Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра прикладної радіоелектроніки

[RE-347] ЗАХИСТ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ РАДІОЕЛЕКТРОННИХ СИСТЕМАХ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	G Інженерія, виробництво та будівництво
Спеціальність	G5 Електроніка, електронні комунікації, приладобудування та радіотехніка
Освітня програма	172Б ІТРЕТ+ - Інтелектуальні технології радіоелектронної техніки (ЄДЕБО id: 57907)G5Б ІТРЕТ - Інтелектуальні технології радіоелектронної техніки (ЄДЕБО id: 83616)
Статус дисципліни	Нормативна
Форма здобуття вищої освіти	Очна
Рік підготовки, семестр	4 курс, осінній семестр
Обсяг дисципліни	4 кред. (Лекц. 20 год, Практ. 30 год, Лаб. год, СРС. год)
Семестровий контроль/контрольні заходи	Залік
Розклад занять	https://schedule.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лекц.: Навроцький Д. О., Практ.: Степанов М. М.,
Розміщення курсу	

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Дисципліна «Захист інформації в інтелектуальних радіоелектронних системах» призначена для надання студентами знань та навачок із забезпечення захисту інформації, яка циркулює і обробляється в інтелектуальних радіоелектронних системах та телекомунікаційних системах і мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в інтелектуальних системах з метою запобігання несанкціонованому доступи, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.

Дисципліна забезпечує такі загальні, фахові компетенції та програмні результати навчання:

ЗК 01 Здатність до абстрактного мислення, аналізу та синтезу

ЗК 02 Здатність застосовувати знання у практичних ситуаціях.

ЗК 04 Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 07 Здатність вчитися і оволодівати сучасними знаннями.

ФК 01 Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства

ФК 02 Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки

ФК 03 Здатність використовувати базові методи, способи та засоби отримання, передавання, обробки та зберігання інформації

ФК 14 Готовність до вивчення науково-технічної інформації, вітчизняного і закордонного досвіду з тематики інвестиційного (або іншого) проекту засобів телекомунікацій та радіотехніки.

ФК 18 Здатність оцінювати місце та переваги впровадження елементів інтелектуальних технологій та інтелектуальної радіоелектроніки в різні галузі діяльності людини

ФК 20 Здатність обирати методи та засоби обробки інформації із застосуванням інтелектуальних технологій.

ФК 24 Здатність до розробки алгоритмів та їх реалізації в програмно-конфігурованих радіоелектронних системах

ПРН 01 Аналізувати та приймати обґрунтовані рішення при розв’язанні спеціалізованих задач та практичних проблем телекомунікацій та радіотехніки, які характеризуються комплексністю та неповнотою визначеності умов

ПРН 13 Застосувувати фундаментальні і прикладні науки для аналізу та розробки процесів, що відбуваються в телекомунікаційних та радіотехнічних системах

ПРН 18 Знаходити, оцінювати і використовувати інформацію з різних джерел, необхідну для розв’язання професійних завдань, включаючи відтворення інформації через електронний пошук

ПРН 21 Забезпечувати надійну та якісну роботу інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем

ПРН 24 Реалізовувати методи цифрового оброблення сигналів на програмному та апаратному рівнях

ПРН 25 Обирати та реалізовувати засоби та методи передачі інформації в мережах зв'язку та застосовувати мережні технології

ПРН 27 Застосовувати основні методи та способи отримання інформації

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна «Захист інформації в інтелектуальних радіоелектронних системах» базується на дисциплінах: «Засоби зв'язку в інтелектуальних радіоелектронних системах».

В результаті вивчення дисципліни «Захист інформації в інтелектуальних радіоелектронних системах» студенти здобувають навики кваліфікованих спеціалістів з захисту інформації та зможуть використати їх в «Дипломному проектуванні».

3. Зміст навчальної дисципліни

Тема 1. Проблеми захисту інформації

Лб1 Ідентифікація загроз для об'єктів господарської діяльності

Тема 2. Характеристика загроз безпеки інформації. Несанкціонований доступ.

