ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

01 вересня 2025 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				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
ДФН	1	1	5,0	150	50	16	18	16	-	100	-	-	-	+
Разом ДФН			**5,0**	**150**	**50**	**16**	**18**	**16**	**-**	**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 _____ д-р. техн. наук, професор Юлій БОЙКО
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Телекомунікацій, медійних та інтелектуальних технологій

Протокол №1 від 28.08.2025 р. Зав. кафедри _____ Сергій ПІДЧЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

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 із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів другого (магістерського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Електронні системи та мережі комунікацій» в 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.08), Кваліфікаційна робота (ОФП.08).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** здатність розв'язувати задачі дослідницького та/або інноваційного характеру у 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 пропускної 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 сферах інформаційно-комунікаційних мереж, електронних комунікацій, радіотехнічних систем, технологій, приладів і їх компонентів. (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 проєкти, враховуючі 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 надання студентам знань, навиків та умінь, 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 та спеціальних 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. Студент, 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 принципи супроводження комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	Денна форма навчання			
	Лекції	**Лабор. роботи**	**Практ.**	**СРС**
Тема1. 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.	3	2	4	14
Тема 3. Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	3	4	4	15
Тема 4. Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах.	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	4	14
Тема 7. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій	2	4	-	14
Разом за семестр	**16**	**18**	**16**	**100**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Забезпечення захисту інформації в інформаційно-комунікаційних та телекомунікаційних системах.	**2**
1	**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. Літ.: [1] с. 6….21; [3] с. 17….31.	2
	Тема 2. Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях.	**3**
2	**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 підвищення завадостійкості електронних комунікацій. Канальне кодування. Літ.: [1] с. 22….50; [4] с. 7-55; [8] с. 140…205	3
	Тема 3. Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	**3**
3	**Сервісні та функціональні засоби безпеки та механізми їх реалізації.** Автентифікація, ідентифікація та керування доступом в контексті забезпечення цілісності системи. Криптографічні системи. Технології шифрування, теорія, алгоритми, криптографічні підсистеми. Літ.: [1] с. 25….44; [2] с. 74….156.	3
	Тема 4. Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах.	**2**
4	**Помилки програмної реалізації систем.** Облік вад захисту в залежності від розміщення їх 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…..148; [3] с. 4414….432	2
	Тема 5. Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах..	**2**
5	**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. 399…..342; [3] с. 124….148	2
	Тема 6. Методи та засоби блокування технічних каналів витоку інформації.	**2**
6	**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 по технічних каналах, утворених допоміжними технічними засобами, звукозаписувальними та оптичними пристроями. Літ.: [1] с. 84-96; [3] с. 124-139	2
	Тема 7. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій.	**2**
7	**Інформаційна безпека як складова національної безпеки.** Стандартизація та специфікація вимог захисту інформації в системах. Критериальні ознаки оцінювання захищеності інфокомунікаційних систем. Концепція профілю захисту. Розгляд напрямів призначення стандартів інформаційної безпеки. Література: [1] с. 99 ……..103; [3] с. 371…..392.	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.	2
5	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	**16**

