т1–Т3.	12
9, 10	Опрацювання теоретичного матеріалу з Т4. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 4	12
11, 12	Опрацювання теоретичного матеріалу з Т5.	10
13, 14	Опрацювання теоретичного матеріалу з Т6. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 5	10
15, 16	Підготовка до практичного заняття ПЗ 6.	10
17	Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 7	10
	Разом за семестр	100

Примітки: Т – тема навчальної дисципліни, ПЗ – практичне заняття, КР – контрольна робота.

Керівництво самостійною роботою та контроль за її виконанням здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій і методів навчання, зокрема лекції: з використанням мультимедійних презентацій, методів візуалізації, пояснення, проблемного й інтерактивного навчання, інформаційно-комунікаційних технологій, інтенсифікації та індивідуалізації навчання; практичні заняття: бесіда, інструктування, демонстрування, розв'язування ситуаційних завдань, презентації; лабораторні заняття: з використанням методів комп'ютерного моделювання, методів проектної діяльності, аналізу проблемних ситуацій, пояснення, дискусії; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних і лабораторних робіт, поточного та підсумкового контролю) з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних та лабораторних занять, а також у дні проведення контрольних заходів, установлених робочою програмою і графіком освітнього процесу, у тому числі з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів роботи на практичних заняттях (опитування теоретичного матеріалу, розв'язування задач, участь в обговоренні ситуацій);
- захист лабораторних робіт;
- оцінювання контрольної роботи.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи суму балів нижчу за 60 відсотків від максимального балу, не допускається до семестрового контролю, поки не виконає обсяг роботи, передбачений робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал з усіх видів поточного контролю і не склав іспит, вважається таким, який має академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, установленим деканатом відповідно до Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ.

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, передбачених чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки, відвідування занять з дисципліни є обов'язковим. За об'єктивних причин, підтверджених документально, теоретичне навчання за погодженням із лектором може відбуватися в онлайн-режимі. Успішне опанування дисципліни і формування загальних і фахових компетентностей та програмних результатів навчання, визначених освітньою програмою, передбачає підготовку до практичних занять (вивчення теоретичного матеріалу з теми), активну роботу на занятті, розв'язування задач, участь у дискусіях щодо прийнятих рішень. Підготовка до лабораторного заняття передбачає вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття, активну роботу на занятті, якісне оформлення звіту та захист результатів виконаної роботи. Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене практичне або лабораторне заняття здобувач зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять, тестування та виконання контрольної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу з дисципліни, має дотримуватися політики академічної доброчесності (заборонені списування та плагіат, у тому числі з використанням мобільних девайсів). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми або виду роботи, що передбачені робочою програмою.

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (курси Cisco з кібербезпеки, програмування з допомогою MATLAB (Simulink)), які сприяють формуванню компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання здобувачів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє певну кількість балів із

встановлених робочою програмою для цього виду роботи. Кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків від максимально можливої суми балів, призначеної структурній одиниці.

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	Узагальнений зміст критерію оцінювання
Відмінно (високий)	Здобувач вищої освіти глибоко і в повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат, уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання, якісне оформлення роботи, володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнювальні висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві або три несуттєві похибки
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі, свідомо використовує теоретичні знання для вирішення практичних задач. Виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил і закономірностей. Відповідь будується на основі самостійного мислення. Здобувач допустив дві або три несуттєві помилки
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Відповідь будується на рівні репродуктивного мислення, здобувач має слабкі знання структури навчальної дисципліни, допускає неточності і суттєві помилки, вагається при відповіді на видозмінене запитання. Разом з тим набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів денної форми здобуття освіти у семестрі

Аудиторна робота		Контрольні заходи	Семестровий контроль	Разом
Практичні заняття (ПЗ 1, ПЗ 4, ПЗ 7)	Лабораторні роботи № 1–7	Контрольна робота	Іспит	Сума балів
3–5 за кожне заняття	3–5 за кожну роботу	6–10	24–40	60–100*
9–15	21–35	6–10	24–40	

* Позитивною є сума від 60 балів за умови, що з кожного виду навчальної роботи здобувач набрав не менше 60 відсотків від максимального балу, встановленого для цієї структурної одиниці.

Оцінювання на практичних заняттях

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування на знання теоретичного матеріалу з теми; вільне володіння термінологією та уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач; результати самостійних робіт. При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними в таблиці критеріїв оцінювання (мінімальний позитивний бал – 3, максимальний – 5). У разі виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, практичне заняття не зараховується, і для його зарахування здобувач має детальніше опрацювати матеріал з теми заняття, виправити грубі помилки в розв'язуванні задач та повторно пройти опитування у призначений викладачем час.

