КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
КАФЕДРА МАТЕМАТИЧНОЇ ІНФОРМАТИКИ

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Олена КАШПУР
«12» лютого 2021 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	**денна**
Навчальний рік	**2022/2023**
Семестр	**6**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладачі: **професор Анісімов А.В., д.ф.-м.н.,член-кореспондент НАН України**

Пролонговано: на 20 /20.р. ( ) « » 20 р.
на 20 /20 н.р. ( ) « » 20 р.

КИЇВ – 2021

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

ЗАТВЕРДЖЕНО
Завідувач кафедри математичної інформатики

_____Василь ТЕРЕШЕНКО
(підпис)

Протокол №6 від «11» 02 2021 р.

Схвалено гарантом освітньо-професійної програми «Інформатика»

_____ Людмила ОМЕЛЬЧУК «11» лютого 2021 року

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

Протокол від "11" лютого 2021 року № 7

Голова науково-методичної комісії _____доцент, к.ф.-м.н.Людмила ОМЕЛЬЧУК
(підпис)

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, структур даних, програмування.

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

3.Анотація навчальної дисципліни: 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, біткоін 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 аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

5. Результати навчання за дисципліною:

Результат навчання (РН) (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		**Форми (та/або методи і технології) викладання і навчання**	**Методи оцінювання та пороговий критерій оцінювання (за необхідності)**	**Відсоток у підсумковій оцінці з дисциплін и**
Код	**Результат навчання**			
РН 1.1	Знати основні принципи криптографії з відкритими ключами	*Лекції. самостійна робота*	*Реферати, іспит, усні відповіді, 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. самостійна робота*	*іспит, усні відповіді, 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.			*5%*

РН3.1	Оцінювати власні пропозиції по створенню систем криптозахисту, обговорювати з колегами проекти систем.	*Лекції. самостійна робота*	*Захист рефератів.*	*5%*
РН4.1	Демонструвати академічне та професійне володіння предметом , вміння створювати та обгрунтовувати нові системи захисту інформації.			*5%*
РН4.2	Демонструвати вміння працювати в групових виконаннях проектів			*5%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН1.1**	**РН1.2**	**РН1.3**	**РН1.4**	**РН2.1**	**РН2.2**	**РН2.3**	**РН3.1**	**РН4.1**	**РН4.2**
(з опису освітньої програми)										
ПРН18.1. 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. Активна робота на лекції, усні відповіді: РН1.1, РН1.2, РН1.3, РН1.4– 10 балів/6 бали;

2. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2 – 10 балів/6 бали;

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

- підсумкове оцінювання: іспит.

- 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:

У частину 1 входять теми 1 - 15, у частину 2 – теми 3,6.9. Обов’язковим для іспиту є виконання усіх форм оцінюваннння 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. Активна робота на лекції, усні відповіді: протягом семестру.

2. Виконання завдань, винесених на самостійну роботу: протягом семестру.

3. Захист реферату: до 10-го тижня навчального періоду.

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

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.	2		
2	**Тема 2.** Квадратичні лишки.	2		
3	**Тема 3.** Одностороння функція. Приклади. *Самостійна робота: опрацювання лекційного матеріалу, програмування пошуку простих чисел.*	2		8
4	**Тема 4.** Метод Діффі-Хеллмана розповсюдження ключів. Груповий GDH-алгоритм. *Самостійна робота: опрацювання лекційного матеріалу, програмування пошуку простих чисел.*	2		8
5	**Тема 5.**. RSA-алгоритм та його узагальнення. Цифровий підпис. *Самостійна робота: опрацювання лекційного матеріалу, підготовка реферату.*	2		
6	**Тема 6.** Геш-функції. MD 5 and SHA. Дерево Меркля. Блокчейн. *Самостійна робота:програмування дерева Меркля. опрацювання лекційного матеріалу.*	4		8
Частина 2. «Недетерміновані та ймовірнісні схеми кодування»				

7	**Тема 7.** Схема Голдвассер-Мікалі, що базується на квадратичних лишках *Самостійна робота: опрацювання лекційного матеріалу, підготовка реферату.*	2		8
8	**Тема 8.** RSA в недетермінованому варіанті (OAEP). Pailier та Benaloh схеми. *Самостійна робота: опрацювання лекційного матеріалу, , підготовка реферату.*	2		8
9	**Тема 9.** Методи автентифікації. Схема Фіата-Шаміра автентифікації смарт-карти.. Схема Шнорра. *Самостійна робота: опрацювання лекційного матеріалу, , підготовка реферату.*	2		8
10	**Тема 10.** Доведення з нульовим розголошенням. Застосування. *Самостійна робота: програмування протоколу Фіата-Шаміра автентифікації.*	4		12
	Захист реферату	4		

Частина 3 «Криптографія на еліптичних кривих»

11	**Тема 11.** Група точок еліптичної кривої *Самостійна робота: опрацювання лекційного матеріалу.*	2		
12	**Тема 12.** Кодування інформації точками еліптичної кривої *Самостійна робота: опрацювання лекційного матеріалу.*	2		8
13	**Тема 13.** Цифровий підпис на ЕК. *Самостійна робота: опрацювання лекційного матеріалу.*	2		

Частина 4. «Біткоін та інші криптовалюти»

14	**Тема 14.** Структура біткоін мережі. *Самостійна робота: опрацювання лекційного матеріалу.*	**4**		8
15	**Тема 15.** Майнинг та блокчейн *Самостійна робота: опрацювання лекційного матеріалу.*	**2**		
16	**Тема 16.** Інші криптовалюти. Ефір та смарт-контракти. Інтернет речей. *Самостійна робота: опрацювання лекційного матеріалу.*	**2**		
	Всього	**42**		**76**

Загальний об'єм *120 годин*:
Лекцій 42 *годин*.
Консультації - 2 *годин*.
Індивідуальна робота – 76 *годин*.

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 с.