Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут *фізико-технічних та комп'ютерних наук*
Кафедра *програмного забезпечення комп'ютерних систем*

"ЗАТВЕРДЖУЮ"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ Олег АНГЕЛЬСЬКИЙ
"31" *серпня* 2022 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ
вибіркова

Освітньо-професійна програма *«Інформаційні системи та технології»*

Спеціальність *126 Інформаційні системи та технології*

Галузь знань *12 Інформаційні технології*

Рівень вищої освіти *перший бакалаврський*

Мова навчання *українська*

Чернівці 2022 рік

Робоча програма навчальної дисципліни «БЕЗПЕКА ПРОГРАМ ТА ДАНИХ» складена відповідно до освітньо-професійної програми першого (бакалаврського) рівня вищої освіти *«Інформаційні системи та технології»* за спеціальністю *126 Інформаційні системи та технології* галузі знань *12 Інформаційні технології*, затвердженої Вченою радою Чернівецького національного університету імені Юрія Федьковича (Протокол № *7* від «*31*» *серпня* 2020 року).

Розробник: *Остапов Сергій Едуардович, завідувач кафедри програмного забезпечення комп'ютерних систем, доктор фізико-математичних наук, професор.*

Погоджено з гарантом ОПП і затверджено на засіданні кафедри
інформаційних технологій та комп'ютерної фізики

Протокол № *1* від "*29*" *серпня* 2022 року

Завідувачка кафедри ІТКФ _____ Борча М.Д.

Робоча програма затверджена на засіданні кафедри
програмного забезпечення комп'ютерних систем

Протокол № *1* від "*29*" *серпня* 2022 року

Завідувач кафедри ПЗКС _____ Остапов С.Е.

Схвалено методичною радою навчально-наукового інституту
фізико-технічних та комп'ютерних наук

Протокол № *1* від "*31*" *серпня* 2022 року

Голова методичної ради ННІФТКН _____ Струк Я.М.

1. Анотація дисципліни.

Навчальна дисципліна «Безпека програм та даних. Частина І: Основи криптографії» призначена для формування у студентів знань, вмінь та навичок з сучасних методів та засобів криптографії, які будуть корисними при розгортання та обслуговуванні сучасних інформаційних систем.

Мета навчальної дисципліни: забезпечення підготовки студентів технічної спеціальності 126 — Інформаційні системи та технології. Він є одним з основних курсів, призначеним для набуття студентами базових знань з основ захисту інформації у комп'ютерних мережах, які необхідні у подальшому навчанні, а також у практичній діяльності на виробництві. Основною метою викладання дисципліни є формування у студентів знань і навичок, які забезпечують кваліфікацію майбутнього спеціаліста в області програмної інженерії.

Завдання дисципліни випливають з ролі дисципліни у системі підготовки спеціалістів: вивчення студентами основних теоретичних понять з криптографії; уміння застосовувати їх для розв'язку завдань, що ставить перед ними виробництво; набуття студентами практичних навичок криптографії та криптоаналізу; вільне володіння основними алгоритмами криптографії; розуміння основних понять і сучасного стану даного предмету.

Пререквізити: студенти повинні опанувати знаннями з дисциплін: «Операційні системи», «Основи програмування», «Комп'ютерні мережі».

2. Результати навчання.

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- найновіші досягнення криптографічних методів захисту інформації;
- характеристики основних найбільш відомих криптографічних алгоритмів;
- основні алгоритми електронного цифрового підпису;
- методи управління криптографічними ключами;
- організаційно-правові аспекти криптографічного захисту в Україні.

вміти:

- застосовувати криптографічні алгоритми для визначеного програмою класу задач;
- розробляти програмне забезпечення з елементами криптографічного захисту конфіденційності інформації;
- розробляти програмні продукти з можливістю криптографічного захисту цілісності інформації;
- реалізовувати алгоритми розподілу криптографічних ключів;
- розробляти програмні продукти з використанням криптографічного інтерфейсу Microsoft CryptoAPI або аналогічних криптобібліотек.

Набути компетентностей:

загальних

КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

спеціальних

КС 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації.

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Програмні результати навчання:

ПР 2. **Застосовувати** знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій.

ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПР 9. **Здійснювати** системний аналіз архітектури підприємства та його ІТінфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

ПР 10. **Розуміти і враховувати** соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.

