

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Кафедра прикладної математики



«ЗАТВЕРДЖЕНО»
завідувачка кафедри

О.О. Сдвижкова

«29» серпня 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Математичні основи захисту даних»

Галузь знань	11 Математика та статистика
Спеціальність	113 Прикладна математика
Рівень вищої освіти	Перший (бакалаврський)
Статус	Обов'язкова
Загальний обсяг	3 кредити ЄКТС (90 годин)
Форма підсумкового контролю	диференційований залік
Термін викладання	5-й семестр
Мова викладання	українська

Викладачі: проф. Бабець Дмитро Володимирович

Пролонговано: на 20__/20__ н.р. _____ (_____) «__»__ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____ (_____) «__»__ 20__р.
(підпис, ПІБ, дата)

Дніпро
НТУ «ДП»
2025

Робоча програма навчальної дисципліни **«Математичні основи захисту даних»** для бакалаврів освітньо-професійної програми вищої освіти **«Математичне моделювання систем і процесів»** зі спеціальності F1 «Прикладна математика» / Нац. техн. ун-т. «Дніпровська політехніка», каф. прикладної математики. – Д. : НТУ «ДП», 2025. – 14 с.

Розробник: Д.В. Бабець, д-р техн. наук, проф.

Робоча програма регламентує:

- мету дисципліни;
- дисциплінарні результати навчання;
- базові дисципліни;
- обсяг і розподіл за формами організації освітнього процесу та видами навчальних занять;
- програму дисципліни (тематичний план за видами навчальних занять);
- алгоритм оцінювання рівня досягнення дисциплінарних результатів навчання (шкали, засоби, процедури та критерії оцінювання);
- інструменти, обладнання та програмне забезпечення;
- рекомендовані джерела інформації.

Робоча програма призначена для реалізації компетентнісного підходу під час планування освітнього процесу, викладання дисципліни, підготовки студентів до контрольних заходів, контролю провадження освітньої діяльності, внутрішнього та зовнішнього контролю забезпечення якості вищої освіти, акредитації освітніх програм у межах спеціальності.

Робоча програма буде в пригоді для формування змісту підвищення кваліфікації науково-педагогічних працівників кафедр університету.

Погоджено рішенням науково-методичної комісії спеціальності F1 «Прикладна математика» (протокол № 8 від 29 серпня 2025).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	4
2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ.....	4
3. БАЗОВІ ДИСЦИПЛІНИ.....	5
4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ	6
5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ.....	6
6. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ.....	7
6.1 Шкали.....	7
6.2 Засоби та процедури	8
6.3 Критерії.....	9
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	12
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ.....	12
9. ІНФОРМАЦІЙНІ РЕСУРСИ	13

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

В освітньо-професійній програмі «Математичне моделювання систем і процесів» спеціальності 113 «Прикладна математика» здійснено розподіл програмних результатів навчання за організаційними формами освітнього процесу. Зокрема, до дисципліни Ф4 «Математичні основи захисту даних» віднесені такі результати навчання:

РН08	Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень.
РН09	Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач.

Мета дисципліни – формування у здобувачів вищої освіти компетентностей щодо розуміння математичних принципів та алгоритмічних основ криптографії, вивчення методів шифрування, зокрема блокових і поточкових шифрів, а також основ асиметричної криптографії. Курс спрямований на розвиток навичок застосування математичного апарату для проєктування, аналізу та реалізації методів захисту даних у різних задачах інформаційної безпеки при професійній підготовці бакалаврів за спеціальністю 113 Прикладна математика.

Реалізація мети вимагає трансформації програмних результатів навчання в дисциплінарні та відбір змісту навчальної дисципліни за цим критерієм.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Очікувані дисциплінарні результати навчання надані у таблиці 1.1.

Таблиця 1.1 – Очікувані дисциплінарні результати навчання з дисципліни «Математичні основи захисту даних»

Дисциплінарні результати навчання (ДРН)		
ПРН	шифр ДРН	зміст
РН08	РН08.1-Ф4	Застосовувати методи математичного моделювання та елементи експертного аналізу для оцінювання рівня захисту інформаційних систем, аналізу типів атак і криптостійкості класичних та сучасних шифрів.
	РН08.2- Ф4	Використовувати апарат теорії чисел і модульної арифметики для побудови та математичного обґрунтування криптографічних алгоритмів симетричного й асиметричного шифрування.

Дисциплінарні результати навчання (ДРН)		
ПРН	шифр ДРН	зміст
РН09	РН09.1- Ф4	Розробляти та реалізовувати алгоритми симетричної криптографії (блокові та потокові шифри) з урахуванням вимог до ефективності, стійкості.
	РН09.2- Ф4	Створювати та досліджувати алгоритми асиметричної криптографії, зокрема RSA, з аналізом їхньої обчислювальної складності, надійності та застосувань у забезпеченні конфіденційності та автентичності даних.

3. БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті дисциплінарні результати навчання
Б2 Алгебра та геометрія	Знати основи та принципи застосування лінійної та векторної алгебри, аналітичної геометрії.
Б1 Математичний аналіз	Знати основи та принципи теорії границь, застосування диференціального та інтегрального числення, принципи вирішення технічних завдань на основі математичного аналізу.
Б3 Теорія ймовірностей	Знати основи та принципи застосування фундаментальних понять теорії ймовірностей та певних методів оцінки ймовірностей
Б5 Математична статистика	Знати основи та принципи застосування фундаментальних понять математичної статистики, обирання та застосування певних критеріїв оцінки результатів експериментів
Ф7 Теорія чисел	Знати модульну арифметику та основні поняття, що базуються на теорії порівнянь.

4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Вид навчальних занять	Розподіл за формами навчання, години							
	денна			вечірня		заочна		
	Обсяг	аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота	Обсяг	аудиторні заняття	самостійна робота
лекційні	45	16	29	-	-			
практичні	45	16	29	-	-			
лабораторні	-	-	-	-	-			
семінари	-	-	-	-	-			
РАЗОМ	90	32	58	-	-			

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ЛЕКЦІЇ	45
РН08.1-Ф4	Тема 1. Вступ до криптології та основи захисту інформації	6
	Ознайомлення з базовими поняттями інформаційної безпеки, типи атак, принципи конфіденційності, цілісності та автентичності даних. Особливу увагу приділено класичним криптографічним системам, зокрема шифрам Цезаря, Гілла та методам перестановки. Аналізується криптостійкість класичних методів.	
РН08.2-Ф4	Тема 2. Математичні основи криптографії: теорія чисел і модульна арифметика	12
	Вивчення математичного апарату, що лежить в основі сучасної криптографії. Розглядаються поняття подільності, алгоритм Евкліда, операції в модульній арифметиці, зокрема знаходження обернених елементів, модульне піднесення до степеня, теореми Ферма та Ейлера, а також Китайська теорема про остачі.	
РН09.1-Ф4	Тема 3. Симетрична криптографія: алгоритми та реалізація	12
	Розглядаються принципи роботи симетричних шифрів. Вивчаються блокові шифри, зокрема структура Фейстеля, загальні принципи DES та AES. Також розглядаються потокові шифри, генерація псевдовипадкових послідовностей.	
РН09.2-Ф4	Тема 4. Асиметрична криптографія: алгоритм RSA	15
	Вивчення основ криптографії з відкритим ключем. Розглядається проблема факторизації великих чисел, принципи побудови алгоритму RSA, генерація ключів, процеси шифрування, розшифрування та створення електронного підпису.	

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ПРАКТИЧНІ ЗАНЯТТЯ	45
RH08.1-Ф4 RH08.2-Ф4	1. Математична криптологія – шифри простої моноалфавітної підстановки, шифр Гілла, шифри перестановки (шифрування та криптоаналіз)	10
RH09.1-Ф4	2. Блокові шифри – математичні основи і реалізація блокових шифрів DES та AES.	12
RH09.1-Ф4	3. Поточкові шифри – криптоаналіз Лінійного конгруентного генератора та n - бітового регістру із зворотним лінійним зв'язком	12
RH09.2-Ф4	4. Практичне застосування та криптоаналіз алгоритму RSA.	11
	РАЗОМ	90

6. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Сертифікація досягнень студентів здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях відповідно до Положення університету «Про оцінювання результатів навчання здобувачів вищої освіти».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання студента за дисципліною.

6.1 Шкали

Оцінювання навчальних досягнень студентів НТУ «ДП» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за офіційною відсутністю національної шкали) для конвертації (переведення) оцінок здобувачів вищої освіти різних закладів.

Шкали оцінювання навчальних досягнень студентів НТУ «ДП»

Рейтингова	Інституційна
90...100	відмінно / Excellent
74...89	добре / Good
60...73	задовільно / Satisfactory
0...59	незадовільно / Fail

Кредити навчальної дисципліни зараховуються, якщо студент отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації відповідно до Положення про організацію освітнього процесу НТУ «ДП».

6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь/навичок, комунікації, автономії та відповідальності студента за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Студент під час контрольних заходів має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ 2).

Засоби діагностики, що надаються студентам на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних результатів навчання.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			ПІДСУМКОВИЙ КОНТРОЛЬ	
навчальне заняття	засоби діагностики	процедури	засоби діагностики	процедури
лекції	контрольні завдання за кожною темою	виконання завдання під час лекцій	комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів;
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		виконання за бажанням студента

Під час поточного контролю лекційні заняття оцінюються шляхом визначення якості виконання контрольних конкретизованих завдань. Практичні заняття оцінюються якістю виконання контрольного або індивідуального завдання.

Якщо зміст певного виду занять підпорядковано декільком складовим опису кваліфікаційного рівня, то інтегральне значення оцінки може визначатися з урахуванням вагових коефіцієнтів, що встановлюються викладачем.

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі студента шляхом визначення середньозваженого значення поточних оцінок.

Незалежно від результатів поточного контролю кожен студент має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

Кількість конкретизованих завдань ККР повинна відповідати відведеному часу на виконання. Кількість варіантів ККР має забезпечити індивідуалізацію завдання.

Значення оцінки за виконання ККР визначається середньою оцінкою складових (конкретизованих завдань) і є остаточним.

