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» 08 2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ІНФОРМАЦІЙНА БЕЗПЕКА/ INFORMATION SECURITY

для студентів / for students

галузь знань	**12 «Інформаційні технології» / "Information Technologies"**
спеціальність	**122 «Комп'ютерні науки» / "Computer Science"**
освітній рівень	**магістр / masters**
освітньо-наукова програма	**«Штучний Інтелект» / "Artificial Intelligence"**
вид дисципліни	**обов'язкова/ mandatory**

Форма навчання	**денна / заочна**
Навчальний рік	**2019/2020**
Семестр	**1**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**англійська, українська /English, Ukrainian**
Форма заключного контролю	**іспит / exam**

Викладачі: **професор ОлійникАндрій Степанович,д.ф.-м.н.**

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

КИЇВ – 2019

Розробник: **Олійник Андрій Степанович**, д. ф.-м. н., професор кафедри математичної інформатики

ЗАТВЕРДЖЕНО
Завідувач кафедри математичної інформатики

_____Терещенко В.М.
(підпис)

Протокол № 10 від «23» 05 2019 р.

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

Протокол від "30" 08 2019 року № 1

Голова науково-методичної комісії _____ (Омельчук Л.Л.)
(підпис)

1. Мета дисципліни: дати знання про захист сучасних інформаційних систем, захист персональних даних та захист комп'ютерних мереж, зрозуміти ключові терміни та поняття в інформаційній безпеці, зрозуміти криптографію, її розвиток та деякі ключові методи шифрування, що використовуються сьогодні, а також криптографічні протоколи.
/
Discipline aim. To give knowledge about securing modern information systems, protect personal data, and secure computer networks, understand key terms and concepts in information security, gain an understanding of cryptography, how it has evolved, and some key encryption techniques used today, as well as cryptographic protocols.

2. Попередні вимоги до опанування або вибору навчальної дисципліни/:

Preliminary demands to master or choice of the course discipline:

1. *Знати*: основні компоненти інформаційних систем, основи алгебри, теорії ймовірностей та теорії чисел. Знання технічної англійської мови на рівні B1.
2. *Вміти*: розробляти, аналізувати та застосовувати програмні системи для розв'язання завдань та прикладних задач, використовуючи сучасні методи розробки програм.

/

1. To know: basic components of information systems, foundations of algebra, probability theory and number theory. Level B1 technical English skills.
2. To be able to: develop, analyse and apply software systems to solve problems and applied tasks using modern software development methods.

3. Анотація навчальної дисципіни / Synopsis of the course:

Навчальна дисципліна «Інформаційна безпека» є обов'язковою навчальною дисципліною у складі освітньо-наукової програми підготовки фахівців «Штучний інтелект» за другим (магістерським) рівнем вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки». Вона забезпечує професійний розвиток студентів магістратури, спрямована на формування теоретичних основ та практичних навичок забезпечення безпеки інформаційних систем, дослідження і використання криптографічних алгоритмів і протоколів для досягнення цілей інформаційної безпеки.

Дана дисципліна є обов'язковою навчальною дисципліною за *програмою "Штучний інтелект"*. Викладається у 1 семестрі 1 курсу магістратури в обсязі – *5 кредитів ECTS*.

У курсі передбачено 2 *змістових частини*, 1 *колоквіум*, *6 лабораторних робіт*. Завершується дисципліна екзаменом в 1 семестрі 1 курсу магістратури.

/

The discipline "Information Security" belongs to the list of mandatory discipline. It provides professional development for graduate students, aimed at forming the theoretical foundations and practical skills of information systems security, research and use of cryptographic algorithms and protocols to achieve information security goals.

4. Завдання (навчальні цілі)/ Objectivesofstudy:

Основними завданнями дисципліни «Інформаційна безпека» є набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень в області 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 проектувати та забезпечувати впровадження серверної інфраструктури корпоративного центру обробки даних компанії (СК17).
  /

Objectives (learning objectives): acquiring knowledge, skills and competences at the level of the latest achievements in programming, according to the scientific and educational qualification of "Master". In particular, to develop:

- The ability to think, analyze and synthesize abstract
- The ability to communicate in a foreign language.
- The ability to investigate the functional and economical efficiency and reliability of information systems.
- The ability to design and implement the server infrastructure of corporative level datacenter.

