МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Факультет математики та інформатики
Кафедра диференціальних рівнянь і прикладної математики

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«МАТЕМАТИЧНІ ТА КОМП'ЮТЕРНІ МЕТОДИ КРИПТОЛОГІЇ»

Освітня програма: Прикладна математика
Спеціальність: 113 Прикладна математика
Галузь знань: 11 Математика та статистика

Затверджено на засіданні кафедри
диференціальних рівнянь і прикладної математики
Протокол №1 від 31 серпня 2021 р.

м. Івано-Франківськ – 2021 рік

ЗМІСТ

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Назва дисципліни	Математичні та комп'ютерні методи криптології
Рівень вищої освіти	Другий рівень вищої освіти
Викладач(-і)	Василишин П. Б.
Контактний телефон	8(0342) 596027
E-mail	pavlo.vasylyshyn@pnu.edu.ua
Формат дисципліни	Очний
Обсяг дисципліни	6 кредитів, 180 год.
Посилання на сайт дистанційного навчання	ceeq.pnu.edu.ua
Консультації	Згідно розкладу

2. АНОТАЦІЯ ДО КУРСУ

Предметом вивчення дисципліни є криптографія — наука про методи захисту конфіденційності, цілісності і автентичності інформації.

Даний курс знайомить студентів із:

- основними фундаментальними поняттями і законами криптографічного захисту інформації для їх використання в сучасних комп'ютерних системах;
- основним математичним апаратом криптографії;
- принципами побудови криптографічних протоколів та їх використання в задачах захисту інформації та даних;
- програмними засобами, які реалізують основні криптографічні протоколи;
- методами та засобами криптографічного захисту даних.

3. МЕТА ТА ЦІЛІ КУРСУ

Дисципліна спрямована на формування у студентів умінь і компетенцій для забезпечення ефективного криптографічного захисту інформації і використання алгоритмів криптографічного захисту при розробці сучасних інформаційних систем.

Дисципліна передбачає ознайомлення студентів з класичними техніками шифрування, алгоритмами сучасних криптосистем та основними засобами криптографі-

чного захисту інформації, формування навиків проектування нових алгоритмів криптографічних перетворень під час реалізації захисту програм і даних.

4. КОМПЕТЕНТНОСТІ

Загальні компетентності:

ЗК-1. Здатність до абстрактного мислення, аналізу та синтезу, до застосування теорії у практичних ситуаціях.

Спеціальні (фахові, предметні) компетентності:

ФК-4. Здатність використовувати навички роботи з комп'ютером та знання й уміння в галузі сучасних інформаційних технологій для вирішення експериментальних і практичних завдань.

ФК-11. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: структурного, об’єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами та алгоритмами обчислень, структурами даних і механізмами управління.

5. РЕЗУЛЬТАТИ НАВЧАННЯ

В результаті вивчення курсу студенти повинні

знати:

- основні криптографічні алгоритми симетричного та асиметричного шифрування, хешування та цифрового підпису;
- стандартні криптографічні примітиви та порядок їх застосування;
- базові стандарти в галузі криптографічного захисту інформації.

вміти:

- працювати з технічною літературою і документацією;
- проектувати алгоритми криптографічних перетворень;
- розробляти криптографічні системи та криптографічні примітиви;
- здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційних системах.

Програмні результати навчання:

РН-6. Уміти розробляти алгоритми моделювання складних систем та проводити комп’ютерне моделювання.

6. ОРГАНІЗАЦІЯ НАВЧАННЯ КУРСУ

Обсяг курсу	
Вид заняття	**Загальна кількість годин**
Лекції	20
Практичні	—
Лабораторні	40
Самостійна робота	120

Ознаки курсу			
Семестр	**Спеціальність**	**Курс (рік навчання)**	**Нормативний/ вибірковий**
2	113 Прикладна математика	1-й	Вибірковий

Тематика дисципліни						
Назви змістових модулів і тем	**Кількість годин**					
	вс.	лек.	пр.	лаб.	інд.	сам.
Семестр 1						
Змістовий модуль 1. ***Класичні та сучасні симетричні***						
Тема 1. Вступ. Основні поняття. Шифри перестановки та простої заміни. Криптографічна стійкість шифрів.	12	1		2		8
Тема 2. Шифри складної заміни. Шифрод-норазового блокноту.	12	1		2		8
Тема 3. Сучасні симетричні криптосистеми. Мережі Фейстеля. Опис алгоритму DES.	14	2		4		8
Всього за модуль:	**38**	**4**		**8**		**24**
Змістовий модуль 2. ***Математичний апарат та його застосування в криптографії***						
Тема 4. Арифметика. Прості числа. НСД. Розширений алгоритм Евкліда. Конгруенції. Кільце лишків. Модульна арифметика. Функція Ейлера. Теореми Ейлера та Ферма.	12			2		8