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до методичних рекомендацій лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; повнота відповіді; знання методики проведення дослідження; уміння інтерпретувати результати; володіння відповідним програмним забезпеченням; обґрунтованість висновків. Лабораторні роботи виконуються на комп'ютері

з використанням спеціалізованих програм, що дозволяють моделювати, аналізувати та досліджувати відповідні технічні процеси. Результат виконання і захисту кожної лабораторної роботи оцінюється відповідно до таблиці критеріїв оцінювання (мінімальний позитивний бал – 3, максимальний – 5). У разі виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, лабораторна робота не зараховується, і для її захисту здобувач має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на захист у призначений викладачем час.

Оцінювання контрольної роботи

Контрольна робота передбачає виконання трьох завдань. При оцінюванні контрольної роботи враховуються повнота відповіді та якість виконання. Загальна сума балів на позитивну оцінку становить від 6 до 10. Завдання № 1 і № 2 теоретичні (по 3 бали максимально, мінімальний позитивний бал – 2), завдання № 3 практичне (4 бали максимально, мінімальний позитивний бал – 2). При отриманні негативної оцінки контрольну роботу слід перездати до терміну наступного контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. В екзаменаційному білеті пропонується поєднання питань теоретичного (у тому числі в тестовій формі) та практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю (40 балів)

Види завдань	Мінімальний (достатній) бал	Потенційні позитивні бали (середній бал)	Максимальний (високий) бал
Теоретичне питання № 1	3	4	5
Теоретичне питання № 2	3	4	5
Практичне завдання (задача)	18	24	30
Разом	24		40

Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25–39 балів і розраховується як сума балів за всі структурні елементи іспиту.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Залік	Іспит / диференційований залік
A	90–100	Зараховано	Відмінно / Excellent — високий рівень досягнення запланованих результатів навчання
B	83–89	Зараховано	Добре / Good — середній (максимально достатній) рівень досягнення запланованих результатів навчання
C	73–82	Зараховано	Добре / Good
D	66–72	Зараховано	Задовільно / Satisfactory — мінімально достатні результати навчання
E	60–65	Зараховано	Задовільно / Satisfactory
FX	40–59	Незараховано	Незадовільно / Fail — низка запланованих результатів навчання відсутня
F	0–39	Незараховано	Незадовільно / Fail — результати навчання відсутні

10. Питання для самоконтролю результатів навчання

1. Які зі способів реалізації загрози розглядаються в моделі загроз.
2. На порушення яких властивостей інформації та системи спрямована загроза прослуховування трафіку.
3. Наведіть визначення інформаційної безпеки.

4. Назвіть об'єкти інформаційної безпеки.
5. Назвіть основні напрями забезпечення безпеки інформації.
6. Які існують базові принципи захисту інформаційних систем.
7. Які рівні захисту інформаційних систем вам відомі.
8. Принципи роботи блокових та потокових шифрів, переваги та недоліки.
9. Призначення, способи генерації та використання ключів.
10. Вимоги до криптосистем та шифрів.
11. Криптографічна стійкість шифрів.
12. Ненадійність ключів та повідомлень.
13. Досконалі шифри.
14. Яка різниця між циклічними кодами і кодами Хеммінга.
15. Поясніть реалізацію стохастичних алгоритмів Шеннона–Фано та Хаффмана.
16. Яка особливість декодування при використанні методу LZW.
17. Принципи реалізації алгоритмів з несиметричним ключем.
18. У чому ідея шифрів підстановки.
19. У чому ідея шифрів перестановки.
20. Яка відмінність моноалфавітних шифрів від поліалфавітних.
21. На якій ідеї побудований алгоритм RSA.
22. Що таке комп'ютерний вірус. Поняття зараженої програми.
23. Як функціонують антивірусні програми. Класи антивірусних програм.
24. Визначте можливості і недоліки використовуваного брандмауера.
25. Що таке ідентифікація користувачів.
26. Які види ідентифікації вам відомі.
27. Що таке парольна ідентифікація.
28. Що таке автентифікація користувачів.
29. Чим забезпечується криптостійкість алгоритму.
30. Наведіть основні переваги та недоліки асиметричних шифрів.
31. Які засоби контролю використовуються при управлінні безпекою.
32. Які аспекти розглядаються при оцінюванні ризиків безпеки.
33. Що таке математична модель безпеки.
34. Які моделі безпеки здобули найбільшого поширення.
35. Назвіть основні причини появи вразливостей у сучасних телекомунікаційних і інформаційно-комунікаційних системах.
36. Назвіть типові помилки, що з'являються під час програмної реалізації системи і можуть спричиняти появу вразливостей.
37. Які головні ознаки мережних хробаків, що вирізняють їх з-поміж інших шкідливих програм.
38. Наведіть класифікацію комп'ютерних вірусів.
39. Які програмні засоби дістали назву «троянські коні». Наведіть їх класифікацію.
40. З яких джерел беруть дані для пошуку атак і які можливості мають відповідні сенсори.
41. Методики підвищення завадостійкості телекомунікаційних систем.
42. Методи завадостійкого кодування інформації в електронних комунікаціях.
43. Формування оціночних показників ефективності завадостійкого кодування в електронних комунікаціях.
44. Методика формування та дослідження телекомунікаційного каналу передачі інформації із завадостійким кодуванням.
45. Формування завадостійких сигнально-кодових конструкцій у електронних комунікаціях. Коди з прямим виправленням помилок (FEC). Можливості турбо-кодів, LDPC, полярних кодів.
46. Наведіть склад моделі загроз у середовищі IoT та 5G.
47. Класифікація атак на IoT/5G-системи: назвіть групи та наведіть приклади атак у кожній з них.
48. Як віртуалізація мережевих функцій (NFV), програмно-конфігуровані мережі (SDN) та периферійні обчислення (MEC) впливають на поверхню атаки в мережах 5G.

