Силабус навчальної дисципліни

«Теоретичні основи криптографії»

Спеціальність	*125 Кібербезпека*
Освітня програма	*Кібербезпека*
Освітній рівень	*Перший (бакалаврський) рівень вищої освіти*
Статус дисципліни	*Обов'язкова*
Мова викладання	*Українська*
Курс / семестр	*2 курс, 4 семестр*
Кількість кредитів ЄКТС	*5 кредитів*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.* *Лабораторні – 24 год.* *Самостійна робота – 102 год.*
Форма підсумкового контролю	*Іспит*
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 теоретичними основами криптології, 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: *Вступ до фаху, Основи програмування*

Зміст навчальної дисципліни

Змістовий модуль 1. *Види криптографічних перетворень інформації. Сучасні симетричні криптографічні системи*

Тема 1. *Основні поняття і визначення криптографії. Принципи криптографічного захисту інформації. Історія розвитку криптографії.*

Тема 2. *Шифрувальні криптографічні перетворення. Односторонні функції. Хеш- функції. Електронний цифровий підпис. Генератори псевдовипадкових послідовностей.*

Тема 3. *Шифри перестановки. Шифри заміни (підстановки). Шифри гамування.*

Тема 4. *Композиційні блокові шифри і принципи їх побудови.*

Тема 5. *Криптоаналіз і види криптоаналітичних атак.*

Тема 6. *Стандарт шифрування даних DES. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Стандарт шифрування США нового покоління (AES).*

Змістовий модуль 2. *Криптографічні системи з відкритим ключем*

Тема 7. *Алгоритми шифрування з відкритим ключем.*

Тема 8. *Криптосистема шифрування RSA. Алгоритм цифрового підпису RSA.*

Тема 9. *Криптосистема Діффі-Хеллмана. Криптосистема Ель Гамаля. Алгоритм цифрового підпису Ель Гамаля (EGSA).*

Тема 10. *Криптосистема на основі еліптичних кривих.*

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=8567*

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 контроль упродовж семестру – 60 та підсумковий (іспит) – 40 балів, мінімально можлива кількість балів за поточний контроль – 35 та підсумковий (іспит) – 25 балів.

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=8567).

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