Лб2 Розроблення моделей загроз

Лб3 Розроблення моделей порушника

Тема 3. Шляхи забезпечення безпеки інформації

Лб4 Система управління безпекою підприємства.

Лб5 Методи безпечного програмування.

Лб6 Виявлення та усунення недоліків безпеки.

Тема 4. Політика безпеки інформації.

Лб7 Політика безпеки інформації- складова безпеки інформаційно-комунікаційних систем інформації.

Лб8 Моделі політики безпеки.

Тема 5. Криптографічні методи захисту інформації.

Лб9 Блочні шифри.

Лб10 RSA-алгоритм шифрування

Тема 6. Оцінювання захищеності інформаційно-комунікаційних систем.

Лб11 Захищеність систем від порушень конфіденційності

Лб12 Захищеність систем від порушень доступності

4. Навчальні матеріали та ресурси

Основна література

1. Жилін А. В. 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.https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf

2. Демчинський В. В. Основи технологій захисту інформації [електронний ресурс]: В. В. Демчинський, М.В. Грайворонський, О.В. Кіреєнко/Навчальний посібник/ Київ: КПІ, 2022. 107 с.

https://ela.kpi.ua/bitstream/123456789/53203/1/OTZI_Practices_plan_v115.pdf

3. Кушнерьов, О. С. Безпека інформації [Електронний ресурс] : конспект лекцій / О. С. Кушнерьов. — Суми : СумДУ, 2021. — 99

с.https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf

Допоміжна література

4. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. –Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print); 978-3-319-46529-6 (online). 127 p.

5. Тарнавський Ю.А. Технології захисту інформації [електронний ресурс]: підручник для студентів спеціальності 122 «Компютерні науки»/ Київ: КПІ, 2018. 162 с. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Інформаційні ресурси в Інтернеті

1. Державна служба спеціального зв'язку та захисту інформації України -https://cip.gov.ua/ua

2. Ободяк В.К. Матеріали навчального курсу "Технології захисту інформації" на платформі MIX - https://mix.sumdu.edu.ua/textbooks/66503/index.htm

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Тема 1. Проблеми захисту інформації

Періоди розвитку теорії захисту інформації у комп’ютерних системах та мережах. Основні підходи до розгляду питань теорії захисту інформації безпеки. Базові принципи захисту інформації. Забезпечення виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. Мережева модель OSI. Загальна характеристика проблем безпеки в розподілених інтелектуальних системах. Моделі розподілених систем в процесах розмежування доступу.

Лб1 Ідентифікація загроз для об’єктів господарської діяльності

Ідентифікація загроз для об’єктів господарської діяльності

Тема 2. Характеристика загроз безпеки інформації. Несанкціонований доступ.

Порушники безпеки. Характеристика загроз безпеки інформації. Порушення конфіденційності, цілісності та доступності інформації. Класифікація загроз безпеки інформації. Загроза розкриття. Способи несанкціонованого доступу. Загроза порушення цілісності. Загроза відмови в обслуговуванні. Порушники безпеки. Модель порушника.

Лб2 Розроблення моделей загроз

Розроблення моделей загроз інформаційної безпеки.

Лб3 Розроблення моделей порушника

Розроблення моделей порушника в інформаційному середовищі

Тема 3. Шляхи забезпечення безпеки інформації

Шляхи забезпечення безпеки інформації. Принципи створення безпечного програмного забезпечення. Концепція захисту інформації. Стратегія та архітектура захисту інформації. Використання сукупностей заходів, спрямованих на запобігання появи і усунення вразливостей програм.

Лб4 Система управління безпекою підприємства.

Управління безпекою підприємства (структура системи безпеки та структура концепції безпеки).

Лб5 Методи безпечного програмування.

Використання методів безпечного програмування. Їх поєднання з безпечним середовищем виконання.

Лб6 Виявлення та усунення недоліків безпеки.

Використання інструментів статичного та динамічного аналізу для виявлення та усунення недоліків безпеки.