5.3 Зміст лабораторних занять

№ п/п	Теми лабораторних занять	Кількість годин
1	Лаб. роб. №1 Ознайомлення з інструментами по захисту інформації у MS Word	2
2	Лаб. роб. №2 Дослідження завадостійкості широкосмугових телекомунікаційних каналів засобами Matlab/Simulink	4
3	Лаб. роб. №3 Визначення пропускної здатності каналів передачі інформації	2
4	Лаб. роб. № 4 Ознайомлення з поняттям захисту інформації та інформаційної безпеки. Визначення критеріїв та аспектів захисту при оцінці інформаційної безпеки	2
5	Лаб. роб. № 5 Принципи захисту інформації на основі генератора шуму Базальт - 5 ГЭШ	2
6	Лаб. роб. № 6 Використання радіолокаційної станції ПСНР-1 для захисту інформації та визначення дальності до цілі	2
7	Лаб. роб. № 7 Ознайомлення з засобами технічного захисту інформації	4
	Разом за семестр	**18**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до практичних занять, контрольних робіт, тестування, виконанні індивідуальних завдань тощо. Крім цього до послуг студентів 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 (ЛЗ), підготовка до практичного заняття ПЗ 1, виконання ІДЗ	12
3,4	Опрацювання теоретичного матеріалу з Т2. Підготовка до лабораторного заняття, виконання ІДЗ	12
5,6	Опрацювання теоретичного матеріалу з Т3. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 2,3, виконання ІДЗ	12
7,8	Підготовка до контрольної роботи з Т1-3 (КР). Підготовка до тестового контролю з ТК 1, виконання ІДЗ	12
9,10	Опрацювання теоретичного матеріалу з Т4. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 4, виконання ІДЗ	12
11,12	Опрацювання теоретичного матеріалу з Т5. Підготовка до тестового контролю з Т 2, виконання ІДЗ	10
13,14	Опрацювання теоретичного матеріалу з Т6. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 5, виконання ІДЗ	10
15,16	Підготовка до практичного заняття ПЗ 6. Підготовка до контрольної роботи з Т7, виконання ІДЗ	10
17	Підготовка до тестового контролю з Т 2. Підготовка до лабораторного заняття, підготовка до практичного заняття ПЗ 7, виконання ІДЗ	10
	Разом за семестр:	**100**

***Примітки*:** Т – тема навчальної дисципліни, КР– контрольна робота, ТК – тестовий контроль, КР – контрольна робота, ІДЗ - індивідуальне завдання

На самостійне опрацювання студентів виносяться визначені у робочій програмі індивідуальні домашні завдання (ІДЗ) з відповідних тем. Керівництво самостійною роботою та контроль за виконанням індивідуального завдання здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

Вимоги до виконання індивідуального домашнього завдання викладені в робочій програмі навчальної дисципліни.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та 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, презентацій; лабораторні заняття: з використанням методів комп’ютерного моделювання, методів проєктної діяльності, аналіз проблемних ситуацій, пояснення, дискусія; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), 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, встановлених робочою програмою і графіком освітнього процесу, в т.ч. 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 у обговоренні ситуацій);

- усне опитування перед допуском до лабораторного заняття;
- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу з розділу;
- захист індивідуальних завдань;
- оцінювання результатів виконання домашніх завдань;
- оцінювання контрольних робіт.

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 (60 відсотків і більше від максимального балу) 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, встановленим 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, що передбачені 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 відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до практичних занять (вивчення теоретичного матеріалу з теми), активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач тощо. Також до лабораторного заняття (вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, якісно підготувати звіт (протокол роботи відповідно до теми), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо.

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 студент захистив її на наступному після виконання роботи занятті. Пропущене практичне (лабораторне)заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять, тестування й виконання індивідуального домашнього завдання та контрольної роботи. Виконання індивідуального завдання завершується його здачею на перевірку у терміни, встановлені графіком самостійної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із 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 (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

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 формування 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 студентів 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 йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у 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 (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–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, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–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. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
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. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

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

Аудиторна робота			**Контрольні заходи**								**Семестровий контроль**	**Разом**
Практичні заняття (1, 4, 7)			Лабораторні роботи №:1-7							Контрольна робота КР	**Іспит**	Сума балів
1	2	3	1	2	3	4	5	6	7	1		
Кількість балів за вид навчальної роботи (мінімум-максимум)												
3-5			3-5	3-5	3-5	3-5	3-5	3-5	3-5	6-10	24-40	**60-100***
9-15			**21-35**							**6-10**	**24-40**	

Оцінювання на практичних заняттях

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; вільне володіння студентом математичною термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач; результати самостійних робіт.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями визначено, що 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 із використанням спеціалізованих програм, що дозволяють моделювати, аналізувати та досліджувати відповідні технічні процеси.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання контрольної роботи

Контрольна робота передбачає виконання трьох завдань (практичне завдання передбачає розв'язування задач з даної теми). При оцінюванні контрольної роботи враховуються: повнота відповіді та якість виконання. Загальна сума балів на позитивну оцінку становить від 6 до 10.

