

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ



Декан факультету інформаційних технологій

Тетяна ГОВОРУЩЕНКО

Ім'я, прізвище

2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в телекомунікаційних системах та мережах

Назва дисципліни

Призначення Робочої програми

Для освітніх програм різних спеціальностей

Рівень вищої освіти

Перший (бакалаврський)

Мова навчання

Українська

Обсяг дисципліни, кредитів ЕКТС

8

Статус дисципліни

Вибіркова

Факультет

Інформаційних технологій

Кафедра

Телекомунікацій, медійних та інтелектуальних технологій

Форма здобуття освіти	Обсяг дисципліни		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота (в т.ч. ІРС)	Залік
	Кредити ЕКТС	Години	Разом	Лекції	Лабораторні і роботи	Практичні заняття	Семінарські заняття		
Д	8	240	82	32	32	18		158	+

Робоча програма складена на основі освітніх програм підготовки бакалавра.

Робоча програма складена

канд. тех. наук, доцент Олег ПИВОВАР

Науковий ступінь, вчене звання, ім'я, прізвище

Схвалена на засіданні кафедри Телекомунікацій, медійних та інтелектуальних технологій

Назва

Протокол від 28.08 2025 № 1.

Зав. кафедри ТМІТ

Сергій ПІДЧЕНКО

Ім'я, прізвище

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, д-р. техн. н., проф.	Телекомунікацій, медійних та інтелектуальних технологій	_____	Сергій ПІДЧЕНКО
Гарант освітньо-професійної програми, к. техн. н., доц.	Телекомунікацій, медійних та інтелектуальних технологій		Олег ПИВОВАР

3. Пояснювальна записка

Дисципліна «Захист інформації в телекомунікаційних системах та мережах» є однією із важливих фахових вибіркових дисциплін підготовки бакалаврів.

Мета дисципліни. Формування особистості фахівця здатного вирішувати питання виявлення загроз та захисту інформації від несанкціонованого доступу в телекомунікаційних системах та мережах із застосуванням інформаційно-комп'ютерних технологій.

Предмет дисципліни. Теоретичні основи радіоелектронної розвідки, радіоелектронної боротьби, прихованості дії, шифрування та комплексу організаційних заходів для захисту інформації в телекомунікаційних системах та мережах.

Завдання дисципліни. Формування у здобувачів необхідного обсягу знань та умінь щодо безпекових аспектів функціонування телекомунікаційних систем та мереж; методи та методики підвищення стійкості електронних комунікацій до несанкціонованого доступу; технології організації безпеки в спільних програмних середовищах; методи дослідження можливих каналів витоку інформації; методи та методики забезпечення прихованості дії в умовах радіоелектронної боротьби; алгоритми шифрування та криптографічного захисту; розробка комплексу рекомендацій щодо організації підсистеми захисту інформації телекомунікаційного апаратно-програмного устаткування.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вміло використовувати понятійний апарат прихованості дії та захисту інформації від несанкціонованого доступу в цифрових та аналогових каналах електронних комунікацій; проводити аналіз вразливостей діючих систем зв'язку; виконувати розрахунки параметрів телекомунікаційних засобів із метою мінімізації можливостей щодо несанкціонованого витоку інформації; розробляти методи тики організаційного забезпечення захисту інформації в програмному середовищі протокольної взаємодії багатокоритувацьких телекомунікаційних систем та мереж на рівні ідентифікації, аутентифікації та арбітражу; обґрунтовано обирати системи шифрування для забезпечення заданого рівня захисту телекомунікаційних систем та мереж.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	Денна та скорочена форма			
	Лекції	Лабораторні роботи	Практичні роботи	Самостійна робота Здобувачів
Тема 1. Електромагнітна сумісність та канали витоку інформації	8	8	6	38
Тема 2. Радіоелектронна розвідка та радіоелектронна боротьба	8	8	4	40
Тема 3. Аналогові та цифрові алгоритми шифрування	8	8	4	40
Тема 4. Перспективні технології та оцінювання захисту інформації	8	8	4	40
Разом за семестр:	32	32	18	158

