



Силабус навчальної дисципліни «Математичні основи криптології»

Спеціальність	F5 Кібербезпека та захист інформації
Освітня програма	Кібербезпека
Освітній рівень	Перший (бакалаврський) рівень вищої освіти
Статус дисципліни	Обов'язкова
Мова викладання та оцінювання	Українська
Курс / семестр	2 курс, 3 семестр
Кількість кредитів ЄКТС	4 кредитів
Розподіл за видами занять та годинами навчання	Лекції – 20 год. Лабораторні – 20 год. Практичні (семінарські) – 0 год. Самостійна робота – 80 год.
Форма підсумкового контролю	Залік
Кафедра	Кібербезпеки та інформаційних технологій, гол. корпус. 412 ауд, тел. +380577020674(додатковий 3-04), http://www.kafcbt.hneu.edu.ua
Викладач (-і)	Чугай Андрій Михайлович, д.т.н., ст.н.с.;
Контактна інформація викладача (-ів)	andrey.chugay@hneu.net
Дні занять	Лекція: згідно діючого розкладу занять Лабораторні: згідно діючого розкладу занять
Консультації	Дистанційні консультації в ZOOM, за домовленістю зі здобувачами, чат в ПНС

Мета навчальної дисципліни: формування у здобувачів вищої освіти системних знань з математичного апарату, що лежить в основі сучасних криптографічних алгоритмів та методів криптоаналізу, а також розвиток практичних навичок їх застосування для забезпечення інформаційної безпеки.

Ознайомити з фундаментальними математичними концепціями криптографії: теорією чисел, алгебраїчними структурами, складністю обчислень, ймовірнісними методами.

Структурно-логічна схема вивчення навчальної дисципліни

Пререквізити	Постреквізити
Вища математика	Основи криптографічного захисту
Програмування	

Зміст навчальної дисципліни

Змістовий модуль 1. Теоретичні основи криптології

Тема 1. Вступ до криптології.

Тема 2. Інформація та ентропія.

Тема 3. Оцінка трудомісткості криптографічного алгоритму.

Тема 4. Елементарні поняття теорії чисел.

Змістовий модуль 2. Теорія чисел та алгебраїчні структури

Тема 5. Важливі функції теорії чисел.

Тема 6. Теорія чисел. Конгруенції



Тема 7. Алгебраїчні структури.

Тема 8. Еліптичні криві.

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, , ПНС ХНЕУ ім.С.Кузнеця, ZOOM, MS Office

Форми та методи оцінювання

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів.

Підсумковий контроль включає семестровий контроль, який проводиться у формі диференційованого заліку.

Максимально можлива кількість балів за поточний контроль упродовж семестру для дисципліни форма контролю якої залік – 100 та мінімально можлива кількість балів – 60.

Поточний контроль включає наступні контрольні заходи: захист звітів з лабораторних робіт; поточні контрольні роботи; самостійна робота за темами.

Більш детальна інформація щодо системи оцінювання та накопичування балів з навчальної дисципліни наведена у робочому плані (технологічній карті) з навчальної дисципліни

Політики навчальної дисципліни

Викладання навчальної дисципліни ґрунтується на засадах академічної доброчесності. Порушеннями академічної доброчесності вважаються: академічний плагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання. За порушення академічної доброчесності здобувачі освіти притягуються до такої академічної відповідальності: повторне проходження оцінювання відповідного виду навчальної роботи.

Більш детальну інформацію щодо компетентностей, результатів навчання, методів навчання, форм оцінювання, самостійної роботи наведено у Робочій програмі навчальної дисципліни.