Силабус навчальної дисципліни
«*ТЕОРЕТИЧНІ ОСНОВИ КРИПТОГРАФІЇ*»

Спеціальність	*125 Кібербезпека*
Освітня програма	*Кібербезпека*
Освітній рівень	*Бакалавр*
Статус дисципліни	*Обов'язкова*
Мова викладання	*Українська*
Курс / семестр	*3 курс, 5 семестр*
Кількість кредитів ЄКТС	*5*
Розподіл за видами занять та годинами навчання	*Лекції – 24 год.*
	Практичні (семінарські) – немає
	Лабораторні – 24 год.
	Самостійна робота – 102 год.
Форма підсумкового контролю	*Екзамен*
Кафедра	*Кібербезпеки та інформаційних технологій, м. Харків, пр-т Науки 9-А, 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Викладач (-і)	*Мілов Олександр Володимирович, д.т.н., проф.*
Контактна інформація викладача (-ів)	*oleksandr.milov@hneu.net*
Дні занять	*Згідно діючого розкладу занять*
Консультації	*Відповідно до графіку*

Мета навчальної дисципліни "Теоретичні основи криптографії" – є 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

Вступ до фаху, Основи програмування

Зміст навчальної дисципліни

Змістовій модуль 1. Традиційне шифрування

Тема 1. Вступ до криптології.
Тема 2. Модульна арифметика.
Тема 3. Матриці.
Тема 4. Традиційні шифри з симетричним ключем
Тема 5. Алгебраїчні структури.
Тема 6. Сучасні блокові шифри.

Змістовій модуль 2. Сучасні методи шифрування

Тема 7. Перетворення.
Тема 8. Застосування сучасних блокових шифрів.
Тема 9. Прості числа.
Тема 10. Квадратичне порівняння з модулем.
Тема 11. Криптографічна система RSA.
Тема 12. Криптосистема Рабина.

Матеріально-технічне (програмне) забезпечення дисципліни *Internet, MS Office*	
Сторінка курсу на платформі Moodle (персональна навчальна система) Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Теоретичні основи криптографії»	*https://pns.hneu.edu.ua/enrol/index.php?id=5733*

Система оцінювання результатів навчання

Оцінювання результатів навчання здійснюється за накопичувальною 100-бальною системою. Мінімально кількість балів за поточний контроль упродовж семестру, яка дозволяє студенту складати екзамен, – 35, максимальна – 60. Підсумковий контроль проводиться у формі семестрового екзамену. Мінімальний бал, що дозволяє успішно скласти екзамен, – 25, максимальний – 40. Підсумкова кількість балів з навчальної дисципліни визначається як проста сума балів за результатами успішності студента (максимум – 100 балів).

Накопичування рейтингових балів з навчальної дисципліни *(приклад)*

Види навчальної роботи	**Мах кількість балів**
Лекційні заняття	**12**
Виконання лабораторних робіт	**30**
Поточні КР	**18**
Екзамен	**40**
Максимальна кількість балів	**100**

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 «Теоретичні основи криптографії», http://www.repository.hneu.edu.ua/handle/123456789/24649.

Силабус затверджено на засіданні кафедри «11» червня 2021 р. Протокол № 17