49. Наведіть структурну схему архітектури фізичного каналу PDSCH у 5G та поясніть призначення блоків обчислення CRC, сегментації і буферизації HARQ.
50. Призначення процедур узгодження швидкості (Rate Matching) та вибору версії надлишковості (RV) у 5G NR.
51. Порівняйте сфери застосування LDPC-кодів і полярних кодів у 5G NR. Що таке базові графи BG1 і BG2.
52. Поясніть механізм HARQ та роль підтверджень ACK/NACK у забезпеченні достовірності передавання.
53. Які підходи до інтелектуалізації декодування LDPC і полярних кодів вам відомі. Поясніть схему DRL+Soft-Decision за архітектурою Actor-Critic.
54. За якими показниками оцінюють ефективність інтелектуального декодера.
55. Сформулюйте вимоги до криптографії в середовищі IoT та 5G.
56. Наведіть рівні стеку безпеки 5G (NAS, AS, Transport) та вкажіть, що саме захищає кожен з них.
57. Опишіть ієрархію ключів 5G, починаючи з кореневого ключа K.
58. Порівняйте AES, ZUC і SNOW 3G за швидкістю, енергоспоживанням та сферою застосування.
59. Які вразливості процедури SSB beam sweeping використовуються для перехоплення, глушіння та спуфінгу.
60. Як застосування нейромережових методів у керуванні променями впливає на захищеність керуючої площини мережі 5G.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Завадостійкість та інформаційна безпека інфокомунікацій» забезпечений необхідною навчально-методичною літературою. Зокрема, викладачами кафедри підготовлені і видані такі роботи:

1. Бойко Ю. М. Завадостійкість та інформаційна безпека інфокомунікацій : конспект лекцій з дисципліни для здобувачів другого (магістерського) рівня вищої освіти / Ю. М. Бойко, Л. В. Карпова. – Хмельницький : ХНУ, 2024. – 111 с.
2. Шинкарук О. М. Основи функціонування багатоканальних систем передачі інформації : навч. посіб. / О. М. Шинкарук, Ю. М. Бойко, І. І. Чесановський. – Хмельницький : ХНУ, 2011. – 231 с.

12. Матеріально-технічне та програмне забезпечення дисципліни

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office, MATLAB, EWB (Multisim) або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

13. Рекомендована література

Основна

1. Бойко Ю. М. Завадостійкість та інформаційна безпека інфокомунікацій : конспект лекцій з дисципліни для здобувачів другого (магістерського) рівня вищої освіти / Ю. М. Бойко, Л. В. Карпова. – Хмельницький : ХНУ, 2024. – 111 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с.
3. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. – Київ : Логос, 2018. – 227 с.
4. Науково-прикладні питання забезпечення роздільної здатності і ефективності обробки сигналів у радіотехнічних та телекомунікаційних системах за наявності завад : монографія / Ю. М. Бойко, О. М. Шинкарук, Л. В. Карпова, І. І. Чесановський. – Хмельницький : ХНУ, 2019. – 218 с.

