ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. І. ВЕРНАДСЬКОГО
Навчально-науковий інститут муніципального управління
та міського господарства
Кафедра комп'ютерних та інформаційних технологій

ЗАТВЕРДЖУЮ

Директор інституту

_____Володимир КИСЕЛЬОВ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КРИПТОЛОГІЇ

першого (бакалаврського) рівня вищої освіти

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітньо–професійна програма: «Комп'ютерні науки»

Форма здобуття освіти: очна (денна)

КИЇВ 2025

УКЛАДАЧ силабусу д.т.н., професор, професор кафедри комп'ютерних та інформаційних технологій

_____ Олександр СЄЛЮКОВ

(підпис)

Розглянуто та схвалено на засіданні кафедри комп'ютерних та інформаційних технологій

Протокол № 1 від 26.08.2025

Завідувач кафедри _____ Олександр ГУЙДА

(підпис)

Гарант освітньо-професійної програми «Комп'ютерні науки»

к.т.н., доцент _____ Сергій ЛІСОВЕЦЬ

(підпис)

1. Загальна інформація про навчальну дисципліну	
1.Назва навчальної дисципліни, код в ОПП	**ОСНОВИ КРИПТОЛОГІЇ** Код ОК 1.2.16
2.Статус навчальної дисципліни	Навчальні дисципліни професійної підготовки
3.Рік навчання, семестр у якому викладається дисципліна	4 рік навчання 7 семестр
4.Обсяг навчальної дисципліни (кількість кредитів, загальна кількість годин (аудиторних за видами занять, самостійної роботи здобувача вищої освіти)	4 кредитів загальна кількість годин: 120 год. аудиторних: лекцій: 14 год. практичні: 28 год. самостійна робота: 78 год.
5.Вид підсумкового (семестрового) контролю	екзамен (7 семестр)
6.Інформація про консультації	Протягом семестра згідно з графіком
7.Мова викладання	українська
8.Прізвище, ім’я, по батькові викладача (науковий ступінь, вчене звання, посада)	д.т.н.,професор Олександр СЄЛЮКОВ
9.Контактна інформація викладача	seliukov.oleksandr@tnu.edu.ua
10.Посилання на силабус на вебсайті Університету	http://tnu.edu.ua
2. Опис навчальної дисципліни	
Анотація дисципліни	Дисципліна “Основи криптології” є нормативною дисципліною зі спеціальності 122 – комп’ютерні науки для освітньої програми Комп’ютерні науки, яка викладається у 7-му семестрі в обсязі 4-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Мета, завдання та цілі вивчення дисципліни	Мета навчальної дисципліни “Основи криптології” – ознайомлення з основами математичної теорії криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.
Пререквізити	«Алгоритми та методи обчислень», «Системне програмування», «Паралельні та розподілені обчислення», «Комп’ютерна логіка», «Теорія інформації та кодування»
Постреквізити	«Переддипломна практика», «Дипломне проектування».

Формат проведення дисципліни	Змішаний; У разі роботи в дистанційному режимі використовується корпоративне середовище Google Classroom; Лекції та практичні у дистанційному режимі проводитимуться через Google Meet; поточна комунікація з викладачем здійснюється корпоративну пошту.

3. Результати навчання відповідно до освітньопрофесійної програми:

Загальні компетентності

ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК8. Здатність генерувати нові ідеї (креативність).
ЗК10. Здатність бути критичним і самокритичним.
ЗК11. Здатність розробляти й управляти проектами.
ЗК12. Здатність приймати обґрунтовані рішення.

Фахові компетентності

ФК3. Здатність до побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.

ФК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об'єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління.

Програмні результати навчання

ПРН5.Проектувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій.

ПРН13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення

4.Тематика та зміст навчальної дисципліни

Номер та назва розділу, теми, перелік основних питань	Вид навчального заняття	Форми і методи контролю знань	Кількість годин Лекція/ практичне заняття
Розділ 1. Основні поняття криптології			
Тема 1. Основні поняття криптології. Загроза інформації та можливості прихованої її передачі. Основні поняття стеганографії. Предмет криптологія.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4
Тема 2. Основні принципи криптології. Класифікація шифрів. Поняття абсолютно стійкого шифру.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4
Тема 3. Класичні шифри перестановки. Загальна характеристика шифрів перестановки. Звичайна перестановка. Звичайні рядково-стовпчикові табличні перестановки. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків. Рядково-стовпчикові табличні перестановки із застосуванням ключа рядків. Рядково-стовпчикові табличні перестановки з двома ключами. Табличні перестановки з використанням трафарету.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4
Розділ 2. Практичне шифрування			
Тема 4. Стандарти шифрування даних. Стандарт DES. Стандарт ДСТУ 28147-2006. Порівняння шифрів ДСТУ 28147-2006 і DES. Стандарт ISO/IEC 18033-1:2021.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4

Тема 5. ХЕШ-функція. Односторонні функції і функції з лазівками. Загальні поняття хеш-функцій. Вимоги до хеш-функцій. Криптографічні хеш-функції.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4
Тема 6. Ідентифікація і аутентифікація об'єкта. Ідентифікація, аутентифікація та авторизація об'єкта. Взаємна перевірка істинності сторін інформаційного обміну. Протоколи аутентифікації з нульовою передачею знань.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4
Тема 7. Електронний цифровий підпис. Атаки на ЕЦП. Алгоритми ЕЦП. Арбітраж ЕЦП.	Лекція/ практичне заняття	усне опитування/*розвязок задач за темою*	2/4

5.Інформація про індивідуальне завдання

Курс «Основи криптології» передбачає виконання індивідуальних завдань у вигляді самостійної роботи.

