ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____Олег САВЕНКО
«__» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Завадостійкість та інформаційна безпека інфокомунікацій

Галузь знань – 17 Електроніка, автоматизація та електронні комунікації
Спеціальність – 172 Електронні комунікації та радіотехніка
Рівень вищої освіти – Другий (магістерський)
Освітньо-професійна програма – Електронні інформаційно-комунікаційні системи та мережі
Обсяг дисципліни – 5 кредитів ЄКТС ***Шифр дисципліни***– ОПП.01
Мова навчання – українська
Статус дисципліни: обов'язкова (цикл професійної 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				Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття				Залік	Іспит
Д	1	1	5	150	51	17	17	17	99	-	-	-	+
Разом ДФН			**5**	**150**	**51**	**17**	**17**	**17**	**99**	**-**	**-**	**-**	**+**

Робоча програма складена на основі освітньо-професійної програми

Програму складено _____ Юлій БОЙКО

Схвалено на засіданні кафедри телекомунікацій, медійних та інтелектуальних технологій
Протокол *№ 1 від 31 серпня 2023 року*

Завідувач кафедри ТМІТ _____ Сергій ПІДЧЕНКО

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради _____ Олег САВЕНКО

Хмельницький 2023

ЗАВАДОСТІЙКІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОКОМУНІКАЦІЙ

Опис дисципліни (анотація)

Тип дисципліни	Нормативна
Цикл (перший/другий/третій)	Другий (магістерський)
Мова викладання	Українська
Рік навчання	Перший
Семестр	Перший
Кількість встановлених кредитів ЄКТС	5,0
Форми навчання, для яких викладається дисципліна	денна

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.

Зміст навчальної 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.

Запланована навчальна діяльність: лекцій 17 год., практичних занять 17, лабораторних занять 17 год., самостійної роботи 99 год.; разом 150 год.

Форми (методи) викладання: лекції (з використанням методів проблемного навчання і візуалізації); лабораторны роботи, практичні заняття, самостійна робота (індивідуальні завдання).

Форми та критерії оцінювання: усне опитування, тестування. Критерії оцінювання наведені у робочій програмі дисципліни та MOODLE.

Вид семестрового контролю: іспит

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.Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=7972

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Інформація, незалежно від того чи становить вона власність держави, суспільства, певних організацій і фірм, а також фізичних осіб, володіє певною цінністю. Звідки можна констатувати, що інформаційні ресурси неодмінно вимагають засобів захисту від різноманітних впливів дія яких може спричинити до руйнування та нівелювання їх цінності. В контексті телекомунікаційних і загалом інформаційно-комунікаційних систем потрібно акцентувати увагу на системах оброки і зберігання даних. Наявність шкідливого і навіть руйнівного програмного забезпечення призводить до ускладнення і унеможливлення усіх базових функцій програмного забезпечення засобів телекомунікацій. Тобто програмні продукти можуть містити приховані функції які можуть бути реалізовані навмисно, які неописані в документації і до яких можна віднести, зокрема, віруси які здатні поширюватись і розмножуватись. Отже, існування сучасних телекомунікаційних і інформаційно-комунікаційних систем в цілому, на сучасному етапі розвитку інформаційних технологій неможливе без застосування спеціальних заходів захисту з метою запобігання пошкодження і руйнування інформації в телекомунікаційних системах. Дисципліна «Завадостійкість та інформаційна безпека інфокомунікацій» є однією із обов'язкових дисциплін і займає провідне місце у підготовці фахівців освітнього рівня «магістр» за спеціальністю 172 Електронні комунікації та радіотехніка, особливо в контексті підготовки фахівців здатних розуміти і працювати із сучасними телекомунікаційними технологіями.

Пререквізити – методологія та організація наукових досліджень; програмно-конфігуровані системи передавання, приймання та обробки інформації.

Кореквізити – апаратно-програмне забезпечення інформаційно-комунікаційних систем та мереж; системний аналіз інформаційно-комунікаційних систем та мереж; моделювання і оптимізація радіотехнічних засобів електронних комунікацій.

