СИСТЕМА НАКОПИЧЕННЯ БАЛІВ

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(7) семестр			
Поточний контроль (max 60%)			
Змістовий модуль 1	*Теоретичний контроль*	*Тижні 1–5*	**4**
	Практичні завдання	*Тижні 1–5*	**10**
	Реферат	*Тиждень 4*	**3**
	Тест за змістовим модулем	*Тиждень 5*	**5**
Змістовий модуль 2	*Теоретичний контроль*	*Тижні 6–10*	**5**
	Практичні завдання	*Тижні 6–10*	**10**
	Тест за змістовим модулем	*Тиждень 10*	**5**
Змістовий модуль 3	*Теоретичний контроль*	*Тижні 11–14*	**5**
	Практичні завдання	*Тижні 11–14*	**10**

	Реферат	*Тиждень 13*	**3**
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**	**Кількість балів**
Змістовий модуль 1.			
Тижні 1–2 Лекція 1 Практичні 1-2	Вступ. Основні поняття безпеки інформації, криптографії Математичні основи . Теорія чисел. Модульна арифметика.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2
Тижні 3–4 Лекція 3 Практичні 3-4	Математичні основи . Кінцеві групи, кільця і поля Мультиплікативні групи полів і кілець	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 4
Тижні 5–6 Лекція 5 Практичні 5-6	Розподіл ключів за схемою Діффі-Хелмана Модульний контроль	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 4 3

		Співбесіда за матеріалом реферату Тест за змістовим модулем	5
Змістовий модуль 2.			
Тижні 7–8 Лекція 7 Практичні 7-8	Криптосистема RSA Ключові пари RSA	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 9–10 Лекція 9 Практичні 9-10	Цифровий підпис RSA Безпека RSA	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками Тест за змістовим модулем	3 5 5
Змістовий модуль 3.			
Тижні 11–12 Лекція 11 Практичні 11-12	Еліптичні криві над полем дійсних чисел Криптосистема Ель-Гамаля над еліптичною кривою.	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками	2 5
Тижні 13–14 Лекція 13 Практичні 13-14	Цифровий підпис. Стандарти цифрового підпису	Фронтальне опитування (усне, письмове). Згідно плану заняття, перевірка виконання д/з, оволодіння теоретичним матеріалом, практичними вміннями та навичками Співбесіда за матеріалом реферату	3 5 3
Тижні 13–14	Підсумковий контроль	Захист ІДЗ	20
Тижні 13–14	Підсумковий контроль Екзамен	Тестування (проводиться у системі Moodle або MyTestXPro)	20
Всього			**100**