КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет радіофізики, електроніки та комп'ютерних систем

Кафедра радіотехніки та радіоелектронних систем

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ О. Нечипорук
«30» 06 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ І МЕРЕЖ ТЕЛЕКОМУНІКАЦІЙ

для студентів

галузь знань	**17 Електроніка та телекомунікації**
спеціальність	**172 Телекомунікації та радіотехніка**
освітній рівень	**другий (магістр)**
освітня програма	**Захист інформації в телекомунікаціях**
спеціалізація	**Системи та мережі телекомунікацій**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2021/2022**
Семестр	**2**
Кількість кредитів ECTS	**5**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладач:
Давиденко Анатолій Миколайович, доктор технічних наук, доцент кафедри радіотехніки та радіоелектронних систем

Пролонговано: на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р.
на 20__/20__ н.р. _____ (_____) «___» _____ 20__ р.

КИЇВ – 2021

Розробник:

Давиденко Анатолій Миколайович, доктор технічних наук, доцент кафедри радіотехніки та радіоелектронних систем

ЗАТВЕРДЖЕНО

Завідувач кафедри радіотехніки та радіоелектронних систем

_____ І. Анісімов

Протокол № 15 від «23» 06 2021 р.

Схвалено науково-методичною комісією факультету радіофізики, електроніки та комп'ютерних систем

Протокол № 6 від «29» 06 2021 р.

Голова науково-методичної комісії _____ С. Радченко

« ___ » _____ 2021 року.

Мета дисципліни – надання основних відомостей про принципи та методи розробки і використання програмних та програмно-апаратних засобів для захисту інформації в інформаційно-телекомунікаційних системах (ІТС).

Набуття теоретичних знань:

- основні уразливості програмного забезпечення;
- сценарії атак на програмне забезпечення;
- власні засоби захисту;
- засоби захисту у складі комп'ютерних систем;
- засоби захисту з запитом інформації;
- засоби активного та пасивного захисту;
- копіювання інформації та її захист від неавторизованої сторони.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

Навчальна дисципліна «Програмне забезпечення систем і мереж телекомунікацій» є частиною вибіркового блоку дисциплін та базується на циклі дисциплін професійної та практичної підготовки, зокрема: “Теорія передавання інформації ”, “Оптимізація проектування радіоелектронних засобів”, «Адаптивні системи обробки сигналів», «Супутникові інформаційні системи», «Комплексні системи захисту інформації», «Моделі та побудова систем захисту інформації», «Курсовий проект з розробки та конструювання складових систем захисту інформації», «Безпека інформації та конкурентна розвідка в інженерії». Попередні вимоги:

1. Вміти запускати прикладні програмні засоби та керувати ними на основі графічного інтерфейсу користувача, знаходити інформацію в Інтернеті.
2. Знати основи побудови засобів та систем захисту інформації.
3. Знати порядок побудови комплексних систем захисту інформації та комплексів технічного захисту інформації з використання засобів захисту інформації.

3. Анотація навчальної дисципліни:

Вивчення дисципліни «Програмне забезпечення систем і мереж телекомунікацій» дозволяє зрозуміти сутність процесу використання технології програмного захисту в системах та мережах телекомунікацій. Розглядаються загальні вимоги до організації технологій програмного захисту. А саме: предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні уразливості програмного забезпечення. Сценарії атак на програмне забезпечення. Власні засоби захисту (документація, завантажувальні модулі, супроводження, обмежене використання, замовлене проектування). Засоби захисту у складі комп'ютерних систем (захист дисків, спеціальна апаратура, замки захисту, зміна функцій в системі). Засоби захисту з запитом інформації (паролі, шифри, сигнатури, апаратура). Засоби активного захисту (внутрішні та зовнішні). Засоби пасивного захисту (ідентифікація, засоби контролю, водяні знаки, психологічні міри). Копіювання інформації та її захист від неавторизованої сторони. Розробники та хакери. Взаємозв'язок захисту програм від копіювання, дезасемблювання та налагодження. Захист програм від копіювання та його подолання. Статичні та динамічні методи. Статичні методи захисту (неявні та динамічні переходи, перевизначення кодів через стек та їх самогенерація, конкатенація з навантажувальним кодом, захоплення універсальним захисним модулем та криптографічне перетворення коду). Динамічні методи (дозвіл та заборона переривань, контроль програми в пам'яті та часу виконання, відновлення та перевизначення векторів переривань, блокування консолі, перевірка вільної пам'яті та її доступних областей, використання специфіки функціонування налагоджувальних і апаратних засобів комп'ютерних систем). Механізми дії руйнівних програмних впливів та їх класифікація (комп'ютерні віруси, логічні бомби, потайні ходи та лазівки, програми відкриття паролів, реплікаторів, програмні аналізатори для мереж, суперзапингові утиліти, троянські коні).

