ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
Кафедра алгебри та диференціальних рівнянь

«ЗАТВЕРДЖУЮ»
Декан факультету математики та
цифрових технологій
_____/ Микола МАЛЯР /
«27» ____06_____20___року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Рівень вищої освіти	**другий (магістерський)**
Галузь знань	**Е Природничі науки, математика та статистика**
Спеціальність	**Е7 Математика**
Освітня програма	**Комп'ютерно-математичне моделювання**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2025

Робоча програма навчальної дисципліни «**Методи криптографічного захисту інформації**» для здобувачів другого (магістерського) рівня вищої освіти галузі знань **Е Природничі науки, математика та статистика** спеціальності **Е7 Математика** освітньої програми «**Комп'ютерно-математичне моделювання».**

Розробники: Бортош М.Ю., канд. фіз.-мат. наук, доцент кафедри алгебри та диференціальних рівнянь

Робочу програму розглянуто та затверджено на засіданні
кафедри алгебри та диференціальних рівнянь

протокол № 10 від « 18 » червня 2025р.

Завідувач кафедри _____ Олександр РЕЙТІЙ

Схвалено науково-методичною комісією

Факультету математики та цифрових технологій

протокол № 10 від « 26 » червня 2025 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 colspan="2">Денна 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 colspan="2">1-й</td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для денної форми навчання: 2,8 год.</td><td>1-й</td><td>2-ий</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>24</td><td>—</td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>24</td><td>—</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: екзамен</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>—</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 вивчення навчальної дисципліни **«Методи криптографічного захисту інформації»** є ознайомлення студентів з класичними поняттями, методами та досягненнями теорії захисту інформації; ознайомлення з моделями систем передачі даних, сучасними методами, класичними техніками шифрування, вивчення широко використовуваних криптографічних алгоритмів симетричного і асиметричного шифрування.

Відповідно до освітньої програми «**Комп'ютерно-математичне моделювання**» спеціальності «**Математика**», вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

– Здатність учитися, здобувати нові знання, уміння, у тому числі в галузях, відмінних від математики; (ЗК01)

–Здатність використовувати у професійній діяльності знання з галузей математичних, природничих, соціально-гуманітарних та економічних наук; (ЗК02)

– Здатність вирішувати проблеми у професійній діяльності на основі абстрактного мислення, аналізу, синтезу та прогнозу; (ЗК03)

– Здатність до пошуку, оброблення й аналізу інформації з різних джерел, необхідної для розв'язування наукових і професійних завдань; (ЗК04)

– Здатність генерувати нові ідеї; (ЗК05)

– Здатність спілкуватися державною мовою і усно, і письмово; (ЗК08)

– Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування; (ЗК10)

– Знання на рівні новітніх досягнень, необхідні для дослідницької та/або інноваційної діяльності у сфері математики та її практичних застосувань; (ФК01)

– Здатність застосовувати міждисциплінарні підходи при критичному осмисленні математичних проблем; (ФК02)

– Спроможність розуміти проблеми та виділяти їхні суттєві риси; (ФК04)

– Спроможність розробляти математичну модель ситуації з реального світу та переносити математичні знання у нематематичні контексти; (ФК05)

– Здатність доводити знання та власні висновки до фахівців та нефахівців; (ФК06)

– Здатність до розвитку нових та удосконалення існуючих математичних методів аналізу, моделювання, прогнозування, розв'язування нових проблем у нових галузях знань; (ФК08)

– Здатність до самоосвіти та підвищення кваліфікації на основі інноваційних підходів у сфері математики (ФК10).

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни «**Методи криптографічного захисту інформації**» є опанування навчальної дисципліни освітньої програми «Комп'ютерно-математичне моделювання»:

