

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ НАФТИ І ГАЗУ

Інститут інформаційних технологій

(назва інституту)

Кафедра інформаційно-телекомунікаційних технологій та систем

(назва кафедри)

ЗАТВЕРДЖУЮ

Директор інституту
інформаційних технологій
(назва інституту)

І.З. Лютак
(підпис) (прізвище та ініціали)

« » 2019 р.

ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

(назва навчальної дисципліни)

РОБОЧА ПРОГРАМА

Перший (бакалаврський) рівень
(рівень вищої освіти)

галузь знань

17 Електроніка та телекомунікації
(шифр і назва)

спеціальність

172 Телекомунікації та радіотехніка
(шифр і назва)

спеціалізація

(назва)

вид дисципліни

вибіркова
обов'язкова /вибіркова

Івано-Франківськ-2019

Робоча програма дисципліни «Захист інформації в телекомунікаційних системах» для студентів, що навчаються за освітньо-професійною програмою на здобуття ступеня бакалавра за спеціальністю «172 Телекомунікації та радіотехніка».

Розробник:

доц. кафедри ІТТС, к.т.н.
(посада, назва кафедри, науковий ступінь, вчене звання)



Гринчишин Т.М.
(прізвище та ініціали)

Робочу програму схвалено на засіданні кафедри інформаційно-телекомунікаційних технологій
та систем
(назва кафедри)

Протокол від «29» 08 2019 року № 1.

Завідувач кафедри ІТТС
(назва кафедри)



Заміховський Л.М.
(прізвище та ініціали)

Узгоджено:

Завідувач випускової кафедри

інформаційно-телекомунікаційних технологій
та систем
(назва кафедри)



Заміховський Л.М.
(прізвище та ініціали)

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Ресурс годин на вивчення дисципліни «Захист інформації в телекомунікаційних системах» згідно з чинним РНП, розподіл по семестрах і видах навчальної роботи для різних форм навчання характеризує таблиця 1.

Таблиця 1 – Розподіл годин, виділених на вивчення дисципліни «Захист інформації в телекомунікаційних системах»

Найменування показників	Всього		Розподіл по семестрах			
			Семестр 7		Семестр ____	
	Денна форма навчання (ДФН)	Заочна (дистанційна) форма навчання (ЗФН)	Денна форма навчання (ДФН)	Заочна (дистанційна) форма навчання (ЗФН)	Денна форма навчання (ДФН)	Заочна (дистанційна) форма навчання (ЗФН)
Кількість кредитів ECTS	5	5	5	5		
Кількість модулів	1	1	1	1		
Загальний обсяг часу, год	150	150	150	150		
Аудиторні заняття, год, у т.ч.:	72	16	72	16		
лекційні заняття	36	8	36	8		
семінарські заняття	-	-	-	-		
практичні заняття	-	-	-	-		
лабораторні заняття	36	8	36	8		
Самостійна робота, год, у т.ч.	78	134	78	134		
виконання курсової роботи	-	-	-	-		
виконання контрольних (розрахунково-графічних) робіт		2		2		
опрацювання матеріалу, викладеного на лекціях	38	70	30	54		
опрацювання матеріалу, винесеного на самостійне вивчення	30	54	38	70		
підготовка до практичних занять та контрольних заходів	-	-	-	-		
підготовка звітів з лабораторних робіт	10	10	10	10		
підготовка до екзамену	-	-	-	-		
Форма семестрового контролю	Диференційований залік		Диференційований залік			

2 МЕТА ТА РЕЗУЛЬТАТИ НАВЧАННЯ

Навчальна дисципліна “Захист інформації в телекомунікаційних системах” відноситься до дисциплін підготовки студентів з спеціальності і дає теоретичні та практичні основи організації та забезпечення технічного та криптографічного захисту інформації в інформаційно-телекомунікаційних системах та мережах.

Мета вивчення дисципліни – формування у студентів теоретичних та практичних основ організації систем та криптографічного захисту інформації в телекомунікаційних системах.

У результаті вивчення дисципліни студент повинен демонструвати такі **результати навчання** через знання, уміння та навички:

- вимоги нормативно-керівних документів України з технічного захисту інформації в телекомунікаційних системах;
- основні методи та заходи захисту інформації технічними каналами;
- основи забезпечення технічного та криптографічного захисту інформації;
- запропонувати криптографічний метод захисту інформації в телекомунікаційних системах
- забезпечувати виконання вимог відповідальних нормативно-керівних документів України по захисту інформації в телекомунікаційних системах;
- створювати обґрунтування та вибір необхідних заходів по забезпеченню захисту інформації в телекомунікаційних системах;
- забезпечувати надійні, ефективні, економічні та безпечні технічні обслуговування та методи захисту інформації від витоку інформації.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **компетентностей, передбачених відповідним стандартом вищої освіти України:**

загальних:

- навички використання інформаційних і комунікаційних технологій;
- здатність приймати обґрунтовані рішення;
- здатність розробляти та управляти проектами.