Інтегральне значення оцінки виконання ККР може визначатися з урахуванням вагових коефіцієнтів, що встановлюється кафедрою для кожної складової опису кваліфікаційного рівня НРК.

6.3 Критерії

Реальні результати навчання студента ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерію використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$O_i = 100 a/m,$$

де a – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення; m – загальна кількість запитань або суттєвих операцій еталону.

Індивідуальні завдання та комплексні контрольні роботи оцінюються експертно за допомогою критеріїв, що характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.

Зміст критеріїв спирається на компетентнісні характеристики, визначені НРК для магістерського рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
Знання		
– спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне	Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: – спеціалізованих концептуальних знань на рівні новітніх досягнень; – критичне осмислення проблем у навчанні та/або професійній діяльності та на межі предметних галузей	95-100
	Відповідь містить не грубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
осмислення проблем у галузі та на межі галузей знань	Відповідь демонструє нечіткі уявлення студента про об'єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
Уміння/навички		
– спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур; – здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; – здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	Відповідь характеризує уміння: – виявляти проблеми; – формулювати гіпотези; – розв'язувати проблеми; – оновлювати знання; – інтегрувати знання; – провадити інноваційну діяльність; – провадити наукову діяльність	95-100
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності з не грубими помилками	90-94
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння/навички застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння/навички застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь/навичок незадовільний	<60
Комунікація		
– зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	Зрозумілість відповіді (доповіді). <i>Мова:</i> – правильна; – чиста; – ясна; – точна; – логічна; – виразна; – лаконічна.	95-100

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
	Комунікаційна стратегія: — послідовний і несуперечливий розвиток думки; — наявність логічних власних суджень; — доречна аргументації та її відповідність відстоюваним положенням; — правильна структура відповіді (доповіді); — правильність відповідей на запитання; — доречна техніка відповідей на запитання; — здатність робити висновки та формулювати пропозиції; — використання іноземних мов у професійній діяльності	
	Достатня зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія з незначними хибами	90-94
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
Рівень комунікації незадовільний		<60
Відповідальність і автономія		
— управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів; — відповідальність за внесок до професійних знань і практики та/або	Відмінне володіння компетенціями: — використання принципів та методів організації діяльності команди; — ефективний розподіл повноважень в структурі команди; — підтримка врівноважених стосунків з членами команди (відповідальність за взаємовідносини); — стресовитривалість; — саморегуляція; — трудова активність в екстремальних ситуаціях; — високий рівень особистого ставлення до справи; — володіння всіма видами навчальної діяльності;	95-100

	Вимоги до знань, умінь/навичок, комунікації, відповідальності і автономії	Показники оцінки
оцінювання результатів діяльності команд та колективів; – здатність продовжувати навчання з високим ступенем автономії	– належний рівень фундаментальних знань; – належний рівень сформованості загальнонавчальних умінь і навичок	
	Упевнене володіння компетенціями відповідальності і автономії з незначними хибами	90-94
	Добре володіння компетенціями відповідальності і автономії (не реалізовано дві вимоги)	85-89
	Добре володіння компетенціями відповідальності і автономії (не реалізовано три вимоги)	80-84
	Добре володіння компетенціями відповідальності і автономії (не реалізовано чотири вимоги)	74-79
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано п'ять вимог)	70-73
	Задовільне володіння компетенціями відповідальності і автономії (не реалізовано шість вимог)	65-69
	Задовільне володіння компетенціями відповідальності і автономії (рівень фрагментарний)	60-64
	Рівень відповідальності і автономії незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання:

– мультимедійне обладнання;

Під час проведення практичних занять використовується MS Excel та мова програмування Python.

Дистанційна платформа MOODLE, MS Teams.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Математичні основи криптографії: навч. посіб. / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я Фомичова – Д.: НГУ. 2004. – 391 с.
2. Математичні основи криптоаналізу навч. посіб. / С.О. Сушко, Г.В. Кузнецов, Л.Я Фомичова, А.В. Корабльов. – Д.: НГУ. 2010.
3. Криптологія у прикладах, тестах і задачах: навч. посіб. / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я Фомичова. – Д.: НГУ. 2013. – 318 с.
4. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с
5. A course in cryptography / Heiko Knospe. - American Mathematical Society, 2019. – 323 pp.

9. ІНФОРМАЦІЙНІ РЕСУРСИ

1. <https://do.nmu.org.ua/course/view.php?id=7271> - 113 - Математичні основи захисту даних – дистанційний курс.
2. <https://vm.nmu.org.ua/metod.html> - Література на сайті кафедри прикладної математики НТУ «Дніпровська політехніка»
3. <http://www.nbuv.gov.ua> – Національна бібліотека України імені В. І. Вернадського.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Математичні основи захисту даних»
для бакалаврів
спеціальності F1 «Прикладна математика»

Розробник:
Дмитро Володимирович Бабець

Підготовлено до виходу в світ
у Національному технічному університеті
«Дніпровська політехніка».
Свідоцтво про внесення до Державного реєстру ДК № 1842
49005, м. Дніпро, просп. Д. Яворницького, 19