Силабус навчальної дисципліни
«Основи криптографічного захисту»

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	*3 курс, 4 семестр*
Кількість кредитів ЄКТС	*5 кредитів*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.* *Лабораторні – 26 год.* *Практичні (семінарські) – 0 год.* *Самостійна робота – 100 год.*
Форма підсумкового контролю	*Екзамен*
Кафедра	*Кібербезпеки та інформаційних технологій, гол. корпус. 412 ауд, тел. +380577020674(додатковий 3-04), http://www.kafcbit.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: сформувати у здобувачів вищої освіти системні знання про сучасні методи шифрування, хешування та інші криптографічні механізми, а також розвинути практичні навички їх застосування для захисту даних, оцінки стійкості криптосистем та аналізу потенційних загроз у сфері інформаційної безпеки.

Структурно-логічна схема вивчення навчальної дисципліни

Пререквізити	Постреквізити
Математичні основи криптографії	Основи стеганографічного захисту інформації
Програмування	

Зміст навчальної дисципліни

Змістовий модуль 1. *Історія розвитку криптографії. Класичні криптосистеми*
Тема 1. Основні поняття і визначення криптографії. Історія розвитку
Тема 2. Класифікація сучасних криптосистем та вимоги до них. Класичні криптосистеми.
Тема 3. Традиційні симетричні криптосистеми
Тема 4. Шифрування на методом складної заміни.

Змістовий модуль 2. *Сучасні принципи та стандарти шифрування даних*
Тема 5. Шифрування методом гамування Генерація псевдовипадкових чисел.
Тема 6. Криптоаналіз та криптоаналітичні атаки
Тема 7. Хеш-функції
Тема 8. Принципи побудови симетричних шифрів. Блокові шифри

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 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.