Рівненський державний гуманітарний університет
факультет математики та інформатики
Кафедра інформаційних технологій та моделювання

АНОТАЦІЯ

Назва дисципліни / освітнього компонента	ВК 29 Криптологія
Освітня програма	Прикладна математика
Компонент освітньої програми	Вибірковий
Загальна кількість кредитів та кількість годин для вивчення дисципліни	3 кредити / 90 годин
Вид підсумкового контролю з	залік
Мова викладання	українська
Викладач	кандидат юридичних наук, доцент кафедри Інформаційно-комунікаційних технологій та методики викладання інформатики Кіндрат Павло Вадимович
CV викладача на сайті кафедри	https://iktmvi.rshu.edu.ua/pro-kafedru/teachers/teacher/kindrat-pavlo-vadymovych.html
E-mail викладача	pavlo.kindrat@rshu.edu.ua

Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Криптологія» є:

- ознайомлення з теорію криптографічного захисту інформації, її історичними та сучасними викликами, програмними та апаратними засобами реалізації;
- дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів симетричного та асиметричного шифрування для забезпечення автентичності, цілісності та конфіденційності інформаційних систем;
- вивчення методів аналізу шифрованих повідомлень та алгоритмів їх шифрування з метою виявлення та усунення вразливостей при застосуванні криптографічного захисту інформації.

Основними **завданнями** вивчення дисципліни «Криптологія» є ознайомлення студентів з основними поняттями та положеннями криптографічного захисту інформації, вивчення ними основних методів збереження конфіденційності та цілісності інформації.

Успішно пройшовши та засвоївши матеріали навчальної дисципліни «Криптологія» студенти отримають уміння обґрунтовано обирати та реалізовувати алгоритми і засоби крипторгафічоного захисту інформації що застосовуються як в програмному так і в апаратному забезпечені інформаційних систем. А також, застосовуючи методи криптоаналізу, виявляти та усувати вразливості інформації. Це дозволить суттєво підвищити захищеність як оброблюваної студентами інформації так і розроблюваними ними інформаційних систем вціому.

У результаті освоєння курсу навчальної дисципліни «Криптологія» у здобувачів вищої освіти мають сформуватися визначені нижче компетентності, а також здобувачі отримають наступні програмні результати навчання (згідно з освітньо-професійною програмою):

Зміст навчальної дисципліни

Змістовий модуль 1. Криптографія

Тема 1. Криптографія як наукова та прикладна галузь.

Тема 2. Симетричні шифри

Тема 3. Асиметричні шифри

Тема 4. Апаратні засоби криптографії

Тема 5. Сучасні тенденції розвитку криптографії

Змістовий модуль 2. Криптоаналіз

Тема 6. Основи криптоаналізу

Тема 7. Криптоаналіз класичних алгоритмів шифрування

Тема 8. Сучасні методи криптоаналізу