ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
Кафедра кібернетики і прикладної математики

«ЗАТВЕРДЖУЮ»
Декан факультету математики та цифрових технологій
_____ /проф. Микола МАЛЯР/
«26» 05 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні методи криптографії

Рівень вищої освіти	**магістерський**
Галузь знань	**11 Математика та статистика**
Спеціальність	**113 Прикладна математика**
Освітня програма	**Науки про дані та інтелектуальні рішення**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2023

Робоча програма навчальної дисципліни «**Математичні методи криптографії**» для здобувачів вищої освіти галузі знань **11 Математика та статистика** спеціальності **113 Прикладна математика** освітньої програми **Науки про дані та інтелектуальні рішення**.

Розробник: **Повідайчик М.М.**, к.е.н.,
доцент кафедри кібернетики і прикладної математики

Робочу програму розглянуто на засіданні кафедри **кібернетики і прикладної математики**
протокол № 12 від «5» червня 2023 р.
Завідувач кафедри _____ Павло МУЛЕСА

Схвалено науково-методичною комісією **факультету математики та цифрових технологій**
протокол № 10 від «20» червня 2023 р.
Голова науково-методичної комісії _____ Наталія ЮРЧЕНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування
Показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Очна форма навчання</td><td>Заочна форма Навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>1-ий</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для очної форми навчання:

аудиторних – 4

самостійної роботи здобувача – 6</td><td>1-ий</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>20</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: іспит</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>28</td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:
усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>72</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни «Математичні методи криптографії» є вивчення теоретичних основ криптографії та математичних методів захисту інформації, а також розробка комп'ютерних програм, які реалізують відповідні алгоритми.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗК01. Здатність до абстрактного мислення, аналізу і синтезу;

ЗК02. Здатність до самонавчання, пошуку, оброблення та аналізу інформації з різних джерел;

ЗК04. Здатність генерувати нові ідеї (креативність).

ФК01. Здатність використовувати математичний апарат, розробляти моделі для розв'язання задач широкого спектру;

ФК02. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, прогнозування, прийняття рішень, аналізу даних;

ФК04. Здатність розробляти нові та адаптовувати вже існуючі методи та алгоритми розв'язання прикладних задач моделювання та аналізу даних, проводити відповідні експерименти з аналізом одержаних результатів.

ФК06. Здатність досліджувати наукові проблеми за фахом.

ФК07. Здатність пропонувати практичні рішення за фахом з урахуванням сучасних досягнень науки.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Науки про дані та інтелектуальні рішення»,** вивчення навчальної дисципліни «Математичні методи криптографії» повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	**Шифр ПРН**
Використовувати й адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач.	ПР01
Формулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.	ПР05
Уміти будувати комп'ютерний експеримент для конкретних задач прикладної математики шляхом використання спеціалізованих (у тому числі й створених) програмних засобів, та виконувати опис та аналіз результатів експерименту	ПР06
Вміти спроектувати архітектуру системи з великими обсягами даних, моделювати штучні нейронні мережі та використовувати їх на практиці, застосовувати технологію блокчейн.	ПР10

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Математичні методи криптографії»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Використовувати математичні моделі та методи для захисту даних	ПР01
Обирати метод розв'язання задачі захисту даних, що забезпечує потрібну надійність результату	ПР05
Уміти проводити комп'ютерний експеримент для задач криптографії шляхом використання спеціалізованих (у тому числі й створених) програмних засобів та виконувати опис та аналіз результатів експерименту	ПР06
Вміти проектувати архітектуру комп'ютерних систем, використовувати їх на практиці, застосовувати технологію блокчейн.	ПР10

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- виконання індивідуальних та групових завдань;
- презентація результатів виконаної індивідуальної роботи студента.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: усне опитування, тестування, лабораторна робота.

Форма модульного контролю: письмова контрольна робота.

Форма семестрового контролю: іспит.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота				**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	40	100
15	15	15	15		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота				**Модульна контрольна робота**	**Сума**
Т5	Т6	Т7	Т8	40	100
15	15	15	15		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (виконання та захист)	4	40	4	40
Самостійна робота, написання рефератів за темами, поданими у табл. «Самостійна робота»	1	20	1	20
Модульна контрольна робота	1	40	1	40
Разом		100		100

Критерії оцінювання модульної контрольної роботи.

Модульна контрольна робота проводиться у формі практичних завдань, які виконуються в аудиторії. Варіант модульної контрольної роботи складається з двох блоків.

Перший блок складається з теоретичних питань (20 балів).

Другий блок присвячений розв'язанню задач (20 балів).

