НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРИКЛАДНОЇ МАТЕМАТИКИ І МЕХАНІКИ

«ЗАТВЕРДЖУЮ»

Директор ІПММ НАН України
академік НАН України

_____ Ігор СКРИПНІК
«_25_» __вересня__2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Сучасні алгоритми та математичні методи захисту інформації

підготовки здобувачів ступеня вищої освіти
третій (освітньо-науковий)
доктора філософії

галузь знань 11 Математика та статистика

спеціальність 113 Прикладна математика

Черкаси – 2025 р.

Робоча навчальна програма навчальної дисципліни «Сучасні алгоритми та математичні методи захисту інформації» для здобувачів наукового ступеня доктора філософії за спеціальністю 113 Прикладна математика.

Розробник:

Сенченко Олексій Сергійович, старший науковий співробітник відділу теорії керуючих систем, кандидат фізико-математичних наук, доцент.

Робочу програму схвалено на засіданні відділу теорії керуючих систем
Протокол № 4 від 18 вересня 2025 року.

Завідувач відділу  Кононов Ю.М.

Схвалено Науково-методичною радою Інституту прикладної математики і механіки НАН України
Протокол № 4 від 22 вересня 2025 року.

.

Голова науково-методичної ради  Нєсмєлова О.В.

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Кількість кредитів - 4</td><td>Галузь знань:
11 «Математика та статистика»</td><td>дисципліна вільного вибору аспіранта</td></tr>
<tr><td rowspan="5">Загальна кількість годин – 120</td><td rowspan="5">Спеціальність:
113 «Прикладна математика»</td><td>Рік підготовки:</td></tr>
<tr><td>1-2</td></tr>
<tr><td>Семестр</td></tr>
<tr><td>2, 3</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="6">Тижневих годин:
аудиторних – 1,5
самостійної роботи – 1,7</td><td rowspan="6">Освітньо-кваліфікаційний рівень:
доктор філософії</td><td>28 год</td></tr>
<tr><td>Практичні</td></tr>
<tr><td>28 год</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>64 год</td></tr>
<tr><td>Вид контролю: іспит</td></tr>
</table>

2. Мета, завдання та очікувані результати навчальної дисципліни.

Метою навчальної дисципліни «Сучасні алгоритми та математичні методи захисту інформації» є послідовне викладення історії розвитку криптології та розгляд основних алгоритмів і методів захисту інформації, що були широко вживаними на різних етапах розвитку криптології.

Завдання навчальної дисципліни:

- ознайомлення та оволодіння класичними та сучасними методами криптології та криптоаналізу;
- оволодіння теоретичними положеннями та основними застосуваннями алгебри, дискретної математики та теорії алгоритмів у цих методах;
- розвиток у аспірантів вміння правильного логічного та математичного мислення, побудови повноцінної аргументації, здійснення логічного та методологічного аналізу.

Очікувані результати навчальної дисципліни

Загальні компетентності:

- ЗК1. Аналіз і синтез. Здатність до аналізу та синтезу на основі логічних аргументів та перевірених фактів; навички управління інформацією (уміння знаходити та аналізувати інформацію з різних джерел).
- ЗК3. Гнучкість мислення. Набуття гнучкого способу мислення, який дає можливість зрозуміти й розв’язати проблеми та задачі, зберігаючи при цьому критичне відношення до усталених наукових концепцій.
- ЗК4. Креативність. Потенціал креативності у генеруванні ідей та досягненні наукових цілей.
- ЗК5. Групова робота. Здатність до взаємодії (робота в команді); здатність працювати в міждисциплінарній команді.
- ЗК7. Міжнародний кругозір. Здатність працювати в міжнародному середовищі, ставитися із повагою до національних та культурних традицій, способів роботи інших членів групи.
- ЗК8. Популяризаційні навички. Вміння спілкуватися із нефахівцями; здатність провести усну презентацію та написати зрозумілу статтю за результатами проведених досліджень, а також щодо сучасних концепцій у прикладній математиці для нефахівців у цій галузі; здатність спілкуватися з експертами з інших галузей.
- ЗК11. Етичні установки. Етика поведінки в наукових дослідженнях; турбота про якість результату.
- ЗК12. Особисті якості. Здатність до навчання, саморозвитку та самовдосконалення протягом життя; визначеність і наполегливість щодо поставлених завдань і взятих обов’язків.

