



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Основи криптології»

Компонента освітньої програми – вибіркова (3 кредитів)

Освітньо-професійна програма	Математика
Спеціальність	111 Математика
Галузь знань	11 Математика і статистика
Рівень вищої освіти	Перший (бакалаврський)
Мова навчання	українська
Профайл викладача (-ів)	Карлова Олена Олексіївна, доктор фіз.-мат. наук, професор кафедри математичного аналізу https://scholar.google.com/citations?user=0Qly_uMAAAAJ&hl=uk
Контактний тел.	+380509860336
E-mail:	o.karlova@chnu.edu.ua
Сторінка курсу в Moodle	
Консультації	За домовленістю

АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс знайомить студентів з математичними основами теорії шифрування, історією розвитку криптографії включно із сучасними тенденціями, основними алгоритмами шифрування, хешування та цифрового підпису, криптографічними протоколами обміну інформацією, методами криптоаналізу, сучасними тенденціями в криптографії.

Метою навчальної дисципліни є виклад базових принципів захисту інформації з допомогою криптографічних методів та приклади реалізації цих методів на практиці.

НАВЧАЛЬНИЙ КОНТЕНТ ОСВІТНЬОЇ КОМПОНЕНТИ

МОДУЛЬ 1. КЛАСИЧНІ ШИФРИ	
Тема 1	Класичні шифри
Тема 2	Шифри Вернама та Гілла
Тема 3	Системи числення та шифр одноразового записника
Тема 4	Складність алгоритмів
МОДУЛЬ 2. ТЕОРЕТИКО-ЧИСЛОВІ АЛГОРИТМИ	
Тема 5	Конгруенції. Теореми Ейлера, Ферма та Вільсона
Тема 6	Алгоритми факторизації
Тема 7	Тестування простоти
МОДУЛЬ 3. АСИМЕТРИЧНІ КРИПТОСИСТЕМИ	
Тема 8	Криптосистеми з відкритим ключем
Тема 9	Криптографічні протоколи
Тема 10	Генерація випадкових чисел. Дискретні логарифми

ФОРМИ, МЕТОДИ ТА ОСВІТНІ ТЕХНОЛОГІЇ НАВЧАННЯ

Вивчення навчальної дисципліни проводиться у вигляді лекційних і практичних занять.

ФОРМИ Й МЕТОДИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ

Поточний контроль: письмові (тестування, самостійні роботи, модульні контрольні роботи) та усні: відповідь студента та ін.

Підсумковий контроль – *екзамен*.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання програмних результатів навчання здобувачів освіти здійснюється за шкалою європейської кредитно-трансферної системи (ECTS).

Критерієм успішного оцінювання є досягнення здобувачем вищої освіти мінімальних порогових рівнів (балів) за кожним запланованим результатом навчання.

ПОЛІТИКА ЩОДО АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні навчальної дисципліни регламентовано такими документами:

- ✓ «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича» <https://www.chnu.edu.ua/media/jxpbs0zb/etychnyi-kodeks-chernivetsko-ho-natsionalnoho-universytetu.pdf>
- ✓ «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університету імені Юрія Федьковича» <https://www.chnu.edu.ua/media/n5nbzwgb/polozhennia-chnu-pro-plahi-at-2023plusdodatky-31102023.pdf>

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Офіційний сайт факультету прикладної математики Чернівецького національного університету імені Юрія Федьковича <http://fmi.org.ua/>
2. Сайт наукової бібліотеки Чернівецького національного університету імені Юрія Федьковича <http://www.library.chnu.edu.ua/>
3. Віртуальна математична бібліотека <http://euclid.math.fsu.edu/Science/math.html>

Детальна інформація щодо вивчення курсу «Основи криптології» висвітлена у робочій програмі навчальної дисципліни

https://backend.chnu.edu.ua/media/hwqbw2u/rp_kryptolohiia.pdf