Комп'ютерні віруси та їх класифікація. За середовищем розповсюдження, за способом маскування в середовищі, за інфікованими об'єктами, за способом інфікування об'єкту, за способом розміщення в інфікованому об'єкті, за руйнівною дією, за здатністю до зміни, за стилем написання, за типом коду. Способи розповсюдження комп'ютерних вірусів та їх структура. Виявлення та вилучення вірусів. Засоби захисту від комп'ютерних вірусів. Моделі поведінки програмних закладок у комп'ютерних системах та їх вплив на програми захисту інформації. Деструктивні функції закладок. Руйнівний вплив програмних закладок на захищені програмні середовища та на програмно-апаратні засоби захисту. Захист від впливів програмних закладок. Аналіз характеристик програм, стилю програмування та ідентифікаційних міток. Достовірність ідентифікації. Метод водяних знаків. Аналіз програмних процедур. Програмне забезпечення захисту інформації. Програми захисту від копіювання. Антивірусні програми. Програми захисту даних, що передаються телекомунікаційними каналами загального користування. Програми захисту дисків та файлів. Загальні положення, основні терміни та визначення, критерії оцінки захищеності, стандартні функціональні профілі захищеності та їх використання для побудови програмних засобів захисту інформації.

4. Завдання (навчальні цілі):

1. Надати основні відомості курсу «Програмне забезпечення систем і мереж телекомунікацій», які складають важливу частину *Вибіркового блоку " Системи та мережі телекомунікацій "*.
2. Узагальнити та розширити відомі поняття курсів "Теорія передавання інформації ", "Оптимізація проектування радіоелектронних засобів", «Адаптивні системи обробки сигналів», «Супутникові інформаційні системи», «Комплексні системи захисту інформації», «Моделі та побудова систем захисту інформації», «Курсовий проект з розробки та конструювання складових систем захисту інформації», «Безпека інформації та конкурентна розвідка в інженерії», простежити взаємозв'язок об'єктів досліджень засобів захисту інформації з іншими компонентами інформаційно-телекомунікаційних систем; продемонструвати застосування теоретичних відомостей до розв'язання практичних та експериментальних задач;
3. Навчити застосовувати знання, уміння, навички і комунікації у професійній діяльності, розвивати логічне та аналітичне мислення студентів.
4. Прищепити вміння розв'язувати прикладні задачі методами системного підходу (декомпозиція складної системи, аналіз складових процесів та підсистем, визначення вимог з захисту інформації, визначення методик випробувань, оцінка захищеності інформації).

Забезпечити досягнення компетентностей:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Навички використання інформаційних і комунікаційних технологій.

5. Результати навчання за дисципліною:

Результат навчання (1, знати; 2, вміти; 3, комунікація; 4, автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	Результат навчання			
1	студент повинен **знати**:	лекційні заняття	письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи	до 45