5.Результати навчання за дисципліною/ Results of learning:

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	Знати основні завдання інформаційної безпеки, загрози та вразливості/ To know main goals of information security, vulnerabilities and threats	*Лекція/ Lecture*	*Колоквіум (60% правильних відповідей), екзамен, лабораторні роботи 1–5/* Colloquium (60% correct answers), exam, labs	*20%*
РН 1.2	Знати основні криптографічні інструменти для досягнення цілей інформаційної безпеки / To know the basic cryptographic tools to achieve information security goals			
РН 1.3	Знати математичні основи криптографічних алгоритмів/ To know mathematical foundations of cryptographic algorithms			*20%*
РН 1.4	Знати основні криптографічні протоколи/ To know the basic cryptographic protocols			
РН 2.1	Вміти розробляти і аналізувати засоби інформаційної безпеки/ Be able to develop and analyze information security tools	*Лекція, лабораторна робота, самостійна робота/ Lecture, lab,individual work*	*Колоквіум (60% правильних відповідей), екзамен, лабораторні роботи 1–5/* Colloquium (60% correct answers), exam, labs	*20%*
РН 2.2	Вміти застосовувати криптографічні засоби для забезпечення інформаційної безпеки/ Be able to use cryptographic tools to ensure information security			*20%*
РН 2.3	Вміти застосовувати програмні засоби розробки систем / Be able to use systems development tools	*Лабораторна робота, самостійна робота/ Lab, individualwork*	*Лабораторні роботи 1–5/Labs*	*5%*
РН3.1	Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань проектування та розробки програм, складати письмові звіти / Be able to justify own view of the problem, communicate with colleagues in the design and development of programs, prepare written reports			*5%*
РН4.1	Демонстрація авторитетності, інноваційності, високого ступеня самостійності, академічної та професійної доброчесності, послідовної відданості розвитку нових ідей або процесів у передових			*5%*

	контекстах професійної та наукової діяльності, що стосується теорії та технології програмування. / Demonstration of authority, innovativeness, high degree of independence, academic and professional integrity, consistent dedication to the development of new ideas or processes in advanced contexts of professional and scientific activity related to the theory and technology of programming.			
РН4.2	Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість / Responsibly treat the works performed, be responsible for their quality			*5%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання / Correspondensebetweenlearningresultsandprogramstudyresults

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)										
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.	+	+	+			+	+	+	+	+
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.				+	+		+			

7. Схема формування оцінки.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду:

1. Колоквіум: РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2 – 15 балів/9 балів;

2. Лабораторні роботи: РН1.3, РН1.4, РН2.1, РН2.2, РН2.3, РН3.1, РН4.1, РН4.2 – 45 балів/27 балів;

- 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, РН2.1, РН2.2;
- *форма проведення і види завдань:* письмова робота.
- *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.

Критерії оцінювання на іспиті

Завдання	Тема завдання	Максимальний відсоток від 40 балів	Всього відсотків
Завдання 1	Теоретичне питання за матеріалами курсу	40%	40%
Завдання 2		По 30%	60%
Завдання 3			
			100%

Для отримання загальної позитивної оцінки з дисципліни оцінка за екзамен не може бути меншою 24 балів. Студент не допускається до екзамену, якщо під час семестру набрав менше 20 балів.

Умови лабораторних робіт/Laboratory works:

Приклад лабораторної роботи:

Імплементувати задані алгоритми симетричного блочного шифрування. Порівняти швидкості шифрування для заданих режимів шифрування. Підготувати звіт і вихідний код.

Sample Lab:

Implement given algorithms of symmetric block encryption. Compare encryption speeds for given encryption modes. Prepare report and source code.

Запитання до колоквіуму/Test questions

Приклади завдань:

1. Поняття про вразливості.
2. Синтаксис криптосистем з секретним ключем.
3. Побудувати модель загроз конфіденційності даних у смартфоні.

Sample tasks:

1. Vulnarability notion.
2. Syntax of secret key cryptosystems.
3. Treat modelling for data confidentiality in smartphone.

7.2. Організація оцінювання:

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

Терміни проведення форм оцінювання:

1. Колоквіум: до 8 тижня навчального періоду.

2. Лабораторні роботи 1–5: до 4,5,6,8,10 тижнів навчального періоду відповідно.

