Харківський національний економічний університет імені Семена Кузнеця

Силабус навчальної дисципліни
«Математичні основи криптології»

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, 3 семестр*
Кількість кредитів ЄКТС	*4 кредити*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.* *Практичні (семінарські) – 0.* *Лабораторні – 24 год.* *Самостійна робота – 72 год.*
Форма підсумкового контролю	*Залік*
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 " Математичні основи криптології" є навчання студентів основам математичної теорії 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:

Вища математика

Зміст навчальної дисципліни

Змістовій модуль 1. *Традиційне шифрування*

Тема 1. Вступ.

Тема 2. Модульна арифметика.

Тема 3. Матриці.

Тема 4. Традиційні шифри з симетричним ключем

Тема 5. Алгебраїчні структури.

Тема 6. Сучасні блокові шифри.

Тема 7. DES

Змістовій модуль 2. *Сучасні методи шифрування*

Тема 8. Перетворення.

Тема 9. Розширення ключів.

Тема 10. Застосування сучасних блокових шифрів. Тема 11. Прості числа.

Тема 12. Квадратичне порівняння за модулем. Тема 13. Криптографічна система RSA.

Тема 14. Криптосистема Рабина.

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=8608

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.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням 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 «Математичні основи криптології» (посилання).

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