ОК 5 «Алгебраїчна теорія кодування».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Комп'ютерно-математичне моделювання»,** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	Шифр ПРН
Знати та розуміти фундаментальні і прикладні аспекти наук у сфері математики;	**ПРН-З-1.**
Відтворювати знання фундаментальних розділів математики в обсязі, необхідному для володіння математичним апаратом відповідної галузі знань і використання математичних методів у обраній професії;	**ПРН-З-2.**
Володіти основами математичних дисциплін і теорій, зокрема які вивчають моделі природничих і соціальних процесів;	**ПРН-З-3.**
Володіти математичними методами аналізу, прогнозування та оцінки параметрів моделей, математичними способами інтерпретації числових даних та принципами функціонування природничих процесів;	**ПРН-З-4.**
Вміти застосовувати на практиці методи теорії кодувань, актуарної та фінансової математики, використовувати динамічні моделі при дослідженні прикладних задач;	**ПРН-З-6.**
Уміти використовувати фундаментальні математичні закономірності у професійній діяльності;	**ПРН-У-1**.
Доносити професійні знання, власні обґрунтування і висновки до фахівців і широкого загалу;	**ПРН-У-3**.
Інтегрувати знання з різних галузей для вирішення теоретичних та/або практичних задач і проблем;	**ПРН-У-5**.
Усно й письмово спілкуватися рідною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності із професійних питань; читати спеціальну літературу; знаходити, аналізувати та використовувати інформацію з різних довідкових джерел;	**ПРН-У-10**.
Використовувати раціональні способи пошуку та використання науково-технічної інформації, включаючи засоби електронних інформаційних мереж; застосовувати інформаційні ресурси, у тому числі електронні, для пошуку відповідних математичних моделей;	**ПРН-У-11**.
Застосовувати комп'ютерні технології, прикладні математичні пакети, інші програмні продукти, інформаційні ресурси для розв'язування математичних задач, моделювання, аналізу моделей, для інших професійних цілей.	**ПРН-У-13**.

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Методи криптографічного захисту інформації**»:

Очікувані результати навчання з дисципліни	Шифр ПРН
Знання основних понять криптографії та криптографічного аналізу, сучасних принципів побудови сучасних криптографічних систем; знання загальних відомостей про потокові шифри; знання принципів використання генераторів псевдовипадкових чисел; принципів побудови алгоритмів блокового симетричного шифрування даних; знання моделі та протоколів асиметричної системи.	ПРН-З-1, ПРН-З-2, ПРН-З-3, ПРН-З-4, ПРН-У-1, ПРН-У-5, ПРН-У-10
Вміння моделювати та розв'язувати поставлені задачі в різних областях	ПРН-З-1, ПРН-З-2,

математики, бути підготовленим до використання в подальших дослідженнях, вміння обґрунтовувати та чітко формулювати висновки.	ПРН-З-3, ПРН-З-4, ПРН-З-6, ПРН-У-1, ПРН-У-3, ПРН-У-5, ПРН-У-10, ПРН-У-11, ПРН-У-13
Вміння використовувати моделі систем передачі даних; застосовувати результати теорії інформації та криптографії для шифрування та дешифрування даних; вміння застосовувати принципи побудови симетричних криптосистем; вміння моделювати асиметричні криптосистеми.	ПРН-З-1, ПРН-З-2, ПРН-З-3, ПРН-З-6, ПРН-У-1, ПРН-У-5, ПРН-У-11, ПРН-У-13

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Для визначення рівня засвоєння студентами навчального матеріалу використовуються такі методи оцінювання знань: виконання самостійних домашніх робіт; опитування підчас практичних занять; підсумкова модульна контрольна робота, екзамен.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю. Поточний контроль знань студентів упродовж семестру включає оцінювання роботи студентів на практичних заняттях, а також оцінювання всіх видів самостійної роботи.

Форми модульного контролю: письмова. До модульного контролю допускаються всі студенти. Модульний контроль проводиться за розкладом, затвердженим деканом факультету.

Форма підсумкового контролю: усна.

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

Поточне оцінювання та самостійна робота					**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	**50**	**100**
5	5	10	15	15		

Т1, Т2 ... – теми

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

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	**50**	**100**
10	10	5	10	10	5		

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)
Практичні заняття	7	10	7	10
Виконання самостійних домашніх робіт	3	40	3	40
Модульна контрольна робота	1	50	1	50
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Оцінювання модульної контрольної роботи здійснюється за шкалою від «0» до «50». Вплив поточого контролю та модульної контрольної роботи на модульну оцінку (100 бальну оцінку) однаковий (50 балів максимум). Після завершення вивчення дисципліни викладач виводить підсумкову модульну оцінку за 100-бальною шкалою, шкалою ЄКТС та національною шкалою.

Критерії оцінювання підсумкового семестрового контролю

Оцінювання знань студента здійснюється за 100-бальною шкалою.

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

Здобувач вищої освіти, підсумкова модульна оцінка якого складає від 0 до 34 балів, зобов'язаний скласти (перескласти) модуль до початку підсумкового контролю у строки, визначені викладачем дисципліни та погоджені деканатом факультету.