5 Програма навчальної дисципліни

5.1. Зміст лекційного курсу*

Но мер лек ції	Перелік тем лекцій та їх анотації	Кіль кість годи н
	Тема 1. Електромагнітна сумісність та канали витоку інформації	
1	Завдання захисту інформації. Окреслення загроз захисту інформації та їх класифікації. Поняття та параметри електромагнітної сумісності. Літ.: [1] с.30,42, 71-74; [2] с.9-15, [3] с. 21-35	2
2	Канали витоку інформації телекомунікаційних систем та оцінювання рівня ризику . Літ.: [1] с.32-39; [2] с.21-30; [3] с. 35-39	2
3	Методи та методики забезпечення електромагнітної сумісності. Літ.: [1] с.277-308; [2] с.31-40, 168-185; [3] с.23-34	2
4	Забезпечення стійкості телекомунікаційних систем до імпульсних та квазігармонічних завад Літ.: [1] с.41-52; [2] с.39-49	2
	Тема 2. Радіoeлектронна розвідка та радіoeлектронна боротьба	
5	Поняття та класифікація радіoeлектронної розвідки. Енергетичні рівняння радіoeлектронної розвідки. Літ.: [1] с.104-107; [2] с.52-63	2
6	Стійкість телекомунікаційних систем до завад подібних до сигналу. Методи забезпечення прихованості дії високошвидкісних каналів. Літ.: [1] с.113-127; [2] с.72-78	2
7	Радіoeлектронна боротьба та радіoeлектронна протидія. Детектори шумових випромінювань. Радіотеплолокатори. Нелінійні локатори. Літ.: [1] с.122-127, [2] с.41-78, [3] с.61-65	2
8	Генерація імітаційних та маскуючих завад в умовах радіoeлектронної боротьби. Літ.: [1] с.148-164, [2] с.30-41, [3] с.133-142	2
	Тема 3. Аналогові та цифрові алгоритми шифрування	
9	Основні поняття криптографічного захисту. Властивості шифрів. Ключі шифрування. . Літ: [1] с.91-104 , [2] с.30-41; [3] с.112-133,207-214	2
10	Апаратні та апаратно-програмні засоби забезпечення захисту від несанкціонованого доступу. Літ: [1] с.91-104 , [2] с.63-66; [3] с.232-237	2
11	Програмні протоколи шифрування. Симетричні та несиметричні алгоритми шифрування. Літ: [1] с.196-204 , [2] с.110-126	2
12	Алгоритми забезпечення захисту інтелектуальної власності. Цифрові підписи. Стеганографія. Скреблювання. Літ: [1] с.676-692 , [2] с.164-161	2
	Тема 4. Перспективні технології та оцінювання захисту інформації	
13	Стандартизація алгоритмів та систем захисту інформації в телекомунікаційних системах та мережах. Літ: [1] с.734-759 , [2] с.100-110; [3] с.67-87	2
14	Застосування сигналів детермінованого хаосу для побудови систем та мереж із підвищеним рівнем захисту від несанкціонованого доступу. Літ: [1] с.976-993 , [2] с.203-208; [3] с.216-229	2
15	Поняття квантових алгоритмів передачі інформації та квантових систем криптографічного захисту. Літ: [1] с.983-1005 , [2] с.152-156; [3] с.145-160	2
16	Організація захисту в програмних середовищах на базі алгоритмів ідентифікації, аутентифікації та арбітражу в сучасних комп'ютерних та телекомунікаційних мережах. Літ: [1] с.995-1016 , [2] с.219-222	2
Разом за семестр:		32

5.2 Зміст практичних занять

№ з/п	Тема практичного заняття	Кільк. годин
1	Стандарти та норми електромагнітної сумісності. Літ: [1] с.107-111 , [2] с.41-45, [3] с.35-45	2
2	Функціональна та схемотехнічна будова генераторів завад. . Літ.: [1] с.242-352; [2] с.23-47; [3] с.48-66	2
3	Розрахунок зон ураження завадою радіотехнічних та телекомунікаційних систем за енергетичними рівняннями Літ: [1] с.148-159 , [2] с.41-52	2
4	Розрахунки параметрів радіотеплолокаторів. Літ.: [1] с.211-227; [2] с.100-107; [3] с.46-49	2
5	Методики шифрування інформації методом заміни. [1] с.620-659; [2] с.142-144	2
6	Методики та алгоритми використання асиметричних шифрів даних. Літ.: [1] с.675-692; [2] с.144-161	2
7	Практичні питання застосування цифрових підписів . Літ.: [1] с.742-752; [2] с.78-87; [3] с.98-101	2
8	Можливості використання технології хаотичної обробки сигналів для завдань захисту інформації. Літ.: [1] с.148-159, 204-210; [2] с.185-203; [3] с.84-97	2
9	Можливості застосування квантових алгоритмів захисту та передачі інформації. Літ.: [1] с.734-740; [3] с.162-169	2
Разом за семестр:		18