Розподіл балів при оцінюванні завдань контрольної роботи

Кількість правильних відповідей	1	2	3
Відсоток правильних відповідей	**0-60**		**40**
Кількість отриманих балів	6		4

При отриманні негативної оцінки контрольну роботу слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів виконання індивідуального домашнього завдання

Виконане та оформлене відповідно до вимог, визначених методичними рекомендаціями, індивідуальне домашнє завдання (ІДЗ) комплексно оцінюється викладачем з урахуванням таких критеріїв: самостійність виконання; правильність розв'язання поставлених задач; обґрунтованість вибору методів розв'язання; повнота пояснень та аргументованість відповідей; якість оформлення та дотримання вимог до структури і змісту роботи.

Результат виконання здобувачем вищої освіти кожного ІДЗ оцінюється відповідно до таблиці **Критеріїв оцінювання навчальних досягнень здобувача вищої освіти** з урахуванням рівня досягнення запланованих програмних результатів навчання та сформованих компетентностей. За підсумками захисту присвоюється відповідна сума балів (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

У разі, якщо здобувач вищої освіти виявив рівень знань і виконання ІДЗ, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку доопрацьоване ІДЗ у терміни, погоджені з викладачем.

Оцінювання результатів тестового контролю

Тест 1(2) (ТК1, 2) складається з 40 питань, що охоплюють основні теми дисципліни «Завадостійкість та інформаційна безпека інфокомунікацій». Тест поділяється на дві частини: перша частина — до першої атестації, друга частина — після першої атестації та до підсумкової атестації. Студентам надається 2 спроби для проходження тесту. Після кожної спроби вони отримують зворотний зв'язок з викладачем або навчальним та довідковим матеріалом з дисциаліни розміщеним в модульному середовищі - https://msn.khmnu.edu.ua/course/view.php?id=7972)) щодо своїх помилок, щоб мати змогу виправити знання перед наступною спробою. Для успішного проходження тесту студент повинен набрати не менше ніж 70% правильних відповідей (28 правильних відповідей з 40). У разі невдалого проходження тесту після двох спроб студенту надається додатковий час для усунення помилок і повторного складання тесту.

Критерії оцінювання.

Оцінка тесту здійснюється за 4-бальною шкалою, з урахуванням процентного співвідношення правильних відповідей: - менше 70% правильних відповідей (0-27 правильних відповідей) — 2 бали (Незадовільно). Студент має значні прогалини в знаннях і потребує додаткової роботи. - 70-79% правильних відповідей (28-31 правильна відповідь) — 3 бали (Задовільно). Студент володіє базовими знаннями, але допустив кілька помилок. - 80-89% правильних відповідей (32-35 правильних відповідей) — 4 бали (Добре). Студент продемонстрував хороші знання, але є незначні недоліки. - 90-100% правильних відповідей (36-40 правильних відповідей) — 5 балів (Відмінно). Студент має відмінні знання дисципліни та правильно відповідає на більшість питань.

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 з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	Для кожного окремого виду завдань		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	3	4	5
Теоретичне питання № 2	3	4	5
Практичне завдання (задача)	18	24	30
Разом:	**24**		**40**

***Примітка*. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.**

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

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. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="4">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="3">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td></tr>
<tr><td>E</td><td>60-65</td><td>Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

