КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
Кафедра математичної інформатики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Кашпур О.Ф.
«28» серпня 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Основи криптографії
для студентів

галузь знань **12 « Інформаційні технології»**
спеціальність **122 «Комп'ютерні науки»**

освітній рівень **бакалавр**

освітня програма **«Інформатика»**

вид дисципліни **вибіркова**
вибірковий блок **«Інтелектуальні інформаційні технології»**

Форма навчання	**заочна**
Навчальний рік	**2020/2021**
Семестр	**7**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Пролонговано: на 2021/2022 н. р. _____ «7»05 2021 р.

на 20__/20__ н. р. _____ «__»___ 20__ р.

КИЇВ – 2020

Розробник: **Анісімов Анатолій Васильович**, д. ф.-м. н., проф., декан факультету комп'ютерних наук та кібернетики

ЗАТВЕРДЖЕНО
Завідувач кафедри математичної інформатики

_____Терещенко В.М.
(підпис)

Протокол № 1 від «28» 08 2020 р.

Схвалено Гарантом освітньо-професійної програми «Інформатика»
_____(Омельчук Л.Л.)
(підпис)
«28» серпня 2020 р.

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від «28» серпня 2020 року № 1
Голова науково-методичної комісії _____ (Омельчук Л.Л.)
(підпис) (прізвище та ініціали)

«28» серпня 2020 року

1. Мета дисципліни. Метою курсу «Основи криптографії» є ознайомлення та вивчення студентами сучасних методів захисту інформації шляхом її перетворення (кодування) у цифровому форматі.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

а) Знати: основні поняття і методи дискретної математики, теорії чисел, математичного аналізу, алгоритмики, структур даних, програмування.

б) Вміти: по опису перетворень створювати алгоритми і програми, що іх реалізують.

3.Анотація навчальної дисципіни: Дисципліна «Основи криптографії» спрямована на вивчення основних задач передачі та захисту інформації від несанкціонованого доступу. Вона забезпечує оволодіння сучасними методами криптографічних перетворень інформації. Криптографія включає криптографію з відкритими ключами: основні протоколи, цифровий підпис, геш-функції, блокчейн технологію, доведення з нульовим розкриттям, методи автентифікації, біт-коін та інші криптовалютні системи.

4. Завдання (навчальні цілі):

набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у розв'язанні задач кодування інформації, відповідно науково-освітньої кваліфікації «Бакалавр». Зокрема, розвивати: здатність застосовувати теоретичні та практичні основи криптографічного захисту інформації.

- 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 до інтелектуального багатовимірного аналізу даних та їхньої оперативної аналітичної обробки з візуалізацією результатів аналізу в процесі розв'язування прикладних задач у галузі комп'ютерних наук
- здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
- здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

5Результати навчання за дисципліною:

Результат навчання (РН) **(1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)**	**Форми (та/або методи і технології)**	**Методи оцінювання та пороговий критерій**	**Відсоток у підсумковій**

Код	Результат навчання	викладання і навчання	оцінювання (за необхідності)	оцінці з дисципліни
РН 1.1	Знати основні принципи криптографії з відкритими ключами	*Лекції, лабораторні заняття, самостійна робота*	*Реферати, іспит, вирішення задач по темі.*	*20%*
РН 1.2	Знати основні схеми криптографічних перетворень на основі односторонніх функцій.			
РН 1.3	Знати основні протоколи розповсюдження ключів.			*20%*
РН 1.4	Знати основні схеми цифрового підпису.			
РН 2.1	Вміти створювати алгоритми та програми, що реалізують криптографічні перетворення.	*Лекції, лабораторні заняття, самостійна робота*	*іспит, вирішення задач по темі.*	*20%*
РН 2.2	Вміти створювати системи захисту інформації, що передається по відкритим каналам зв'язку.			*20%*
РН 2.3	Вміти програмувати цифрові підписи.	*Лекції, лабораторні заняття, самостійна робота*	*Захист рефератів.*	*5%*
РН3.1	Оцінювати власні пропозиції по створенню систем криптозахисту, обговорювати з колегами проекти систем.			*5%*
РН4.1	Демонструвати академічне та професійне володіння предметом , вміння створювати та обґрунтовувати нові системи захисту інформації.			*5%*
РН4.2	Демонструвати вміння працювати в групових виконаннях практівю			*5%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни / Програмні результати навчання	РН 1.1	РН 1.2	РН 1.3	РН 1.4	РН 2.1	РН 2.2	РН 2.3	РН 3.1	РН 4.1	РН 4.2
(з опису освітньої програми)										
ПРН17.1 Знати, аналізувати, вибирати та кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	+	+	+	+	+	+	+	+	+	+

7. Схема формування оцінки.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду:

1. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2 – 20 балів/12 бали;

2. Реферат, захист реферату: РН1.1, РН1.2, РН2.1, РН2.2 – 40 балів/24 бали;

- підсумкове оцінювання: екзамен.