Фахові компетентності:

- ФК2. Здатність застосовувати сучасну методологію, загальні та спеціальні методи наукового дослідження за спеціальністю та обраною спеціалізацією.
- ФК 5. Уміння будувати адекватні математичні моделі, досліджувати побудовані моделі та визначати можливості їх застосування.
- ФК 8. Здатність здійснювати дослідження прикладних математичних задач з використанням спеціальних математичних пакетів та аналізувати отримані дані.
- ФК18. Здатність ефективно аналізувати великі набори різнорідних даних із використанням методів машинного навчання, статистики, штучного інтелекту тощо.
- ФК19. Знання сучасних технологій створення та захисту програмних продуктів, компетентність у алгоритмізації обчислювальних процесів та методів, знання та уміння використовувати сучасні мови програмування

Програмні результати навчання:

- ПРН 1. Знати та розуміти традиційні та передові тенденції в галузі прикладної математики, етапи історичного розвитку математичних знань і парадигм, формування поглибленої системи наукових знань за напрямом досліджень.
- ПРН 3. Знати основні принципи, форми та методи проведення наукових досліджень в галузі прикладної математики, володіти математичним апаратом в об’ємі, достатньому для професійної діяльності.
- ПРН 4. Вміти будувати та досліджувати математичні моделі фізичних, соціально-економічних, технічних, біологічних тощо процесів, систем, процесів, формалізувати проблеми, описані природною мовою, за допомогою математичних методів, застосовувати загальні підходи до математичного моделювання конкретних процесів.
- ПРН5. Мати навички використання загальних офісних та спеціалізованих програмних засобів за напрямом професійної діяльності, вміти користуватися спеціалізованими інтернет-ресурсами.
- ПРН9. Вміти організувати неперервний власний саморозвиток і самовдосконалення, набуття гнучкого способу мислення при творчому дослідженні, в тому числі прикладних математичних проблем.
- ПРН16. Вміти застосовувати сучасні технології алгоритмізації обчислювальних процесів, методів програмування, програмної реалізації чисельних і символьних алгоритмів.
- ПРН 17. Знати основні чисельні методи та алгоритми розв’язання задач прикладної та обчислювальної математики.
- РН 18. Знати та вміти досліджувати основні математичні моделі, що використовуються для описання та дослідження дискретних систем різних типів, реалізовувати алгоритми моделювання для дослідження

характеристик і поведінки складних об’єктів і систем, проводити експерименти.

За результатами вивчення навчальної дисципліни здобувач доктора філософії повинен:

знати:

- основні поняття і методи криптології, теорії алгоритмів, алгебри та дискретної математики (криптостійкість, однобічна функція, конгруенції, обчислювальна складність алгоритму тощо);
- основні сучасні симетричні та асиметричні алгоритми шифрування;
- основні поняття, що лежать у основі створення та використання електронного цифрового підпису.

вміти:

- розв’язувати практичні задачі зі шифрування/дешифрування повідомлення заданим алгоритмом із заданим ключем (ключами);
- розробляти програмні системи, які зашифровують та розшифровують інформацію симетричними та асиметричними алгоритмами шифрування та проводити криптоаналіз розглянутих алгоритмів шифрування;
- розробляти математичні моделі інформаційних процесів.

3. Програма навчальної дисципліни

Тема 1. Основні поняття криптології. [1:12-20; 2:8-14; 3:14-41; 4:9-19; 7:35-84; Д3:6-27; Д3:6-35]

1. Коротка історія криптології.
2. Шифри зсуву.
3. Шифри заміни.
4. Методи криптоаналізу.

Тема 2. Класичні симетричні шифри. [1:22-27; 3:56-69; 4:20-37; 6:13-32]

1. Біграмний шифр (шифрування, дешифрування, криптоаналіз).
2. Шифр Віженера (шифрування, дешифрування, криптоаналіз).
3. Шифр з автоключем (шифрування, дешифрування, криптоаналіз).
4. Матричний шифр обходу (шифрування, дешифрування, криптоаналіз).

