ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Інформаційна безпека в галузі»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 172 «Електронні комунікації та радіотехніка»
освітньо-професійна програма «Телекомунікації та радіотехніка»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерних технологій у медицині та телекомунікаціях

Схвалено на засіданні кафедри комп'ютерних технологій у медицині та телекомунікаціях
28 серпня 2023 р., протокол №7
Завідувач кафедри
_____ Владислав ЧУХОВ

Гарант освітньо-професійної програми
_____ Владислав ЧУХОВ

Розробник: к.т.н., доцент кафедри комп'ютерних технологій у медицині та телекомунікаціях ЦИПОРЕНКО Віталій

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів 5	Галузь знань: 17 «Електроніка, автоматизація та електронні комунікації»	Нормативна (нормативна, за вибором)	
Модулів – 1	Спеціальність: 172 «Електронні комунікації та радіотехніка»	Рік підготовки:	
Змістових модулів – 3		2024-й	2024-й
		Семестр	
Загальна кількість годин - 150		2-й	2-й
		Лекції	
Тижневих годин для денної форми навчання: аудиторних – 4, самостійної роботи – 5,3	Освітній ступінь «магістр»	32 год.	8 год.
		Практичні	
		32 год.	6 год.
		Лабораторні	
		__ год.	__ год.
		Самостійна робота	
		86 год.	136 год.
		Вид контролю: Екзамен	

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 43 % аудиторних занять, 57 % самостійної та індивідуальної роботи;

для заочної форми навчання 9 % аудиторних занять, 91 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є вивчення методів та засобів інформаційної безпеки. Вивчення каналів поширення інформації та способів захисту від несанкціонованого доступу до інформації, засобів виявлення каналів витоку та активного захисту інформації, контролю території та приміщень. Вивчення основ мережної безпеки.

Завданнями вивчення навчальної дисципліни є:

– вивчити інформації щодо каналів поширення інформації та способів захисту від несанкціонованого доступу до інформації. Засобів виявлення каналів витоку та активного захисту інформації, контролю території та приміщень;

– навчитися застосовувати комплексний підхід до вирішення задач забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних та радіотехнічних систем.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 172 «Телекомунікації та радіотехніка»:

ЗК6. Здатність використовувати інформаційні та комунікаційні технології.

ЗК8. Здатність генерувати нові ідеї (креативність).

ЗК10. Здатність розробляти проекти та управляти ними, оцінювати та забезпечувати якість виконуваних робіт.

СК2. Здатність до реалізації принципів системного підходу при проведенні досліджень процесів, що протікають в телекомунікаційних і радіотехнічних системах, комплексах та пристроях.

СК4. Здатність застосовувати комплексний підхід до вирішення задач забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних та радіотехнічних систем.

СК7. Здатність працювати з науково-технічною літературою та іншими джерелами інформації.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 172 «Телекомунікації та радіотехніка»:

ПРН2. Вміти враховувати соціальні і морально-етичні норми, налагоджувати результативне співробітництво у колективі при проведенні наукових досліджень;

ПРН3. Знати теоретичні основи, принципи побудови і функціонування сучасних та перспективних телекомунікаційних і радіотехнічних систем, комплексів, технологій, пристроїв та їх компонентів;

ПРН7. Вміти аналізувати напрями перспективного розвитку і новітні стандарти у сфері телекомунікацій та радіотехніки;

ПРН11. Вміти застосовувати комплексний підхід до вирішення задач забезпечення надійності, живучості, завадозахищеності, інформаційної безпеки та пропускної здатності телекомунікаційних та радіотехнічних систем.

3. Програма навчальної дисципліни

Змістовий модуль 1. Технічні канали витоку інформації

Тема 1. Введення в дисципліну. Предмет і завдання навчальної дисципліни. Канали поширення інформації та способи несанкціонованого доступу до інформації. Технічні канали витоку інформації. Загальна характеристика методів розвідки. Система захисту інформації.

Тема 2. Організація захисту інформації від витоку при роботі обчислювальної техніки. Види і природа побічного електромагнітного випромінювання (ПЕМВ) персонального комп'ютера. Способи і методи забезпечення захисту інформації від витоку через ПЕМВ. Оцінка рівня ПЕМВ. Екранування приміщень. Конструктивні особливості приміщень.

