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

«ЗАТВЕРДЖУЮ»
Декан факультету математики
та цифрових технологій
_____ Микола МАЛЯР
«_30_» ____08_____ 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КРИПТОЛОГІЇ

Рівень вищої освіти	**перший (бакалаврський)**
Галузь знань	**11 Математика та статистика**
Спеціальність	**113 Прикладна математика**
Освітня програма	**Системи штучного інтелекту**
Статус дисципліни	**вибіркова**
Мова навчання	**українська**

Ужгород 2023

Робоча програма навчальної дисципліни «**Основи криптології**» для здобувачів вищої освіти галузі знань **11 Математика та статистика** спеціальності **113 Прикладна математика** освітньої програми **Системи штучного інтелекту**.

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

Робочу програму розглянуто та затверджено на засіданні кафедри **кібернетики і прикладної математики.**

Протокол № 12 від «05» 06 2023 року.

Завідувач кафедри _____ Павло МУЛЕСА

Схвалено науково-методичною комісією **факультету математики та цифрових технологій.**

Протокол № 10 від «20» червня 2023 року.

Голова науково-методичної комісії _____ Наталія ЮРЧЕНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td>Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>4-й</td></tr>
<tr><td>Кількість модулів – 2</td><td>Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин
для очної форми навчання:

аудиторних – 3

самостійної роботи здобувача – 3</td><td>7-й</td></tr>
<tr><td>Лекції:</td></tr>
<tr><td>30</td></tr>
<tr><td>Практичні (семінарські):</td></tr>
<tr><td>-</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: залік</td><td>Лабораторні:</td></tr>
<tr><td>30</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: письмова</td><td>Самостійна робота:</td></tr>
<tr><td>60</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни «**Основи криптології**» є вивчення теоретичних основ криптографії, криптоаналізу 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 учитися і оволодівати сучасними знаннями.

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК05. Здатність проведення досліджень на відповідному рівні.

ЗК08. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК16. Здатність до планування та розподілу часу.

ФК03. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Системи штучного інтелекту»,** вивчення навчальної дисципліни «**Основи криптології**» повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	**Шифр ПРН**
Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.	РН01
Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.	РН15

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Основи криптології**»:

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Використовувати математичні моделі та методи для захисту даних	РН01
Обирати алгоритм розв'язання задачі захисту даних, що забезпечує потрібну надійність результату	РН01
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	РН15
Вміти проектувати архітектуру комп'ютерних систем, використовувати їх на практиці, застосовувати технології захисту даних	РН15

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Методи навчання

Метод проблемного викладення матеріалу, пояснювально-ілюстративний метод, пошуковий та дослідницький методи, інтерактивний метод.

Засоби оцінювання та методи демонстрування результатів навчання

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

- виконання завдань лабораторних робіт
- модульні контрольні роботи;
- залік.

Форми контролю та критерії оцінювання результатів навчання

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

Форма модульного контролю: письмова контрольна робота.

Форма семестрового контролю: залік.

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

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	40	100
9	9	9	9	8	8	8		

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

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т8	Т9	Т10	Т11	Т12	Т13	40	100
10	10	10	10	10	10		

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	3	40
Тестування	4	20	3	20
Модульна контрольна робота	1	40	1	40
Разом		100		100

Критерії оцінювання модульної контрольної роботи

Методика оцінювання. Матеріал кожного модуля, який здобувачі вищої освіти повинні засвоїти протягом семестру, виноситься на одну з двох модульних контрольних робіт.

Модульна контрольна робота складається із 4-ох завдань (2-ох теоретичних питань та 2-ох практичних завдань), кожне з яких оцінюється в 10 балів.

За виконання лабораторних робіт здобувачу вищої освіти також нараховується різна кількість балів, в залежності від складності матеріалу.

Критерієм успішного проходження здобувачем освіти поточного оцінювання (включно із захистом лабораторних робіт) є досягнення здобувачем освіти не менше 50% балів від загальної кількості запланованої за конкретною темою. Конкретна максимальна кількість балів подається у таблицях розподілу балів, які отримують здобувачі за модуль та за окремі види навчальної роботи.

Невиконані та незахищені лабораторні роботи, а також неявка на модульну контрольну роботу оцінюються в 0 балів незалежно від причини невиконання (неявки).

