МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ТРАНСПОРТНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
інформаційних систем і технологій
_____ проф. Гавриленко В.В.
«28» _____08_____ 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК9 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ТРАНСПОРТНОЇ ГАЛУЗІ

(шифр і назва навчальної дисципліни)

Лектор	**Аль Амморі Алі** (Прізвище, ім'я, по-батькові)
Рівень вищої освіти	**Третій (освітньо-науковий)** перший (бакалаврський) / другий (магістерський)/трейй(освітньо-науковий)
галузі знань	**12 «Інформаційні технології»** **(шифр і назва галузі знань)**
спеціальність	**122 «Комп'ютерні науки»** **(шифр і назва спеціальності)**
ОНП	**Комп'терні науки** (повна назва освітньо-професійної програми)
Освітня кваліфікація	**Доктор філософії з Комп'ютерних наук**
Тип дисципліни	**обов'язкова** (обов'язкова/вибіркова/факультативна)
форма навчання	**Денна, вечірня, заочна** **(денна, вечірня, заочна (дистанційна), екстернат)**
Мова викладання	**українська** (українська / англійська / німецька / російська)

2024 – 2025 н.р.

Робоча програма навчальної дисципліни «Методи та засоби захисту інформації на об'єктах транспортної галузі» для підготовки фахівців галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки», що навчаються за освітньою-науковою програмою Комп'ютерні науки для здобуття третього (освітньо-наукового) рівня вищої освіти.

РОЗРОБНИКИ ПРОГРАМИ:
зав.кафедри ІАДІБ, д.т.н., професор Аль-Амморі Алі
доцент каф. ІСТ, доктор філософії Лемешко А. В.

Робочу програму розглянуто та затверджено на засіданні кафедри інформаційних систем і технологій.
Протокол № 1 від «26» серпня 2024 року

ПОГОДЖЕНО на засіданні Вченої ради факультету транспортних та інформаційних технологій
Протокол № 1 від «27» серпня 2024 року

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти, ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 5</td><td>Галузь знань
12 «Інформаційні технології»</td><td>Тип дисципліни: обов’язкова</td></tr>
<tr><td rowspan="3">Кількість модулів – 2</td><td rowspan="5">Спеціальність:
122 «Комп’ютерні науки»</td><td>Рік підготовки</td></tr>
<tr><td>3-й</td></tr>
<tr><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td>5-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3 самостійної роботи студента
– 7</td><td rowspan="10">Третій (освітньо-науковий) рівень вищої освіти</td><td>15 год.</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>–</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>30 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>105 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>Екзамен</td></tr>
</table>

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної роботи і індивідуальної роботи становить (%): 43%.

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни «Методи та засоби захисту інформації на об’єктах транспортної галузі» полягає в ознайомленні PhD-студентів з теоретичними основами сучасних методів захисту інформації на об’єктах транспортної галузі.

Завдання навчальної дисципліни – отримання теоретичних знань про математичні засади криптографічних методів захисту інформації; набуття практичних навичок реалізації криптографічних алгоритмів та протоколів, ознайомлення з теоретичними основами та методами реалізації просунутих криптосистем з відкритим ключем.

В результаті вивчення дисципліни здобувач повинен

знати математичне підґрунтя, на якому побудовані сучасні методи захисту інформації; основні алгоритми, які використовуються в сучасній криптографії; теоретичні основи побудови криптосистем на еліптичних кривих; протоколи на основі ймовірнісного шифрування.

уміти реалізовувати алгоритми шифрування та криптографічні протоколи; оцінювати гарантії безпеки, які надають відомі криптосистеми, та проводити оцінку для нових криптографічних схем.

3. Компетентності

В результаті вивчення дисципліни «Методи та засоби захисту інформації на об’єктах транспортної галузі» здобувачі набувають наступних компетентностей. **Загальні компетентності**

ЗК1	Здатність до абстрактного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності

СК01	Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей.
СК02	Здатність застосовувати сучасні методології, .методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.

Фахові компетентності освітньо-наукової програми (ФКП)

ФКП02	Здатність застосовувати набуті уміння та навички професійної та наукової діяльності у сфері розвитку та впровадження інноваційних інформаційних технологій в інтегровані виробничі та транспортні системи.