Тема 3. Стеганографія. Кількаразове шифрування. [1: 27-30, 37-40; 4:10-13; 7:39-40; 9: 110-112]

1. Шифр Кардано (шифрування, дешифрування, криптоаналіз).
2. Шифр ADFGVX (шифрування, дешифрування, криптоаналіз).

Тема 4. Сучасні симетричні криптосистеми. [1:34-37,40-44; 2:72-89; 3:100-134, 172-227; 4:71-78; 6:42-75; 8:55-86]

1. Шифр одноразового блокноту (шифрування, дешифрування, криптоаналіз).
2. Криптосистема DES (шифрування, дешифрування, криптоаналіз).
3. Криптосистеми, що засновані на криптосистемі DES.

Тема 5. Сучасні криптографічні інструменти. [1:146-159; 2:48-71; 3:138-148; 6:38-41; 9:250-282]

1. Важкооборотні функції.
2. Генератори псевдовипадкових бітів.

Тема 6. Алгебраїчний апарат асиметричних криптосистем. [1:118-120; 2:128-141; 3: 395-403; 4:44-60; 7:85-115; 10:261-302; Д1:28-77, 85-104]

1. Прості числа. Функція Ейлера.
2. Конгруенції.
3. Однобічні функції.
4. Алгоритм швидкого піднесення до степеню.

Тема 7. Криптосистема RSA. [1:130-136; 2:114-119; 3:409-414; 5:38-47; 8:173-204; 10:436-460; 11:139-149]

1. Шифрування у криптосистемі RSA.
2. Дешифрування у криптосистемі RSA.
3. Криптоаналіз системи RSA.

Тема 8. Криптосистема Рабіна. [1:137-139; 3:414-418; 10:556-566]

1. Шифрування у криптосистемі Рабіна.
2. Дешифрування у криптосистемі Рабіна.
3. Криптоаналіз системи Рабіна.

Тема 9. Криптосистема Ель-Гамаля. [1:143-145; 3:406-409; 4:84-88]

1. Шифрування у криптосистемі Ель-Гамаля.
2. Дешифрування у криптосистемі Ель-Гамаля.
3. Криптоаналіз системи Ель-Гамаля.

Тема 10. Криптосистеми Меркля-Хелмана та Шора-Рівеста. [6:76-80; 7:222-228]

1. Шифрування та дешифрування у криптосистемі Меркля-Хелмана.
2. Шифрування та дешифрування у криптосистемі Шора-Рівеста.
3. Криптоаналіз систем Меркля-Хелмана та Шора-Рівеста.

Тема 11. Еліптична криптографія. [2:120-126; 5:81-102; 6:97-111; 8:205-238; 10:336-353]

1. Математичні поняття, пов’язані з еліптичними кривими.
2. Загальні принципи еліптичної криптографії.
3. Алгоритм Діффі-Хелмана.

Тема 12. Хешування даних. [2:147-149; 4:88-108; 6:86-92; 8:293-318; 9:339-380; 10:167-206; 11:32-54]

1. Загальні принципи хешування даних.
2. Класифікація хеш-функцій.
3. Застосування хеш-функцій.

Тема 13. Електронний цифровий підпис. [1:164-172; 2:142-147, 180-195; 4:117-129; 5:59-80, 102-164; 7:228-236; 8:259-292; 9:419-440; Д5]

1. Стандарти систем цифрового підпису.
2. Цифровий підпис у криптосистемі RSA.
3. Цифровий підпис у криптосистемі Ель-Гамаля.
4. Цифровий підпис з використанням алгоритму ECDSA.

Тема 14. Елементи квантової криптології. [7:415-446; 10:499-524; 11:348-376; Д4]

1. Загальні принципи квантової криптології. Алгоритм Беннета.
2. Реалізовані на практиці квантові криптосистеми.
3. Квантовий криптоаналіз.