1.1	Основні уразливості програмного забезпечення	*лекція*	–//–	до 2
1.2	Сценарії атак на програмне забезпечення	–//–	–//–	до 3
1.3	Власні засоби захисту	–//–	–//–	до 5
1.4	Засоби захисту у складі комп'ютерних систем	–//–	–//–	до 5
1.5	Засоби захисту з запитом інформації	–//–	–//–	до 5
1.6	Засоби активного та пасивного захисту	–//–	–//–	до 5
1.7	Копіювання інформації та її захист від неавторизованої сторони	–//–	–//–	до 5
1.8	Взаємозв'язок захисту програм від копіювання, дезасемблювання та налагодження	–//–	–//–	до 5
1.9	Статичні та динамічні методи захисту	–//–	–//–	до 5
1.10	Механізми дії руйнівних програмних впливів та їх класифікація	–//–	–//–	до 5
2	студент повинен **вміти**:	лекційні заняття, практичні та лабораторні заняття	письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи	до 45
2.1	Самостійно проектувати програмне забезпечення	–//–	–//–	до 15
2.2	Самостійно експлуатувати програмні засоби захисту інформації в ІТС, які забезпечують потрібний рівень захисту	–//–	–//–	до 15
2.3	Самостійно вміти підібрати комплекс вказаних програмних засобів для забезпечення заданого рівня	–//–	–//–	до 15
3	**комунікація**	лекційні заняття, практичні та лабораторні заняття		до 5
3.1	здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування			до 3
3.2	здатність бути відповідальним за внесок в роботу команди при вирішенні проблеми	лекційні заняття з використанням роботи у підгрупах	оцінювання виконання завдань для самостійної	до 2
4	автономність та відповідальність	лекційні заняття, практичні та лабораторні заняття	письмові модульні контрольні роботи, оцінювання виконання завдань для самостійної роботи	до 5
4.1	самостійність у навчанні та/або професійній діяльності			до 5

6. Забезпечення програмних результатів навчання при вивченні дисципліни

ПРН 4. Знати аналогові та цифрові, в тому числі адаптивні, методи обробки інформації

ПРН 5. Знати архітектуру телекомунікаційних систем, їх апаратні та програмні складові, тенденції їх розвитку.

ПРН 15. Застосовувати знання для вирішення конкретних інженерно-технічних задач телекомунікації та захисту інформації.

ПРН 20. Розв’язувати складні дослідницькі та інженерно-технічні задачі у галузі телекомунікацій та радіотехніки та інформаційної безпеки, які вимагають фундаментальних знань у галузі фізики, математики, комп’ютерних технологій, моделювання.

7. Схема формування оцінки

7.1. Форми оцінювання студентів: рівень досягнення всіх запланованих результатів навчання визначається за результатами написання письмових контрольних робіт і за результатами виконання самостійних завдань. Вклад результатів навчання у підсумкову оцінку, за умови їх опанування на належному рівні і успішної здачі всіх лабораторних робіт наступний:

- результати навчання 1.1 – 1.10 [**знання**] до 45 %;
- результат навчання 2.1 – 2.3 [**вміння**] – до 45%;
- результат навчання 3.1 [**комунікація**] – до 5%;
- результат навчання 4.1 [**автономність та відповідальність**] – до 5%.

Форми оцінювання студентів:

- **семестрове оцінювання**: контроль здійснюється за таким принципом. Навчальний семестр має один змістовний модуль. Після завершення відповідних тем проводяться письмова модульна контрольна робота. Для визначення рівня досягнення результатів навчання завдання для модульної контрольної роботи перевіряють уміння розв’язувати конкретні задачі з теорії адаптивних систем. Обов’язковим для допуску до іспиту є написання модульної контрольної роботи з кількістю балів не менше 7 балів та виступу з доповідь на семінарі.
- **підсумкове оцінювання (у формі іспиту):** форма іспиту – письмово-усна. Екзаменаційний білет складається із 2 питань, питання оцінюються по 20 балів. Всього на іспиті можна отримати від 0 до 40 балів. Умовою досягнення позитивної оцінки за дисципліну є отримання не менш ніж 60 балів, при цьому оцінка за результатами навчання 2 [вміння] і 3 [комунікативність та відповідальність] не може бути меншою ніж 50% від максимального рівня (23 і 5 балів відповідно), оцінка за іспит не може бути меншою **24 балів.**
- **умови допуску до підсумкового іспиту:** умовою допуску до іспиту є отримання студентом сумарно не менше, ніж *критично-розрахунковий мінімум 36 балів* за семестр. Студенти, які протягом семестру набрали сумарно меншу кількість балів, ніж критично-розрахунковий мінімум **36 балів**, для одержання допуску до іспиту обов’язково повинні написати, на необхідну порогову кількість балів, додаткову контрольну роботу за матеріалом модуля.