3. Опис навчальної дисципліни

3.1. Загальна інформація

Назва навчальної дисципліни: «Безпека програм та даних»													
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	3	6	4	120	4	30	-	-	30	60		іспит

3.2. Структура змісту навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Класичні криптосистеми												
Тема 1.1. Вступ	8	4	-		-	4	-	-	-	-	-	-
Тема 1.2. Класичні техніки шифрування. Елементи теорії зв'язку.	20	6	-	6	-	8	-	-	-	-	-	-
Тема 1.3. Потокові та блокові шифри.	12	2	-	4	-	6	-	-	-	-	-	-
Разом за змістовим модулем 1	**40**	**12**	-	**10**	-	**18**	-	-	-	-	-	-
Змістовий модуль 2. Моделі і методи забезпечення безпеки БД.												
Тема 2.1. Стандарт шифрування DES	10	2	-	4	-	4	-	-	-	-	-	-
Тема 2.2. Сучасні симетричні криптоалгоритми.	4	2	-		-	2	-	-	-	-	-	-
Тема 2.3. Український стандарт шифрування ДСТУ 7624-2014.	6	2	-		-	4	-	-	-	-	-	-
Тема 2.4. Елементи теорії чисел	5	1	-		-	4	-	-	-	-	-	-
Тема 2.5. Асиметрична криптосистема RSA	7	1	-	2	-	4	-	-	-	-	-	-
Тема 2.6. Інші асиметричні криптосистеми	9	1	-	4	-	4	-	-	-	-	-	-
Тема 2.7. Функції хешування	6	2	-		-	4	-	-	-	-	-	-

Тема 2.8. Алгоритми електронного цифрового підпису	10	2	-	4	-	4	-	-	-	-	-	-
Тема 2.9. Класифікація атак на криптографічні системи	6	2	-		-	4	-	-	-	-	-	-
Тема 2.10. Розподіл криптографічних ключів	8	2	-	2	-	4	-	-	-	-	-	-
Тема 2.11. Генерування випадкових та псевдовипадкових послідовностей	9	1	-	4	-	4	-	-	-	-	-	-
Разом за змістовим модулем 2	**80**	**18**	**-**	**20**	-	**42**	-	-	-	-	-	-
Усього годин	**120**	**30**	**-**	**30**	-	**60**	-	-	-	-	-	-

3.2.1. Теми лабораторних занять

№ з/п	Назва теми
1	Шифрувальна система на основі шифру Цезаря
2	Дослідження афінної системи шифрування Цезаря
3	Шифрувальна система на основі шифру гаммування
4	Система блокового шифрування S-DES
5	Дослідження розсіювальних властивостей S-DES
6	Використання асиметричної системи RSA для цифрового підпису
7	Відкритий розподіл криптографічних ключів
8	Потоковий шифр на основі генератора BBS
9	Шифрувальна система на основі шифру простої заміни
10	Використання CryptoAPI Windows XP для розробки криптографічного ПЗ
11	Дослідження розповсюдження помилки в симетричних шифрах
12	Вивчення можливостей статистичного пакету NIST STS
13	Порівняльні дослідження потокових шифрів власної розробки
14	Розробка та дослідження генератора випадкових чисел за допомогою пристроїв комп—ютера
15	Коди аутентифікації повідомлень на основі хеш-функцій
16	Електронний цифровий підпис на основі симетричної криптосистеми
	Разом

Лабораторний практикум складається з 16 робіт і має кілька рівнів складності.

Студент може обирати будь-яку кількість робіт, виконувати їх в будьякому порядку (за винятком випадків, коли для виконання певної роботи необхідно виконати попередню/попередні).

Задача студента — набрати максимально можливу кількість балів. У навчальному плані на лабораторний практикум відводиться 50 балів (20 в

першому модулі + 30 — в другому). Звісно, можна набрати й більше/менше балів, виконавши більшу/меншу кількість лабораторних робіт.

Лабораторні роботи будуть оцінюватися так, як подано в таблиці. Звісно, якщо робота виконана не повністю, або якщо виконано полегшений варіант — повна кількість балів не нараховується.

Можливий варіант дистанційного захисту лабораторної роботи, коли студент, зробивши роботу, знімає скрин-каст протоколу дій, робить архів зі звітом та кодом, і відправляє це викладачу (попередньо домовившись про такий спосіб захисту!).

Таблиця: Оцінювання лабораторних робіт з курсу ―Основи криптографії‖

ЛР№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
К-сть балів	4	4	4	6	6	4	4	4	4	8	10/6	8	10	10	10	10
	- лабораторні роботи I рівня;															
	- лабораторні роботи II рівня;															
	- лабораторні роботи III рівня.															

Лабораторні роботи I рівня — прості роботи, в яких необхідно розробити програмне забезпечення, що використовує класичні криптоалгоритми (шифр Цезаря, спрощені потокові шифри, спрощений RSA).
Лабораторні роботи II рівня вимагають більш ретельної роботи та написання більших об’ємів коду.
Лабораторні роботи III рівня — досить серйозні криптографічні застосування, які продемонструють студенту, що їх виконав, можливості сучасного криптографічного програмного забезпечення та принципів його розробки.

