Львівський національний університет імені Івана Франка

Кафедра теорії оптимальних процесів

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Галузь знань *0403 – системні науки та кібернетика*

Напрям підготовки *6.040303 – системний аналіз*

Факультет *прикладної математики та інформатики*

КРЕДИТНО-МОДУЛЬНА СИСТЕМА ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(витяг з програми дисципліни "*Системи захисту інформації*")

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни
Кількість кредитів - 2 Модулів – 2 Змістових модулів – 4 Курсова робота – Загальна кількість годин – 72 Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 2	Галузь знань *0403 – системні науки та кібернетика* (шифр, назва) Напрям *6.040303 – системний аналіз* (шифр, назва) Освітньо-кваліфікаційний рівень: *бакалавр*	*денна форма навчання* Нормативна *Рік підготовки*: 3-й *Семестр*: 5-й *Лекції* - 2 год. *Практичні, семінарські* - 0 *Лабораторні*: 2 год. *Самостійна робота*: 2 год. *Вид контролю*: іспит

МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета. Надати студентам знання та практичні навички використання сучасних систем захисту інформації, криптографії, криптоаналізу. Вивчити програмні засоби захисту від несанкціонованого доступу до мережі та цифрових даних..

Завдання. Навчити студентів: основних методів захисту інформації від вірусної атаки, несанкціоновонаго доступу до файлів, застосування симетричних та асиметричних

алгоритмів криптографії, алгоритмам генерування ключів, цифрового підпису, розподілу таємниці.

В результаті вивчення даного курсу студент повинен

знати: основні способи несанкціонованого доступу до інформації та методи захисту; типи вірусів та антивірусних систем; алгоритми симетричного шифрування та дешифрування; основні криптологічні алгоритми з відкритим ключем; системи цифрового підпису.

вміти: застосовувати набуті знання для захисту цифрової інформації.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1 (шифр *ЗМ1*). **Основні види атаки на інформацію та моделі захисту.**

Тема 1. **Основні види та джерела атак на інформацію**. *Категорії інформаційної безпеки. Абстрактні моделі захисту інформації (моделі Біба, Гогена-Мезігера, Сазерландська, Кларка-Вільсона). Типові методи „злому" систем (пошук слабкої ланки, термінали інформаційної системи, отримання пароля на основі помилок адміністратора та користувачів, отримання пароля на основі помилок в реалізації, використання соціальної психології для отримання паролів).*

Тема 2. Комп'ютерні віруси. *Структура віруса. Симптоми зараження. Шляхи проникнення вірусів. Середовище існування віруса. Файлові віруси. Макровіруси. Троянські програми. Мережеві віруси.*

Тема 3. Антивіруси. *Сканери. Евристичне сканування. Монітори. Ревізори. Антивірусний блокувальник.*

Змістовий модуль 2 (шифр *ЗМ2*). **Симетричні криптосистеми.**

Тема 4. Елементарна криптологія: *Термінологія та позначення. Історичний огляд. Класичні криптологічні методи (шифр простої заміни, частотний аналіз, гомофонний шифр заміни, поліграмні шифри, поліалфавітні шифри, шифри перестановок).*

Тема 5. Шифри з використанням булевої алгебри: *Шифр одноразового блокноту. Композиція (добуток) шифрів. Криптосистема DES. Модифікації блокових шифрів.*

Тема 6. Математичні основи криптографії: *Дешифрування ітераціями. Алгоритм Евкліда. Розклад на прості співмножники. Конгруенції. Кільце лишків. Кільце матриць.*

Тема 7. Афінні шифри: *Шифри простої заміни. Афінні шифри вищих порядків. Криптоаналіз. Вправи.*

Змістовий модуль 3 (шифр *ЗМ3*). **Криптосистеми з відкритим ключем**

Тема 8. Арифметичні задачі та алгоритми: *Бінарний метод піднесення до степеня. Випадковий вибір. Первісні корені. Квадратичні лишки. Символ Якобі. Розподіл простих чисел. Ймовірносний тест Соловея-Штрассена. Псевдопрості числа. Ймовірносний тест Міллера-Рабіна.*

Тема 9. Факторизація. Розпізнавання квадратичності і добування квадратних коренів: *Факторизація. Квадратичність у випадку простого модуля. Добування квадратного кореня за простим модулем. Випадок модуля n=pq. Вправи*

Тема 10. Криптосистеми з відкритим ключем: *Концепція асинхронних криптосистем. Криптосистема RSA. Криптосистема Рабіна. Криптосистема Ель-Гамаля. Ймовірносне криптування. Криптосистеми на основі еліптичних кривих.*

Змістовий модуль 4 (шифр *ЗМ4*). **Застосування криптосистем з відкритим ключем**

Тема 11. Генератори псевдовипадкових бітів: *Означення. BBS генератор. Генератор Blum-Micali. Застосування псевдовипадкових генераторів (потокове шифрування, алгоритм Blum-Goldwasser).*

Тема 12. Важкооборотні функції: *Означення і приклади. Застосування. Поняття ядра функції. Предикат із секретом і ймовірносне криптування. Геш-функції.*

Тема 13. Цифровий підпис: *Підпис у системі RSA. Загальна схема цифрового підпису. Система цифрового підпису Ель-Гамаля. Система цифрового підпису Шнорра. Підпис у системі DSA*

Тема 14. Адміністрування ключами: *Ключ. Практика адміністрування ключами. Обмін ключами. Розподіл таємниці. Доведення квадратичності. Доведення не квадратичності. Ідентифікація за допомогою симетричної криптосистеми. Ідентифікація на основі цифрового підпису. Ідентифікація як доведення без розголошення.*

ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Номер і назва теми	Кількість годин
Елементарна криптологія		
1	Програмна реалізація шифру простої заміни	2
2	Дешифрування частотним аналізом	2
3	Програмна реалізація шифру Віженера	2
Шифри з використанням булевої алгебри		
4	Програмна реалізація шифру одноразоваого блокноту	2
Арифметичні задачі та алгоритми		
5	Програмна реалізація розширеного алгоритму Евкліда	2
6	Програмна реалізація бінарного методу піднесення до степеня	2
7	Програмна реалізація вибору випадкового елемента з Z_n	2
8	Програмна реалізація алгоритма обчислення символа Якобі	4
Криптосистеми з відкритим ключем		
9	Програмна реалізація криптосистеми RSA	6
Цифровий підпис		
10	Програмна реалізація цифрового підпису у системі RSA	3
11	Програмна реалізація цифрового підпису у системі Ель Гамаля	3
Адміністрування ключами		
12	Програмна реалізація протоколу експоненційного обміну ключем	3
13	Програмна реалізація алгоритму поділу таємниці	3

	Разом	**36**

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

БАЗОВА

1. О.В.Вербіцький. Вступ до криптології. – Львів: ВНТЛ, 1998. - 246с.
2. І.Я. Берегуляк.Класичні методи криптування. – Львів: Львівський ун-т, 1997. – 180с.
3. В.Ємець, А.Мельник, Р.Попович. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. – 144с.

ДОПОМІЖНА

4. Введение в криптографию / Под общ. ред. В.В.Ященко, СПб., 2001
5. С.Г.Бабичев, В.В.Гончаров, Р.Е.Серов. Основи современной криптографии. – М.: 2001
6. Глушаков С.В., Сурядный А.С., Тесленко Н.С. Антихакер. – М.:АСТ, 2008. – 501с.
7. Б.М.Голуб. Системи захисту інформації. Текст лекцій. – Львів, 2010. Електронна версія.

Програму склав доцент Голуб Б. М.