

Дисципліна	КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
Кафедра	Комп'ютерних наук та інженерії програмного забезпечення
Рівень ВО	Перший (бакалаврський)
Мета	формування у здобувачів вищої освіти знань в області криптографічних методів захисту інформації, а також умінь щодо застосування криптографічних систем захисту інформації для розв'язання задач професійної діяльності.
Зміст (теми) дисципліни	Тема 1. Математичні основи криптографії. Тема 2. Основні поняття криптографії. Тема 3. Стандарт шифрування даних DES. Тема 4. Сучасні блочні шифри. Тема 5. Генератори послідовностей і потокові шифри. Тема 6. Однонапрямлені хеш-функції. Тема 7. Алгоритми з відкритими ключами. Тема 8. Алгоритми цифрового підпису з відкритим ключем. Тема 9. Схеми ідентифікації. Тема 10. Алгоритми обміну ключами.