Відповідно до проекту Стандарту вищої освіти із зазначеної спеціальності та освітньої програми дисципліна має забезпечити:

- ***компетентності:*** Здатність розв'язувати задачі забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних та радіотехнічних систем з урахуванням економічних, правових, безпекових та інших аспектів. Здатність відшуковувати та оцінювати інформацію з проблем телекомунікацій, радіотехніки та дотичних питань. Здатність розв'язувати складні професійні задачі на основі застосування новітніх технологій передавання, приймання і обробки інформації. Здатність до реалізації принципів системного підходу при проведенні досліджень процесів, що протікають в телекомунікаційних і радіотехнічних системах, комплексах та пристроях. Здатність обґрунтовано обирати та ефективно застосовувати математичні методи, комп'ютерні технології моделювання, а також підходи та методи оптимізації телекомунікаційних і радіотехнічних систем, комплексів, технологій, пристроїв та їх компонентів на всіх етапах їх життєвого циклу.

- ***програмні результати навчання:*** Забезпечувати надійність, живучість, завадозахищеність, інформаційну безпеку та пропускну здатність телекомунікаційних та радіотехнічних систем. Захищати інтелектуальну власність, розробляти відповідні охоронні документи, аналізувати патентну чистоту, відповідність наукових та дослідно-конструкторських розробок нормам законодавства України та міжнародних стандартів щодо інтелектуальної власності. Локалізовувати та оцінювати стан проблемної ситуації на етапах дослідження, проектування, модернізації, впровадження та експлуатації сучасних та перспективних телекомунікаційних і радіотехнічних систем, комплексів, технологій, пристроїв та їх компонентів, формулювати пропозиції щодо її вирішення з усуненням виявлених недоліків. Аналізувати напрями розвитку і новітні стандарти у сфері телекомунікацій та радіотехніки. Розуміти принципи організації інформаційно-комунікаційних мереж, технології мультиплексування та комутації, технології фізичного рівня, ієрархію швидкостей, концептуальні засади щодо формування сигнально-кодових конструкцій та завадостійкого кодування.

Дисципліни, що передують вивченню ***«Завадостійкість та інформаційна безпека інфокомунікацій»*** – методологія та організація наукових досліджень; програмно-конфігуровані системи передавання, приймання та обробки інформації.

Мета викладання 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.

Предметом курсу «Завадостійкість та інформаційна безпека інфокомунікацій» є 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.

2. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:			
	Денна форма навчання			
	Лекції	Лабор. роботи	Практ.	СРС
Перший семестр				
Тема1. Принципи організації захисту інформації в телекомунікаційних системах	*2*	*2*	-	*12*
Тема 2. Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях.	*3*	*2*	*4*	*12*

Тема 3. Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	*2*	*4*	*5*	*13*
Тема 4. Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах. Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	*2*	*3*	*6*	*12*
Тема 5. Концепція передачі інформації використовуючи захищені телекомунікаційні та інформаційно-комунікаційні системи.	*2*	*2*	-	*12*
Тема 6. Забезпечення безпеки мережних протоколів у телекомунікаційних і інформаційно-комунікаційних системах.	*2*	*2*	*2*	*13*
Тема 7. Розробка та моніторинг комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.	*2*	*2*	-	*12*
Тема 8. Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій.	*2*	-	-	*13*
Разом за семестр	***17***	***17***	***17***	***99***

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1 Зміст лекційного курсу

Номер лекції	*Перелік тем лекцій, їх анотації*	*Кіль-кість годин*
1	**Принципи організації захисту інформації в телекомунікаційних системах.** Завдання захисту інформації. Окреслення загроз захисту інформації та їх класифікації. Типи атак та моделі загроз. Оцінювання, моніторинг та аспекти розробки захищених систем. Література: [1] с. 3….18; [2] с. 6….17.	*2*
2	**Методика підвищення завадостійкості телекомунікаційних систем. Методи завадостійкого кодування інформації в електронних комунікаціях.** 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. Література: [3] с. 7….55; [4] с. 143….189	*3*
3	**Теоретичні засади захисту інформації. Методи криптографічного захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.** Сервісні та функціональні засоби безпеки та	*2*