Змістовий модуль 2. Засоби виявлення каналів витоку та активного захисту інформації

Тема 3. Детектори поля. Детектори поля. Загальні відомості. Конструктивні особливості пристроїв. Схемні рішення. Технічні характеристики. Багатофункціональні пошукові пристрої Andre, ST-033/131. Пошуковий комплекс Delta X 2000/6 Real-Time. Канали виявлення пристроїв. Технічні характеристики.

Тема 4. Скануючі пристрої. Активні засоби захисту інформації. Програмні комплекси. Скануючий радіоприймач AR8200 Mk3. Цифрові генератори шуму. Сканер безпровідних відеокамер Protect C-Hunter 935B. Локатори нелінійних переходів для виявлення прихованих електронних компонентів. SDR радіоприймач Hack RF. Програмне забезпечення SDR sharp. Програмне забезпечення управління перестройкою радіоприймача DigiScan EX.

Змістовий модуль 3. Системи контролю і управління доступом. Основи мережної безпеки.

Тема 5. Засоби спостереження території та виявлення. Системи контролю доступу. Телевізійні камери. Пристрої для оснащення телевізійних

камер. Периметрові засоби виявлення. Засоби виявлення для приміщень. Засоби збору та обробки інформації. Периферійне обладнання і носії інформації систем контролю доступу. Засоби ідентифікації і автентифікації.

Тема 6. Основи мережної безпеки. Загрози безпеці та вразливості. Мережні атаки. Нейтралізація мережних атак. Захист пристроїв.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	самостійна робота	усього	лекції	практичні	самостійна робота
Модуль 1								
Змістовий модуль 1. Технічні канали витоку інформації								
Тема 1. Введення в дисципліну. Предмет і завдання навчальної дисципліни. Канали поширення інформації та способи несанкціонованого доступу до інформації. Технічні канали витоку інформації. Загальна характеристика методів розвідки. Система захисту інформації.		6	6	10		2	2	20
Тема 2. Організація захисту інформації від витоку при роботі обчислювальної техніки. Види і природа побічного електромагнітного випромінювання (ПЕМВ) персонального комп'ютера. Способи і методи забезпечення захисту інформації від витоку через ПЕМВ. Оцінка рівня ПЕМВ. Екранування приміщень. Конструктивні особливості приміщень.		6	6	16		2	2	22
Разом за змістовий модуль 1	***50***	***12***	***12***	***26***	***50***	***4***	***4***	***42***
Змістовий модуль 2. Засоби виявлення каналів витоку та активного захисту інформації								
Тема 3. Детектори поля. Детектори поля. Загальні відомості. Конструктивні особливості пристроїв. Схемні рішення. Технічні характеристики. Багатофункціональні пошукові пристрої Andre, ST-033/131.		6	6	16		2	-	22

Пошуковий комплекс Delta X 2000/6 Real-Time. Канали виявлення пристроїв. Технічні характеристики.								
Тема 4. Скануючі пристрої. Активні засоби захисту інформації. Програмні комплекси. Скануючий радіоприймач AR8200 Mk3. Цифрові генератори шуму. Сканер безпровідних відеокамер Protect C-Hunter 935B. Локатори нелінійних переходів для виявлення прихованих електронних компонентів. SDR радіоприймач Hack RF. Програмне забезпечення SDR sharp. Програмне забезпечення управління перестройкою радіоприймача DigiScan EX.		4	4	14		2	2	22
Разом за змістовий модуль 2	***50***	***10***	***10***	***30***	***50***	***4***	***2***	***44***
Змістовий модуль 3. Засоби контролю території та приміщень. Системи контролю і управління доступом								
Тема 5. Засоби спостереження території та виявлення. Системи контролю доступу. Телевізійні камери. Пристрої для оснащення телевізійних камер. Периметрові засоби виявлення. Засоби виявлення для приміщень. Засоби збору та обробки інфорації. Периферійне обладнання і носії інформації систем контролю доступу. Засоби ідентифікації і аутентифікації.		6	6	16		-	-	24
Тема 6. Основи мережної безпеки. Загрози безпеці та вразливості. Мережні атаки. Нейтралізація мережних атак. Захист пристроїв.		4	4	14		-	-	26
Разом за змістовий модуль 3	***50***	***10***	***10***	***30***	***50***	***-***	***-***	***50***
ВСЬОГО	***150***	***32***	***32***	***86***	***150***	***8***	***6***	***136***

