КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
Кафедра математичної інформатики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Кашпур О.Ф.
«30» 08 2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Основи криптографії та захисту інформації
Cryptography and Information Security Fundamentals

Для студентів / for students

галузь знань	**12 "Інформаційні технології" / "Information Technologies"**
спеціальність	**122 "Комп'ютерні науки" / "Computer Science"**
освітній рівень	**магістр / master**
освітня програма	**Штучний інтелект / "Artificial Intelligence"**
вид дисципліни	**Обов'язкова навчальна дисципліна / mandatory**

Форма навчання	**денна**
Навчальний рік	**2019/2020**
Семестр	**2**
Кількість кредитів ECTS	**5**
Мова викладання, навчання та оцінювання	**англійська, українська / English, Ukrainian**
Форма заключного контролю	**іспит / exam**

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

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

КИЇВ – 2019

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) (прізвище та ініціали)
Протокол №10 від «23» травня 2019 р.

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

Протокол від «30» серпня 2019 року №1

Голова науково-методичної комісії _____ (Омельчук Л.Л.)
(підпис) (прізвище та ініціали)
«30» серпня 2019 року

1. Мета дисципліни. Мета дисципліни — ознайомлення та вивчення магістрами сучасних методів передачі та захисту інформації шляхом її перетворення у цифровому форматі.

1. The purpose of the discipline. The purpose of the course "Fundamentals of Cryptography and and Information Security" 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:

a) Знати: основні поняття і методи дискретної математики, теорії чисел, математичного аналізу, алгоритміки, структур даних, програмування. Знання технічної англійської мови на рівні B1-B2.

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

2. Prerequisites for mastering or choosing a course:

a) Know: basic concepts and methods of discrete mathematics, number theory, mathematical analysis, algorithms, data structures, programming. Level B1-B2 technical English skills.

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

3.Анотація навчальної дисципіни: Дисципліна «Основи криптографії та захисту інформації» належить до переліку обов'язкових навчальних дисциплін освітньо-наукової програми підготовки фахівців «Штучний інтелект» за другим (магістерським) рівнем вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки». Вона 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.
Завершується дисципліна екзаменом в 2 семестрі 1 курсу магістратури.

3.Annotation of the discipline: The discipline " Fundamentals of Cryptography and Information Security " belongs to the list of mandatory disciplines as a component of the educational-scientific training program for the second (master's) level of higher education in the field of knowledge 12 "Information Technology" specialty 122 "Computer Science", educational-professional program "Artificial Intelligence". It 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.
The discipline ends with an exam in the 2nd semester of the 1st year of master's degree study.

4. Завдання (навчальні цілі):

Основними завданнями дисципліни «Основи криптографії та захисту інформації» є набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень в області

криптографії та інформаційної безпеки відповідно до освітньої кваліфікації магістр комп'ютерних наук. Зокрема, розвивати:

- здатність до абстрактного мислення, аналізу та синтезу (ЗК1);
- здатність спілкуватися іноземною мовою (ЗК5);
- здатність проводити дослідження функціональної та економічної ефективності та надійності інформаційних систем (СК13);
- здатність до алгоритмічного та логічного мислення (СК18).

4. Tasks (learning objectives):

acquiring knowledge, skills and competences at the level of the latest achievements in Computer Science, according to the scientific and educational qualification of "Master". In particular, to develop:

- the ability of abstract thinking, analysis and synthesis;
- the ability to communicate in a foreign language (English);
- the ability to investigate the functional and economical efficiency and reliability of information systems;
- the ability to algorithmic and logical thinking.

5. Results of learning / 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 дисципліни**
Код	**Результат навчання**			
РН 1.1	To know. Main algorithms of error correction codes. Знати. Основні коди, що виправляють похибки.	*Лекції, самостійна робота / Lectures, Individual work*	*Захист реферату, Активна робота на лекції, усні відповіді, іспит / Review defense, exam, active participation in lectures, oral answers, exam*	*20%*
РН 1.2	To know. Main methods of data compression. Знати. Основні методи стискання даних.			
РН 1.3	To know. Main paradigms and protocols of PK-cryptography. Знати. Основні парадигми і протоколі криптографії з відкритими ключами (РК).			*20%*
РН 1.4	To know: Huffman codes. Encoding integers. Elias codes. Знати. Коди Хаффмана. Кодування чисел. Коди Еліаса.			
РН 2.1	To be able to correctly create algorithms and programs for data (texts and video) compression Вміти створювати алгоритми і програми для стискання даних (тексті та відеозображення)	*Лекції, самостійна робота / Lectures, Individual work*	*Захист реферату, Виконання завдань, винесених на самостійну роботу / Review defense, exam, tutorial exercises*	*20%*
РН 2.2	To be able to formulate unsolved problems on the topic. To be able to create programs for described algorithms. Вміти формулювати не розв'язані проблеми по темі. Вміти створювати програми для описаних алгоритмів.			*20%*
РН 2.3	To be able to solve practical problems for PK-communications.	*Лекції, самостійна*	*Захист реферату /*	*5%*

	Вміти вирішувати практичні проблеми стосовно РК-комунікацій.	*робота / Lectures, Individual work*	*Review defense*	
РН3.1	Validate the own approach to the problem, discuss with colleagues the aspects of the PK-applications. Оцінювати власний підхід до проблеми, обговорювати аспекти РК-застосувань.			*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 in the frame of professional and scientific activity. Демонструвати глибоке розуміння, креативність, високий рівень само-зосередження, академічну та професійну доброчесність, постійне прагнення до розвитку нових ідей в рамках професійної і наукової активності.			*5%*
РН4.2	Demonstrate responsibility towards the work, ability to work in middle-size group projects. Демонструвати відповідальність в роботі, 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)										
ПРН8. Аналізувати особливості використання сучасних квантових технологій для забезпечення вирішення проблем, зокрема конфіденційного зв'язку, квантової криптографії, здійснювати дослідження теоретичних та експериментальних аспектів квантової інформатики. / To analyze the peculiarities of using modern quantum technologies in order to solve problems, in particular confidential communication, quantum cryptography, to carry out research on theoretical and experimental aspects of quantum informatics	+	+	+	+	+	+	+	+	+	+
ПРН11. Вміти аналізувати ризики з урахуванням корпоративних цінностей та інтересів, розробляти план управління ризиками для визначення необхідних профілактичних заходів, застосовувати дії для пом'якшення наслідків ризиків та непередбачених дій.				+		+		+	+	+

/ To be able to analyze risks taking into account corporate values and interests, develop a risk management plan to determine the necessary preventive measures, and take actions to mitigate the effects of risks and unforeseen actions.										

7. Схема формування оцінки / Mark forming scheme.

7.1. Форми оцінювання студентів / Student evaluation forms:

- оцінювання впродовж навчального періоду/evaluation in semester:

1. Активна робота на лекції, усні відповіді / Active participation in lectures, oral answers: РН1.1, РН1.2, РН1.3, РН1.4– 10 балів/6 балів;

2. Виконання завдань, винесених на самостійну роботу / Tutorial exercises: РН2.1, РН2.2 – 10 балів (points)/6 балів (points);

3. Захист реферату / Review defense: РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2, РН 2.3, РН 3.1, РН 4.1, РН 4.2 – 40 балів (points) /24 бали (points);

- підсумкове оцінювання/final evaluation: іспит/exam.

- *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;
- *види завдань*: 2 письмових завдання (практичні завдання) та 1 усне теоретичне питання;
- для отримання загальної позитивної оцінки з дисципліни оцінка за іспит повинна бути не меншою ніж 24 бали;
- студенти не допускаються до іспит, якщо протягом семестру вони набрали менше ніж 36 балів;
- студенти не допускаються до іспиту, якщо протягом семестру вони не виконали та не захистили реферат.

/

- *maximum points that can be obtained by a student:* 40 points;
- *learning outcomes that will be evaluated:* РН1.1, РН1.2, РН1.3, РН1.4;
- *form of conducting and types of tasks:* oral-written;
- *types of tasks:* 2 written tasks (practical tasks) and 1 oral theoretical question;
- to obtain an overall positive grade in the discipline, the grade for the exam must be not less than 24 points;
- students are not allowed to take the exam if they scored less than 36 points during the semester;
- Students are not allowed to take the exam if they have not completed and defended the abstract during the semester.

Критерії оцінювання на іспиті / Exam evaluation criteria

Завдання/ Task	**Тема завдання / Task topic**	**Максимальний відсоток від 40 балів/ Maximum percentage of 40 points**	**Всього відсотків/ Total**
Завдання 1 / Task 1	Теоретичне питання за матеріалами курсу / Theoretical question on the course materials	40%	40%
Завдання 2 / Task 2		По 30%	60%
Завдання 3 / Task 3			
			100%

7.2. Організація оцінювання / Evaluation organization::

Обов'язковим є виконання завдань, винесених на самостійну роботу, та захист реферату.

/
It is mandatory to complete the tasks assigned to independent work and defend the abstract.

Терміни проведення форм оцінювання / Terms of evaluation forms:

1. *Захист реферату: до 10-го тижня навчального періоду.*
2. *Виконання завдань, винесених на самостійну роботу: протягом семестру.*
3. *Активна робота на лекції, усні відповіді: : протягом семестру*;

/

1. Defense of the abstract: up to the 10th week of the academic period.

2. Tutorial exercises: during the semester.

3. Active participation in lectures, oral answers: during the semester.

7.3. Шкала відповідності оцінок / Mark correspondence scale

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

8. STRUCTURE OF THE DISCIPLINE. THEMATIC PLAN OF LECTURES (СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ)

№	Lecture title (Назва лекції)	Лекції Lectures	Самостійна робота Individual work
1	**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) **Тема1.** Вступ. Поняття ентропії. Підхід Шеннона. Метрика Хеммінга. Моделі комунікацій через канали з шумом та присутності зловмисника. *Індивідуальна робота.* Підрахувати ентропію текстів (Wikipedia, тексти за вибором)	6	12
2	**Theme 2.** Forward error correction codes. Hamming codes. Convolution codes. Viterbi decoder. Reed-Solomon codes. *Individual work:* To program Hamming's algorithm. **Тема 2.** Коди що виправляють похибки. Коди Хеммінга. Конволяційні коди. Декодер Вітербі. Коди Ріда-Соломона. *Індивідуальна робота.* Запрограмувати алгоритм Хеммінга.	4	14

3	**Theme 3.** Data compression. Instantaneous codes. Prefix codes. Kraft-MacMillan inequalities. Pattern codes. Completeness. *Individual work:* Create some (individual) prefix codes **Тема 3.** Стикання даних. Миттєві коди. Префіксні коди. Нерівність Крафта-МакМіллана. Патерні коди. Повнота. *Індивідуальна робота.* Створити якийсь (свій) префіксний код.	4	14
4	**Theme 4.** Huffman codes. Burrous- Wheeler transform. Lempel-Ziv-Welsh compression algorithm. *Individual work:* To program Huffman codes. To program Burrous- Wheeler transform. **Тема4.** Коди Хаффмана. Перетворення Барроуза-Вілера. Алгоритм Лемпела-Зіва-Велша. *Індивідуальна робота:* Запрограмувати коди Хаффмана та перетворення Барроуза-Вілера	4	14
5	**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. **Тема 5.** Основні парадигми криптографії з відкритими ключами. Односторонні функції. Алгоритм Діффі-Хеллмана. Груповий ДХ алгоритм. Коаліційні протоколи. *Індивідуальна робота:* Запрограмувати ГДХ-алгоритм для 3 користувачів.	6	14
6	**Theme 6.** RSA and similar protocols for transfer. Pailier and Benaloh schemes. *Individual work* To program Pailier or Benaloh schemes **Тема 6.** RSA та подібні протоколи. Схеми Пєйе та Бенало. *Індивідуальна робота:* Запрограмувати схему Пєйе або Бенало.	6	14
7	**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. **Тема 7.** Цифрові підписи. Підписи на еліптичних кривих. Групові підписи. Кольцові підписи. Підписи для крипто валют. Методи автентифікації.	6	12

	Індивідуальна робота: Розробити сліпий та 2 із 3 підписи.		
8	**Theme 8.** Hash-functions. MD 5 and SHA functions. Mercle tree. Block-chain technology. Bit-coin network *Individual work:* To study the structure of SHA and MD5 hash-algorithms. **Тума 8.** Геш-функції. MD 5 і SHA функції. Дерево Меркля. Блокчейн технології. Мережа біткоін. *Індивідуальна робот* Вивчити структуру MD 5 та SHA геш алгоритмі**в.**	4	14
		40	**108**

Total duration / загальний об'єм *150 hours*, namely:
Lectures/Лекцій – **40** *hours/годин*,
Consultations/Консультації - **2** *hours/годин.*
Individual work/Самостійна робота– **108** *hours/годин***.**

9. Recommended sources / Рекомендовані джерела (Доступні через Internet)

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
5. O. Goldreich, Foundations of Cryptography, Cambridge University Press, 2004, 372p.

Additional / Додаткові:

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