ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра інформаційних технологій
Факультет економіки і підприємництва

Викладач: Мазур Ю.П.

Анотація:

Мета курсу (інтегральна компетентність) – здобуття знань для розв'язання складних спеціалізованих задач та практичних проблем у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук, інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Цілі курсу (програмні компетентності):

- здатність до абстрактного мислення, аналізу та синтезу.
- здатність застосовувати знання у практичних ситуаціях.
- знання та розуміння предметної області та розуміння професійної діяльності.
- здатність вчитися й оволодівати сучасними знаннями.
- здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- здатність генерувати нові ідеї (креативність).
- здатність до математичного та логічного мислення, формулювання та досліджування математичних моделей, зокрема дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач в галузі комп'ютерних наук, інтерпретування отриманих результатів;
- здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника
- здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення;
- здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти та експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Програмні результати навчання:

- базові знання сучасних технологій та інструментальних засобів розробки складних програмних систем, уміння їх застосовувати на всіх етапах життєвого циклу розробки;
- базові знання в галузі сучасних інформаційних технологій;

- уміння здійснювати постановку і проведення експериментів за заданою методикою і аналіз результатів.

Короткий зміст курсу:

Захист інформації, його складові і рівні формування режиму інформаційної безпеки. Властивості інформації з точки зору її захисту. Традиційні криптографічні системи. Криптографія і її основні поняття. Модель криптографічної системи. Криптографічна стійкість шифрів. Блокові шифри як основа сучасних криптосистем. Криптосистема DES. Сучасні симетричні криптосистеми. Модель асиметричної системи. Протоколи асиметричної криптографії. Цифровий (електронний) підпис