5.3 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кільк. годин
1	Техніка безпеки. Методи використання радіовимірювальних приладів для аналізу ЕМС. Дослідження детекторів електромагнітного випромінювання радіочастотного діапазону. Літ: [1] с.107-111 , [2] с.41-45, [3] с.35-45	4
2	Дослідження параметрів аналогових генераторів електромагнітних завад . Літ: [1] с.148-159 , [2] с.41-52	4
3	Дослідження параметрів цифрових генераторів широкосмугових та імпульсних завад Літ.: [1] с.211-227; [2] с.100-107; [3] с.46-49	4
4	Дослідження ефективності захисту від радіочастотних завад сітчастими екранами. [1] с.620-659; [2] с.142-144	4
5	Застосування програмних алгоритмів симетричного шифрування та методів розподілу ключів шифрування. Літ.: [1] с.675-692; [2] с.144-161	4
6	Застосування програмних алгоритмів несиметричного шифрування та методів розподілу ключів шифрування. Літ.: [1] с.742-752; [2] с.78-87; [3] с.98-101	4
7	Застосування програмної реалізації електронного підпису та варіантів стеганографії. Літ.: [1] с.148-159, 204-210; [2] с.185-203; [3] с.84-97	4
8	Використання генераторів детермінованого хаосу для апаратно-програмної підтримки захисту інформації від несанкціонованого доступу. Літ.: [1] с.334-340; [3] с.162-169	4
Разом за семестр:		32

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

Самостійна робота здобувачів *денної (скороченої)* форми навчання полягає у опрацюванні щотижневого лекційного матеріалу, виконанні завдань підготовки до лабораторних та практичних робіт, виконанні домашніх завдань практичних робіт, підготовці до захисту лабораторних робіт, виконанні завдань із практичних робіт, виконанні

індивідуальних завдань, підготовці до проведення та проведення електронного тестування, підготовці до письмового бліц-тестування або до письмового або усного опитування, а також у підготовці до підсумкового контрольного заходу.

Номер тижня	Вид самостійної роботи	К-ть годин
1	Підготовка до опанування курсу, реєстрація в модульному середовищі (встановлення індивідуальних планів та графіку дистанційного навчання, графіку консультацій, способам взаємодії із викладачем), підготовка до лабораторної роботи 1, підготовка до проведення практичної роботи 1, підготовка до проведення електронного тестування 1	8
2	Вибір індивідуальних завдань та тем рефератів. Опрацювання матеріалів лекції 1, підготовка до проведення електронного тестування 1, захист лабораторних робіт 1, виконання домашніх завдань практичного заняття 1, тестовий контроль збереження знань Т1	10
3	Опрацювання матеріалів лекції 2, підготовка до лабораторної роботи 2, підготовка до практичної роботи 2, виконання індивідуальних завдань , підготовка до письмового опитування 1	10
4	Опрацювання матеріалу лекції 3, підготовка до лабораторної роботи 2, захист результатів виконання лабораторної роботи 2, захист домашніх завдань практичної роботи 2, виконання індивідуальних завдань , підготовка до письмового опитування 1	10
5	Опрацювання матеріалу лекції 4, підготовка до лабораторної роботи 3, захист результатів виконання лабораторної роботи 2, підготовка до проведення практичної роботи 3, виконання індивідуальних завдань , підготовка до проведення електронного тестування 2	10
6	Опрацювання матеріалів лекції 5, підготовка до лабораторної роботи 3, захист результатів виконання лабораторної роботи 3, захист домашніх завдань із практичної роботи 3, виконання індивідуальних завдань , підготовка до проведення електронного тестування 2, тестовий контроль Т2	10
7	Опрацювання матеріалів лекції 6, підготовка до лабораторної роботи 4, захист результатів виконання лабораторної роботи 3, підготовка до проведення практичної роботи 4, виконання індивідуальних завдань , підготовка до письмового опитування 2	10
8	Опрацювання матеріалів лекції 7, підготовка до лабораторної роботи 4, захист результатів виконання лабораторної роботи 4, захист результатів виконання домашнього завдання із практичної роботи 4, виконання індивідуальних завдань , підготовка до письмового опитування 2	10
9	Опрацювання матеріалів лекції 8, підготовка до лабораторної роботи 5, підготовка до проведення практичної роботи 5, підготовка до проміжної контрольної роботи,	10
10	Опрацювання матеріалів лекції 9, підготовка до лабораторної роботи 5, захист результатів виконання домашньої роботи із практичного заняття 5, виконання індивідуальних завдань , підготовка до проведення електронного тестування 3	10
11	Опрацювання матеріалів лекції 10, підготовка до лабораторної роботи 6, захист результатів виконання лабораторної роботи 6, підготовка до проведення практичної роботи 6, виконання індивідуальних завдань , підготовка до проведення електронного тестування 3, тестовий контроль Т3	10