Сумарна оцінка (від 0 до 100 балів) виставляється у відомість модульного контролю. Модуль зараховується, якщо сумарний бал складає не менше 60 балів, і студент виконав і захистив всі лабораторні роботи, які є складовими даного модуля.

Здобувач вищої освіти, який не з’явився на модульну контрольну роботу, або ж його модульна оцінка складає від 0 до 34 балів, зобов’язаний скласти (перескласти) модуль до початку підсумкового контролю у строки, визначені викладачем дисципліни та погоджені деканатом факультету.

Критерії оцінювання підсумкового контролю

Залікова методика оцінювання. За результатами модульних контролів визначається підсумкова модульна оцінка, як середнє арифметичне значення двох модулів. Залікова оцінка визначається в залежності від рейтингового балу, або балів за залік.

До складання заліку допускаються здобувачі вищої освіти, у яких підсумкова модульна оцінка за семестр становить не менше 35.

Здобувач вищої освіти, підсумкова модульна оцінка якого складає від 0 до 34 балів, зобов'язаний покращити її до початку підсумкового семестрового контролю під час чергування викладача на кафедрі у строки, визначені викладачем дисципліни та погоджені деканатом факультету. В протилежному випадку, здобувач не допускається до заліку і у нього виникає академічна заборгованість.

Залік з навчальної дисципліни здобувач вищої освіти може не складати, якщо він успішно пройшов усі модульні контролі та його влаштовує підсумкова модульна оцінка. Здобувачі вищої освіти, підсумкова модульна оцінка яких становить від 35 до 59, залік складають обов'язково. Здобувач освіти може підвищити на заліку рейтинговий бал, при цьому, за результатами складання заліку оцінка не може бути менша за підсумкову модульну оцінку, яку він отримав за результатами модульних контролів.

Залік проводиться в письмовій формі. Заліковий білет складається з одного теоретичного питання та двох практичних завдань. Оцінювання результатів навчання на заліку здійснюється за 100-бальною шкалою. Оцінка за залік вноситься у відомість обліку успішності.

Таблиця відповідності оцінок за різними шкалами оцінювання

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену	для заліку
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

Критерій оцінювання підсумкового контролю з дисципліни

— «зараховано» (90-100 балів, A) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії;

— **«зараховано» (82-89 балів, B)** заслуговує студент, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер

знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності;

— **«зараховано» (74-81 бал, C)** заслуговує студент, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності;

— **«зараховано» (64-73 бали, D**) заслуговує студент, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, дана оцінка виставляється студентам, що допустили помилки у відповіді на заліку чи екзамені та при виконанні залікових або екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;

— **«зараховано» (60-63 балів, E)** заслуговує студент, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, дана оцінка виставляється студентам, що допустили грубі помилки у відповіді на заліку чи екзамені та при виконанні залікових або екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача.

— **«не зараховано» (35-59 балів, FX)** виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

— **«не зараховано» (0-34 балів, F)** виставляється студенту коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.

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, Вернама.

Тема 2. Поняття про асиметричні методи.

Система шифрування RSA. Системи символьних обчислень. Ферма, Ейлер та Гаус. Проблеми теорії чисел. Теореми та доведення.

Тема 3. Фундаментальні алгоритми.

Алгоритми. Алгоритм ділення. Теорема ділення. Алгоритм Евкліда. Доведення коректності алгоритму Евкліда. Розширений алгоритм Евкліда.

Тема 4. Розкладання на множники.

Теорема про розкладання. Існування розкладання. Ефективність алгоритму розкладу методом проб. Алгоритм Ферма розкладання на множники. Доведення

коректності алгоритму Ферма. Одна фундаментальна властивість простих чисел. Єдиність розкладання.

Тема 5. Прості числа.

Поліноміальна формула. Експоненційні формули: числа Мерсенна. Експоненційні формули: числа Ферма. Прайморіальна формула. Нескінченність безлічі простих чисел. Решето Ератосфена.

Тема 6. Арифметика залишків.

Відношення еквівалентності. Порівняння. Арифметика лишків. Критерій подільності. Степені. Діофантові рівняння. Поділ за модулем *n*.

Тема 7. Індукція та Ферма.

Математична індукція. Теорема Ферма. Обчислення коренів.

Модуль 2.

Тема 8. Псевдопрості числа.

Числа Кармайкла. Тест Міллера. Тестування простоти та системи символьних обчислень.

Тема 9. Системи порівнянь.