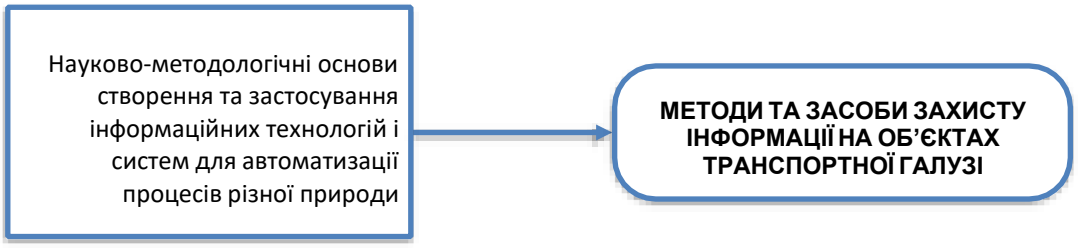
Результати навчання

РН04	Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямах.
РН05.	Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

Результати навчання освітньо-наукової програми

РНП02	Здатність застосовувати набуті уміння та навички професійної та наукової діяльності у сфері розвитку та впровадження інноваційних інформаційних технологій в інтегровані виробничі та транспортні системи.
РНП 03	Використовувати інноваційні інструменти і технології пошуку, оброблення та інтелектуального аналізу інформації в умовах неповної або обмеженої інформації при розробці розробки інформаційних транспортних систем

4. МІЖДИСЦИПЛІНАРНІ ЗВ'ЯЗКИ



5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни складається з таких модулів:

Модуль 1. Алгоритми теорії чисел та криптографії.

Тема 1. Арифметичні операції в скінченних полях. Функція Ойлера. Квадратичні лишки.

Тема 2. Алгоритми тестування простоти. Факторизація натуральних чисел. Первісні корені за простим модулем.

Тема 3. Ймовірнісні алгоритми. Порівняння складності задач. Ймовірнісне криптування.

Тема 4. Важкооборотні функції. Генератори псевдовипадкових бітів.

Модуль 2. Просунуті криптосистеми з відкритим ключем.

Тема 5. Еліптичні криві та криптосистеми на еліптичних кривих.

Тема 6. Протоколи на основі ймовірнісного криптування.

Тема 7. Криптосистема Рабина. Тема 8. Криптосистема Голдвассера-Мікалі.

1. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви модулів і тем лекцій	Кількість годин			
	денна форма			
	Всього	Лекції	Лабораторні	Самостійна робота
Модуль 1. Алгоритми теорії чисел та криптографія.				
1. Арифметичні операції в скінченних полях. Функція Ойлера. Квадратичні лишки.	**17**	2	3	12
2. Алгоритми тестування простоти. Факторизація натуральних чисел. Первісні корені за простим модулем.	**17**	2	3	12
Назви модулів і тем лекцій	Кількість годин			
	денна форма			
	Всього	Лекц ії	Лабораторні	Самостійна робота
3. Ймовірнісні алгоритми. Порівняння складності задач. Ймовірнісне криптування.	**24**	2	6	16
4. Важкооборотні функції. Генератори псевдовипадкових бітів.	**17**	2	3	12
Всього за модуль 1	**75**	8	15	52
Модуль 2. Просунуті криптосистеми з відкритим ключем.				
5. Еліптичні криві та криптосистеми на еліптичних кривих.	**23**	2	6	15
6. Протоколи на основі ймовірнісного криптування.	**20**	2	3	15
7. Криптосистема Рабина.	**20**	2	3	15

8. Криптосистема Голдвассера-Мікалі.	**12**	1	3	8
Всього за модуль 2	**75**	7	15	53
Всього за курс	**150**	**15**	**30**	**105**

2. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

На кожному лабораторному занятті до виконання лабораторної роботи студент має відповісти на контрольні питання, які відображають його готовність до виконання лабораторної роботи, зокрема оволодіння необхідними теоретичними знаннями та усвідомлення мети роботи. По закінченні виконання лабораторної роботи викладач оцінює ступінь оволодіння навичками та досягнення мети даної роботи.

Для здачі лабораторної роботи студенту необхідно оформити індивідуальний звіт, у якому повинна бути: постановка завдання, роздруковані основні результати роботи, аналіз розрахунків та чіткі висновки.

Підсумкові оцінки за виконання кожної лабораторної роботи вносяться у відповідний журнал. Отримані студентом оцінки за лабораторні роботи враховуються при виставленні підсумкової оцінки з даної навчальної дисципліни.

№	Назва теми	Кількість годин
1	Арифметичні операції в скінченних полях. Функція Ойлера. Квадратичні лишки.	3
2	Алгоритми тестування простоти. Факторизація натуральних чисел. Первісні корені за простим модулем.	3
3	Ймовірнісні алгоритми. Порівняння складності задач. Ймовірнісне криптування.	6
4	Важкооборотні функції. Генератори псевдовипадкових бітів.	3
5	Еліптичні криві та криптосистеми на еліптичних кривих.	6
6	Протоколи на основі ймовірнісного криптування.	3
7	Криптосистема Рабина.	3
8	Криптосистема Голдвассера-Мікалі.	3
РАЗОМ		30

3. САМОСТІЙНА РОБОТА

Для опанування матеріалу дисципліни «Методи та засоби захисту інформації на об’єктах транспортної галузі» окрім лекційних і лабораторних занять, тобто аудиторної роботи, значну увагу необхідно приділяти самостійній роботі.

