Дисципліна	КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІС
Кафедра	Інформаційних та комунікаційних технологій
Рівень ВО	Другий (магістерський)
Мета	Формування у здобувачів вищої освіти поглиблених теоретичних знань та практичних навичок щодо застосування математичних методів перетворення інформації з метою забезпечення її конфіденційності, цілісності та автентичності. Дисципліна спрямована на вивчення сучасних криптографічних протоколів, побудову інфраструктури відкритих ключів (PKI), захист каналів зв'язку та впровадження стандартів криптографічного захисту в корпоративних інформаційних системах.
Зміст (теми) дисципліни	**Тема 1. Теоретичні основи криптології та класичні алгоритми** Історія та еволюція криптографії. Математичні засади: теорія чисел, скінченні поля, модульна арифметика. Класифікація криптосистем та основні вимоги до стійкості. **Тема 2. Симетричні методи шифрування** Блокові та потокові шифри. Алгоритми DES, 3DES, AES. Режими роботи блокових шифрів (ECB, CBC, GCM). Генерація та розподіл симетричних ключів. **Тема 3. Асиметрична криптографія та керування ключами** Криптосистеми з відкритим ключем: RSA, ElGamal, криптографія на еліптичних кривих (ECC). Алгоритм Діффі-Гелмана. Стійкість до атак на основі факторизації та дискретного логарифмування. **Тема 4. Цілісність даних та електронний підпис** Хеш-функції (MD5, SHA-2, SHA-3) та їх властивості. Алгоритми цифрового підпису (DSA, ECDSA). Забезпечення неспростовності (non-repudiation) та автентифікація повідомлень (MAC). **Тема 5. Інфраструктура відкритих ключів (PKI) та сертифікати** Стандарт X.509. Центри сертифікації (CA), реєстрації та відкликання сертифікатів. Життєвий цикл цифрових сертифікатів. Довірчі моделі в ієрархічних та мережевих структурах. **Тема 6. Криптографічні протоколи та захист мережевої взаємодії** Протоколи TLS/SSL, IPsec, SSH. Криптографічний захист у бездротових мережах. Засади квантової криптографії та постквантові алгоритми шифрування.