12	Опрацювання матеріалів лекції 11, підготовка до лабораторних робіт 6, захист результатів лабораторної роботи 6, захист домашніх завдань практичної роботи 6, виконання індивідуальних завдань , підготовка до письмового опитування 3	10
13	Опрацювання матеріалів лекції 12, підготовка до лабораторних робіт 7, захист результатів лабораторної роботи 6, підготовка до проведення практичної роботи 7, виконання індивідуальних завдань , підготовка до письмового опитування 3	10
14	Опрацювання матеріалів лекції 13, підготовка до лабораторних робіт 7, захист результатів лабораторної роботи 7, захист домашніх завдань із практичної роботи 7, виконання індивідуальних завдань , підготовка до проведення електронного тестування 4	10
15	Опрацювання матеріалів лекції 14, підготовка до лабораторної роботи 8, захист результатів виконання лабораторної роботи 7, підготовка до проведення практичної роботи 8, виконання індивідуальних завдань , підготовка до проведення електронного тестування 4, підготовка до захисту індивідуальних завдань	10
16	Опрацювання матеріалів лекції 15, підготовка за захист результатів виконання лабораторної роботи 8, захист результатів виконання домашнього завдання із практичної роботи 8, виконання індивідуальних завдань , підготовка до проведення електронного тестування 4, підготовка до письмового опитування , підготовка до колоквиумів за результатами виконання завдань лабораторних та практичних робіт, тестовий контроль Т4	10
Разом за семестр:		158

6. Технології та методи навчання

Процес навчання з дисципліни базується як на застосуванні традиційних так і прогресивних технологій освітнього середовища. Прогресивними технологіями, що застосовано під час набуття вказаних вище компетенцій є застосування візуалізації лекційного матеріалу за допомогою мультимедійного контенту, динамічного та статичного наглядного матеріалу (демонстрація пристроїв та їх функціонування), електронних плакатів, навчальних фільмів, виконання віртуальних лабораторних робіт в середовищі МАТЛАБ, використання методів автоматизованих комплексних розрахунків, застосування комп'ютерних симуляцій під час виконання практичних та лабораторних робіт, опрацювання та оформлення результатів лабораторних та практичних робіт за допомогою офісних та спеціалізованих програм, проведення електронних аудиторних автоматичних письмових бліц-тестів із обмеженням у часі, проведення тестування (в тому числі і навчального тестування) у модульному середовищі за різними напрямками та компетенціями, опанування компетенцій на основі інформації з інтернет-ресурсів під час виконання індивідуальних завдань.

Традиційними технологіями освітнього середовища є: викладання лекційного матеріалу із застосуваннями візуалізації на дошці, виконання лабораторних робіт за допомогою типового вимірювального устаткування та спеціально розроблених лабораторних макетів, письмове та усне опитування під час поточного та підсумкового контролю, виконання індивідуальних завдань в рамках самостійної роботи.