фахових:

- здатність розроблення криптографічного методу захисту інформації з використанням математичного апарату та програмного забезпечення;
- здатність аналізувати використаний криптографічний захист інформації.

Результати навчання дисципліни **деталізують такі програмні результати навчання, передбачені відповідним стандартом вищої освіти України:**

- демонструвати здатність генерувати нові ідеї, приймати нестандартні рішення у процесі забезпечення технічного та криптографічного захисту інформації;
- демонструвати вміння приймати технічно та економічно обґрунтовані рішення на всіх етапах забезпечення технічного та криптографічного захисту інформації;
- демонструвати навички розроблення та практичної реалізації науково-технічних проектів, щодо забезпечення технічного та криптографічного захисту інформації.

3 ПРОГРАМА ТА СТРУКТУРА ДИСЦИПЛІНИ

3.1 Тематичний план лекційних занять

Тематичний план лекційних занять дисципліни “Захист інформації в телекомунікаційних системах” характеризує таблиця 2.

Таблиця 2 – Тематичний план лекційних занять

Шифр	Назви модулів (М), змістових модулів (ЗМ), тем (Т) та їх зміст	Обсяг годин		Література	
		ДФН	ЗФН	порядковий номер	розділ, підрозділ
М 1	ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ	36	8		
ЗМ1	Законодавство України про захист інформації в телекомунікаційних системах та методи, системи криптографічного захисту інформації в телекомунікаційних системах.	24	8	1	1.3
Т 1.1	Вступ. Основні поняття, терміни та визначення телекомунікаційних систем та захисту інформації, їх класифікація, основні компоненти.	4	6	1	1
Т 1.2	Захист інформації у інформаційних системах. Законодавство України про захист інформації в телекомунікаційних системах. Класифікація методів і засобів захисту інформації. Приклади.	6		1, 2	1.1 1.2
Т 1.3	Основні терміни та поняття криптографічного захисту. Вступ. Історичний нарис розвитку криптографії.	6		1	1
Т 1.4	Криптографічний захист інформації. Теоретичні основи криптографічного захисту інформації. Шифрування методами перестановки та простої заміни. Шифрування методами складної заміни, гамування. Приклади.	8		1 3	1,2
ЗМ2	ЗАГАЛЬНІ ПОЛОЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТИВ.	12	2	2	1.3
Т 1.5	Загальні положення захисту інформації Безпека інформаційних ресурсів у інформаційно-комунікаційних системах. Організація технічного захисту інформації. Методика і критерії оцінки захищеності інформації. Методика захисту інформації шляхом відновлення втрачених даних.	6		2	2.1-2.3
Т 1.6	Міжнародні стандарти захисту інформації. Захист інформації на базі ISO/IEC. Задачі організації безпеки інформації. Управління доступом і забезпечення цілісності програмного забезпечення.	6		2	2.1 2.2

Всього:

Модуль 1 – змістових модулів -2.

3.2 Теми лабораторних занять

Теми лабораторних занять дисципліни “Захист інформації в телекомунікаційних системах”

Таблиця 3 – Теми лабораторних занять

Шифр	Назви модулів (М), змістових модулів (ЗМ), теми лабораторних занять	Обсяг годин		Література	
		ДФН	ЗФН	порядковий номер	розділ, підрозділ
М 1	ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ	36	6	1	1.3
ЗМ1	Законодавство України про захист інформації в телекомунікаційних системах та методи, системи криптографічного захисту інформації в телекомунікаційних системах.	26	4		
Л 1.1	Шифри заміни	2	2	2	1.1
Л 1.2	Шифри перестановок	4	2	2	1.1
Л 1.3	Теоретичні передумови створення секретних кодів або шифрів	4		1	1.1
Л 1.4	Шифр Гронсфельда	2		1	1.1
Л 1.5	Шифри перестановок	4		2	1.1
Л 1.6	Шифр Плейфера	4		5	
Л 1.7	Комп'ютерна програма шифрування і цифрового підпису	2		2	4
Л 1.8	Шифр Вернама	4		6	
ЗМ2	Загальні положення захисту інформації на основі міжнародних стандартів.	10	2		
Л 2.1	Шифрування даних та передача даних	4		1	1
Л 2.2	Методика захисту інформації шляхом відновлення втрачених даних. Засоби захисту комп'ютерів від вірусів.	6		1	1

3.3 Завдання для самостійної роботи студента

Перелік матеріалу, який виноситься на самостійне вивчення, наведено у таблиці 4.