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Дослідження затухання радіохвиль на шляху поширення в залежності від місцевості	8	2
2	Розрахунок показників ефективності екранування приміщень.	4	

3	Дослідження параметрів завади при попаданні в систему заземлення.	4	
4	Дослідження можливостей програмного забезпечення DigiScan EX для широкосмугового приймача фірми AOR	4	
5	Дослідження можливостей програмного забезпечення SDR sharp з SDR радіоприймачем Hack RF	4	2
6	Створення проекту системи відеоспостереження та розпізнавання облич офісної будівлі	4	
7	Дослідження процесу розпізнавання мовної інформації	4	
РАЗОМ		32	4

6. Завдання для самостійної роботи

Тема 1. Способи і методи забезпечення інформаційної безпеки від витоку через побічне електромагнітне випромінювання (ПЕМВ).

1. Усі навчальні елементи: опрацювання лекційного матеріалу, підготовка до лабораторного практикуму, оформлення звітів з лабораторних робіт. Основа методології розробки концепції комплексного забезпечення інформаційної безпеки об'єктів охорони. Технічні канали витоку інформації.
2. Способи і методи забезпечення інформаційної безпеки від витоку через ПЕМВ. Класифікація чутливих елементів засобів виявлення.
3. Комплекс технічних засобів забезпечення безпеки об'єкта. Екранування приміщень.
4. Конструктивні особливості детектора поля.
5. Частотний спектр електромагнітних хвиль.

Тема 2. Віддалене відеоспостереження

1. Аналогові, цифрові та IP-відеокамери.
2. Хмарні технології. Порядок підключення IP-відеокамер до Інтернет.

Тема 3. Система контролю і управління доступом (СКУД)

1. Склад і види елементів СКУД.
2. Інтегровані СКУД. Біометричні СКУД.

Тема 4. Основи мережної безпеки.

1. Мережні атаки. Нейтралізація мережних атак.
2. Захист пристроїв.

7. Індивідуальні завдання

Індивідуальні завдання не передбачені програмою дисципліни.

8. Методи навчання

Проведення лекцій, практичних робіт, контрольно-модульних робіт, захист звітів з лабораторних робіт, екзамен.

9. Методи контролю

Лекційний, контрольно-модульні роботи, звіти з практичних робіт, екзамен.

10. Розподіл балів

Поточне тестування та самостійна робота						Сума
Змістовий модуль 1,2			Змістовий модуль 3			
Т1,2	Т3,4		Т5	Т6		100
35	35		20	10		

1. За роботу на лекційних заняттях, конспект – 10б.
2. Контрольно-модульні роботи: 2*25б = 50б.
3. Захист звітів з лабораторних (практичних) робіт: 8*5б = 40б.

Всього: 100балів.

Шкала оцінювання

За шкалою	Екзамен		Бали
A	Відмінно		90-100
B	Добре		82-89
C			74-81
D	Задовільно		64-73
E			60-63
FX	Незадовільно		35-59
F			0-34

11. Рекомендована література

Основна література

1. Барило Г.І., Вісьтак М.В., Готра З.Ю., Лесінський В.В., Політанський Л.Ф. Електронні елементи та пристрої систем безпеки й охорони: Навчальний посібник. – За ред. Готри З.Ю. – Чернівці: Рута, 2017. – 216 с.

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

3. Лизанчук В. Інформаційна безпека України: теорія і практика: навч. посібник / В. Лизанчук. Львів: ЛНУ, 2017. – 728 с.

4. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

5. Graham Bartlett, Amjad Inamdar. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. – Cisco Press, 2016 – 608 с.

Допоміжна література

6. Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.97 р., № 1126.

7. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

8. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s

9. Доктрини «Інформаційної безпеки України» від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/uk-ru/47/2017?lang=uk#Text

12. Інформаційні ресурси в Інтернеті

Файли дисципліни: https://learn.ztu.edu.ua/course/view.php?id=5928