5. Проектування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало та ін. – Львів : Вид-во Львівської політехніки, 2020. – 320 с.
6. Buriachok V. L. Methods of information protection in telecommunication systems : manual / V. L. Buriachok, Ie. V. Duravkin, N. V. Lukova-Chuyko, P. M. Skladanniy. – Kyiv : KUBG, 2019. – 74 p.
7. Сучасні технології інфокомунікаційних та комп'ютерних мереж : монографія / А. І. Семенко, Ю. М. Бойко, О. М. Шпур та ін. ; за заг. ред. А. І. Семенка. – Київ : Європейський університет, 2024. – 557 с.
8. Бойко Ю. Аналіз алгоритмів декодування LDPC та Polar-кодів у стандарті 5G: оцінка складності та ефективності / Ю. Бойко, Д. Суберляк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2025. – № 3. – С. 226–236.
9. Бойко Ю. Легкі криптосистеми в телекомунікаційних середовищах IoT і 5G: виклики, архітектури та компроміси безпеки / Ю. Бойко, В. Мішан, Д. Явтушенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2025. – № 3. – С. 265–275.
10. Boiko J. Intelligent DRL-assisted decoding of error-correcting codes for 5G/6G telecommunication channels / J. Boiko, I. Pyatin, O. Eromenko // Journal of Electrical Engineering. – 2025. – Vol. 76, No. 6. – P. 509–523.
11. Boiko J. Neural Network-Based Secure Beam Management in 5G Networks for Cyberspace Protection / J. Boiko, I. Pyatin // CEUR Workshop Proceedings. – 2025. – Vol. 4170. – P. 1–15.
12. 3GPP TS 38.212. NR; Multiplexing and channel coding : технічна специфікація / 3rd Generation Partnership Project, 2024.
13. 3GPP TS 33.501. Security architecture and procedures for 5G System : технічна специфікація / 3rd Generation Partnership Project, 2024.

Додаткова

1. Богуш В. М. Технічний захист інформації : навч. посіб. / В. М. Богуш, В. Д. Бровко, О. С. Кобус, В. Д. Козюра. – Київ : Ліра-К, 2022. – 508 с.
2. Інформаційна безпека : підручник / за ред. Ю. Я. Бобала та І. В. Горбатого. – Львів : Вид-во Львівської політехніки, 2019. – 580 с.
3. Когут Ю. Корпоративна безпека / Ю. Когут. – Київ : КК Сідкон, 2018. – 276 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – Київ : ДУТ–КНУ, 2016. – 178 с.
5. Freeman R. L. Telecommunication System Engineering. 4th ed. / R. L. Freeman. – Wiley, 2015. – 1024 p.
6. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник / В. Л. Бурячок, С. В. Толюпа, А. О. Аносов та ін. – Київ : ДУТ, 2015. – 345 с.
7. Вакалюк Т. А. Захист інформації в комп'ютерних системах : навч.-метод. посіб. / Т. А. Вакалюк. – Житомир : Вид-во ЖДУ, 2013. – 136 с.
8. Комплексні системи захисту інформації : навч. посіб. / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Вінниця : ВНТУ, 2018. – 118 с.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL: <https://msn.khmnu.edu.ua/course/view.php?id=7972>
2. Електронна бібліотека ХНУ. URL: <https://library.khmnu.edu.ua/>
3. Інституційний репозитарій ХНУ. URL: <https://elar.khmnu.edu.ua/home>

ЗАВАДОСТІЙКІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОКОМУНІКАЦІЙ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	Перший
Кількість призначених кредитів ЄКТС	5,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни здобувач повинен: розуміти загальні принципи організації безпекових та інших аспектів функціонування телекомунікаційних та інформаційно-комунікаційних систем, локалізувати та оцінювати стан проблемної ситуації на етапах дослідження інформаційної безпеки телекомунікаційних систем, їх проєктування, модернізації, впровадження та експлуатації, а також формулювати пропозиції щодо її вирішення з усуненням виявлених недоліків; забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних та радіотехнічних систем в умовах інформаційних загроз; розуміти концептуальні засади та таксономію функцій щодо методів технічного захисту інформації та криптографічних методів захисту інформації; володіти навичками застосування нормативних вітчизняних і міжнародних документів (стандартів) з оцінювання захищеності інформації; опанувати апаратні та програмні засоби захисту і принципи супроводження комплексної системи захисту інформації.

