Код та назва дисципліни українською мовою/ Назва дисципліни англійською мовою	1-ф09-2 - Криптографія та злам шифрів / Cryptography and code cracking
Рекомендується для галузі знань *(спеціальності, освітньої програми)*	Для спеціальностей усіх галузей знань
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	Криптографія є основою сучасної кібербезпеки та захисту даних у цифровому світі. Знання з криптографії дозволяють забезпечити конфіденційність, цілісність та справжність інформації, а також грають важливу роль в роботі цифрових технологій, забезпечуючи безпеку транзакцій та захист від зламу. Криптографія є важливим інструментом для захисту особистих даних, фінансових операцій та інших чуттєвих відомостей, зокрема запобігає шахрайству в електронній комерції, дозволяє підтвердити особистість та захистити анонімність користувача. Під час опанування даного курсу здобувач освіти, використовуючи сучасну мову програмування Python, опановує практичні кейси з розробки, тестування та зламу шифрів, за допомогою яких пересилаються повідомлення. Засвоївши цей курс, здобувач освіти набуває навичок створення власних криптографічних систем. Набуті знання з криптографії є актуальними та затребувані в умовах сьогодення у фінансових установах, технологічних компаніях та урядових організаціях.
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 компетенцій щодо цифрових технологій в криптографії.

	• Формування комплексного теоретичного уявлення про принципи та підходи щодо програмування мовою Python. • Ознайомлення із парадигмою структурного програмування. • Опанування теоретико-понятійної бази курсу. • Розвиток навичок аналітичного мислення для практичної розробки криптографічних алгоритмів та аналізу структур даних. • Ознайомлення з сучасними практиками та інструментальними засобами щодо основ криптографії та криптоаналітики. • Розуміння принципів тестування розроблених шифрів.
Очікувані результати навчання	• Знати і розуміти наукові і математичні положення, що лежать в основі функціонування криптографічних алгоритмів. • Мати навички створення власних криптографічних шифрів засобами мови Python. • Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач шифрування, дешифрування, зламу та тестування шифрів, використовуючи методи криптографії та криптоаналітики. • Вміти ідентифікувати, класифікувати та описувати роботу криптографічних модулів та їх компонентів. • Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань курсу з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих 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*