У випадку відсутності студента з поважних причин відпрацювання та перездачі модульних контрольних робіт здійснюються у відповідності до „Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу” від 1 жовтня 2010 року.

7.2. Організація оцінювання (*обов’язково зазначається порядок організації передбачених робочою навчальною програмою форм оцінювання із зазначенням орієнтованого графіку оцінювання*):

Оцінювання за формами контролю:

	ЗМ	
	Мін. – балів	*Мах. – балів*
Модульна контрольна робота	7	12
Виступ на семінарі	15	25
Виконання студентами самостійних робіт	5	8

Виконання студентами лабораторних робіт	9	15

Орієнтований графік оцінювання:

	Орієнтовний період для здійснення відповідної форма оцінювання
Модульна контрольна робота	травень
Виступ на семінарі	травень
Виконання студентами самостійних робіт	січень-травень
Добір балів/додаткова контрольна робота та/або доскладання домашніх завдань	травень
Іспит	червень

Розрахунок балів, які студент отримує при успішній здачі іспиту:

	Змістовий модуль	Іспит	Підсумкова оцінка
Мінімум	*36*	*24*	*60*
Максимум	**60**	**40**	**100**

7.3. Шкала відповідності оцінок

Оцінка (за національною шкалою) / National grade	Рівень досягнень, % / Marks, %
Відмінно / Excellent	90-100%
Добре / Good	75-89%
Задовільно / Satisfactory	60-74%
Незадовільно / Fail	0-59%

8. Структура навчальної дисципліни. Тематичний план лекційних занять

№ з/п	Назва теми	У тому числі			
		Лекції	Семінарські заняття	Лабораторні заняття	Самостійна робота
1.	Місце дисципліни в системі підготовки фахівця із організації інформаційної безпеки.	2			6
2.	Основні уразливості програмного забезпечення.	2	2		7
3.	Сценарії атак на програмне забезпечення.	2			6
4.	Власні засоби захисту.	2	2		8
5.	Засоби захисту у складі комп'ютерних систем.	2		2	6
6.	Засоби захисту з запитом інформації.	2	2		7
7.	Засоби активного захисту.	2			6
8.	Засоби пасивного захисту.	2	2		8
9.	Копіювання інформації та її захист від неавторизованої сторони.	2		2	6

10.	Взаємозв'язок захисту програм від копіювання, дезасемблювання та налагодження.	2	2		7
11.	Статичні та динамічні методи захисту.	2			6
12.	Механізми дії руйнівних програмних впливів та їх класифікація.	2	2		8
13.	Комп'ютерні віруси та їх класифікація.	2		2	6
14.	Руйнівний вплив програмних закладок на захищені програмні середовища та на програмно-апаратні засоби захисту.	2	2		7
15.	Захист від впливів програмних закладок.	2			6
ЗАГАЛОМ		30	14	6	100

Загальний обсяг **150** год., в тому числі:
Лекції **– 30** год.
Семінарські заняття – **14** год.
Лабораторні заняття – **6** год.
Самостійна робота **- 100** год.

9. Рекомендовані джерела:

Основна література:

1. Семененко В. А., Федоров Н. В. Программно-аппаратная защита информации: Учебное пособие. – М.: МГИУ, 2007. – 340 с.

2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. – 2-е изд., стер. / Клейменов С. А., ред. – М.: Академия, 2007. – 332 с.

3. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с.

4. Юдін О.І., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2009. – 716 с.

Додаткова література:

1. Кулик Н.С., Харченко В.П., Луцкий М.Г. и др. Энциклопедия безопасности авиации; Под. ред. Н.С. Кулика. – К.: Техніка, 2008. – 1000с.; ил. – Библиогр.: с. 977-999.