КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи

Теоретичний контроль *(кількість балів зазначено на сторінці дисципліни в moodle) – усні (до 2 балів за один контроль) та письмові (до 5 балів за один контроль) опитування на лекціях, практичних заняттях, тестування – (до 5 балів за тест).*

Практичний контроль *(кількість балів зазначено на сторінці дисципліни в moodle) – розв'язання практичних домашніх завдань, завдань самостійної роботи (до 5 балів за один контроль), письмові контрольні роботи (до 5 балів за один контроль, двічі на семестр), тестування – (до 5 балів за тест).*

Реферат *– оволодіння матеріалом, що виноситься на самостійну роботу (до 3 балів за один реферат, двічі на семестр).*

Підсумкові контрольні заходи:

Індивідуальне дослідницьке завдання, проект (ІДЗ, можливо виконання у групі з двох, трьох студентів).

ІДЗ видається за один – два місяці до завершення теоретичного навчання поточного семестру. Термін виконання не менше одного місяця. Виконане ІДЗ, на передостанньому тижні теоретичного навчання поточного семестру подається викладачеві у вигляді оформленої пояснювальної записки (постановка задачі (змістовна, концептуальна, конкретна, математична), побудова та обґрунтування адекватності математичної моделі, обґрунтування методу розв'язання, його достовірності, розв'язок задачі, інтерпретація отриманих результатів, прогнозування або рекомендації до застосування моделі).

На останньому тижні проводиться публічний захист у групі (до 20 балів).

Формат захисту ІДЗ проекту: презентація, тривалістю до 10 хвилин та відповідь на задані присутніми питання (до 5 хвилин).

Детальні вимоги та практичні рекомендації до виконання ІДЗ на сторінці курсу у Moodle та на поточних консультаціях.

Результати ІДЗ можуть стати основою для доповідей на студентських науково-практичних конференціях.

Залікове тестове завдання *(до 20 балів)– проводиться у системі Moodle або MyTestXPro із використанням (за необхідністю) розроблених програмних продуктів, MsExcel, Maple. Критерії оцінювання та вимоги до тесту наведено в інструкції до тесту та поточній консультації.*

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
1(6) семестр			
Поточний контроль (max 60%)			
Змістовий модуль 1	*Теоретичний контроль*	*Тижні 1–8*	**4**
	Лабораторні роботи	*Тижні 1–8*	**20**
	Тест за змістовим модулем	*Тиждень 8*	**6**
Змістовий модуль 2	*Теоретичний контроль*	*Тижні 9–16*	**4**
	Лабораторні роботи	*Тижні 9–16*	**20**
	Тест за змістовим модулем	*Тиждень 16*	**6**
Підсумковий контроль (max 40%)			
Заліковий тест за курс			**20**
Захист індивідуального дослідницького завдання або групового проекту			**20**

Разом		**100**

Шкала оцінювання: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Тиждень і вид заняття	**Тема заняття**	**Контрольне завдання**	**Кільк. балів**
Змістовий модуль 1. Математичні основи криптології.			
Тижні 1–2 Лекції Лаб.роботи	*Основні поняття криптології.* *Арифметичні основи криптографії.* Алгоритм ділення з остачею. Найбільший спільний дільник. Взаємно прості числа. Найменше спільне кратне. Прості числа. Порівняння. Класи лишків. Функція Ейлера. Порівняння першого степеня. Первісні корені. Існування первісних коренів. Індекси за модулем p^k і $2p^k$. Символ Лежандра. Квадратичний закон взаємності. Символ Якобі.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	5
Тижні 3–4 Лекції Лаб.роботи	*Алгебраїчні основи криптографії.* Поняття групи. Підгрупи груп. Циклічні групи. Гомоморфізм груп. Групи підстановок. Дії групи на множині. Кільця і поля. Підкільця. Гомоморфізм кілець. Евклідові кільця. Прості і максимальні ідеали. Скінченні розширення полів. Поле розкладу. Скінченні поля. Порядки незвідних многочленів. Лінійні рекурентні послідовності. Послідовності максимального періоду	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5

Тижні 5–6 Лекції Лаб.роботи	Генератори псевдовипадкових чисел. Принципи використання генераторів псевдовипадкових чисел під час потокового шифрування. Генератори псевдовипадкових чисел. Потокові шифри A5, RC4 та опис їх алгоритмів.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 7–8 Лекції Лаб.роботи	*Класичні алгоритми криптографії.* Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками Тест за змістовим модулем	 5 6
Змістовий модуль 2. Сучасні системи комп'ютерної криптології			
Тижні 9–10 Лекції Лаб.роботи	Стандарти симетричних алгоритмів блокового шифрування даних. Принципи та структура побудови алгоритму *DES* (Data Encription Standard). Генерація раундових ключів. Процес шифрування даних. Функція *DES*. Аналіз алгоритму.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	 5
Тижні 11–12 Лекції Лаб.роботи	Симетричний алгоритм блокового шифрування даних *IDEA* (International Data Encryption Algorithm). Принципи та структура побудови алгоритму *IDEA*. Генерація раундових ключів для зашифрування та розшифрування даних . Процес шифрування даних. Аналіз алгоритму *IDEA*.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 13–14 Лекції Лаб.роботи	Стандарт симетричного алгоритму блокового шифрування даних ДСТУ ГОСТ 28147:2009 Принципи побудови алгоритму. Структура криптографічної системи шифрування даних у режимі простої заміни. Шифрування даних у режимі гамування. Аналіз шифру. Криптографічна стійкість.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 15–16 Лекції Лаб.роботи	Асиметричні криптографічні системи шифрування Основні ідеї та принципи. Перша криптографічна система з відкритим ключем — система Діффі–Хеллмана. Криптографічна система Шаміра. Криптографічна система Ель-Гамаля. Криптографічна система RSA. Криптографічна система Рабіна.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	 5 6

	Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні.	Тест за змістовим модулем	
Тижні 15–16	Підсумковий контроль	Захист ІДЗ	20
Тижні 16	Підсумковий контроль Залік	Тестування (проводиться у системі Moodle або MyTestXPro)	20
Всього			**100**