Критерії оцінювання підсумкового семестрового контролю

Відповідно до ***«Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті»*** (затверджено Наказом Ректора ДВНЗ «УжНУ» № 698/01-17 від 08.05.2015 р.), знання здобувачів оцінюється як з теоретичної, так і з практичної підготовки за такими критеріями:

оцінку «відмінно» (90-100 балів, А) заслуговує здобувач, який:

- всебічно і глибоко володіє навчально-програмовим матеріалом;
- вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;
- засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;
- засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;
- вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;
- самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку «добре» (82-89 балів, В) – заслуговує здобувач, який:

- повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання в

достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;
- має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування
проблем професійного спрямування;
- під час відповіді допустив деякі неточності, які самостійно виправив, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) заслуговує здобувач, який:

- в цілому навчальну програму засвоїв, але відповідає на екзамені з певною кількістю помилок;
- вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;
- опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує здобувач, який:

- знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;
- виконує завдання непогано, але зі значною кількістю помилок;
- ознайомлений з основною літературою, яка рекомендована програмою;
- допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує здобувач, який:

- володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється здобувачу, який:

- виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінка «незадовільно» (35 балів, F) – виставляється здобувачу, який:

- володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;
- допускає грубі помилки при виконанні завдань, передбачених програмою;
- не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Таблиця відповідності оцінок за різними шкалами

Оцінка за 100-бальною шкалою	**Оцінка ЄКТС**	**Оцінка за національною шкалою**	
		Диференційована	**Недиференційована**
90 – 100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		

64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	незараховано з обов'язковим повторним вивченням дисципліни

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1.

Тема 1. Докомп'ютерний захист інформації.

Основні поняття криптографії. Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама.

Тема 2. Арифметичні основи криптографії.

Алгоритм ділення з остачею. Найбільший спільний дільник. Взаємно прості числа. Найменше спільне кратне. Прості числа. Порівняння. Класи лишків. Функція Ейлера. Порівняння першого степеня. Первісні корені. Існування первісних коренів. Індекси за модулем pk і 2pk. Символ Лежандра. Квадратичний закон взаємності. Символ Якобі.

Тема 3. Статистичне тестування випадкових і псевдовипадкових послідовностей.

Рівномірно розподілена випадкова послідовність і її властивості. Універсальний алгоритм статистичного тестування випадкових і псевдовипадкових послідовностей. Тест n-серій. Тест інтервалів. Узагальнений покер-тетст. Тест «збирача купонів». Тест перестановок. Тест перетинаючихся n-грам. Тест, заснований на рангах двійкових матриць. Спектральні тести. Тест випадкового блуждання. Універсальний статистичний тест Мауера. Тест на основі прирощеної ентропії. Тест, заснований на алгоритмі стиснення Лемпеля-Зіва. Тест, заснований на лінійній складності. Тест на основі екстремальної статистики скалярного добутку. Тест на основі екстремальної статистики дельта-добутку. Алгоритмічне визначення випадковості.

Тема 4. Криптосистеми з відкритим ключем.

Описання RSA–криптосистеми. Можливі атаки на криптосистему RSA. Стійкість RSA проти методу повторного шифрування. Пошук секретного ключа d і факторизації модуля N. Біти в RSA-криптосистемі. Система Рабина. Ранцевий метод шифрування. Стійкість ранцевого шифру. Теорема Вінера про малий секретний ключ. Арифметика великих чисел. Модулярна арифметика. Ознака простоти. Алгоритми генерації простих чисел. Задача факторизації.

Модуль 2.

Тема 5. Функції хешування.

Визначення і властивості. Блочно-ітераційні функції хешування. Використання блочних криптосистем. Атака «днів народження». Криптосистеми аутетифікації. Функція хешування СТБ 1176.1-99.

Тема 6. Електронний цифровий підпис.

Узагальнена модель ЕЦП. Схема ЕЦП Рабина. Схема Діффі-Лампорта. Імовірнісна схема підпису Рабина. Стандарт ЕЦП DSS. Схема ЕЦП Ель Гамаля. Арифметичні властивості російського стандарту цифрового підпису. Еквівалентність задач фальсифікації підпису в DSS схемою Ель Гамаля. Електронний цифровий підпис СТБ 1176.1-99. Задача дискретного логарифмування.

Тема 7. Протоколи управління криптографічними ключами.

Протоколи генерації ключів. Протоколи взаємної аутентифікації. Протоколи прямого обміну ключами. Протоколи розподілу сеансових ключів з використанням центру розподілу ключів.

Тема 8. Технологія блокчейн.

Історія блокчейну. Структура: блоки, децентралізація, відкритість, використання. Типи: публічні, приватні, гібридні блокчейни. Сумісність.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
		у тому числі				
	Усього	лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1	15	2		4		9
Тема 2	15	2		4		9
Тема 3	15	2		4		9
Тема 4	15	2		4		9
Модульна контрольна робота № 1	2	2				
Модуль 2						
Тема 5	15	2		4		9
Тема 6	15	2		4		9
Тема 7	13	2		2		9
Тема 8	13	2		2		9
Модульна контрольна робота № 2	2	2				
Усього годин	120	20	0	28	0	72

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Докомп’ютерний захист інформації.	4
2.	Арифметичні основи криптографії.	4
3.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	4
4.	Криптосистеми з відкритим ключем.	4
5.	Функції хешування.	4
6.	Електронний цифровий підпис.	4
7.	Протоколи управління криптографічними ключами.	2
8.	Технологія блокчейн.	2

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
9.	Докомп’ютерний захист інформації.	9
10.	Арифметичні основи криптографії.	9
11.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	9
12.	Криптосистеми з відкритим ключем.	9
13.	Функції хешування.	9
14.	Електронний цифровий підпис.	9
15.	Протоколи управління криптографічними ключами.	9
16.	Технологія блокчейн.	9

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби – комп’ютер.

