ЗАПОРІЗЬКА ПОЛІТЕХНІКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційної безпеки та електронних комунікацій
Кафедра радіотехніки та телекомунікацій

СИЛАБУС
вибіркової навчальної дисципліни
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ
Обсяг освітнього компоненту (6 кредитів ECTS / 180 годин)

Освітня програма «Радіотехніка»
другого рівня вищої освіти
Спеціальність – 172 «Електронні комунікації та радіотехніка»

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

СМЕТАНІН Ігор Миколайович,
старший викладач

Контактна інформація:
- +38(061)7698596;
- smeig@zp.edu.ua;
- навчальний корпус №3, аудиторія 32-б

Час і місце проведення консультацій:
згідно з графіком консультацій

ОПИС КУРСУ

Даний курс познайомить студентів з основами інформаційної безпеки, теорією виникнення технічних каналів просочування інформації і їх виявлення та принципами побудови сучасних систем захисту від несанкціонованого доступу, зокрема з використанням сучасних технічних і криптографічних засобів з сучасними можливостями шифрування і апаратною реалізацією відповідних стандартів.

МЕТА, КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ

1. Метою викладання навчальної дисципліни «Методи і засоби захисту інформації» є формування у студентів знань, навиків та уміння, які дозволять їм здійснювати аналіз, проектування і експлуатацію радіотехнічних систем урахуванням основних вимог інформаційної безпеки.

2. Компетентності та результати навчання, формування яких забезпечує вивчення дисципліни.

Загальні компетентності:

– ЗК 1 Здатність вчитися і бути навченим;

– ЗК 2. Знання та розуміння предметної області та розуміння професії;

– ЗК 3. Здатність застосовувати знання у практичних ситуаціях;
– ЗК 5. Здатність до адаптації та дії в новій ситуації;
– ЗК 7. Здатність до критичного аналізу, оцінки і синтезу нових та складних ідей;
– ЗК 8. Здатність вільно володіти державною та спілкуватися іноземною мовами;
– ЗК 10. Здатність до пошуку, оброблення та аналізу інформації з різних джерел;
– ЗК 12. Здатність приймати обґрунтовані рішення;
– ЗК 13. Здатність працювати як автономно, так і в команді.

Спеціальні (фахові, предметні) компетентності:

– СК 1. Проведення розробки і дослідження теоретичних і експериментальних моделей об’єктів професійної діяльності;
– СК 2. Здатність здійснювати збір, аналіз науково-технічної інформації, вітчизняного і зарубіжного досвіду по тематиці дослідження;
– СК 3. Вміння здійснювати постановку та проведення експериментів по заданій методиці;
– СК 4. Здатність проводити аналіз результатів проведення експериментів, здійснювати вибір оптимальних рішень, готувати і складати огляди, звіти та наукові публікації;
– СК 7. Здатність демонструвати і використовувати фундаментальні знання принципів побудови сучасних електронних систем, систем контролю та керування, систем перетворення та збереження електричної енергії, перспективні напрямки розвитку їх елементної бази;
– СК 8. Здатність демонструвати і використовувати знання сучасних комп’ютерних та інформаційних технологій та інструментів інженерних і наукових досліджень, розрахунків, обробки та аналізу даних, моделювання та оптимізації;
– СК 9. Здатність демонструвати, аналізувати і використовувати знання сучасних друкованих та електронних ресурсів (в тому числі іншомовних) науково-технічної, довідникової та наукової інформації щодо стану, тенденцій та розвитку електронної техніки;
– СК 10. Здатність демонструвати і використовувати знання методів та технологій розробки, тестування та застосування інформаційно-вимірювальних, мікропроцесорних електронних систем, систем перетворення та передачі даних;
– СК 11. Здатність прогнозувати зміни в технологіях та параметрах радіотехнічних та телекомунікаційних систем та їх складових, використовуючи патентні дослідження, рекомендації і стандарти, світову наукову та технічну літературу.

Програмні результати навчання:

– РН 2. Знати принципи побудови і функціонування радіоелектронних систем та комплексів, принципи побудови і функціонування цифрових систем зв'язку та вміти проектувати цифрові системи зв'язку, основні задачі синтезу оптимальних радіотехнічних систем, основні методи оптимального виявлення і розпізнавання сигналів в радіотехнічних системах. Вміти оцінювати показники оптимальності проектування радіотехнічних та телекомунікаційних систем, застосовувати математичний апарат та алгоритми при проектуванні радіотехнічних пристрої, систем та комплексів. Вміти формулювати вимоги до технічних параметрів, проводити розрахунок і побудову, проводити енергетичний розрахунок радіоелектронних систем та комплексів;

– РН 7. Знати методологію наукових досліджень, процес і підходи до обробки теоретичної та практичної інформації; знати порядок апробації основних елементів наукової новизни. Вміти застосовувати знання з методології та організації наукових досліджень при вирішенні конкретних практичних завдань.

ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

Для успішного навчання та опанування компетентностями з даної дисципліни необхідно мати базові знання та вміння з наступних дисциплін:

– Теорія електричних кіл та сигналів;

– Антени спеціального призначення та системи автоматизованого проектування антен;

– Моделювання радіотехнічних систем;

– Теорія і проектування радіотехнічних систем.

ПЕРЕЛІК ТЕМ (ТЕМАТИЧНИЙ ПЛАН) ДИСЦИПЛІНИ

Таблиця 1 – Загальний тематичний план аудиторної роботи

Номер тижня	Теми лекцій, год.	Теми лабораторних/практичних робіт або семінарів, год.
1	2	3
МОДУЛЬ 1		
Змістовий модуль 1. Основи інформаційної безпеки і захисту інформації		
1	Вступ. Основні концептуальні положення системи захисту інформації, (2 год.)	
2	Об'єкти захисту, відомості, що охороняються, і демаскуючі ознаки, (4 год.)	Лр. № 1. «Дослідження регламенту радіочастотного діапазону від 30 МГц до 1ГГц м. Запоріжжя », (4 год.)
3	Класифікація і основні характеристики технічних каналів просочування інформації, (6 год.)	
4		
5	Акустичні і віброакустичні канали просочування мовної інформації з об'ємів виділених приміщень, (4 год.)	Лр. № 2. «Дослідження спрямованих мікрофонів», (5 год.)
6		
7	Знімання інформації з використанням закладних пристроїв. Загальні характеристики і побудова закладних пристроїв, (6 год.)	Лр. № 3. «Контактне зняття мовної інформації з телефонної лінії з використанням програмно-апаратного комплексу», (6 год.)
8		
МОДУЛЬ 2		
Змістовий модуль 2. Методи і способи захисту інформації		
9	Виявлення каналів просочування інформації, (6 год.)	Лр. № 4. «Вивчення характеристик та будови пристрою СРМ-700 («Акула»)», (4 год.)
10		
11	Захист мовної інформації, (4 год.)	Лр. № 5. «Дослідження генератору акустичного зашумлення ANG-2200», (6 год.)
12		
13	Основи сучасної криптографії і питання шифрування. Криптографія і криптосистеми, (6 год.)	Лр. № 6. «Дослідження маскувача мовних сигналів», (5 год.)
14		
15	Огляд сучасних крипто-систем. Засоби аутентифікації даних і управління ключами шифрування, (6 год.)	
16		

САМОСТІЙНА РОБОТА

Таблиця 2 – Розподіл годин самостійної роботи студентів

№ тижня	Назва видів самостійної роботи студентів	Кількість годин
	МОДУЛЬ 1	
1	Забезпечення інформаційної безпеки. Основні принципи забезпечення інформаційної безпеки. Об'єкти захисту, відомості, що охороняються, і демаскуючі ознаки. Правові основи захисту інформації. Структура законодавства України в області захисту інформації. Інженерно-технічний захист та його класифікація.	7
2	Об'єкти, які підлягають захисту в технічних засобах передачі, зберігання і обробки інформації. Об'єкти, які підлягають захисту в допоміжних технічних засобах і системах.	4
	Первинні та вторинні демаскуючі ознаки. Формування переліку демаскуючих ознак методом експертних оцінок.	3
3		3
	Акустичні, вібраційні, акустоелектричні, оптоелектронні (лазерні) і параметричні канали витоку інформації.	3
	Електромагнітні, електричні та індукційні канали витоку інформації.	1
4		2
	Спроби злому засобів обчислювальної техніки	3
	Класифікація каналів по середовищу поширення, за способом створення, по фізичній природі	2
5		1
	Коефіцієнти поглинання, відображення, звукопроникності та звукоізоляція.	6
6		2
	Види об'єктів, які визначають вибір каналу прослуховування і тактику дій зловмисника.	5
7		3
	Радіозакладні пристрої, що перевипромінюють	4
8	Мережеві закладні пристрої	4
	МОДУЛЬ 2	
9	Автоматизовані пошукові комплекси.	5
	Засоби радіаційного контролю.	2
10		3
	Вібродатчики систем віброакустичного зашумлення.	4
11		3
	Особливості постановки активних перешкод.	4
12		3
	Блокові шифри. Шифри Хілла і Плейфера. Системи шифрування Віжинера.	4
13		3
	Системи одноразового використання. Датчики М-послідовностей.	4
14		3
	Криптосистема Ель-Гамаля. Криптосистеми на основі еліптичних рівнянь.	4
15		1
	Електронний підпис на основі алгоритму RSA. Цифрова сигнатура.	5
	Механізм запиту-відповіді. Механізм відмітки часу ("часовий штемпель").	1
16		4