7. Методи контролю

Завдяки виділенню достатнього часу на практичні та лабораторні заняття за навчальним планом, засоби поточного контролю реалізуються переважно в рамках виконання практичних та лабораторних робіт. Під час поточного контролю використовуються такі методи:

- усне опитування із теоретичного матеріалу завдання для підготовки до роботи перед допуском до лабораторного заняття;
- захист індивідуального письмового завдання для підготовки до лабораторної роботи;

- захист письмового домашнього завдання до підготовки до кожної практичної роботи;
- контроль якості оформлення звітів лабораторних робіт та відповідність його стандартам університету;
- усний захист за результатами підготовки та виконання лабораторної роботи;
- усне опитування за лекційним та практичним матеріалом під час проведення практичних робіт;
- контроль практичних навичок коректного використання лабораторного устаткування та метрологічних правил проведення вимірювання під час виконання лабораторних робіт;
- тестовий тематичний контроль (аудиторний, бліц-тест) теоретичного матеріалу у модульному середовищі під час виконання практичних робіт;
- презентація та захист індивідуальних завдань;
- захист тематичних рефератів;
- рівень допомоги у створенні та модернізації технічної бази лабораторії;
- письмове опитування (контрольна роботи) як засіб проміжного контролю опанування лекційного матеріалу.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами або тестами, 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 Здобувач захистив її на наступному після виконання роботи занятті. Пропущене практичне (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 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, 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 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 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.

Кількість балів, що отримує здобувач за *практичне заняття*, складається на основі врахування таких елементів:

- відповіді на поточні запитання із матеріалу, що пройдено, в тому числі на лекції;
- результати проходження тестів у модульному середовищі;
- рівень інтерактивної взаємодії із викладачем під час аудиторного заняття;
- рівень виконання домашніх, додаткових та самостійних завдань, рефератів;
- результати бліц-тестування.
- захист та оформлення результатів письмового виконання домашнього завдання практичної роботи;
- рівень опанування здобувачами методик розрахунків, оцінювання та оперативності виконання практичної роботи;
- рівень компетенцій у володінні здобувачем спеціальною термінологією і уміння професійно обґрунтувати отримані розрахункові результати;
- своєчасний захист практичних завдань.

Кількість балів, що отримує здобувач за *лабораторне заняття*, складається на основі врахування таких елементів:

- результати захисту та якість оформлення завдання для підготовки до лабораторної роботи;
- рівень опанування методів вимірювання та методик розрахунків під час виконання роботи;
- якість оформлення протоколу отриманих даних та форма представлення графічної та текстової частини лабораторної роботи;
- рівень компетенцій щодо використання спеціальної термінології, уміння професійно обґрунтувати отримані результати під час захисту лабораторної роботи;
- своєчасний захист лабораторної роботи.

Термін захисту лабораторної роботи та результатів практичної роботи вважається своєчасним, якщо здобувач оформив та захистив роботу на наступному після виконання роботи аудиторному занятті (не більше 2 тижнів). Пропущене аудиторне лабораторне або практичне заняття здобувач має відпрацювати в окремий, встановлений викладачем, термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до закінчення аудиторних занять

у семестрі.

Підсумковий контрольний захід (контрольна робота) виконується в письмовій формі під час останнього практичного заняття, або у вигляді комплексного тестування. Завдання підсумкової роботи включає в себе 2-4 теоретичних запитання та 1-2 практичних задачі, комплексне тестування вбирає в себе не менш як 40 тестових запитань, кожне із яких оцінюється одним балом.