	механізми їх реалізації. Автентифікація, ідентифікація та керування доступом в контексті забезпечення цілісності системи. Криптографічні системи. Технології шифрування, теорія, алгоритми, криптографічні підсистеми. Література: [1] с. 25….44; [5] с. 258….274.	
4	**Загрози безпеці інформації в програмному забезпеченні телекомунікаційних та інформаційно-комунікаційних системах. Апаратне забезпечення засобів захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.** 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. 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. Література: [1] с. 29…..45; [2] с. 39…..103; [5] с. 54….68.	*2*
5	**Концепція передачі інформації використовуючи захищені телекомунікаційні та інформаційно-комунікаційні системи.** Принципи захисту інформації у відкритих телекомунікаційних каналах. Віртуальні захищені мережі. Заходи захисту віртуальних каналів на мережевому, сеансовому та канальному рівні. Література: [2] с. 112…….154; [5] с. 97….156.	*2*
6	**Забезпечення безпеки мережних протоколів у телекомунікаційних і інформаційно-комунікаційних системах.** Архітектура захищених мереж передачі інформації. Можливості систем виявлення атак. Принципи резервування мережевого обладнання і телекомунікаційних каналів. Засоби протидії прослуховування трафіку. Міжмережні екрани. Реалізація систем оцінювання а аналізу вразливостей. Література: [1] с. 372….407; [2] – 62…..103.	*2*
7	**Розробка та моніторинг комплексної системи захисту інформації в телекомунікаційних і інформаційно-комунікаційних системах.** Структура комплексного захисту інформації. Аналіз та визначення можливих загроз безпеки в інформаційно-комунікаційних каналах. Формулювання вимог до комплексної системи захисту та політика безпеки. Розробка технічного завдання на проектування комплексної захищеної системи. Ведення та супроводження захищеної системи передачі інформації. Література: [1] с. 413……456; [5] с. 80……138.	*2*
8	**Методики оцінювання захищеності інформації. Стандарти та критерії безпеки інформаційних технологій.** 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. 18 ……..44; [5] с. 38…..103	*2*
	Разом за 1 семестр	***17***

3.2 Перелік 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	2
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	3
5	Лаб. роб. № 5 Принципи захисту інформації у мобільних терміналах. Оцінка вірусів та засоби протидії їх впливу	2
6	Лаб. роб. № 6 Використання паролів. Захист та збереження доступу до паролів	2
7	Лаб. роб. № 7 Ознайомлення з засобами технічного захисту інформації	4
	Разом за 1 семестр	***17***

3.3 Перелік 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.	4
3	Практ. роб. № 3 Шифри складної заміни – багатоалфавітні шифри.	3
4	Практ. роб. № 3 Ознайомлення з методикою шифрування методом перестановки.	2
5	Практ. роб. № 4 Ознайомлення з методикою шифрування методом гамування.	3
6	Практ. роб. № 5 Ознайомлення з методикою комбінованих методів шифрування.	3
	Разом за 1 семестр	***17***

3.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів з дисципліни «Програмно-обумовлені радіосистеми телекомунікацій» включає: опрацювання теоретичних основ, прослуханого лекційного матеріалу; підготовку до тестового контролю та лабораторних робіт, контрольної роботи, письмове оформлення індивідуальних завдань тощо.

Зміст самостійної роботи студентів

Номер тижня	*Вид самостійної роботи*	*Кількість годин*
1,2	Опрацювання теоретичного матеріалу з Т1. Підготовка до лабораторного заняття	*12*
3,4	Опрацювання теоретичного матеріалу з Т2. Підготовка до лабораторного заняття	*12*
5,6	Опрацювання теоретичного матеріалу з Т3. Підготовка до лабораторного заняття	*12*
7,8	Підготовка до контрольної роботи з Т1-3. Підготовка до тестового контролю з Т1-3	*12*
9,10	Опрацювання теоретичного матеріалу з Т4-5. Підготовка до лабораторного заняття	*12*
11,12	Опрацювання теоретичного матеріалу з Т6-7. Підготовка до лабораторного заняття	*10*
13,14	Опрацювання теоретичного матеріалу з Т8. Підготовка до лабораторного заняття	*10*
15,16	Підготовка до практичного заняття. Підготовка до контрольної роботи з Т4-8	*10*
17	Підготовка до тестового контролю з Т4-8. Підготовка до лабораторного заняття	*9*
	Разом за 1семестр:	***99***

Завдання для письмового оформлення індивідуального домашнього завдання.