ЗАУВАЖЕННЯ: В усіх лабораторних роботах висуваються вимоги до правил написання коду, наприклад, *C++ Programming Style Guideline* або аналогічного для обраної Вами мови програмування. Змінні типу Form1, Procedure1, a1,b2,c3 не допускаються, і код буде відхилений. Крім цього, код повинен супроводжуватися коментарями, які давали би повне розуміння про функції тієї чи іншої процедури/функції/класу/об’єкту тощо. Код без коментарів також буде відхилятися.

3.2.2. Самостійна робота

№ з/п	Назва теми
1	Методи частотного криптоаналізу

2	Алгоритми потокового шифрування RC2-RC4
3	Алгоритм Лая-Мессі міжнародного стандарту IDEA
4	Алгоритми ЕЦП на еліптичних кривих
5	Стандарт блокового шифрування ГОСТ 28147-89
6	Стандарт цифрового підпису ГОСТ Р.34-10-94
7	Стандарт цифрового підпису ГОСТ Р.34-10-2001
8	Стандарт ЕЦП ДСТУ 4145-2002
9	Диференціальний криптоаналіз
10	Лінійний криптоаналіз
11	Реалізація основних атак на симетричні криптоалгоритми
12	Реалізація основних атак на асиметричні криптоалгоритми
13	Лінійний регістр зсуву зі зворотним зв’язком
14	Протоколи прямого узгодження криптографічних ключів
	Разом

3.2.3. Індивідуальні завдання

1. Аналітичне порівняння методів криптоаналізу.
2. Порівняльний аналіз криптографічних методів аутентифікації.
3. Використання полів Галуа в криптографії.
4. Криптографічні методи захисту інформації в мобільній телефонії.
5. Криптографічний захист інформації в операційних системах сімейства Windows.
6. Криптографічний захист інформації в операційних системах сімейства Linux.
7. Порівняльний аналіз криптосистеми Serpent.
8. Порівняльний аналіз криптосистеми Blowfish.
9. Шифрувальні машини середини 20-сторіччя.
10. Протоколи «з нульовим розголошенням».

4. Система контролю та оцінювання

Види та форми контролю

Формами поточного контролю при вивченні курсу є:

- Усна відповідь студентів під час опитування на лекціях;
- Захист лабораторних робіт;
- Тестування з використанням платформи Moodle; Написання та захист рефератів.

Формами підсумкового контролю служать:

- Іспит;
- Залік, якщо він перебачений освітньою програмою.

Засобами оцінювання є:

- Модульні та поточні контрольні роботи;
- Тестувальна система на платформі Moodle;
- Реферати з тематики курсу;
- Виконання та захист лабораторних робіт.

Критерії оцінювання результатів навчання з навчальної дисципліни

Поточне тестування та самостійна робота														Підсумковий тест (екзамен)	Сума
Змістовий модуль 1				Змістовий модуль 2											
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	30	100
4	10	6	10	5	5	5	5	2	4	4	2	4	4		

Шкала оцінювання знань студентів

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
80-89	**B**	добре	
70-79	**C**		
60-69	**D**	задовільно	
50-59	**E**		
35-49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Методичне забезпечення

Для підготовки до лабораторних занять необхідно користуватися конспектом лекцій і матеріалами зі списку базової та допоміжної літератури. Для отримання розширених і поглиблених знань за тематикою рекомендується користуватися посиланнями зі списку інтернет-ресурсів.

Для організації роботи студентів необхідний комп'ютерний клас з пакетом прикладних програм, у тому числі з встановленими середовищами розробки мовами: C #, C ++, Pascal, Java, с системами керування базами даних: MS SQL Server 2008-2012, Oracle 10g - Oracle 11g, зі засобом моделювання MS Office Visio.

5. Рекомендована література

Базова

1. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник. - Львів: Новий світ-2000, 2019. - 678 с.
2. Остапов С.Е.,Валь Л.О. Основи криптографії. Чернівці: Книги-XXI, 2008. – 188 с.
3. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Чернівці: Родовід, 2015. - 438 С.
4. Ємець А.В., Мельник В.В., Попович П.А. Сучасна криптографія. Основні поняття.

   Львів, 2003 р. – 156 С.

Допоміжна

1. Кан Д. Взломщики кодов. М:Центрополиграф. -2000. -209 с.
2. Сингх С. Книга шифров. М.:Аванта. – 2009. – 464 с.
3. Столингс В. Криптография и защита сетей. М.:Вильямс. – 2001. – 672 с.
4. Закон України «Про захист інформації в автоматизованих системах».
5. Закон України «Про інформацію».
6. Закон України «Про державну таємницю».

6. Інформаційні ресурси

1. Український центр інформаційної безпеки . – Електронний ресурс. – http://www.bezpeka.com/.
2. Криптографічний захист інформації. - Електронний ресурс. Режим доступу: https://web.archive.org/web/20100301080922/http://bezpeka.com/ru/lib/spec/cript.html