Основні види самостійної роботи студента:

1. Вивчення додаткової літератури.
2. Підготовка до лабораторних занять.
3. Підготовка до проміжного та підсумкового контролю.

Розподіл годин самостійної роботи за темами

№ з/п	Назва теми	Кількість годин
1	Арифметичні операції в скінченних полях. Функція Ойлера. Квадратичні лишки.	12
2	Алгоритми тестування простоти. Факторизація натуральних чисел. Первісні корені за простим модулем.	12
3	Ймовірнісні алгоритми. Порівняння складності задач. Ймовірнісне криптування.	16
№ з/п	Назва теми	Кількість годин
4	Важкооборотні функції. Генератори псевдовипадкових бітів.	12
5	Еліптичні криві та криптосистеми на еліптичних кривих.	15
6	Протоколи на основі ймовірнісного криптування.	15
7	Просунуті криптосистеми (криптосистеми Рабина, криптосистема Голдвассера-Мікалі).	23
	Всього	**105**

4. Методи навчання

При вивченні «Методи та засоби захисту інформації на об’єктах транспортної галузі» застосовуються 3 групи методів навчання:

– методи організації і здійснення навчально-пізнавальної діяльності;

– методи стимулювання і мотивації навчально-пізнавальної діяльності;

– методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності.

Перша група охоплює вербальні методи передачі і сприймання навчальної інформації (розповідь, лекція); наочні (ілюстрація, презентація); практичні (вправи, групові та індивідуальні завдання). В межах самостійної роботи – робота з книгами, методичними матеріалами, інтернет-джерелами.

При вивченні курсу активно використовуються інтерактивні методи (при веденні лекцій та лабораторних занять) та проблемно-пошукові методи навчання (як при веденні аудиторних занять, так і при організації самостійної роботи студентів).

5. Методи контролю

Методи поточного контролю: поточне тестування, індивідуальне опитування, фронтальне опитування, перевірка домашніх завдань, перевірка індивідуальних завдань.

Методи модульного контролю: письмова контрольна робота, підсумкове тестування.

Методи підсумкового контролю: екзамен (письмова контрольна робота).

10. Розподіл балів

Поточне оцінювання модулів											Іспит	Сума
	Модуль 1					Модуль 2					40	100
	Т1	Т2	Т3	Т4	МК1	Т5	Т6	Т7	Т8	МК2		
Виконання лабораторних робіт	5	5	5	5	10	5	5	5	5	10		

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	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	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

«Відмінно» - A ***(90-100 балів)***–виставляється студенту, який глибоко та міцно засвоїв матеріал, відмінно справляється з задачами та питаннями, показує знайомство з фаховою літературою, володіє різносторонніми навичками та прийомами виконання практичних завдань, вміє добре орієнтуватись у виробничих ситуаціях.

«Добре» - BC ***(74-89 балів)***–виставляється студенту, який твердо знає програмний матеріал, правильно застосовує теоретичні знання при рішенні практичних завдань, володіє необхідними навичками та прийомами їх виконання.

«Задовільно» - DE ***(64-73балів)***–виставляється студенту, який має знання тільки основного матеріалу, але не засвоїв його деталей, допускає неточності,

неправильне тлумачення окремих елементів завдання та відчуває труднощі при виконанні практичних завдань.

«Незадовільно» - FX *(35-59 балів)* - виставляється студенту, який дає необґрунтованівідповіді на запитання, допускає суттєві помилки у використанні понятійного апарату. Не простежується логічність та послідовність думки. Формулювання хаотичні та не усвідомлені.

«Незадовільно» - F *(1-34 балів)* -виставляється студенту, який не засвоїв зміст дисципліни,вміння та навички не набуті.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. J. Katz, Ye. Lindell. Introduction to Modern Cryptography (2-nd ed.). — CRC Press, 2015.
2. N. Koblitz. Algebraic Aspects of Cryptography. — Vol. 3 — Springer, 2010.
3. N. Koblitz. A Course in Number Theory and Cryptography. — NY, Springer, 2011.
4. Вербіцький О. В. Вступ до криптографії. — Львів, ВНТЛ, 2018.

Додаткова література

1. D. Hankerson, A.J. Menezes, and S.A. Vanstone. Guide to Elliptic Curve Cryptography. — Springer, 2014.

5. D. R. Stinson, M. B. Paterson. Cryptography, Theory and Practice (4-th ed.). — CRC Press, 2019.