- максимальна кількість балів які можуть бути отримані: 40 балів;

- результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3, РН1.4;

- форма проведення і види завдань: усно–письмова форма.

Для здобувачів освітньо-наукового ступеня, які набрали сумарно меншу кількість балів ніж *критично-розрахунковий мінімум – 20 балів* для одержання іспиту за рішенням кафедри не допустити до

складання іспиту із рекомендацією здати контрольні роботи та захистити проект до повторного складання іспиту.

Рекомендований мінімум – 36 балів.

7.2. Організація оцінювання:

Обов'язковим є виконання завдань, винесених на самостійну роботу, та модульних контрольних робіт за графіком робочої програми.

У частину 1 входять теми 1 - 15, у частину 2 – теми 3,6.9. Обов'язковим для екзамену є виконання усіх контрольних робіт та захист проекту до вказаної викладачем дати, перед початком екзаменаційної сесії, згідно навчального плану. Переписування чи перескладання тем не практикується. Дозволяється здача окремих завдань модульних тем у проміжках між написанням модульних контрольних робіт (наприклад, перша тема здається до здачі наступної модульної контрольної роботи у будь-який зручний для викладача та студента час).

Терміни проведення форм оцінювання:

1. Захист реферату: до останнього тижня семестру.

У випадку відсутності з поважних причин відпрацювання та перездачі контрольні роботи здійснюються у відповідності до «Положення про організацію освітнього процесу».

7.3. Шкала відповідності оцінок

Відмінно	90-100
Добре	75-89
Задовільно	60-74
Незадовільно	0-59

При визначені оцінки визначальною є робота в семестрі. Після завершення розгляду тем проводяться письмові контрольні роботи та теоретичне опитування.

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ)

№	Назва лекції	Кількість годин		
		Лекції	Практ.	Самостійна робота
Частина 1. «Базові поняття та схеми криптографічних перетворень»				
1	**Тема 1.** Основи теорії чисел та алгебри.	0,5		10
2	**Тема 2.** Квадратичні лишки.	0,5		10
3	**Тема 3.** Одностороння функція. Приклади. *Індивідуальна робота: програмування пошуку простих чисел*.	0,5		10
4	**Тема 4.** Метод Діффі-Хеллмана розповсюдження ключів. Груповий GDH-алгоритм.	0,5		10
5	**Тема 5.**. RSA-алгоритм та його узагальнення. Цифровий підпис.	0,5	0,5	10
6	**Тема 6.** Геш-функції. MD 5 and SHA. Дерево Меркля. Блокчейн. *Індивідуальна робота: Програмування дерева Меркля.*	0,5	0,5	10
Частина 2. «Недетерміновані та ймовірнісні схеми кодування»				
7	**Тема 7.** Схема Голдвассер-Мікалі, що базується на квадратисчних лишках	0,5		10
8	**Тема 8.** RSA в недетермінованому варіанті (OAEP). Pailier та Benaloh схеми.	0,5		9
9	**Тема 9.** Методи автентифікації. Схема Фіата-Шаміра автентифікації смарт-карти.. Схема Шнорра.	0,5	0,5	5
10	**Тема 10.** Доведення з нульовим розголошенням. Застосування. *Індивідуальна робота: програмування протоколу Фіата-Шаміра автентифікації.*	0,5	0,5	5
Частина 3 « Криптографія на еліптичних кривих»				
11	**Тема 11.** Група точок еліптичної кривої. Кодування інформації точками еліптичної кривої	0,5		5
12	**Тема 12.** Цифровий підпис на ЕК.	0,5		5

Частина 4. «Біткоін та інші криптовалюти»

14	**Тема 13.** Структура біткоін мережі. Майнинг та блокчейн	0,5	0,5	5
16	**Тема 14.** Інші криптовалюти. Ефір та смарт-контракти. Інтернет речей.	0,5	0,5	5
	Всього	**7**	**3**	**109**

Загальний об'єм ***120*** *годин*:»
Лекцій **7 год.**
Лабораторні **3 год**.
Консультації – **1 год.**
Індівідуальна робота **– 109 год**

9. Рекомендовані джерела (Доступні через Internet)

Основні:

1.Oded Goldreich, Foundations of Cryptography, Cambridge University Press, 2004, 372pp.

2 D. Salomon, Handbook of Data Compression.-Springer-Verlag, 2010, 1370pp.
3 J.Kutz, Y.Lindel, Introduction to Modern Cryptography.-Chaptman&Hall, 2014, 603 pp.
4 A.M. Antonopoulas, Mastering Bitcoin Open Edition, 2014

Додаткові:

1. А.В. Анісімов Алгоритмічна теорія великих чисел. // Видавничий дім «Академперіодика», 2001, – 153