Харківський національний економічний університет імені Семена Кузнеця

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	*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	*Екзамен*
Кафедра	*Кафедра кібербезпеки та інформаційних технологій, гол.корпус, 412 ауд. тел. +380577020674 (додатковий 304).* *http://www.kafcbit.hneu.edu.ua*
Викладач (-і)	*Шаповалова Олена Олександрівна, к.т.н., доц.*
Контактна інформація викладача (-ів)	*shap_el@ukr.net*
Дні занять	*Відповідно до розкладу занять* *Лекція:* *http://rozklad.hneu.edu.ua/schedule/schedule?employee=425947&week=39* *Лабораторні:* *http://rozklad.hneu.edu.ua/schedule/schedule?employee=425947&week=39*
Консультації	*відповідно до графіку*

Мета навчальної дисципліни " Основи криптографічного захисту " є 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, 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)	Посилання: https://pns.hneu.edu.ua/course/view.php?id=8607

Система оцінювання результатів навчання

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Більш детальна інформація щодо оцінювання наведена в технологічній карті дисципліни.

Політики навчальної дисципліни

Політика дотримання академічної доброчесності,

Політика щодо пропусків занять,

Політика щодо виконання завдань пізніше встановленого терміну, тощо

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

Силабус затверджено на засіданні кафедри «17» березня 2023 р. Протокол № 13