Провідна мета організації самостійної роботи полягає у необхідності широкого огляду тематики курсу з використанням основної та додаткової літератури, набуття навичок пошуку необхідної інформації, її аналітичного осмислення.

В процесі цієї роботи студенти повинні навчитися робити узагальнюючі висновки, оформляти результати роботи та планувати свою діяльність по вивченню дисципліни.

Контроль за самостійною роботою студентів – поточний контроль, тестування, контрольна робота.

Завдання контрольної роботи для студентів заочної форми навчання містять індивідуальні завдання для кожного студента.

Самостійна робота передбачає:

- підготовку до лекцій;
- підготовку до екзамену.

6.Технічне обладнання та програмне забезпечення

У звичайному режимі навчання вивчення навчальної дисципліни передбачає приєднання кожного здобувача до навчального середовища Google Classroom, оскільки там розміщуються навчальні матеріали, проводиться тестування, ведеться журнал оцінювання навчальних досягнень.

У режимі дистанційного навчання - вивчення курсу додатково передбачає приєднання кожного здобувача вищої освіти до програм Google Meet (для занять у режимі відеоконференцій).

Для комунікації та опитувань, виконання домашніх завдань, виконання завдань самостійної роботи, проходження тестування (поточний, підсумковий контроль) тощо, здобувачу пропонується самостійно потурбуватися про якість доступу до інтернету,

ноутбук або персональний комп'ютер, мобільний пристрій (телефон, планшет) з підключенням до Інтернет.

7. Політика дисципліни.

Політика щодо академічної доброчесності: списування під час тесту, іспиту заборонені.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності.

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу у Таврійському національному університет ім. В.І. Вернадського.

Політика щодо дедлайнів та перескладання: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (до -50% від можливої максимальної кількості балів за вид діяльності).

Перескладання тесту відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: відвідування занять є обов'язковим компонентом. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в онлайн-формі за погодженням.

8. Система оцінювання та вимоги

З дисципліни здобувач вищої освіти може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на екзамені.

Поточний контроль проводиться шляхом спілкування із здобувачем вищої освіти під час лекцій та консультацій та опитувань.

Результати поточного контролю за відповідний модуль оприлюднюються викладачем на наступному аудиторному занятті. Бали, які набрані здобувачем вищої освіти під час аудиторних занять, складають оцінку поточного контролю.

Семестровий контроль у вигляді екзамену проводиться під час сесії з трьома практичними завданнями(40 балів максимум). Оцінка за результатами вивчення дисципліни формується шляхом додавання підсумкових результатів поточного контролю до екзаменаційної оцінки. Взаємозв'язок між набраними балами і оцінкою наведено у розділі 8.1.

Приклади екзаменаційного білету знаходяться у пакеті документів на дисципліну.

У випадку, якщо здобувач вищої освіти протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані роботи або не набрав мінімально необхідну кількість балів (20), він не допускається до складання екзамену під час сесії, але має право ліквідувати академічну заборгованість.

Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється.

8.1.Шкала та схема формування підсумкової оцінки

Теми		Сума
Розділ 1	Розділ 2	**60** балів
30 балів	**30 балів**	
Підсумковий контроль		**40** балів
Максимальна сума балів		**100** балів

8.2 Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	відмінно	A	відмінне виконання
80-89	добре	B	вище середнього рівня
75-79	добре	C	загалом хороша робота
66-74	задовільно	D	непогано
60-65	задовільно	E	виконання відповідає мінімальним критеріям
30-59	незадовільно	FX	необхідне перескладання
0-29	незадовільно	F	необхідне повторне вивчення курсу

9. Рекомендована література

Основна

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
2. Бабенко Т.В. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В.Бабенко, Г.М.Гулак, С.О.Сушко, Л.Я.Фомичова. − Д.: Національний гірничий університет, 2013. − 318 с.
3. Блінцов В. С. Математичні основи криптології + CD : Навчальний посібник для студ. вищих навч. закл. / В. С. Блінцов, Ю. Л. Гальчевський. – Миколаїв : Національний ун-т кораблебудування ім. адмірала Макарова, 2006. – 232 с.
4. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
5. Богуш В. М. Криптографічні застосування елементарної теорії чисел : Навч. посібник / В. М. Богуш, В. А. Мухачов. – К. : Державний ун-т інформаційно комунікаційних технологій, 2006. – 126 с.
6. Болотов А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / Болотов А. А., Гашков С. Б., Фролов А. Б. – М.: КомКнига, 2006. – 280 с.
7. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук – Луцьк: Вежа Друк, 2014. – 164 с.

Допоміжна

1. Горбенко І. Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч.

посіб. для студ. Ч. 1. Криптографічний захист інформації / І. Д. Горбенко, Т. О. Гріненко. – Х. : Харк. нац. ун-т радіоелектрон., 2004. – 368 с.
2. Горбенко І. Д. Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків: Форт, 2013. – 880 с.
3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: Підручник / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.
4. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕ, 2016. – 636 с.
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07-2015. – К. :Мінекономрозвитку України, 2015.
6. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. − К. -Тернопіль: Підручники і посібники, 2007. – 272 с.
7. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
8. Корченко О. Г. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.