Таблиця 4 – Матеріал, що виноситься на самостійне вивчення

Шифри	Назви модулів (М), змістових модулів (ЗМ), питання, що виноситься на самостійне вивчення	Обсяг годин	Література	
			порядковий номер	розділ, підрозділ
М 1	ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ	30		

Шифри	Назви модулів (М), змістових модулів (ЗМ), питання, що виноситься на самостійне вивчення	Обсяг годин	Література	
			порядковий номер	розділ, підрозділ
ЗМ1	Законодавство України про захист інформації в телекомунікаційних системах та методи, системи криптографічного захисту інформації в телекомунікаційних системах.	26		
Т 1.3	Симетричні алгоритми. Асиметричні алгоритми. Приклади.	12	1 4	3
Т 1.4	Хешувальні функції. Цифрові підписи. Приклади	14	1 2	3 6
ЗМ2	Загальні положення захисту інформації на основі міжнародних стандартів.	4		
Т 1.6	Модель безпеки інформаційної системи	4	1	2.4

3.4 Курсове проектування

Курсове проектування не передбачене по дисципліні “Захист інформації в телекомунікаційних системах”

4 НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

4.1 Основна література

1 Добров, Є. Є. Захист інформації і комп'ютерна криптографія [Текст] : конспект лекцій / Є. Є. Добров. – Івано-Франківськ : ІФНТУНГ, 2007. – 47 с. – (Кафедра комп'ютерних технологій в системах управління і автоматики).

4.2 Додаткова література

2 Белей, О. І. Інформаційна безпека та захист інформації [Текст] : конспект лекцій / О. І. Белей. – Івано-Франківськ : ІФНТУНГ, 2017. – 32 с. – (Каф. інформаційно-телекомунікаційних технологій та систем).

4.3 Література та методичне забезпечення лабораторних занять

3 Добров, Є. Є. Захист інформації та комп'ютерна криптографія [Текст] : лаборатор. практикум / Є. Є. Добров, Ю. В. Безгачнюк, О. І. Клапоущак. – Івано-Франківськ : ІФНТУНГ, 2013. – 39 с. : рис. – (Кафедра комп'ютерних технологій в системах управління і автоматики). – 39.

4.4 Література та методичне забезпечення самостійної роботи

4 Белей, О. І. Захист інформації інформації [Текст] : метод. вказ. для самостійної роботи студентів / О. І. Белей. – Івано-Франківськ : ІФНТУНГ, 2017. – 11 с. – (Каф. інформаційно-телекомунікаційних технологій та систем).

4.5 Інформаційні ресурси в Інтернеті

5 Електронний ресурс «Шифр Плейфера»:
<http://neudoff.net/info/informatika/bigrammnyj-shifr-plejfejra/>

6 Електронний ресурс «Шифр Верма»:
http://cryptowiki.net/index.php?title=%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B5%D1%80%D0%BD%D0%B0%D0%BC%D0%B0

5 МЕТОДИ КОНТРОЛЮ ТА СХЕМА НАРАХУВАННЯ БАЛІВ

Оцінювання знань студентів проводиться за результатами комплексних контролів за двома змістовими модулями ЗМ1 і ЗМ2. Модульний контроль за кожним змістовим модулем передбачає контроль теоретичних знань і практичних навиків. Схему нарахування балів при оцінюванні знань студентів з дисципліни наведено в таблиці 5.

Таблиця 5 – Схеми нарахування балів у процесі оцінювання знань студентів з дисципліни “Захист інформації в телекомунікаційних системах”

Види робіт, що контролюються	Максимальна кількість балів
Контроль засвоєння теоретичних знань змістового модуля ЗМ1	30
Контроль засвоєння матеріалу по лабораторних роботах змістового модуля ЗМ1	30
Контроль засвоєння теоретичних знань змістового модуля ЗМ2	20
Контроль засвоєння матеріалу по лабораторних роботах змістового модуля ЗМ2	20
Усього	100

Диференційований залік з дисципліни виставляється студенту відповідно до чинної шкали оцінювання, що наведена нижче.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену, диференційованого заліку, курсового проекту (роботи), практики відмінно
90 – 100	A	добре
82-89	B	
75-81	C	
67-74	D	задовільно
60-66	E	
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни