КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
Кафедра математичної інформатики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Кашпур О.Ф.
«_26_» _____03_____ 2018 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Проблеми кодування та захисту інформації
Problems of Coding and Information protection

для здобувачів освітньо-наукового рівня «доктор філософії»

галузь знань	**12 «Інформаційні технології»**
спеціальність	**122 «Комп'ютерні науки»**
освітній рівень	**третій (освітньо-науковий)**
освітньо-наукова програма	**«Комп'ютерні науки»**
вид дисципліни	**вибіркова**

Форма навчання **денна / заочна**

Навчальний рік **2018/2019**
Рік навчання 2
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 2019/2020 н.р. (прот. №9 «15» 04 2019 р.)
на 2020/2021 н.р. (протокол «30» 03 2020 р. №8)

КИЇВ – 2018

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 №5 від «28» 12 2017 р.

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

Протокол від "14" 02 2018 року № 6

Голова науково-методичної комісії _____ професор, д.ф.-м.н. Хусаінов Д.Я.
(підпис)

1. **Мета дисципліни**. Метою курсу «Проблеми кодування та захисту інформації» є ознайомлення та вивчення здобувачами третього (освітніьо-наукового) рівня вищої освіти сучасних методів передачі та захисту інформації шляхом її перетворення у цифровому форматі.

   The purpose of the discipline. The purpose of the course "Fundamentals of Coding and Cryptography" is to familiarize and study by postgraduate students modern methods of information transmission and protection through its transformation in digital format.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1. *Знати:* основні поняття і методи дискретної математики, теорії чисел, математичного аналізу, алгоритміки, структур даних, програмування.

2. *Вміти*: по опису перетворень створювати алгоритми і програми, що іх реалізують.

Prerequisites for mastering or choosing a course:

1) Know: basic concepts and methods of discrete mathematics, number theory, mathematical analysis, algorithms, data structures, programming.

2) Be able to create algorithms and programs that implement describing transformations.

3.Анотація навчальної дисципіни: Дисципліна «Проблеми кодування та захисту інформації» спрямована на вирішення основних задач передачі та захисту інформації від похибок та несанкціонованого доступу. Вона забезпечує оволодіння сучасними методами стискання, виправлення похибок та криптографічних перетворень інформації. Стискання та виправлення похибок даються оглядово. Криптографія включає криптографію з відкритими ключами: основні протоколи, цифровий підпис, геш-функції, блок-чєйн технологію, методи автентифікації, біт-коін та інші криптовалютні системи.

Annotation of the discipline: The discipline "Fundamentals of coding and cryptography" is aimed at solving the basic problems of transmitting and protecting information from errors and unauthorized access. It provides mastery of modern methods of compression, error correction and cryptographic transformation of information. Error compression and correction are given in a reviewing manner. Cryptography includes public-key cryptography:
core protocols, digital signature, hash functions, blockchain technology, authentication methods, bit-coin and other cryptocurrency systems.

4. Завдання (навчальні цілі):

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

Tasks (learning objectives):

acquisition of knowledge, skills and competences at the level of the latest achievements in solving the problems of coding of information, in accordance with the scientific and educational qualification "Doctor of Philosophy". In particular, to develop: the ability to apply the theoretical and practical basics of compression, error correction and cryptographic information security.

5. Результати навчання за дисципліною:

<table>
<tr><th colspan="2">Результат навчання (РН)
(1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)</th><th rowspan="2">Форми (та/або методи і технології) викладання і навчання</th><th rowspan="2">Методи оцінювання та пороговий критерій оцінювання (за необхідності)</th><th rowspan="2">Відсоток у підсумковій оцінці з дисципліни</th></tr>
<tr><th>Код</th><th>Результат навчання</th></tr>
<tr><td>РН 1.1</td><td>To know main algorithms of error correction codes. /
Знати основні алгоритми виправлення помилок коду.</td><td rowspan="4">Лекції, самостійна робота / Lectures, Individual work</td><td rowspan="4">Захист реферату, екзамен, активна робота на лекціях, усні відповіді/ Review defense, exam, active participation in lectures, oral answers</td><td>20%</td></tr>
<tr><td>РН 1.2</td><td>To know main methods of data compression /
Знати основні методи стиснення даних</td><td rowspan="3">20%</td></tr>
<tr><td>РН 1.3</td><td>To know main paradigms and protocols of PK-cryptography/
Знати основні парадигми та протоколи РК-криптографії.</td></tr>
<tr><td>РН 1.4</td><td>To know Huffman codes, Encoding integers, Elias codes./
Знати коди Хаффмана, кодування цілих чисел, коди Еліаса.</td></tr>
<tr><td>РН 2.1</td><td>To be able to correctly create algorithms and programs for data (texts and video) compression /
Вміти правильно створювати алгоритми та програми для стиснення даних (текстів та відео)</td><td rowspan="3">Лекції, практичні заняття, самостійна робота/ Lectures, Tutorials, Individual work</td><td rowspan="3">Захист реферату, екзамен, виконання завдань винесених на самостійну роботу / Review defense, exam, tutorial exercises</td><td>20%</td></tr>
<tr><td>РН 2.2</td><td>To be able to formulate unsolved problems in the topic. To create programs for described algorithms./
Вміти формулювати невирішені проблеми за темою курсу.
Створення програм для описаних алгоритмів.</td><td>20%</td></tr>
<tr><td>РН 2.3</td><td>To be able to solve practical problems for PK-communications. /
Вміти вирішувати практичні проблеми для РК-комунікацій</td><td>Практичні заняття, самостійна робота/</td><td>Захист проекту/ Review defense</td><td>5%</td></tr>
</table>

РН3.1	Validate the own approach to the problem, discuss with colleagues the aspects of the PK-applications./ Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань РК-застосунків.	*Tutorials, Individual work*		*5%*
РН4.1	Demonstration of the authority, innovativeness, high level of self-determination, academic and professional virtue, consistent devotion to the development of new ideas or processes in progressive contexts in the frame of professional and scientific activity / Демонстрація авторитетності, інноваційності, високого ступеня самостійності, академічної та професійної доброчесності, послідовної відданості розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності.			*5%*
РН4.2	Demonstrate responsibility towards the work, ability to work in middle-size group projects. / Відповідально ставитися до виконуваних робіт, вміння працювати в групових проектах середнього розміру.			*5%*

6. Correspondense between learning results and program study results / 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)										
ПРН-8. Критично оцінювати, аналізувати та пропонувати методи і моделі створення, впровадження, експлуатації інформаційних систем і керування ними на всіх етапах життєвого циклу / Critically evaluate, analyze and propose methods and models for the creation, implementation, operation and management of information systems at all stages of the life cycle	+	+	+	+	+	+	+	+	+	+

7. Схема формування оцінки.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду:

1. Активна робота на лекції, усні відповдіі: 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, РН1.3, РН1.4РН2.1, РН2.2, РН 2.3, РН 4.1, РН 4.2 – 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, РН 2.1, РН 2.2;
- *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 - 4, у частину 2 – теми 5 – 8. 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 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 / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

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

8. STRUCTURE OF THE DISCIPLINE. THEMATIC PLAN OF LECTURES AND TUTORIALS (СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ)

