ПРЕЗЕНТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СУЧАСНА КРИПТОГРАФІЯ

Викладач: кандидат фізико-математичних наук, доцент, Зіновєєв Ігор Валерійович
Кафедра: Загальної математики, І корпус, ауд. 21а
E-mail: zinoveev@znu.edu.ua
Телефон: (061) 289-12-54
Інші засоби зв'язку: Moodle (форум курсу, приватні повідомлення)

Освітня програма, рівень вищої освіти:		Інженерія програмного забезпечення, Магістр					
Статус дисципліни:		Вибіркова					
Кредити ECTS	4	**Навч. рік:**	2024-25 1 семестр	**Рік навчання**	2	**Тижні**	12
Кількість годин	120	**Кількість змістових модулів**	6	**Лекційні заняття – 12** **Лабораторні заняття – 22** **Самостійна робота – 86**			
Вид контролю:		Залік					
Посилання на курс в Moodle			https://moodle.znu.edu.ua/course/view.php?id=97				
Консультації: час консультація за розкладом консультацій (розміщено на веб-сторінках кафедри, факультету) Moodle (форум курсу), Zoom							

ОПИС КУРСУ

Курс є необхідною складовою частиною базової теоретичної та практичної підготовки студента, що навчається за освітньою програмою «Інженерія програмного забезпечення».

Курс «Сучасна криптографія» складається з 6-и змістових модулів:

1. Основні поняття криптографії та захисту інформації. Історичний огляд криптографічних методів захисту інформації. Класичні алгоритми переставляння.
2. Симетрична та асиметрична криптографія. Класичні алгоритми заміни.
3. Симетрична та асиметрична криптографія. Мережі Фейстеля. SP-мережі.
4. Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі мереж Фейстеля та SP-мереж (ДСТУ28147:2009, DES).
5. Сучасні криптосистеми на основі блокового шифрування (AES, Rijndael, ДСТУ 7624:2014 «Калина»). Складені шифри.
6. Алгоритми захисту даних. Електронний цифровий підпис. Алгоритми та технології аутентифікації.

Основною метою викладання курсу є отримання компетентностей в області криптографії, криптографічного захисту.

Основними **завданнями** курсу є: надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації; формування

у студентів категоріальних понять з основ математики симетричної та асиметричної криптографії; формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів; стимулювання студентів до активної аналітико-пошукової роботи.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент **зможе**:

- застосовувати на практиці набуті знання про джерела і способи дії загроз на об'єкти інформаційної безпеки ;
- використовувати фундаментальні та спеціальні знання з математики до розв'язання прикладних задач в галузі шифрування, захисту інформації;
- володіти алгоритмами шифрування інформаційних текстів та застосовувати їх;
- працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;
- створювати засобами стандартного програмного забезпечення елементи захисту даних.

Використання новітніх програмних засобів під час виконання практичних та лабораторних завдань розвине як загальні, так і професійні компетенції слухачів.

Змістове наповнення курсу, що викладається на лекційних і лабораторних заняттях та засвоюється студентом під час самостійної роботи, забезпечує набуття **компетентностей**:

ЗК 01. Здатність до абстрактного мислення, аналізу та синтезу.
СК07 Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах.
СК11 Здатність застосовувати та розвивати фундаментальні та міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення, зокрема задач сучасної криптографії.

Програмні результати навчання:
РН03 Будувати і досліджувати моделі інформаційних процесів у прикладній області, зокрема сучасній криптографії.
РН05 Розробляти, аналізувати, обґрунтовувати та систематизувати вимоги до програмного забезпечення.
РН16 Планувати, організовувати та здійснювати тестування, верифікацію та валідацію програмного забезпечення.
РН17 Збирати, аналізувати, оцінювати необхідну для розв'язання наукових і прикладних задач інформацію, використовуючи науково-технічну літературу,

бази даних та інші джерела. Програмні результати, визначені закладом вищої освіти та освітньою програмою

РН19 Розвивати та застосовувати фундаментальні та міждисциплінарні знання для розв'язання завдань інженерії програмного забезпечення

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани занять, методичні рекомендації до виконання індивідуальних та практичних завдань, групових творчих проектів розміщені на платформі Moodle: https://moodle.znu.edu.ua/course/view.php?id=97