У випадку, якщо за поточну успішність студент набрав більше 59 балів, то за його бажанням може бути виставлена відповідна набраним балам підсумкова оцінка з дисципліни без складання іспиту. Здобувач вищої освіти може підвищити на екзамені підсумковий бал, при цьому, за результатами складання іспиту оцінка не може бути менша за підсумкову модульну оцінку, яку він отримав за результатами модульних контролів у семестрі.

При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань студентів за різними системами.

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка ECTS	Екзаменаційна оцінка за національною шкалою
90–100	**A**	*Відмінно*
82–89	**B**	*Добре*
74–81	**C**	
64–73	**D**	*Задовільно*
60–63	**E**	
35–59	**FX**	*Незадовільно з можливістю повторного складання*
0–34	**F**	*Незадовільно з обов'язковим повторним вивченням дисципліни*

Критерій оцінювання з дисципліни

— **"A"** (90 та вище балів) 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;

— **"B"** (82–89 балів) 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;

— **"C"** (74–81 балів) 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;

— **"D"** (64–73 балів) 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, оцінка "D" виставляється студентам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;

— **"E"** (60–63 балів) 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, оцінка "E" виставляється студентам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача;

— **"FX"** (35–59 балів) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань;

— **"F"** (0–34 балів) 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. Загальні проблеми захисту інформації

Загальні відомості про захист інформації. Небезпека даних. Рівні захисту даних.

Тема 2. Інформаційна ентропія

Моделювання джерел інформації. Властивості інформації з точки зору її захисту. Інформаційна ентропія**.** Визначення функції ентропії.

Тема 3. Характеристики дискретного каналу передавання інформації.

Моделі дискретних каналів. Характеристики дискретного каналу. Безумовна та умовна ентропія повідомлення джерела. Статистична модель канала зв'язку. Узагальнена модель системи передачі даних. Матриця прямих та зворотних переходів повідомлень. Кількісне оцінювання інформації.

Тема 4. Класифікація сучасних криптосистем

Класифікація сучасних криптосистем. Вимоги до сучасних криптосистем Принципи побудови сучасних симетричних криптографічних систем. Сучасні блокові шифри. Атаки на блокові шифри.

Тема 5. Потокові шифри й генератори псевдовипадкових чисел

Генератори псевдовипадкових чисел. Потокові шифри. Класифікація потокових шифрів.

Модуль 2

Тема 1. Стандарт симетричного алгоритму блокового шифрування даних DES.

Історія стандарту. Принципи побудови алгоритму. Структура алгоритму шифрування даних. Генерація раундових ключів. Процес шифрування даних. Аналіз алгоритму. Багаторазове застосування алгоритму. Безпека шифру.

Тема 2. Симетричний алгоритм блокового шифрування даних IDEA

Історія стандарту. Принципи побудови алгоритму. Структура алгоритму шифрування даних. Генерація раундових ключів для за шифрування та розшифрування даних. Процес шифрування даних. Безпека шифру. Застосування алгоритму.

Тема 3. Стандарт шифрування ДСТУ ГОСТ 28147:2009

Історія стандарту. Принципи побудови алгоритму. Шифрування даних у режимі простої заміни. Шифрування даних у режимі гамування та у режимі гамування зі зворотним зв’язком. Аналіз шифру.

Тема 4. Стандарт шифрування даних Advanced Encryption Standard

Історія стандарту. Принципи побудови алгоритму. Формат даних алгоритму. Структура алгоритму. Алгоритм розгортання ключа. Зашифрування та розшифрування даних. Аналіз та безпека шифру.

Тема 5. Асиметричні криптографічні системи шифрування

Модель асиметричної системи. Перша криптографічна система з відкритим ключем. Криптографічна система Шаміра, система Ель-Гамаля, RSA, Рабіна. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні. Алгоритм обчислення порядку.