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	Узагальнений зміст критерія оцінювання
Відмінно	Здобувач у повному обсязі опанував зміст та суть елемента навчання, легко орієнтується у розташуванні та взаємному зв'язку цього елемента із іншими компетенціями; має повні компетенції виконання методик вимірювання, представлення та використання результатів лабораторних та практичних робіт; спроможність аргументовано обґрунтовувати свої судження та представлення. Відмінна оцінка передбачає наявність компетенції коректного та лаконічного подання відповідей із використанням спеціальної термінології. Під час відповіді Здобувач проявляє творчу активність. Допускається наявність декількох несуттєвих помилок та обмовлень.
Добре	Здобувач виявив практично повне засвоєння змісту елемента навчального матеріалу, володіє понятійним апаратом; свідомо використовує набуті знання та компетенції для вирішення необхідних практичних задач; виклад відповіді коректний та загалом відповідає запитанню (умовам), але у змісті і формі відповіді можуть мати місце окремі помилки, неточності, нечіткі формулювання закономірностей, заміна та переплутування понять тощо. Творча активність Здобувача в рамках елемента обмежена.
Задовільно	Засвоєння змісту навчального матеріалу здобувачем знаходиться на мінімально достатньому рівні, він слабо володіє необхідними компетенціями та спеціальною термінологією, але рівень володіння понятійним апаратом достатній для подальшого навчання. Допускається наявність декількох принципових помилок та неточностей, які за умови конкретизованих або додаткових запитань викладача самостійно виправляються здобувачем, або здобувач вказує шляхи їх виправлення. Творча активність здобувача практично не проявляється.
Незадовільно	Здобувач виявив недостатній рівень знань та компетенцій з елемента навчання. Подальше продовження навчання з дисципліни можливо тільки за умови повторного опанування елемента навчання. Під час відповідей у Здобувача відсутня логічна організація відповіді, він допускає велику кількість помилок навіть під час визначення елементарних спеціальних понять, відсутні компетенції щодо виконання лабораторних та практичних робіт, творча активність не виявлена.

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

Аудиторна робота								Самостійна, індивідуальна робота				Семестровий контроль, залік	Разом
Практичні заняття (2,4,6,7)				Лабораторні роботи (2,4,6,7)				Тестовий контроль (Тест 1-4)				Підсумкова контрольна робота	Сума балів
Кількість балів за вид навчальної роботи (мінімум-максимум)													
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	24-40	60-100
12-20				12-20				12-20				24-40	

Електронне тестування проводиться в онлайн режимі в модульному середовищі для навчання (MOODLE) в рамках самостійної роботи. Для перевірки самостійності проходження електронних тестів тестування може бути проведено під час аудиторних робіт або під час консультації під наглядом викладача. Кожен електронний тест складається із 15-35 тестових завдань та охоплює тематику розділу курсу. Кожне тестове завдання оцінюється одним умовним балом. Результати тесту пропорційно приводяться до відповідної кількості балів за таблицею вище

Для відповіді на кожне завдання під час електронного тестування відводиться не більше 2 хвилин (залежно від тесту), наступна спроба проходження тесту можлива не раніше як за годину після закінчення попередньої. Кількість спроб виконання електронного тесту не більше 5. Кінцевий результат виставляється за найкращою спробою. Можливе попереднє включення тесту в режимі навчання. У випадку отримання негативної оцінки тестування проводиться повторно, не раніше ніж за тиждень в установленому порядку, але обов'язково до терміну наступного контролю.

Тестування у формі бліц-тесту проводиться письмово під час виконання лабораторних або практичних робіт, кількість завдань складає 10-20, решта вимог аналогічні поточному тестуванню. Перевірка та апеляція результатів тестування мають бути реалізовані до наступного аудиторного заняття. Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

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 підсумкового семестрового контролю (залік)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі заліку, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання заліку 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». Результати виконання індивідуального завдання враховуються як складання 1-2 тестів.

Семестровий залік 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

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	Іспит/диференційований залік
A	90-100	Зараховано	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
B	83-89		Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
C	73-82		
D	66-72		
E	60-65		
FX	40-59	Незараховано	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
F	0-39		Незадовільно/Fail – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