РЕКОМЕНДОВАНІ ІНФОРМАЦІЙНІ ТА НАВЧАЛЬНО-МЕТОДИЧНІ ДЖЕРЕЛА

Навчально-методичні розробки:

1. Методичні вказівки до виконання лабораторних робіт з дисципліни «Методи і засоби захисту інформації» для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» всіх форм навчання. Частина 1 / Укл. І.М. Сметанін – Запоріжжя: НУ «Запорізька політехніка», 2024. – 79 с.
2. Методичні вказівки до виконання лабораторних робіт з дисципліни «Методи і засоби захисту інформації» для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» всіх форм навчання. Частина 2 / Укл. І.М. Сметанін – Запоріжжя: НУ «Запорізька політехніка», 2024. – 66 с.
3. Методичні вказівки для вивчення дисципліни «Методи і засоби захисту інформації» для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» заочної форми навчання / Укл.: І.М. Сметанін – Запоріжжя: НУ «Запорізька політехніка», 2024. – 62 с.
4. Електронні презентації лекцій в Microsoft PowerPoint / Розр. І.М. Сметанін.

Літературні джерела:

1. 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.
2. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.
4. Вишня В.Б. Основи інформаційної безпеки: навч. посібник / В.Б. Вишня, О.С. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
5. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с.
6. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А.В. Жилін, О.М. Шаповал, О.А. Успенський; ІСЗЗІ КПІ. – Київ: КПІ, Вид-во «Політехніка», 2021.– 213 с
7. Остапов С.Е. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С.Е. Остапов, С.П. Євсеєв, О.Г Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

ОЦІНЮВАННЯ

Види контролю: поточний, рубіжний.

Форма підсумкового контролю – **залік.**

Оцінювання навчальних успіхів студентів реалізується шляхом проведення поточного та рубіжного контролю успішності.

1. Курсом передбачені *лабораторні роботи*. Враховуючи активність студента на лабораторних заняттях та під час їх захисту, результати аудиторних опитувань студент може отримати в кожному модулі максимально 40 балів.

2. По закінченню першого і другого напівсеместру проводиться рубіжні контролі у вигляді *аудиторної модульної контрольної роботи шляхом тестування*. Максимальна рейтингова оцінка цих видів контролю – 60 балів.

3. За підсумками першого та другого рубіжного модульного контролю студент отримує залік з дисципліни за умови досягнення 60 бального порогу.

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота						Підсумкова
Модуль №1			Модуль № 2			
ЛР	МК	ΣМ1	ЛР	МК	ΣМ2	(ΣМ1+ΣМ2)/2
40	60	100	40	60	100	100

ЛР – лабораторні роботи; МК – модульна контрольна робота.

Отже, сумарна кількість балів, яку отримує студент впродовж семестру, складає 100.

ПОЛІТИКИ КУРСУ

Політика щодо відвідування, дедлайнів та перескладання:

- відвідування занять (лекцій, лабораторних робіт) є обов'язковим компонентом навчання;
- усі види робіт, передбачені курсом, усі завдання, передбачені програмою, мають бути виконані у встановлений термін;
- самостійну роботу здобувач виконує відповідно до методичних вказівок та визначених викладачем завдань і термінів;
- ліквідація заборгованості відбувається під час проведення консультацій з дисципліни, за оприлюдненим графіком.

При вивченні курсу також слід дотримуватись *політики академічної доброчесності*, що визначається Кодексом академічної доброчесності Національного університету «Запорізька політехніка» https://zp.edu.ua/uploads/dept_nm/Nakaz_N253_vid_29.06.21.pdf

ТЕХНІЧНІ ВИМОГИ ДЛЯ РОБОТИ НА КУРСІ

Щоб мати доступ до навчально-методичних розробок курсу необхідно мати особистий доступ до університетської навчальної платформи Moodle.

– Система дистанційного навчання НУ «Запорізька політехніка» (Система Moodle) https://moodle.zp.edu.ua/;

– Електронний Інституційний репозитарій НУ «Запорізька політехніка» http://eir.zp.edu.ua/;

– Інформаційні електронні ресурси наукової бібліотеки НУ «Запорізька політехніка» http://library.zp.edu.ua/.