

Код та назва дисципліни українською мовою/ Назва дисципліни англійською мовою	2-ф09-5 Захист інформації / Information protection
Рекомендується для галузі знань (спеціальності, освітньої програми)	F3 Комп'ютерні науки, F7 Комп'ютерна інженерія
Кафедра (зазначати повну назву кафедри)	Кафедра комп'ютерних наук та інформаційних технологій
П.І.П. НПП (за можливості)	
Рівень ВО	2-ий (магістерський)
Курс, семестр (в якому буде викладатись)	1-ий курс, 1-ий або 2-ий семестр
Мова викладання	Українська
Пререквізити (передумови вивчення дисципліни)	Перший (бакалаврський) рівень вищої освіти з відповідної спеціальності. Алгоритмізація та програмування, об'єктно-орієнтоване програмування, операційні системи, системне програмування, архітектура комп'ютера.
Чому це цікаво/треба вивчати	Захист інформації від різноманітних загроз є невід'ємною частиною функціонування різних компаній, організацій та підприємств, а також життя кожної людини.
Перелік тем з дисциплін	1. Різні види загроз інформації. 2. Криптографічні методи захисту інформації. 3. Криптографія та криптоаналіз. Основні поняття. 4. Парольний захист. Створення безпечних паролів. 5. Найпростіші алгоритми шифрування. 6. Блочні алгоритми шифрування. Мережа Фейштеля. 7. Алгоритм блочного шифрування AES. 8. Системи з відкритим ключем. RSA. Система Ель-Гамала. 9. Поточкові шифри. 10. Функції хешування та області їх застосування. 11. ЕЦП. 12. Адміністративні методи захисту. 13. Резервне копіювання та його використання в сучасних СКБД. 14. Апаратні засоби підвищення надійності зберігання інформації. RAID.
Як можна користуватися набутими знаннями і уміннями (компетентності)	ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.
Очікувані результати навчання	Навчитися ефективно використовувати парольний захист, за необхідності обирати та використовувати відповідні алгоритми шифрування, виконувати резервне копіювання даних, включаючи БД, а також застосовувати апаратні рішення для підвищення надійності збереження інформації.
Інформаційне забезпечення	Методичні вказівки до виконання лабораторних робіт
Види навчальних занять (лекції, практичні, семінарські, лабораторні заняття тощо)	лекції, лабораторні заняття
Вид семестрового контролю	Диференційований залік
Максимальна кількість здобувачів на семестр/ Мінімальна кількість здобувачів (тільки для мовних, творчих дисциплін, за необхідності)	Без обмежень