Силабус навчальної дисципліни

«Основи криптографічного захисту»

Спеціальність	*125 Кібербезпека*
Освітня програма	*Кібербезпека*
Освітній рівень	*Перший (бакалаврський) рівень вищої освіти*
Статус дисципліни	*Обов'язкова*
Мова викладання	*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.* *Самостійна робота – 90 год.*
Форма підсумкового контролю	*Залік*
Кафедра	*Кафедра кібербезпеки та інформаційних технологій, ауд. 412 головного корпусу, телефон: (057) 702-06-74, (дод. 3-04), сайт кафедри: http://www.kafcbit.hneu.edu.ua*
Викладач (-і)	*Шаповалова Олена Олександрівна, кандидат технічних наук, доцент*
Контактна інформація викладача (-ів)	*shap_el@ukr.net*
Дні занять	*Лекції: згідно діючого розкладу занять* *Лабораторні: згідно діючого розкладу занять*
Консультації	*На кафедрі кібербезпеки та інформаційних технологій, очні, відповідно до графіка консультацій, індивідуальні*

Мета навчальної дисципліни: *ознайомлення з основами математичної теорії криптології, а саме 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.*

Передумови для навчання

Перелік попередньо прослуханих дисциплін: *Вища математика, Математичні основи криптології*

Зміст навчальної дисципліни

Змістовий модуль 1. *Традиційне шифрування*

Тема 1. *Вступ до криптографічних методів захисту. Модель захисту мережі.*

Тема 2. *Традиційне шифрування: класичні методи. Криптографія, криптоаналіз, стеганографія.*

Тема 3. *Традиційне шифрування: сучасні методи. Спрощений DES. Принципи блочного шифрування. Потокові і блокові шифри.*

Тема 4. *Диференціальний і лінійний криптоаналіз.*

Тема 5. *Традиційне шифрування: алгоритми.*

Тема 6. *Традиційне шифрування і конфіденційність. Канальне і наскрізне шифрування.*

Тема 7. *Розподіл ключів. Сценарії. Управління ієрархією ключів.*

Тема 8. *Генерування випадкових чисел.*

Змістовий модуль 2. *Сучасні методи шифрування*

Тема 9. *Криптографія з відкритим ключем.*

Тема 10. *Алгоритм RSA. Опис алгоритму. Обчислювальні аспекти. Захищеність алгоритму RSA.*

Тема 11. *Управління ключами. Розподіл секретних ключів за допомогою системи з*

відкритим ключем. Обмін ключами за схемою Діффі-Хеллмана.
Тема 12. *Криптографія з використанням еліптичних кривих.*
Тема 13. *Введення в теорію чисел. Прості і взаємно прості числа.*
Тема 14. *Функції хешування. Криптоаналіз. Математичне обгрунтування атак.*
Тема 15. *Алгоритми хешування. Алгоритм MD5 обчислення профілю повідомлення.*
Тема 16. *Цифрові підписи і протоколи аутентифікації.*

Матеріально-технічне (програмне) забезпечення дисципліни

Internet, MS Office, мультимедійний проектор

Сторінка курсу на платформі Moodle (персональна навчальна система)	*https://pns.hneu.edu.ua/course/view.php?id=8607*

Система оцінювання результатів навчання

Система оцінювання сформованих компетентностей враховує види занять, які передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Поточний контроль, що здійснюється протягом семестру під час проведення лабораторних занять та самостійної роботи, оцінюється сумою набраних балів. Максимально можлива кількість балів за поточний та підсумковий контроль упродовж семестру – 100 та мінімально можлива кількість балів – 60.

Більш детальна інформація щодо 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 (https://pns.hneu.edu.ua/course/view.php?id=8607).

Силабус затверджено на засіданні кафедри «03» червня 2022 року. Протокол № 16