Індивідуальне домашнє завдання з дисципліни „ Завадостійкість та інформаційна безпека інфокомунікацій” складається з написання реферату з двох проблемних теоретичних питань у галузі сучасних технологій телекомунікацій. Вибираючи варіант індивідуального домашнього завдання, студент користується таблицею. Варіант домашнього завдання визначається студентом залежно від першої літери прізвища та останньої цифри номера залікової книжки. В таблиці по горизонталі розміщені літери, кожна з яких – перша літера прізвища студента. По вертикалі розміщені цифри, кожна з яких – остання цифра номера залікової книжки студента. На перетині вертикальної та горизонтальної ліній визначаються номера завдань (таблиця 1).

Таблиця 1 - Таблиця вибору завдання домашньої роботи

	А	Перша літера прізвища студента			
	Б	А Б В Г Д Е Є Ж	З И І Ї Й К Л М	Н О П Р С Т У Ф	Х Ц Ч Ш Щ Ю Я
Остання цифра номера залікової книжки	1	1	2	3	4
	1	5	6	7	8
	2	9	10	11	12
	3	13	14	15	1
	4	2	3	4	5
	5	6	7	8	9
	6	10	11	12	13
	7	14	15	1	2
	8	3	4	5	6
	9	7	8	9	10

При виконанні індивідуального домашнього завдання студенти повинні користуватися відповідними рекомендованими підручниками, навчальними посібниками, матеріалами галузевих і періодичних видань.

<u>Орієнтована тематика індивідуального завдання з курсу</u>

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.

4. ТЕХНОЛОГІЇ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами, а лабораторні заняття проводяться з використанням інформаційних технологій, практикумів і мають за мету – набуття студентами практичних навичок аналізу різноманітних характеристик захищених телекомунікаційних та інформаційно-комунікаційних систем, методик шифрування та кодування інформації.

5. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лекційних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі іспиту. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

Процес оцінювання підготовленості студента можна розділити на етапи:

Перший етап оцінювання направлений на визначення знань інформаційного мінімуму. Якщо студент твердо засвоїв визначену навчальним планом суму формальних знань, то це означає, що він вміє використати їх при вирішенні різних питань при аналізі процесів у захищених телекомунікаційних системах, застосуванні методів протидії загрозам і атакам, володіє нормативними документами та стандартами в по захисту інформації.

Перед вивченням дисципліни, як правило, проводиться вхідний контроль знань з дисциплін, що їй передують і забезпечують. При цьому необхідно встановити рівні та критерії сформованості знань щодо змісту навчальних елементів. Такими рівнями є:

Ознайомчо-орієнтовний (ОО) – особа має орієнтовне уявлення щодо понять, які вивчаються, здатна: відтворювати формулювання визначень різноманітних процесів, що використовуються в системах програмно-обумовленого радіо, орієнтуватись в методиках розрахунку підсистем програмно-обумовленого радіо.

Понятійно-аналітичний (ПА) – особа має чітке уявлення щодо навчального об'єкту, здатна здійснювати смислове виділення, пояснення вихідних процесів у системах та пристроях програмно-обумовленого радіо. Може чітко визначити спрощення, які були використані при аналізі і оцінити похибки, що виникають при цьому, тобто здатна перенести раніше засвоєнні знання на типові ситуації.

Продуктивно-синтетичний (ПС) – особа має глибоке розуміння щодо навчального об'єкту, здатна здійснювати синтез, генерувати нові ідеї та уявлення, переносити раніше засвоєнні знання на нетипові, нестандартні ситуації. Тобто на цьому рівні студент повинен на основі теоретичних знань вміти досліджувати нетипові кола, оцінювати їх вихідний сигнал і можливі обмеження.

.

6. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ У СЕМЕСТРІ

Кожний вид роботи з дисципліни оцінюється за чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Оцінювання знань студентів здійснюється за такими критеріями:

Оцінка за національною шкалою	*Узагальнений критерій*
Відмінно	Студент 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 грамотний, логічний виклад відповіді (як в усній, так і у письмовій формі), якісне зовнішнє оформлення роботи. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві–три несуттєві похибки.
Добре	Студент 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 закономірностей тощо. Відповідь студента має будуватися на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент 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 студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, 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	Студент 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 студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у 5 семестрі за ваговими коефіцієнтами

Аудиторна робота	*Самостійна, індивідуальна робота*			*Семестровий контроль*
І семестр				
Захист лабораторної роботи №:	Розв'язок тестових та практичних завдань		Контрольна робота	Підсумковий контрольний захід
	ТК1	ТК2	КР	
ВК: 0,20	0,15		0,25	0,4

Умовні позначення: ВК – ваговий коефіцієнт,

Для переходу від вітчизняної оцінки до оцінки за шкалою ECTS необхідно знайти середньоарифметичну оцінку за вітчизняною шкалою, помножити її на відповідний ваговий коефіцієнт і, додавши всі складові, отримати суму балів, яка визначить конкретну оцінку за шкалою

ECTS.

Таблиця 2 -Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ECTS

Оцінка ECTS	*Бали*	*Вітчизняна оцінка*	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

Залік виставляється при отриманні студентом з дисципліни від 2,75 до 5,00 балів. При цьому за вітчизняною шкалою ставиться «зараховано», а за шкалою ECTS – буквене позначення оцінки, що відповідає набраній студентом кількості балів (таблиця 2).

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; засвоєння теоретичного матеріалу з тем перевіряється тестовим контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи та індивідуального завдання згідно з робочою програмою дисципліни і робочим навчальним планом.

Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і графічної частини; вміння студента обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. За несвоєчасний захист лабораторної роботи з неповажної причини студент за позитивну відповідь отримує оцінку «задовільно».

Пропущене лабораторне заняття студент повинен відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінювання тестових завдань

Тематичний тест для кожного студента складається з 25 тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 25.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту, представлена у нижченаведеній таблиці.

Сума балів за тестове завдання	1–13	14–16	17–22	23–25
Оцінка за 4-ри бальною шкалою	2	3	4	5

Якщо відповідь на тестове завдання має 2-3 правильних значення, а студент зумів вказати частину з них, то сума балів у цьому випадку буде пропорціональна кількості правильних відповідей. Наприклад, у завданні має бути три правильних відповіді, а студент вказав лише дві з них, тоді він отримує за тестове завдання два бали з трьох.

На тестування відводиться 20 хвилин. Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей повинні бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 20 хвилин студенти здають викладачу завдання з талонами відповідей. Викладач на наступному занятті оголошує результати тестування.

Якщо студент отримав негативну оцінку, то він повинен перездати її у встановленому порядку, але обов’язково до терміну наступного контролю. У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час від-працювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно/ E”.

Талон відповідей

на тему _____

Студента гр. _____ _____

Номер завдання	Відповідь	Номер завдання	Відповідь	Номер завдання	Відповідь	Номер завдання	Відповідь
1		6		11		16	
2		7		12		17	
3		8		13		18	
4		9		14		19	
5		10		15		20	

“___” _____ 20___ р. _____

підпис студента

7. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ ЗНАНЬ

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.

8. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Інформаційний захист та апаратно-програмне забезпечення телекомунікаційних систем» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою. Зокрема:

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. Бойко Ю.М. Інформаційний захист та апаратно-програмне забезпечення телекомунікаційних систем. Завдання та методичні рекомендації до курсового проектування з курсу /Ю.М. Бойко. – Хмельницький: ХНУ, 2022.

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.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Рекомендована основна література:

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

2. 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.

3. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

4. 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.

5. 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.

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

Додаткова література:

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.

10 Бойко Ю.М. Інформаційний захист та апаратно-програмне забезпечення телекомунікаційних систем. Завдання та методичні рекомендації до курсового проектування з курсу /Ю.М. Бойко. – Хмельницький: ХНУ, 2022. – 50 с.

10. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань). http://msn.tup.km.ua/ .
2. Електронна бібліотека університету http://library.tup.km.ua/
3. Репозитарій ХНУ. Доступ до ресурсу: http://elar.khnu.km.ua/jspui/?locale=uk.