Тема 4. Політика безпеки інформації.

Політика безпеки інформації. Моделі політики безпеки Політики безпеки інформації. Заходи політики безпеки. Реалізація політики безпеки. Підтримка політики безпеки. Дискреційна політика безпеки. Мандатна політика безпеки. Рольова політика безпеки. Монітор безпеки.

Лб7 Політика безпеки інформації- складова безпеки інформаційно-комунікаційних систем інформації.

Розробка політики безпеки інформації.

Лб8 Моделі політики безпеки.

Захист програмного забезпечення від несанкціонованого доступу.

Тема 5. Криптографічні методи захисту інформації.

Основи теорії шифрування. Блочні шифри. Асиметричне шифрування даних. Основні положення та визначення. Характеристика алгоритмів шифрування. Поняття блочного шифру та принципи його побудови. Схеми Фейстеля. Розширений стандарт шифрування (AES). Впровадження AES. Режими роботи блочних шифрів. Математичні основи RSA-шифрування. Генерація RSA-ключів. Електронні підписи на основі RSA. Реалізація RSA. Функції Діффі-Хеллмана.

Лб9 Блочні шифри.

Моделювання атаки кодової книги. Раунди блочного шифру. Мережі підстановки-перестановки та схеми Фейстеля.

Лб10 RSA-алгоритм шифрування

Генерація RSA-ключів.

Тема 6. Оцінювання захищеності інформаційно-комунікаційних систем.

Оцінювання захищеності інформаційно-комунікаційних систем. Система стандартів комплексних систем захисту інформації та управління інформаційною безпекою. Використання стандартів для проектування та оцінювання комплексних систем захисту інформації. Загальні критерії оцінювання безпеки інформаційних технологій. Методики оцінювання надійності систем захисту інформації від несанкціонованого доступу в

автоматизованих системах

Лб11 Захищеність систем від порушень конфіденційності

Методика оцінювання ефективності системи захисту інформації від несанкціонованого доступу для забезпечення конфіденційності даних

Лб12 Захищеність систем від порушень доступності

Методика оцінювання рівня готовності систем захисту інформації від несанкціонованого доступу для забезпечення доступності даних

6. Самостійна робота студента

Лекційне навчання — зокрема мультимедійні лекції з детальним викладенням навчального матеріалу, що поєднують пасивні методи навчання з елементами активних та інтерактивних підходів, — є основою формування навичок самостійного навчання здобувачів вищої освіти.

Лекційні заняття доповнюються практикоорієнтованими формами роботи, зокрема лабораторними завданнями, що виконуються на персональних комп'ютерах. Такий підхід дає змогу студентам застосовувати набуті теоретичні знання для розв'язання конкретних практичних ситуацій.

Важливу роль у розвитку самостійності відіграє підготовка до лекцій і лабораторних робіт, а також урахування коментарів викладача під час аналізу виконаних завдань чи робіт інших студентів. Це сприяє формуванню навичок самонавчання, покращує здатність ефективно планувати час, визначати пріоритети, виділяти головне й другорядне.

Крім того, студенти мають навчитися використовувати результати власного пошуку, аналізу та синтезу інформації з різних джерел, що формує критичне мислення та забезпечує підґрунтя для подальшого професійного зростання.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Система вимог, які ставляться перед студентом:

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:

• самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
• посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

• дотримання норм законодавства про авторське право і суміжні права;
• надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.
Порушенням академічної доброчесності вважається:
• академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
• самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів.
За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:
• - повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
• - повторне проходження відповідного освітнього компонента освітньої програми.
Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 баллів

від загальної кількості балів за це завдання.

Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування. Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, пандемія, хвороба, міжнародне стажування) навчання може відбуватися в онлайн-формі за погодженням із керівником курсу.
Лекційні та практичні заняття проводяться згідно до діючого положення КПІ ім. Ігоря Сікорського. Відвідування занять є обов'язковим. Для одержання іспиту «автоматом» потрібно набрати більше 60 балів, які можна одержати за виконання обов'язкових завдань (виконання ДКР, практичних робіт та написання модульної контрольної роботи) та систематично відвідавши лекційні заняття (пройшовши експрес-тест за матеріалами лекцій).
Бали за роботу під час лекції нараховуються на основі експрес-опитування. Кожний тест містить 2 запитання до матеріалу лекційного заняття, правильна відповідь на які дасть змогу отримати 2 бали.
Модульна контрольна робота проводиться письмово. Кожне завдання на контрольній роботі містить 2 теоретичних питання та 1 задачу, правильні відповіді на які дають змогу одержати до 100 балів за кожне теоретичне та 100 бали за практичне. Остаточна оцінка – середній бал від отриманих балів.
Індивідуальне завдання (ДКР) – це розв'язання 5 домашніх контрольних задач протягом семестру (по одній задачі на кожне наступне заняття), правильне розв'язання яких дасть змогу одержати до 100 бали за кожну задачу. Виконується у години самостійної роботи письмово.
Іспит є письмовим. Білет на іспиті складається з 3-х завдань (2 теоретичних питання та 1 задача) по тематиці змістовних тем, що виносяться на аудиторні заняття, та окремих питань, які виносяться на самостійне опрацювання.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Рейтинг студента з дисципліни складається із балів які він отримує вході навчання за семестр:

1. середня сума балів за відвідування та відповіді на лекційних заняттях;
2. середня сума балів за виконання модульних, самостійних та домашніх контрольних робот;
3. середня сума балів за виконання та захист лабораторних та практичних робіт;
4. сума заохочувальні та штрафні балів.

Виконання та захист всіх практичних та лабораторних робіт, а також наявність позитивної оцінки з контрольних робіт із частин є умовою допуску до заліку.

Практична, лабораторна, модульна контрольна, домашня та самостійна контрольна робота:

«відмінно», вичерпна відповідь (не менш ніж 95% вірної інформації) від 95 до 100 балів;

«дуже добре», повна відповідь, можливі незначні неточності (не менш ніж 85% вірної інформації) від 85 до 94 балів;

«добре», повна відповідь, можливі незначні неточності (не менш ніж 75% вірної інформації) від 75 до 84 балів;

«задовільно», неповна відповідь (але не менш ніж 60% вірної інформації) та незначні помилки від 60 до 74 балів;

«незадовільно», незадовільна відповідь (неправильний розв'язок задачі), потребує обов'язкового повторного написання в кінці семестру від 0 до 59 балів;.

За всі роботи за весь семестр зводиться середня сума балів, із 100 можливих.

Заохочувальні бали

Загалом, в сумі не більше за 10:

– за виконання творчих робіт з кредитного модуля (наприклад, участь у факультетських та інститутських олімпіадах з навчальних дисциплін, участь у конкурсах робіт, підготовка оглядів наукових праць тощо); успішне проходження рекомендованого дистанційного навчального курсу (що відповідає темам дисципліни) з отриманням відповідного сертифіката; за активну роботу на лекції (важливі запитання, доповнення, зауваження за темою лекції) від 1 до 5 балів;

– презентація за темою СРС – від 1 до 5 балів.

Залік:

Умовою допуску до заліку є зарахування всіх лабораторних та практичних робіт, та семестровий стартовий рейтинг $54 \leq R_{середня} \leq 80$.

Студенти, які виконали умови допуску можуть складати залік, як що загальна (середня) оцінка отримана ними в семестрі їх не задовольняє.

Система оцінювання заліку:

Залік оцінюється за шкалою $R_{залік}$ до 40 балів. Заліковє завдання складається з чотирьох завдань. Кожне завдання оцінюється за такими критеріями:

«*відмінно*» – вичерпна відповідь (не менше 95% вірної інформації), надані відповідні обґрунтування – 10 балів;

«*добре*» – повна відповідь (не менше 80% вірної інформації), що виконана згідно з вимогами до рівня «умінь», або присутні незначні неточності – 8 балів;

«*задовільно*» – неповна відповідь (не менше 60% вірної інформації та є деякі помилки) – 6 балів;

«*незадовільно*» – відсутність правильної відповіді – 0 балів.