1. Обґрунтуйте на історичних прикладах актуальність тематики захисту інформації?
2. Чому електромагнітна сумісність (ЕМС) виділена як окрема галузь знань?.
3. Які є базові параметри та характеристики ЕМС засобів телекомунікацій?
4. Які канали витоку інформації виділяють в рамках ЕМС ?
5. Які базові технічні методи забезпечення ЕМС ?
6. Які базові організаційні методи забезпечення ЕМС ?
7. Як реалізуються методи захисту від квазігармонічних завад?
8. Як реалізуються методи захисту від імпульсних завад?
9. Як класифікують методи та методики радіоелектронної розвідки?
10. Які параметри технічних засобів входять в енергетичні рівняння радіотехнічної розвідки?
11. Які параметри технічних засобів входять в енергетичні рівняння радіорозвідки?
12. Які природні та штучні джерела створюють завади подібні до сигналу?
13. Які є методи та методики боротьби із завадами подібними до сигналу?
14. Які природні та штучні джерела створюють широкосмугові шумоподібні завади?
15. В чому полягає і як реалізується радіоелектронна протидія?
16. Які методи забезпечення прихованості дії можливо застосовувати для забезпечення захисту інформації?
17. Який принцип роботи детекторів радіовипромінювань?
18. Який принцип роботи компенсаційних радіотеплолокаторів?
19. Який принцип роботи комутаційних радіотеплолокаторів?
20. Яким чином утворюються шумоподібні сигнали для завдань радіоелектронної протидії?
21. Які властивості системи кодування повідомлень мають місце бути, щоб таку систему кодування розглядати як систему шифрування?
22. В чому полягає суть криптографічного захисту?
23. Як реалізувати криптографічний захист із максимальною ефективністю?
24. Які варіанти апаратного шифрування застосовуються в електронних комунікаціях?
25. Які варіанти програмного шифрування застосовуються в електронних комунікаціях?
26. В чому полягає суть симетричних алгоритмів шифрування?
27. В чому полягає суть несиметричних алгоритмів шифрування?
28. Як реалізується алгоритм цифрового підпису?
29. Як реалізується стенографічний алгоритм?
30. Які алгоритми та специфікації шифрування використовують на практиці для електронних систем комунікацій?
31. Як визначається криптографічна стійкість шифрування?
32. Чому скреблювання є одним із варіантів шифрування цифрових потоків?
33. Які властивості сигналів детермінованого хаосу надають можливості їх використання в алгоритмах забезпечення прихованості дії?
34. Які властивості сигналів детермінованого хаосу надають можливості їх використання в алгоритмах шифрування?
35. Як квантовий підхід дозволяє максимізувати захист інформації в телекомунікаційних системах?
36. Що називають багатофакторною ідентифікацією користувача в мережі?
37. Як реалізуються алгоритми багатофакторної ідентифікації?
38. Як реалізується ідентифікація абонента в мобільних мережах?
39. Які перспективи застосування алгоритмів захисту інформації в сучасних системах та мережах електронних комунікацій?

11. Тематика індивідуальних завдань

1. Розширена модель загроз каналів електронних комунікацій.
2. Об'єкти та суб'єкти інформаційної безпеки. Приклади на базі діючих систем.

3. Застосування базових принципів захисту інформації в інформаційних системах загального користування.
4. Параметри та характеристики сучасних детекторів випромінювання.
5. Параметри та характеристики сучасних сканерів та приймачів радіосигналів.
6. Параметри та характеристики промислових генераторів шумоподібних сигналів.
7. Параметри та характеристики сучасних генераторів імпульсних сигналів.
8. Параметри та характеристики аналізаторів електромагнітного оточення.
9. Можливості використання технології MIMO для радіоелектронної розвідки.
10. Можливості використання технології WiFi для радіоелектронної розвідки.
11. Ієрархізація рівнів захисту в системах електронних комунікацій.
12. Принципи роботи стандартизованих блокових та поточкових шифрів, переваги та недоліки.
13. Системні засоби генерації та використання ключів шифрування.
14. Використання досконалих шифрів в сучасних системах комунікацій.
15. Застосування алгоритмів ефективного кодування в системах із шифрування інформації
16. Застосування радіоелектронної боротьби в умовах потужних імпульсних завад.
17. Застосування радіоелектронної боротьби в умовах завад подібних до сигналу.
18. Приклади застосування алгоритму RSA в різних галузях електронних комунікацій.
19. Захист мереж від вірусних загроз.
20. Базові алгоритми детектування вірусних мережеских загроз та їх нейтралізації.
21. Базові принципи мережеских брандмауєрів.
22. Реалізація автентифікації користувачів в мережах останніх поколінь.
23. Практичне використання хаотичних сигналів для шифрування повідомлень.
24. Використання квантових обчислень для забезпечення криптографічної стійкості.
25. Сучасні корпоративні моделі організації захисту інформації.
26. Можливі негативні наслідки, що виникають під час використання алгоритмів шифрування.

12. 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, доступ до мережі Інтернет, робота з презентаціями.

13. Рекомендована література

Основна

1. 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.
2. 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
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.осхемотехніка: У 4-х т. Том 3. Цифрові пристрої/ В.І.Сенько - – Київ : Каравелла, 2023.- 400с.
4. 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.