4. Структура навчальної дисципліни

Назва теми	Кількість годин			
	Усього	у тому числі		
		Лекції	Практичні заняття	Самостійна робота
1	**2**	**3**	**4**	**5**
Тема 1. Основні поняття криптології.	7	2	2	3
Тема 2. Класичні симетричні шифри.	7	2	2	3
Тема 3. Стеганографія. Кількаразове шифрування.	10	2	2	6
Тема 4. Сучасні симетричні криптосистеми.	10	2	2	6
Тема 5. Сучасні криптографічні інструменти.	13	2	2	7
Тема 6. Алгебраїчний апарат асиметричних криптосистем.	9	2	2	5
Тема 7. Криптосистема RSA.	9	2	2	5
Тема 8. Криптосистема Рабіна.	8	2	2	4
Тема 9. Криптосистема Ель-Гамаля.	8	2	2	4
Тема 10. Криптосистеми Меркля-Хелмана та Шора-Рівеста.	8	2	2	4
Тема 11. Еліптична криптографія.	8	2	2	4
Тема 12. Хешування даних.	9	2	2	5
Тема 13. Електронний цифровий підпис.	8	2	2	4
Тема 14. Елементи квантової криптології.	8	2	2	4
Усього годин	**120**	**28**	**28**	**64**

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Основні поняття криптології.	2
2	Класичні симетричні шифри.	2
3	Стеганографія. Кількаразове шифрування.	2
4	Сучасні симетричні криптосистеми.	2
5	Сучасні криптографічні інструменти.	2
6	Алгебраїчний апарат асиметричних криптосистем.	2

№ з/п	Назва теми	Кількість годин
7	Криптосистема RSA.	2
8	Криптосистема Рабіна.	2
9	Криптосистема Ель-Гамаля.	2
10	Криптосистеми Меркля-Хелмана та Шора-Рівеста.	2
11	Еліптична криптографія.	2
12	Хешування даних	2
13	Електронний цифровий підпис.	2
14	Елементи квантової криптології.	2
	Разом	**28**

6. Теми для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Основні поняття криптології.	3
2	Класичні симетричні шифри.	3
3	Стеганографія. Кількаразове шифрування.	6
4	Сучасні симетричні криптосистеми.	6
5	Сучасні криптографічні інструменти.	7
6	Алгебраїчний апарат асиметричних криптосистем.	5
7	Криптосистема RSA.	5
8	Криптосистема Рабіна.	4
9	Криптосистема Ель-Гамаля.	4
10	Криптосистеми Меркля-Хелмана та Шора-Рівеста.	4
11	Еліптична криптографія.	4
12	Хешування даних.	5
13	Електронний цифровий підпис.	4
14	Елементи квантової криптології.	4
	Разом	**64**

7. Методи навчання

При вивченні дисципліни використовуються:

1. Дидактичні методи – лекції з використанням мультимедійних презентацій.

2. Практичні методи: практичні роботи з використанням прикладного програмного забезпечення.

3. Метод самостійного навчання.

4. Активні методи: експрес опитування.

5. Словесні методи навчання: лекції, бесіди.

8. Методи контролю

Використовуються наступні методи контролю:

1. Поточний контроль знань:
- усне опитування;
- виконання практичних робіт;
- виконання дослідницьких завдань.
2. Підсумковий контроль знань (іспит):
- екзаменаційні білети.

9. Критерії оцінювання результатів навчання

Розподіл балів, які отримує аспірант

Аудиторна робота														**Самостійна робота**	**Підсумковий контроль (іспит)**	**Загальна кількість отриманих балів**
теми																
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14			
2	4	4	4	2	2	4	4	4	4	4	4	4	4	**10**	**40**	**100**

Шкала оцінювання

Сума балів за всі види навчальної діяльності	**Оцінка за національною шкалою**
	для іспиту
90-100	«відмінно» - здобувач повно і всебічно розкриває питання теми, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідної теми і може аргументовано її доводити
75-89	«добре» - загалом рівень знань здобувачів відповідає викладеному вище, але мають місце деякі упущення при виконанні завдань, обґрунтування неточні, не підтверджуються достатньо обґрунтованими доказами
60-74	«задовільно» - здобувач розкрив питання, в загальних рисах, розуміє їх суть, намагається робити висновки, але при цьому припускається грубих помилок, матеріал викладає нелогічно і не самостійно
35-59	«незадовільно» - з можливістю повторного складання, здобувач не в змозі дати відповідь на поставлене запитання або відповідь неправильна, не розуміє суті питання, не може зробити висновки

0-34	«незадовільно» - з обов'язковим повторним вивченням дисципліни

10. Орієнтовний перелік питань до підсумкового контролю (іспиту)

1. Шифри Цезаря та Скитала.
2. Шифрування та дешифрування методом частоколу.
3. Шифр простої заміни та його криптоаналіз.
4. Гомофонний шифр та його криптоаналіз.
5. Біграмний шифр та його криптоаналіз.
6. Шифрування шифром Віженера.
7. Дешифрування шифром Віженера.
8. Криптоаналіз шифру Віженера.
9. Шифрування шифром з автоключем.
10. Дешифрування шифром з автоключем.
11. Основи стеганографії.
12. Шифрування та дешифрування шифром Кардано.
13. Шифр одноразового блокноту.
14. Криптоаналіз шифру одноразового блокноту.
15. Шифрування шифром ADFGVX.
16. Дешифрування шифром ADFGVX.
17. Криптоаналіз шифру ADFGVX.
18. Криптосистема DES.
19. Криптосистеми, що засновані на криптосистемі DES.
20. Однобічні функції.
21. Алгоритм швидкого піднесення до степеню.
22. Шифрування у криптосистемі RSA.
23. Дешифрування у криптосистемі RSA.
24. Криптоаналіз криптосистеми RSA.
25. Шифрування у криптосистемі Рабіна.
26. Дешифрування у криптосистемі Рабіна.
27. Криптоаналіз криптосистеми Рабіна.
28. Шифрування у криптосистемі Ель-Гамаля.
29. Дешифрування у криптосистемі Ель-Гамаля.
30. Криптоаналіз криптосистеми Ель-Гамаля.
31. Шифрування у криптосистемі Меркля-Хелмана.
32. Дешифрування у криптосистемі Меркля-Хелмана.
33. Шифрування у криптосистемі Шора-Рівеста.
34. Дешифрування у криптосистемі Шора-Рівеста.
35. Загальні принципи еліптичної криптографії.
36. Алгоритм Діффі-Хелмана.
37. Загальні принципи хешування даних.
38. Класифікація хеш-функцій.
39. Застосування хеш-функцій.

40. Стандарти систем цифрового підпису.
41. Генерація цифрового підпису у криптосистемі RSA.
42. Підтвердження цифрового підпису у криптосистемі RSA.
43. Цифровий підпис у криптосистемі Ель-Гамаля.
44. Цифровий підпис з використанням алгоритму ECDSA.
45. Загальні принципи квантової криптології. Алгоритм Беннета.

11. Рекомендована література

Основна література дисципліни

1. Вербіцький О.В. Вступ до криптології. Львів : Науково-технічна література, 1998. 248 с.

2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. Вінниця : ВНТУ, 2011. 199 с.

3. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія : системи шифрування : підручник. Київ : ДУТ, 2014. 448 с.

4. Глинчук Л.Я. Криптологія : навчально-методичний посібник. Луцьк : Вежа-Друк, 2014. 164 с.

5. Козіна Г.Л. Криптографія від історії до сучасних стандартів : навчальний посібник. Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.

6. Щур Н.О., Покотило О.А. Основи криптології : навчальний посібник. Житомир : ДУ «Житомирська політехніка», 2021. 120 с.

7. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. Донецк : ИПММ НАН Украины, 2009. 479 с.

8. Paar C, Pelzl J. Understanding Cryptography. A Textbook for Students and Practitioners. Springer, 2010. 372 p.

9. Stallings W. Cryptography and network security. Principles and practice. Seventh edition. Global edition. Pearson, 2017. 766 p.

10. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd Edition. CRC Press, 2021. 626 p.

11. Wong D. Real-World Cryptography, Version 12. Manning Publications, 2021. 412 p.

Допоміжна література дисципліни

1. Математичні основи криптографії : конспект лекцій / укладачі : В.А. Фільштінський, А.В. Бережний. Суми : СДУ, 2011. 138 с.

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

3. Лісовська Ю.П. Кібербезпека: ризики та заходи : навчальний посібник. Київ : Кондор, 2019. 272 с.

4. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), pp. 145–195.

5. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. [Чинний від 2002-12-28]. Видання офіційне. Київ : Держспоживстандарт, 2003. 31 с.