10. Орієнтована тематика індивідуального завдання з курсу

1. Телекомунікаційні системи передачі інформації із завадостійким кодуванням
2. Телекомунікаційні системи передачі інформації з криптографічним захистом інформації
3. Захищені системи диспетчеризації та моніторингу рухомих об'єктів на основі використання можливостей GSM та GPS.
4. Захищені системи супутникового доступу до мережі Інтернет
5. Захищені персональної мережі радіодоступу на основі стандартів Bluetooth/ IEEE 802.15.4/ Ad Hoc.
6. Захищені безпроводові локальні мережі на основі стандартів IEEE 802.11 (Wi-Fi)
7. Захищені системи мобільного цифрового потокового IP-телебачення.
8. Захищені міські мережі широкосмугового радіодоступу на основи стандартів (WiMAX, LTE, MIMO)
9. Апаратно-програмні комплекси стиснення відеоінформації на базі алгоритму JPEG та віртуального середовища MATLAB
10. Методи побудови захищених систем електронної комерції та білінгу.
11. Технології захисту інформації у корпоративних мережах великих державних та комерційних організацій з використання програмно-апаратних засобів.
12. Методики побудови захищених мереж на базі технології VIPNet
13. Апаратно-програмні комплекси для вимірювання характеристик мобільних мереж радіодоступу на базі апаратури та програмного забезпечення
14. Закриті та/або скритні системи супутникового зв'язку з використанням розширення спектру методом псевдовипадкової перебудови робочої частоти
15. Захищені цифрові транкінгові системи радіозв'язку на основі стандарту (APCO25, EDACS, Tetrapol, TETRA)

Рекомендований обсяг текстового документа, що готується студентом у процесі виконання індивідуального завдання 20-30 сторінок машинописного тексту формату А4. Для більшої наочності рекомендується широко використовувати таблиці та графічний матеріал – графіки, діаграми з обов’язковими поясненнями до них. Оформлення згідно вимог стандартів Хмельницького національного університету:

- Текстові документи. Загальні вимоги СОУ 207.01:2017/Ю.М. Бойко, Г.В. Красильнікова, Л.І. Першина, Т.Ф. Косянчук. т- Хмельницький : ХНУ, 2017. - 45 с.;
- Бібліографічний запис. Загальні вимоги та правила складання. СОУ 207.02:2017 /Ю.М. Бойко, Л.І. Першина. Хмельницький: ХНУ, 2017. - 37 с.

11. Питання для самоконтролю результатів навчання

1. Які з наявних 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 Хемінга.
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. В чому ідея шифрів підстановки.
19. В чому ідея шифрів перестановки.
20. Яка відміна моноалфавітних шифрів від поліалфівітних.
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. Визначити можливості і недоліки використовуваного брандмауера.
25. Що таке ідентифікація користувачів.
26. Які види ідентифікації вам відомі.
27. Що таке парольна ідентифікація.
28. Що таке аутентифікація 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 оцінці 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 у підвищення завадостійкості електронних комунікацій. Канальне кодування.

12. Навчально-методичне забезпечення

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

1. 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.
2. Шинкарук О.М. Основи функціонування багатоканальних систем передачі інформації. навч. посібник /О.М. Шинкарук, Ю.М. Бойко, І.І. Чесановський. – Хмельницький: ХНУ, 2011. – 231 с.
3. Семенко А.І. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / А.І. Семенко, Ю.М. Бойко, О.М. Шпур, І. В. Стрелковська, В. В. Корчинський, Р. О. Яровий ; під заг. ред. А.І.Семенка. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024.- 557 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. Бойко Ю.М. Програмно-конфігуровані системи передавання, приймання та обробки інформації: монографія /Ю. М. Бойко, Л. В. Карпова, О.І. Полікаровських, В.П. Ткачук. – Хмельницький : ХНУ, 2023. – 317с.
6. Бойко Ю.М. Основи радіофотоніки: навч. посіб. Частина 1 / Ю.М. Бойко, В.А. Дружинін, М.П. Трембовецький, М.І. Рєзніков. – Київ : Каравела, 2020. – 184 с.

13. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

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.

14. Рекомендована література:

Основна

1. Бойко Ю.М. Завадостійкість та інформаційна безпека інфокомунікацій : конспект лекцій з дисципліни для здобувачів другого (магістерського) рівня вищої освіти спеціальності 172 «Електронні комунікації та радіо- техніка» / Ю. М. Бойко, Л. В. Карпова. Хмельницький : ХНУ, 2024. 111 с.

2. Остапов С. Технології захисту інформації: посібник / С. Остапов, С.П. Євсеєв, О.Г. Король. – Київ : Родовід, 2014. – 428 с.

3. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,23 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с. – Назва з екрана.

4. 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.

5. Бойко Ю.М. 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.

6. Хорошко В. О. Проєктування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. – Львів : Видавництво Львівської політехніки, 2020. - 320 с.

7. Buriachok V.L. Methods of information protection in telecommunication systems:[manual]. / V.L.Buriachok, Ie.V.Duravkin, N.V. Lukova-Chuyko, P.M.Skladanniy / – Kiev :KUBG, 2019. – 74 с.

8. 3. Семенко А.І. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / А.І. Семенко, Ю.М. Бойко, О.М. Шпур, І. В. Стрелковська, В. В. Корчинський, Р. О. Яровий ; під заг. ред. А.І.Семенка. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024.- 557 с.

Додаткова

1. Богуш В.М. Технічний захист інформації. навч. посіб. / В.М. Богуш, В.Д. Бровко, О.С. Кобус, В.Д. Козюра. - Ліра-К, 2022. – 508 с.

2. Інформаційна безпека : підручник / За ред. Ю. Я. Бобала та І. В. Горбатого. - Видавництво: Львівська політехніка, 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, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – Київ : ДУТ - КНУ, 2016. – 178 с.

5. Хорошко В. О. Проєктування комплексних систем захисту інформації / В. О. Хорошко. - Видавництво: Львівська політехніка, 2020. – 320 с.

6. Freeman R. L. Telecommunication System Engineering, 4th Edition / R. L. Freeman. – Wiley, 2015. – 1024 p.

7. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

8. Вакалюк Т.А. Захист інформації в комп'ютерних системах: навчально-методичний посібник / Т.А. Вакалюк. - Житомир: Вид-во ЖДУ, 2013. – 136 с.

9. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2018. – 118 с.

15. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=7972
2. Електронна бібліотека ХНУ. URL: http://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 студент 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 принципи супроводження комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.

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 в телекомунікаційних і інформаційно-комунікаційних системах; загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах; апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах; методи та засоби блокування технічних каналів витоку інформації; методики оцінювання захищеності інформації, стандарти та критерії безпеки інформаційних технологій.
Пререквізити: вихідна.

Кореквізити: 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: 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, інформаційно-комунікаційних технологій, інтенсифікації та індивідуалізації навчання; практичні заняття: бесіда, інструктування, демонстрування, розв'язування ситуаційних завдань, презентацій; лабораторні заняття: з використанням методів комп'ютерного моделювання, методів проєктної діяльності, аналіз проблемних ситуацій, пояснення, дискусія; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання

Форми оцінювання результатів навчання: оцінювання лабораторних, практичних та контрольних робіт; виконання індивідуального завдання; тестування.

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 спеціальності 172 «Електронні комунікації та радіо- техніка» / Ю. М. Бойко, Л. В. Карпова. Хмельницький : ХНУ, 2024. 111 с.
2. Остапов С. Технології захисту інформації: посібник / С. Остапов, С.П. Євсеєв, О.Г. Король. – Київ : Родовід, 2014. – 428 с.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навчальний посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,23 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 213 с. – Назва з екрана.
4. 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.
5. Бойко Ю.М. 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.
6. Хорошко В. О. Проєктування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. – Львів : Видавництво Львівської політехніки, 2020. - 320 с.
7. Buriachok V.L. Methods of information protection in telecommunication systems:[manual]. / V.L.Buriachok, Ie.V.Duravkin, N.V. Lukova-Chuyko, P.M.Skladanniy / – Kiev :KUBG, 2019. – 74 с.
8. Семенко А.І. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / А.І. Семенко, Ю.М. Бойко, О.М. Шпур, І. В. Стрелковська, В. В. Корчинський, Р. О. Яровий ; під заг. ред. А.І.Семенка. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024.- 557 с.
9. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=7972
10. Електронна бібліотека ХНУ. Доступ до ресурсу: http://library.khmnu.edu.ua/

Викладач: д-р. техн. н., професор Юлій БОЙКО