ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА
ФАКУЛЬТЕТ МАТЕМАТИКИ, ФІЗИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ

Силабус курсу «Криптографія»

Обсяг	загальна кількість: кредитів-4; годин-120;змістових модулів-3
Семестр	осінній
Дні, Час, Місце	за розкладом занять
Викладач	Шпінарева Ірина Михайлівна, канд.фіз.-матем.наук, доцент, доцент кафедри математичного забезпечення комп'ютерних систем
Контактний телефон	(048)7340723
E-mail	iryna.shpinareva@onu.edu.ua
Робоче місце	кафедра математичного забезпечення комп'ютерних систем
Консультації	очні консультації: четвер з 17.00-18.00 on-line консультації: ZOOM (посилання генерується на початку занять)

КОМУНІКАЦІЯ

Комунікація зі студентами буде здійснюватися електронною поштою, в аудиторії або через ZOOM.

АНОТАЦІЯ КУРСУ

Предметом вивчення курсу алгоритми симетричних і асиметричних криптосистем та методи їх криптоаналізу.

Пререквізити курсу

Матеріал курсу ґрунтується на раніше отриманих студентами знаннях, практичних вміннях та навичках з тем та напрямів щодо вищої математики, лінійної алгебри.

Постреквізити курсу

Цей курс є основою для засвоєння наступних дисциплін освітньо-професійної програми підготовки бакалаврів за спеціальністю 123 «Комп'ютерна інженерія»: «Захист інформації в комп'ютерних системах», «Переддипломна практика», «Дипломне проектування», дисциплінах лінії підготовки «Математичне забезпечення комп'ютерних систем».

Метою курсу є оволодіння студентами базових знань в галузі теоретичної криптографії та криптоаналізу, в методах побудови важкооборотних функцій та їх застосувань для побудови асиметричних криптосистем, отримати базові поняття про різноманітні криптографічні протоколи.

Зміст курсу

У курсі розглядаються основні поняття криптографії, симетричні криптосистеми, теоретичні основи асиметричної криптографії, криптосистеми на еліптичних кривих.

ОЧІКУВАНІ РЕЗУЛЬТАТИ

У результаті вивчення курсу студент повинен

знати: основні поняття та методи практичної криптографії, різноманітні типи криптографічних схем та способи їх злому для організації передачі інформації.

вміти: використовувати симетричні та асиметричні криптосистеми для передачі інформації; створювати криптографічні ключі та криптографічні протоколи та застосовувати у прикладних задачах.

Компетентності, які отримує студент у результаті вивчення курсу:

– здатність до абстрактного мислення, аналізу і синтезу;

– здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

Результати навчання: по завершенню курсу студент матиме навички

– знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів систем та мереж;

– знати новітні технології в галузі комп'ютерної інженерії;

– вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності;

– вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

ФОРМИ І МЕТОДИ НАВЧАННЯ

Курс буде викладений у формі лекцій (26 год.) та практичних занять (34 год.), організації самостійної роботи студентів (60 год.).

Основна підготовка студентів здійснюється на лекційних та практичних заняттях, але у значній мірі покладається на самостійне вивчення матеріалу студентами денної форми навчання протягом семестру.

Під час викладання курсу використовуються такі методи навчання: словесні (лекція, пояснення); наочні (презентація Power Point); практичні роботи; робота з літературними джерелами (самостійна робота студентів).

ВІДПОВІДНІСТЬ ЦІЛЯМ СТАЛОГО РОЗВИТКУ ДО 2030 РОКУ

1. Якісна освіта (ЦСР 4)

   Курс сприяє забезпеченню доступу до якісної освіти шляхом поширення знань з криптографії, що є важливим елементом сучасної цифрової епохи. Освітні програми, які включають криптографію, допомагають студентам і професіоналам отримувати навички, необхідні для кар'єри у сфері IT, кібербезпеки та фінансових технологій.

2. Інновації та інфраструктура (ЦСР 9)

   Криптографія є фундаментальною складовою для створення безпечних інфраструктур в епоху цифрових технологій. Розробка криптографічних систем стимулює інновації у таких галузях, як блокчейн, штучний інтелект та Інтернет речей.

3. Гідна праця та економічне зростання (ЦСР 8)

   Вивчення криптографії відкриває нові можливості для працевлаштування у високооплачуваних сферах, таких як IT, фінанси та кібербезпека. Це також сприяє розвитку цифрової економіки, яка підтримує сталий економічний ріст.