Зміст навчальної дисципліни. Забезпечення захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах; методика підвищення завадостійкості телекомунікаційних систем; теоретичні засади захисту інформації, методи криптографічного захисту інформації; загрози безпеці інформації в програмному забезпеченні; апаратне забезпечення засобів захисту інформації; методи та засоби блокування технічних каналів витоку інформації; методики оцінювання захищеності інформації, стандарти та критерії безпеки інформаційних технологій; модель загроз та класифікація атак у середовищі IoT і 5G; вимоги до криптографії IoT/5G та легкі криптоалгоритми; стек безпеки 5G (NAS, AS, Transport) та ієрархія ключів; завадостійке кодування у мережах 5G NR (структура каналу PDSCCH, LDPC та полярні коди, механізм HARQ); інтелектуалізовані процедури декодування і керування променями.

Пререквізити: вихідна.

Постреквізити: моделювання і оптимізація радіотехнічних засобів електронних комунікацій; моделювання і оптимізація радіотехнічних засобів електронних комунікацій (курсова робота); системний аналіз інформаційно-комунікаційних систем та мереж; переддипломна практика; кваліфікаційна робота.

Запланована навчальна діяльність: лекції 16 год., лабораторні заняття 16 год., практичні заняття 18 год., самостійна робота 100 год.; разом 150 год. Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції з використанням мультимедійних презентацій, методів візуалізації, пояснення, проблемного й інтерактивного навчання; практичні заняття: бесіда, інструктування, демонстрування, розв'язування ситуаційних завдань; лабораторні заняття з використанням методів комп'ютерного моделювання, проєктної діяльності, аналізу проблемних ситуацій, дискусії; самостійна робота з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання роботи на практичних заняттях, захист лабораторних робіт, контрольна робота, іспит.

Вид семестрового контролю: іспит – 1 семестр.

Навчальні ресурси:

1. Бойко Ю. М. Завадостійкість та інформаційна безпека інфокомунікацій : конспект лекцій з дисципліни для здобувачів другого (магістерського) рівня вищої освіти / Ю. М. Бойко, Л. В. Карпова. – Хмельницький : ХНУ, 2024. – 111 с.
2. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПП ім. Ігоря Сікорського. – Київ : КПП ім. Ігоря Сікорського, 2021. – 213 с.
3. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. – Київ : Логос, 2018. – 227 с.
4. Науково-прикладні питання забезпечення роздільної здатності і ефективності обробки сигналів у радіотехнічних та телекомунікаційних системах за наявності завад : монографія / Ю. М. Бойко, О. М. Шинкарук, Л. В. Карпова, І. І. Чесановський. – Хмельницький : ХНУ, 2019. – 218 с.
5. Проєктування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало та ін. – Львів : Вид-во Львівської політехніки, 2020. – 320 с.
6. Buriachok V. L. Methods of information protection in telecommunication systems : manual / V. L. Buriachok, Ie. V. Duravkin, N. V. Lukova-Chuyko, P. M. Skladanniy. – Kyiv : KUBG, 2019. – 74 p.
7. Сучасні технології інфокомунікаційних та комп'ютерних мереж : монографія / А. І. Семенко, Ю. М. Бойко, О. М. Шпур та ін. ; за заг. ред. А. І. Семенка. – Київ : Європейський університет, 2024. – 557 с.
8. Бойко Ю. Аналіз алгоритмів декодування LDPC та Polar-кодів у стандарті 5G: оцінка складності та ефективності / Ю. Бойко, Д. Суберляк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2025. – № 3. – С. 226–236.
9. Бойко Ю. Легкі криптосистеми в телекомунікаційних середовищах IoT і 5G: виклики, архітектури та компроміси безпеки / Ю. Бойко, В. Мішан, Д. Явтушенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2025. – № 3. – С. 265–275.
10. Boiko J. Intelligent DRL-assisted decoding of error-correcting codes for 5G/6G telecommunication channels / J. Boiko, I. Pyatin, O. Eromenko // Journal of Electrical Engineering. – 2025. – Vol. 76, No. 6. – P. 509–523.
11. Boiko J. Neural Network-Based Secure Beam Management in 5G Networks for Cyberspace Protection / J. Boiko, I. Pyatin // CEUR Workshop Proceedings. – 2025. – Vol. 4170. – P. 1–15.
12. 3GPP TS 38.212. NR; Multiplexing and channel coding : технічна специфікація / 3rd Generation Partnership Project, 2024.
13. 3GPP TS 33.501. Security architecture and procedures for 5G System : технічна специфікація / 3rd Generation Partnership Project, 2024.
14. Модульне середовище для навчання. URL: <https://msn.khmnu.edu.ua/course/view.php?id=7972>
15. Електронна бібліотека ХНУ. URL: <https://library.khmnu.edu.ua/>

Викладач: д-р техн. наук, професор Юлія БОЙКО