Тематика дисципліни						
Назви змістових модулів і тем	**Кількість годин**					
	вс.	лек.	пр.	лаб.	інд.	сам.
Тема 5. Поля Галуа GF (p^n). Побудова полів Галуа GF (2^n).	12	2		2		8
Тема 6. SP-мережі. Симетричний алгоритм блочного шифрування AES.	12	2		4		8
Всього за модуль:	**36**	**4**		**8**		**24**
Змістовий модуль 3. ***Асиметричні криптосистеми***						
Тема 7. Криптосистеми з відкритим ключем. Алгоритм шифрування RSA.	12	1		2		8
Тема 8. Протокол обміну ключами Діффі-Хелмана. Шифр Шаміра.	12	1		4		8
Тема 9. Схема шифрування Ель-Гамаля.	12			2		8
Тема 10. Еліптична криптографія.	12	2		2		8
Всього за модуль:	**48**	**4**		**10**		**32**
Змістовий модуль 4. ***Криптографічні протоколи та методи криптоаналізу***						
Тема 11. Хешування. Вимоги до хеш-функцій. Схема Меркеля–Дамгарда. Ал- горитми сімейства MD і SHA.	12	2		2		8
Тема 12. Поняття електронного цифрового підпису (ЕЦП). Схеми використання. Система ЕЦП Ель-Гамаля (EGSA).	12	2		2		8
Тема 13. Програмна реалізація ЕЦП ал- горитмом Ель-Гамаля.	10			2		8
Тема 14. Алгоритми цифрових підписів DSA та ECDSA.	12	2		4		8
Тема 15. Загальні поняття криптоаналізу.	14	2		4		8
Всього за модуль:	**60**	**8**		**14**		**40**
Усього годин:	**180**	**20**		**40**		**120**

7. СИСТЕМА ОЦІНЮВАННЯ КУРСУ

Загальна система оцінювання	Підсумкова оцінка з дисципліни є сумою оцінок за виконання лабораторних робіт, оцінки за контрольну роботу і балів за підсумковий контроль (екзамен). Підсумкова оцінка визначається відповідно до поданої нижче таблиці оцінювання за різними шкалами (100-бальна, ECTS, національна).
Лабораторні заняття	Максимальна оцінка за виконання лабораторних робіт становить 40 балів.
Умови допуску до підсумкового контролю	Загальна кількість балів за навчальну (аудиторну) і практичну роботу становить не менше 25 балів.

Вимоги до практикуму	Пакети індивідуальних завдань для проведення контрольних робіт містять до 5 завдань у кожному варіанті. Максимальна сумарна оцінка за виконання контрольних робіт становить 10 балів.
Підсумковий контроль (екзамен)	Максимальна оцінка за підсумковий контроль становить 50 балів.

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**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**		
26 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

7. ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Студент, перебуваючи на лабораторних роботах, отримує індивідуальне завдання та самостійно працює над його виконанням. За результатами виконання лабораторної роботи здається звіт, який захищається усно. Це сприяє розвитку навичок самостійної роботи над поставленою задачею та індивідуальному підходу у опануванні курсу із врахуванням можливостей та базового рівня студента.

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:

самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;

посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

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;

фабрикація — вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація — свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування — виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит тощо); повторне проходження відповідного освітнього компонента освітньої програми.

8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Вербіцький О. В. Вступ до криптології. – Львів: Видавництво НТЛ., 2008. –248 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. – Луцьк: Вежа-Друк, 2014. – 163 с.
3. Остапов С.Е., Валь Л.О. Основи криптографії. Навчальний посібник. – Чернівці: Книги – XXI, 2008. – 188 с.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Харків: Вид. ХНЕУ, 2013. – 476 с.
5. Лахно В. А. Опорний конспект лекцій з дисципліни "Основи криптографічного захисту інформації". – Київ: [Б. в.], 2016. – 172 с.
6. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
7. Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-ПРЕСС, 2007. – 512 с.
8. Ян С. Криптоанализ RSA. – Ижевск: РХД, 2011. – 312 с.

Додаткова література

9. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

10. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

11. Ємець В., Мельник А., Попович Р. Сучасна криптографія: основні поняття – Л.: БаК. – 2003. –144 с.

12. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія: Підручник. – Київ – Тернопіль: Збруч, 2002. – 504 с.

13. Шнайер Б. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – М.: "Триумф", 2001. – 610 с.

14. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

Викладач _____ Василишин П. Б.