Код та назва дисципліни українською мовою/ Назва дисципліни англійською мовою	1-ф09-2 Криптографія в сучасних комп'ютерних технологіях / Cryptography in Modern Computer Technologies
Рекомендується для галузі знань *(спеціальності, освітньої програми)*	F – Інформаційні технології
Кафедра (*зазначати повну назву кафедри*)	Електронних обчислювальних машин
П.І.П. НПП *(за можливості)*	доцент, к.т.н. Спірінцева Ольга Володимирівна
Рівень ВО	перший (бакалаврський)
Курс, семестр *(в якому буде викладатись)*	2-4 курс
Мова викладання	Українська
Пререквізити (передумови вивчення дисципліни)	Не передбачено
Чому це цікаво/треба вивчати	Криптографічні методи є основою сучасної кібербезпеки та застосовуються для забезпечення конфіденційності, цілісності, автентичності й доступності даних у комп'ютерних системах і мережах. Вивчення дисципліни дозволяє здобувачам освіти опанувати принципи побудови та використання алгоритмів шифрування, дешифрування, тестування та зламу шифрів, за допомогою яких безпечно пересилаються повідомлення. Під час опанування курсу здобувачі освіти, використовуючи сучасні мови програмування, зокрема Python, набувають практичного досвіду реалізації криптографічних алгоритмів, тестування захищених систем, аналізу вразливостей та оцінювання стійкості методів захисту. Засвоєння дисципліни сприяє формуванню компетентностей, необхідних для проєктування безпечних комп'ютерних систем, захисту даних користувачів і ресурсів організацій, а також є актуальним для подальшої професійної діяльності у сфері комп'ютерної інженерії, інформаційної безпеки, телекомунікацій та високотехнологічних підприємств.
Перелік тем з дисциплін	• Інструменти «паперової» криптографії • Зворотний шифр • Шифр Цезаря • Злам шифру Цезаря методом грубої сили • Шифрування за допомогою перестановочного шифру • Дешифрування перестановочного шифру

	• Написання тестів • Шифрування та дешифрування файлів • Програмне розпізнавання англійських слів • Злам перестановочного шифру • Афінне шифрування за допомогою модульної арифметики • Злам афінного шифру • Частотний аналіз • Генерування простих чисел
Як можна користуватися набутими знаннями і уміннями *(компетентності)*	• Формування системи компетентностей щодо застосування криптографічних методів у сучасних комп'ютерних технологіях. • Формування комплексного теоретичного уявлення про принципи побудови, функціонування та використання криптографічних систем захисту інформації. • Ознайомлення з основними підходами до реалізації криптографічних алгоритмів засобами сучасних мов програмування, зокрема Python. • Опанування теоретико-понятійної бази курсу у сфері криптографії, кібербезпеки та захисту даних. • Розвиток навичок аналітичного мислення для практичної розробки та оцінювання криптографічних алгоритмів. • Ознайомлення із сучасними практиками та інструментальними засобами у галузі криптографії, криптоаналізу та інформаційної безпеки. • Розуміння принципів тестування, перевірки надійності та оцінювання стійкості криптографічних засобів захисту інформації.
Очікувані результати навчання	• Знати і розуміти наукові і математичні положення, що лежать в основі функціонування сучасних криптографічних алгоритмів. • Мати практичні навички розробки власних криптографічних рішень та шифрів із використанням мови програмування Python. • Уміти застосовувати набуті знання для виявлення, формалізації та розв'язування інженерних задач шифрування, дешифрування, криптоаналізу та тестування криптосистем.

	• Уміти ідентифікувати, класифікувати та описувати принципи роботи криптографічних алгоритмів, модулів і їхніх компонентів. • Уміти інтегрувати теоретичні знання з практичними навичками, приймати обґрунтовані технічні рішення та формувати стратегії розв'язання задач криптографії з урахуванням вимог інформаційної безпеки, суспільних та професійних інтересів.
Інформаційне забезпечення	Методичний посібник для лабораторних робіт Комплект презентацій
Види навчальних занять *(лекції, практичні, семінарські, лабораторні заняття тощо)*	Лекції (28 год), лабораторні заняття (28 год)
Вид семестрового контролю	диф. залік
Максимальна кількість здобувачів на семестр/ Мінімальна кількість здобувачів *(тільки для мовних, творчих дисциплін, за необхідності)*	Без обмежень

Декан факультету _____ *Ігор ГОМІЛКО*