Тема 6. Застосування методів теорії інформації і кодування

Призначення кодів CRC. Загальна характеристика алгоритмів CRC. Принципи побудови кодів CRC. Сучасні методи стиснення даних.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин: 120					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Загальні проблеми захисту інформації	8	2	2	-	-	4
Тема 2. Інформаційна ентропія	12	2	2	-	-	8
Тема 3. Характеристики дискретного каналу передавання інформації.	24	2	4	-	-	18
Тема 4. Класифікація сучасних криптосистем	12	2	2	-	-	8
Тема 5. Потокові шифри й генератори псевдовипадкових чисел	14	2	2	-	-	10
Модульна контрольна робота	2	2	-	-	-	-
Разом за модуль	**72**	**12**	**12**	-	-	**48**
Модуль 2						
Тема 1. Стандарт симетричного алгоритму блокового шифрування даних DES.	8	2	2	-	-	4
Тема 2. Симетричний алгоритм блокового шифрування даних IDEA	8	2	2	-	-	4
Тема 3. Стандарт шифрування ДСТУ ГОСТ 28147:2009	7	1	2	-	-	4
Тема 4. Стандарт шифрування даних Advanced Encryption Standard	7	1	2	-	-	4
Тема 5. Асиметричні криптографічні системи шифрування	8	2	2	-	-	4
Тема 6. Застосування методів теорії інформації і кодування	8	2	2	-	-	4
Модульна контрольна робота	2	2	-	-	-	-
Разом за модуль	**48**	**14**	**12**	-	-	**24**
Разом за семестр	**120**	**24**	**24**	-	-	**72**

6.3. Теми практичних занять

№ з/п	Назва теми	Кількість Годин
1-й семестр		
1.	Загальні відомості про захист інформації	2
2	Моделювання джерел інформації	1
3	Інформаційна ентропія	1

4	Моделі дискретних каналів	1
5	Характеристики дискретного каналу передавання інформації	1
6	Узагальнена модель системи передачі даних	1
7	Матриця прямих та зворотних переходів повідомлень	1
8	Класифікація сучасних криптосистем	1
9	Принципи побудови сучасних симетричних криптографічних систем	1
10	Генератори псевдовипадкових чисел	1
11	Потокові шифри	1
12	Стандарт симетричного алгоритму блокового шифрування даних DES	2
13	Симетричний алгоритм блокового шифрування даних IDEA	2
14	Стандарт шифрування ДСТУ ГОСТ 28147:2009	2
15	Стандарт шифрування даних Advanced Encryption Standard	2
16	Асиметричні криптографічні системи шифрування	2
17	Застосування методів теорії інформації і кодування	2
Усього за перший модуль		**24**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин *Денна форма*
1-й семестр		
1.	Небезпека даних. Рівні захисту даних	4
2	Властивості інформації з точки зору її захисту	4
3	Визначення функції ентропії.	4
4	Безумовна та умовна ентропія повідомлення джерела	4
5	Математичні моделі сигналів	4
6	Статистична модель канала зв’язку	6
7	Кількісне оцінювання інформації	4
8	Вимоги до сучасних криптосистем	4
9	Сучасні блокові шифри. Атаки на блокові шифри	4
10	Генератори псевдовипадкових чисел на основі алгоритму BBS	4
11	Класифікація потокових шифрів	6
12	Багаторазове застосування алгоритму DES	4
13	Застосування алгоритму IDEA	4
14	Нестандартне використання стандарту ДСТУ ГОСТ 28147:2009	4
15	Аналіз та безпека шифру Advanced Encryption Standard	4
16	Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні	4
17	Сучасні методи стиснення даних	4
Разом		**72**

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

Технічні засоби – персональні комп’ютери, мультимедійний проєктор.

Програмне забезпечення – система електронного навчання Moodle.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. Луцьк: Вежа-Друк, 2014. 164 с.

3.Теорія інформації і кодування: курс лекцій: навч. посіб. КПІ ім. Ігоря Сікорського; уклад.: А.Є. Коваленко. Київ: КПІ ім. Ігоря Сікорського, 2020. 248 с.

4. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с.

5. Остапов С.Є., Валь Л.О. Основи крипторгафії. Навчальний посібник: Чернівці: Книги, 2008, 188 с.

Допоміжна література

1. Основи теорії інформації та кодування: навч. посібник / І. А. Прокопишин, Р. Є. Рикалюк, В. Ф. Чекурін, К. А. Червінка. Електрон. вид. Львів: ЛНУ ім. Івана Франка, 2023. 156 с.

2. Фетюхіна Л. В., Бутова О.А. Теорія інформації та кодування: навч.-метод. посібник. Харків: НТУ «ХПІ», 2012. 68 с.

3. 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 в мережі Інтернет

1. https://dspace.uzhnu.edu.ua — репозитарій ДВНЗ «Ужгородський національний університет».
2. http://moodle.uzhnu.edu.ua — сайт електронного навчання ДВНЗ «Ужгородський національний університет».
3. http://www.nbuv.gov.ua — Національна бібліотека України імені В. І. Вернадського.