Програмне забезпечення: MS Excel; середовище розробки, вибране студентом.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Глинчук, Людмила Ярославівна. Криптологія [Текст] : навч.-метод. посіб. / Л. Я. Глинчук ; Східноєвроп. нац. ун-т ім. Лесі Українки. - Луцьк : Вежа-Друк, 2014. - 163 с. : рис., табл. - Бібліогр.: с. 157-158.
2. Горбенко, Іван Дмитрович. Прикладна криптологія. Теорія. Практика. Застосування [Текст] : підручник / Горбенко І. Д., Горбенко Ю. І. ; Харк. нац. ун-т радіоелектроніки, Приват. акціонер. т-во "Ін-т інформ. технологій". - Х. : Форт, 2013. - 878 с. : рис., табл. - Бібліогр.: с. 841-865.
3. Задірака, Валерій Костянтинович. Комп'ютерна криптологія [Текст] : підручник / В. К. Задірака, О. С. Олексюк ; Терноп. акад. нар. госп-ва, НАН України, Ін-т кібернетики ім. В. М. Глушкова. - К. : [б.в.], 2002. - 504 с.: іл. - Бібліогр.: с. 491-502.
4. Інформаційні технології. Методи захисту. Легковагова криптографія [Текст]. - Київ : УкрНДНЦ, [20--] . - (Національний стандарт України).ДСТУ ISO/IEC 29192-5:2018 (ISO/IEC 29192-5:2016, IDT). Геш-функції. - Чинний від 2020-01-01. - 2019. - V, 18 с. : рис., табл. - Бібліогр.: с. 18.
5. Когут Ю. Технології блокчейн та криптовалюта. Ризики та кібербезпека, 2022.
6. Козіна, Г. Л. Криптографія від історії до сучасних стандартів [Текст] : навч. посіб. / Г. Л. Козіна. - Запоріжжя : НУ "Запорізька політехніка", 2020. - 192 с.
7. Комп`ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях [Текст] : навч.посіб. / В. К. Задірака [и др.] ; ред. В. К. Задірака ; НАН України, Ін-т кібернетики ім. В. М. Глушкова. - К. ; Т. : Підручники і посібники, 2007. - 272 с. - Бібліогр.: с. 265-271.
8. Корченко, Олександр Григорович. Прикладна криптологія: системи шифрування [Текст] : підруч. для студентів ВНЗ, які навчаються за напрямом підгот. "Безпека інформаційних і комунікаційних систем" / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс ; Житомир. військ. ін-т ім. С. П. Корольова Держ. ун-ту телекомунікацій. - Житомир : ДУТ, 2014. - 447 с. : рис., табл. - Бібліогр.: с. 439-441.
9. Криптологія у прикладах, тестах і задачах [Текст] : навч. посіб. / Т. В. Бабенко [та ін.] ; Держ. ВНЗ "Нац. гірн. ун-т". - Дніпропетровськ : НГУ, 2013. - 318 с. : рис., табл. - Назва обкл., корінця : Криптологія в тестах, задачах і прикладах. - Бібліогр.: с. 316-318.
10. Прикладна криптологія [Текст] : лаб. практикум для здобувачів вищ. освіти ОС "Бакалавр" спец. 125 "Кібербезпека" / [уклад. А. В. Ільєнко] ; Нац. авіац. ун-т. - Київ : НАУ, 2022. - 57, [1] с. : рис.
11. Системи захисту інформації. Криптографія [Текст] : навч. посіб. / уклад. Б. Д. Шепетюк ; Чернівец. нац. ун-т ім. Юрія Федьковича. - Чернівці : ЧНУ ім. Юрія Федьковича : Рута, 2021. - 75 с. : рис., табл. - Бібліогр.: с. 75.
12. Усатенко, Тетяна Миколаївна. Криптологія [Текст] : навч. посібник / Т. М. Усатенко ; Сумський держ. ун-т. - Суми : СумДУ, 2008. - 164 с.

Допоміжна література

1. Повідайчик М.М. Професійна діяльність вчителя інформатики в сфері інформаційної безпеки / М.М. Повідайчик, І.Я. Шпонтак // Науковий вісник УжНУ. Серія: Педагогіка. Соціальна робота. – Вип. 1 (42). 2018. С. 179-182.
2. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: В-во УжНУ «Говерла», 2020. 28 с.

Інформаційні ресурси у мережі Інтернет

1. https://www.uzhnu.edu.ua/uk/infocentre/60
2. https://ua.udemy.com/course/learn-cryptography-basics-in-python/
3. https://ua.udemy.com/course/advance-cryptography-concepts/