Допоміжна

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. Теорія цифрових систем [Електронний ресурс] : навчальний посібник для студ. спеціальності 126 «Інформаційні системи та технології», освітньої програми «Інформаційне забезпечення робототехнічних систем» / І. Р. Пархомей, В. П. Пасько, О. М. Польшакова, О. А. Стенін ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2.851 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 133 с.
 3. Бортник, Г. Г. Цифрова обробка сигналів в телекомунікаційних системах : підручник / Г. Г. Бортник, В. М. Кичак. – Вінниця : ВНТУ, 2014. – 232 с.
 4. Лосев Ю. І. Основи теорії передачі інформації : навчальний посібник / Ю. І. Лосев, С. І. Шматков ; за ред. Ю. І. Лосева. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 292 с.
 5. Воробієнко П.П. [та ін.]. Телекомунікаційні та інформаційні мережі: Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К. : САММІТ-Книга, 2010. – 708 с.: іл.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL: <https://msn.khnu.km.ua>.
2. Електронна бібліотека ХНУ/ URL: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.
3. Інституційний депозитарій ХНУ. URL: <http://elar.khnu.km.ua/jspui/?locale=uk>.

ЦИФРОВИЙ ЗВ'ЯЗОК

Тип дисципліни	Вибіркова (цикл професійної підготовки)
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	-
Кількість встановлених кредитів ЄКТС	8,0
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вміло використовувати понятійний апарат прихованості дії та захисту інформації від несанкціонованого доступу в цифрових та аналогових каналах електронних комунікацій; проводити аналіз вразливостей діючих систем зв'язку; виконувати розрахунки параметрів телекомунікаційних засобів із метою мінімізації можливостей щодо несанкціонованого витоку інформації; розробляти методи тики організаційного забезпечення захисту інформації в програмному середовищі протокольної взаємодії багатокористувачьких телекомунікаційних систем та мереж на рівні ідентифікації, аутентифікації та арбітражу ; обґрунтовано обирати системи шифрування для забезпечення заданого рівня захисту телекомунікаційних систем та мереж.

Зміст навчальної дисципліни. Окреслення загроз захисту інформації та їх класифікації. Поняття та параметри електромагнітної сумісності. Канали витоку інформації. Стійкість до не флуктуаційних завад. Енергетичні рівняння радіоелектронної розвідки та радіоелектронної протидії. Забезпечення прихованості дії. Радіоелектронна протидія. Детектори випромінювання. Нелінійні локатори. Імітатори сигналів та завад. Основи криптографії. Властивості шифрів. Генерація та поширення ключів шифрування. Захист від витоку мультимедійної інформації. Апаратні алгоритми шифрування. Програмні алгоритми шифрування. Цифрові підписи. Основи стеганографії. Скремблювання та перфорація. Квантові технології в захисті інформації. Організація автентифікації в сучасних мережах електронних комунікацій.

Запланована навчальна діяльність. Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для першого (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і візуалізації); лабораторні заняття (з використанням методів комп'ютерного моделювання), практичні заняття (із використанням засобів математичного моделювання та комп'ютерної обробки даних, практикумів), самостійна робота (індивідуальні завдання), підготовка до проміжного та підсумкового контролю.

Форми оцінювання результатів навчання: захист лабораторних робіт; портфоліо лабораторних робіт; портфоліо завдань для практичної роботи, презентація результатів виконання індивідуальних завдань; письмове опитування (тестування).

Вид семестрового контролю: залік.

Навчальні ресурси:

1. 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.
2. 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
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.осхемотехніка: У 4-х т. Том 3. Цифрові пристрої/ В.І.Сенько - – Київ : Каравелла, 2023.- 400с.
4. Хорошко В. О. Проектування комплексних систем захисту інформації / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опіський, Л. Т. Пархуць. – Львів : Видавництво Львівської політехніки, 2020. – 320 с.
5. Модульне середовище для навчання. Доступ до ресурсу: <https://msn.khmn.edu.ua/user/index.php?id=4180>
6. Електронна бібліотека ХНУ. Доступ до ресурсу: <http://library.khmn.edu.ua/>

Викладач: канд. тех. наук, доцент Олег ПИВОВАР