Силабус навчальної дисципліни

«Основи криптографічного захисту»

Спеціальність	*125 Кібербезпека та захист інформації*
Освітня програма	*Кібербезпека*
Освітній рівень	*Перший (бакалаврський)рівень вищої освіти*
Статус дисципліни	*Обов'язкова*
Мова викладання, навчання та оцінювання	*Українська*
Курс / семестр	*3 курс, 5 семестр*
Кількість кредитів ЄКТС	*5 кредитів*
Розподіл за видами занять та годинами навчання	*Лекції – 30 год.*
	Лабораторні –30 год.
	Практичні – 0 год.
	Самостійна робота – 90 год.
Форма підсумкового контролю	*Екзамен*
Кафедра	*Кафедра кібербезпеки та інформаційних технологій, гол.корпус, 412 ауд. тел. +380577020674 (додатковий 304). http://www.kafcbit.hneu.edu.ua*
Викладач (-і)	*Чугай Андрій Михайлович, д.т.н., проф.*
Контактна інформація викладача (-ів)	*Chugay.anrdiy@hneu.net*
Дні занять	*Лекція: згідно діючого розкладу* *Лабораторні: згідно діючого розкладу*
Консультації	*Дистанційні консультації в Zoom, за домовленістю зі здобувачами*

Мета навчальної дисципліни: формування системи професійних компетентностей (знань і практичних вмінь та навичок) з теоретичних основ криптології та суті інформаційних процесів в криптографічних системах, набуття навичок практичного використання, постановки і вирішенні задач шифрування та дешифрування інформації, зокрема, з застосуванням ПК.

Структурно-логічна схема вивчення навчальної дисципліни

Пререквізити	Постреквізити
Математичні основи криптології	Розробка захищених мобільних застосунків
Дискретна математика	Інформаційні системи та інтернет технології
Основи побудови та захисту сучасних операційних систем	Основи стеганографічного захисту інформації

Зміст навчальної дисципліни

Змістовий модуль 1. *Механізми захисту на основі симетричних та несиметричних алгоритмів*

Тема 1. Теоретичні основи захисту інформації

Тема 2. Протоколи автентичності. Цифровий підпис

Тема 3. Протоколи суворої автентифікації

Тема 4. Протоколи цілісності SSL, TLS

Тема 5. Система PGP

Тема 6. Основи технології PKI

Змістовий модуль 2. *Механізми захисту в умовах постквантового періоду*

Тема 7. Основи постквантової криптографії.

Тема 8. Вимоги до криптоалгоритмів постквантового періоду

Тема 9. Постквантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Гібридні системи захисту на збиткових кодах

Тема 10. Методики оцінки статистичних властивостей криптографічних алгоритмів

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, MS Office, ZOOM

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 екзамену.

Максимально можлива кількість балів за поточний контроль упродовж семестру для дисципліни, форма контролю якої екзамен – 60 та мінімально можлива кількість балів – 35. Максимально можлива кількість балів за екзамен – 40 та мінімально можлива кількість балів – 25.

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.