№	Lecture title (Назва лекції)	Кількість годин Amount of hours		
		Лекції Lectures	Практ. Tutorials	Самостійна робота Individual work
Частина 1. Коди виправлення помилок Part 1. Error correction codes.				
1	**Тема 1.** Вступ. Поняття про ентропію. Міркування Шеннона. Хемінг-метрики. Моделі зв'язку по каналах із шумом та наявністю підслуховувача *Самостійна робота:* Порахуйте ентропію текстів (статті Вікіпедії, тексти за вільним вибором)/ **Theme 1.** Introduction. Notion of entropy. C. Shannon's considerations. Hamming metrics. Models of communication through channels with noise and presence of eavesdropper *Individual work:* Count entropy of texts (articles of Wikipedia, texts by free choice)	2		12
2	**Тема 2.** Коди прямої корекції помилок. Коди Хеммінга. Коди згортання. Декодер Вітербі. Коди Рід-Соломона. *Самостійна робота:* Запрограмувати алгоритм Хеммінга./ **Theme 2.** Forward error correction codes. Hamming codes. Convolution codes. Viterbi decoder. Reed-Solomon codes. *Individual work:* To program Hamming's algorithm.	2		12
3	**Тема 3.** Стиснення даних. Миттєві коди. Префіксні коди. Нерівності Крафта-Макміллана. Коди візерунків Повнота. *Самостійна робота:* Створіть кілька (індивідуальних) кодів префіксів/ **Theme 3.** Data compression. Instantaneous codes. Prefix codes. Kraft-MacMillan inequalities. Pattern codes. Completeness. *Individual work:* Create some (individual) prefix codes	2		12
4	**Тема 4.** Коди Хаффмана. Перетворення Уорллера. Алгоритм стиснення Lempel-Ziv-Welsh.	2	2	12

	Самостійна робота: Програмувати коди Хаффмана. Програмувати перетворення Burrous-Wheeler./ **Theme 4.** Huffman codes. Burrous- Wheeler transform. Lempel-Ziv-Welsh compression algorithm. *Individual work:* To program Huffman codes. To program Burrous-Wheeler transform.			
Частина 2. Криптографія з відкритим ключем/ Part 2. «Public-key cryptography»				
5	**Тема 5.** Основні парадигми криптографії з відкритим ключем. Односторонні функції. Алгоритм Діффі - Гелмана. Група DHA. Протоколи коаліції. *Самостійна робота:* Програмувати GDH-алгоритм для 3 користувачів./ **Theme 5.** Main paradigms of public-key cryptography. One-way functions. Diffie – Hellman algorithm. Group DHA. Coalition protocols. *Individual work:* To program GDH-algorithm for 3 users.	2		12
6	**Тема 6.** RSA та подібні протоколи передачі інформації. Схеми Пейлер і Беналох. *Самостійна робота* Програмувати схеми Пайєра або Беналоха/ **Theme 6.** RSA and similar protocols for information transfer. Pailier and Benaloh schemes. *Individual work* To program Pailier or Benaloh schemes	2		12
7	**Тема 7.** Цифрові підписи. Еліптична крива підписів. Групові підписи. Звоніть підписи. Підписи на криптовалюту. Методи аутентифікації *Самостійна робота:* Розробити сліпих і 2 з 3 підписів**./** **Theme 7.** Digital signatures. Elliptic curve signatures. Group signatures. Ring signatures. Signatures for cryptocurrency. Authentication methods. *Individual work:* To develop blind and 2 from 3 signatures.	2	2	12
8	**Тема 8.** Хеш-функції. Функції MD 5 і SHA. Дерево Меркла. Технологія блокчейн. Мережа біт-монет *Самостійна робота:* Вивчити структуру хеш-алгоритмів SHA та MD5./ **Theme 8.** Hash-functions. MD 5 and SHA functions. Mercle tree. Block-chain technology. Bit-coin network *Individual work:*	2		12

	To study the structure of SHA and MD5 hash-algorithms.			
Захист реферату / Review defense		2		
ВСЬОГО/TOTAL		18	4	96

Total duration / загальний об'єм *120 hours*, namely:
Lectures/Лекцій – **18** *hours*,
Tutorials/Практичні – **4** *hours.*
Consultations/Консультації - **2** *hours.*
Individual work/Самостійна робота – **96** *hours.*

9. Recommended sources / Рекомендовані джерела

Main / Основні:

1. Shi Lin, D.J. Castello, Error Control Coding.- Pearson Publ., 2004, 1272 pp.
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

Additional / Додаткові:

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