Рейтинг сума ($R_{загальний}=R_{середня}+R_{залік}+R_{заохочення}-R_{штрафні}$) переводиться до оцінки згідно з таблицею:

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

1. Загальні питання інформаційної та радіоелектронної безпеки

1. Дайте визначення інформаційної безпеки в радіоелектронних інтелектуальних системах та її основні складники.
2. Що таке технічні канали витоку інформації та які їх основні класи?
3. Охарактеризуйте радіоелектронні системи як об’єкт впливу засобів радіоелектронної боротьби.
4. Які основні види загроз інформації у радіоелектронних системах?
5. Поясніть поняття "радіоелектронна розвідка" та її можливості щодо перехоплення сигналів.

2. Сигнали та моделі в радіоелектронних системах

1. Які основні параметри сигналу впливають на можливість його виявлення в умовах шуму?
2. Поясніть модель виявлення детермінованого сигналу на фоні білого шуму.
3. Що таке співвідношення сигнал/шум (SNR) та як воно впливає на завадостійкість системи?
4. Наведіть основні методи спектрального аналізу сигналів та їх застосування у захисті інформації.
5. Поясніть особливості обробки нестаціонарних сигналів (STFT, Wavelet).

3. Методи захисту радіосигналів

1. Перелічіть основні методи зниження ймовірності перехоплення радіосигналу.
2. Суть маскування сигналу в радіоканалах. У чому полягає принцип шумоподібного сигналоутворення?
3. Що таке псевдовипадкове перестрибування частоти (FHSS) та де воно використовується?
4. Поясніть принцип Direct Sequence Spread Spectrum (DSSS) та його переваги.
5. Які типи штучних завад застосовуються для захисту інформації?

4. Радіоелектронна боротьба та протидія

1. У чому полягає робота засобів радіоелектронної боротьби (РЕБ) щодо придушення каналів зв'язку?
2. Які параметри впливають на ефективність придушення каналу радіозв'язку?
3. Поясніть методи підвищення завадостійкості приймачів.
4. Опишіть принципи оцінки перехоплення радіосигналів засобами РТР.
5. Які особливості захисту сенсорних мереж від перехоплення сигналу?

5. Криптографічні та апаратні методи захисту

1. Яке значення має криптографія у радіоелектронних інтелектуальних системах?
2. Поясніть різницю між симетричними та асиметричними методами шифрування у радіоканалах.
3. Які апаратні засоби можуть застосовуватися для захисту каналів зв'язку?
4. Що таке TPM, HSM та їхня роль у забезпеченні кібер- та радіобезпеки?
5. Які переваги та недоліки має захист сигналу через зменшення зони його приймання?

6. Моніторинг, аналіз та оцінювання безпеки

1. Методи оцінки ймовірності перехоплення сигналу в умовах радіорозвідки.
2. Які метрики використовують для оцінювання ефективності маскування сигналів?
3. Як математичне моделювання допомагає в оцінці захищеності радіоелектронних систем?
4. Розкажіть про статистичні методи аналізу сигналів та виявлення прихованих передач.
5. Які принципи формування захищених каналів у інтелектуальних радіоелектронних системах?

Опис матеріально-технічного та інформаційного забезпечення дисципліни

Мультимедіа, відео- і звуковідтворювальна, проєкційна апаратура (відеокамери, проєктори, екрани, смартдошки тощо). Комп'ютерний клас для лабораторних занять, комп'ютери, комп'ютерні системи та мережі. Програмне забезпечення для підтримки дистанційного навчання.

Робочу програму навчальної дисципліни (силабус):
Складено Навроцький Д. О.; Степанов М. М.;
Ухвалено кафедрою ПРЕ (протокол № 06/2025 від 24.06.2025)
Погоджено методичною комісією факультету/ННІ (протокол № 06/2025 від 26.06.2025)