Лінійні рівняння. Китайський алгоритм лишків: взаємно прості модулі. Китайський алгоритм лишків: загальний випадок.

Тема 10. Групи.

Визначення та приклади. Симетрії. Арифметичні групи. Підгрупи. Циклічні підгрупи. Теорема Лагранжа.

Тема 11. Мерсен і Ферма.

Числа Мерсенна Числа Ферма. Тест Люка-Лемера.

Тема 12. Тести на простоту та примітивні корені.

Тест Люка. Тест на простоту. Числа Кармайкла. Примітивні корені. Обчислення порядків.

Тема 13. Система шифрування RSA.

Шифрування та дешифрування. Обґрунтування. Надійність системи. Вибір простих. ЕЦП.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин:120					
	Денна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Докомп'ютерний захист інформації.	11	2		4		5
Тема 2. Поняття про асиметричні методи.	7	2				5
Тема 3. Фундаментальні алгоритми.	11	2		4		5
Тема 4. Розкладання на множники.	11	2		4		5
Тема 5. Прості числа.	7	2				5

Тема 6. Арифметика залишків.	11	2		4		5
Тема 7. Індукція та Ферма.	7	2				5
Модульна контрольна робота	2	2				
Разом за модуль	**67**	**16**		**16**		**35**
Модуль 2						
Тема 8. Псевдопрості числа.	7	2				5
Тема 9. Системи порівнянь.	10	2		4		4
Тема 10. Групи.	6	2				4
Тема 11. Мерсен і Ферма.	6	2				4
Тема 12. Тести на простоту та примітивні корені.	10	2		4		4
Тема 13. Система шифрування RSA.	12	2		6		4
Модульна контрольна робота	2	2				
Разом за модуль	**53**	**14**		**14**		**25**
Разом за семестр	**120**	**30**		**30**		**60**

6.3. Теми лабораторних занять

№ з/п	**Назва теми**	**Кількість годин**
1.	Докомп’ютерний захист інформації.	4
2.	Фундаментальні алгоритми.	4
3.	Розкладання на множники.	4
4.	Арифметика залишків.	4
5.	Системи порівнянь.	4
6.	Тести на простоту та примітивні корені.	4
7.	Система шифрування RSA.	6
	Разом	30

6.4. Самостійна робота

№ з/п	**Назва теми**	**Кількість годин**
1.	Шифр Хілла.	5
2.	Криптосистеми з відкритим ключем.	5
3.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	5
4.	Функції хешування.	5
5.	Алгоритм «Решето Ератосфена».	5
6.	Модулярна арифметика.	5
7.	Метод математичної індукції.	5
8.	Алгоритми тестування на простоту.	5
9.	Китайський алгоритм лишків.	4
10.	Арифметичні групи.	4
11.	Тест Люка-Лемера.	4
12.	Тест Люка.	4
13.	Технологія блокчейн.	4
	Разом	60

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

Технічні засоби – комп'ютер.

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

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна 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.
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
4. Лісовська Ю.П. Інформаційна безпека України. К.: Кондор. 2018. 172 с.
5. Козіна Г. Л. Криптографія від історії до сучасних стандартів [Текст] : навч. посіб. Запоріжжя : НУ "Запорізька політехніка", 2020. 192 с.
6. Прикладна криптологія [Текст] : лаб. практикум для здобувачів вищ. освіти / [уклад. А. В. Ільєнко] ; Нац. авіац. ун-т. Київ : НАУ, 2022.
7. Гапак О. М. КРИПТОАНАЛІЗ. КРИПТОГРАФІЧНІ ПРОТОКОЛИ. Навчальний посібник. Ужгород: ПП «АУТДОР-ШАРК», 2021. 93 с.
8. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах. Підручник. Ужгород: ПП «АУТДОР-ШАРК», 2021. – 184 с.

Допоміжна література

1. Когут Ю.І. Технології блокчейн та криптовалюта: ризики та кібербезпека. К.: Дакор. 2022. 316 с. ISBN: 978-617-8066-23-9
2. 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.
3. Остапов С.Е., Євсеєв С.П. , Король О.Г. Кібербезпека: сучасні технології захисту. К.: Новий світ-2000. 2020. 678 с.

Інформаційні ресурси у мережі Інтернет

1. http://ni.biz.ua/3/3_3/3_37326_metodi-perestanovki.html
2. https://www.slideshare.net/sitecdtu/i-75720925