Інформація про вибіркову навчальну дисципліну
циклу професійної підготовки
для кафедрального каталогу вибіркових навчальних дисциплін
на 2026/2027 н. р.

Назва дисципліни	Математичні методи захисту інформації
Рівень вищої освіти	Бакалавр
Курс (рік) навчання	3
Семестр	5 або 6
Обсяг дисципліни у кредитах*	4 кредити ЄКТС
Мова викладання	українська
Передумови для вивчення дисципліни	немає
Кафедра, яка забезпечує викладання дисципліни	кафедра кібернетики і прикладної математики
Інформаційне забезпечення	Moodle
Форма проведення занять	лекції, лабораторні заняття
Форма семестрового контролю*	залік

Ключові результати навчання (знання, уміння та інші компетентності):
Критично осмислювати, вибирати та використовувати необхідний науковий, методичний і аналітичний інструментарій криптографії та захисту даних
Класифікувати задачі криптографії та захисту даних
Застосовувати математичні методи криптографії у відповідності до класу прикладної задачі, яка вирішується
Аналізувати отримані результати, оцінювати їхню адекватність та приймати рішення щодо їхнього впровадження

Короткий зміст дисципліни (що буде вивчатися, перелік тем):
Тема 1. Докомп’ютерний захист інформації.
Основні поняття криптографії. Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама.
Тема 2. Поняття про асиметричні методи.
Система шифрування RSA. Системи символьних обчислень. Ферма, Ейлер та Гаус. Проблеми теорії чисел. Теореми та доведення.
Тема 3. Фундаментальні алгоритми.
Алгоритми. Алгоритм ділення. Теорема ділення. Алгоритм Евкліда. Доведення коректності алгоритму Евкліда. Розширений алгоритм Евкліда.
Тема 4. Розкладання на множники.
Теорема про розкладання. Існування розкладання. Ефективність алгоритму розкладу методом проб. Алгоритм Ферма розкладання на множники. Доведення

коректності алгоритму Ферма. Одна фундаментальна властивість простих чисел. Єдиність розкладання.
Тема 5. Прості числа.
Поліноміальна формула. Експоненційні формули: числа Мерсенна. Експоненційні формули: числа Ферма. Прайморіальна формула. Нескінченність безлічі простих чисел. Решето Ератосфена.
Тема 6. Арифметика залишків.
Відношення еквівалентності. Порівняння. Арифметика лишків. Критерій подільності. Степені. Діофантові рівняння. Поділ за модулем n.
Тема 7. Індукція та Ферма.
Математична індукція. Теорема Ферма. Обчислення коренів.
Модуль 2.
Тема 8. Псевдопрості числа.
Числа Кармайкла. Тест Міллера. Тестування простоти та системи символьних обчислень.
Тема 9. Системи порівнянь.
Лінійні рівняння. Китайський алгоритм лишків: взаємно прості модулі. Китайський алгоритм лишків: загальний випадок.
Тема 10. Групи.
Визначення та приклади. Симетрії. Арифметичні групи. Підгрупи. Циклічні підгрупи. Теорема Лагранжа.
Тема 11. Мерсен і Ферма.
Числа Мерсенна Числа Ферма. Тест Люка-Лемера.
Тема 12. Тести на простоту та примітивні корені.
Тест Люка. Тест на простоту. Числа Кармайкла. Примітивні корені. Обчислення порядків.
Тема 13. Система шифрування RSA.
Шифрування та дешифрування. Обґрунтування. Надійність системи. Вибір простих. ЕЦП.