У випадку відсутності студента з поважних причин відпрацювання та перездачі лабораторних робіт і колоквіуму здійснюються у відповідності до „Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу" від 1 жовтня 2010 року.

7.3. Шкала відповідності оцінок

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

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№	Назва лекції	Кількість годин		
		Лекції	Лабораторні	Самостійна робота
Частина 1.«Основні цілі інформаційної безпеки» Part 1. "Main goals of information security"				
1	**Тема 1.** Основні завдання інформаційної безпеки.Вразливості і загрози. *Самостійна робота:* Вивчити причини загроз і вразливостей на прикладах . / **Theme 1.**Main tasks of information security. Vulnerabilities and threats. *Individual work:* Case study of reasons why vulnerabilities and threats appear.	2		6
2	**Тема 2.**Атаки на інформаційні системи. Моделювання загроз. Розробка засобів безпеки. *Самостійна робота:* Моделювання загроз на прикладах. / **Theme2**.Attacks on information systems. Threat modelling. Design of security solutions. *Individual work:* Case study of threat modelling.	2		6
3	**Тема 3.**Симетричні шифри для забезпечення конфіденційності даних. Потокові режими. *Самостійна робота:* Вивчити стандарти симетричного шифрування. / **Theme 3**. Symmetric ciphers for dataconfidentiality. *Individual work:* Study standards for symmetric encryption. Stream modes.	4	2	10
4	**Тема 4.** Потокові шифри. *Самостійна робота:* Вивчити методи шифрування сховищ даних. / **Theme 4**. Stream ciphers. *Individual work:* Study methods to encrypt data storages.	2	2	6
5	**Тема 5.**Криптографічні хеш функції для	4	2	12

	забезпечення цілісності даних. Схеми доповнення. Функції генерування ключів. *Самостійна робота:* Вивчити стандарти криптографічного хешування. Технології блокчейну. / **Theme 5**. Cryptographic hash functions for data integrity. Padding schemes. Key derivation functions. *Individual work:* Study standards for cryptographic hashing. Blockchain technologies.			
	Колоквіум / *Colloquium.*	2		
Частина 2.«Забезпечення завдань інформаційної безпеки засобами криптографії з публічним ключем»/ Part 2. "Ensuring information security tasks by means of public key cryptography"				
6	**Тема 6.**Криптосистеми з публічним ключем. *Самостійна робота:* Вивчити методи ймовірносного шифрування. / **Theme 6.** Public key cryptosystems. *Individual work:* Study methods of probabilistic encryption.	2	2	10
7	**Тема 7.**Схеми цифрового підпису та коди аутентифікації повідомлень. *Самостійна робота:* Вивчити стандарти цифрових підписів. / **Theme 7.** Schemes of digital signatures and message authentication codes. *Individual work:* Study standards for digital signatures.	2	2	10
8	**Тема 8.**Математичні основи криптографії на основі еліптичних кривих. Задача дискретного логарифма. *Самостійна робота:* Вивчити алгоритми розв'язування задачі дискретного логарифма. / **Theme 8.** Mathematical foundations of elliptic curve cryptography. Discrete logarithm problem. *Individual work:* Study algorithms for solving discrete logarithm problem.	2	2	10
9	**Тема 9.** Протоколи узгодження ключів. Безпека даних в інтернеті. *Самостійна робота:* Вивчити формальні методиа налізу протоколів узгодження ключів. / **Theme 9.** Key establishment protocols. Internet data security. *Individual work:*	4		10

	Study formal methods of analysis of key establishment protocols.			
ВСЬОГО/ TOTAL		26	12	80

Загальний обсяг ***120*** *годин*, в тому числі / **Total duration** ***120*** *hours*, namely:
Лекції/ Lectures – **26** *годин / hours*,
Лабораторні/Labs – **12** годин / *hours***,**
Консультації / Consultations – **2** *години / hours.*
Самостійна робота / Individual work – **80** *годин / hours***.**

9. Рекомендовані джерела / Literature

Основні / Main:

1. H.Bidgoli (Ed.) *Handbook of Information Security, Volume 1*. JohnWiley&SonsInc., 2006.
2. H.Bidgoli (Ed.) *Handbook of Information Security, Volume 2*. JohnWiley&SonsInc., 2006.
3. H.Bidgoli (Ed.) *Handbook of Information Security, Volume 3*. JohnWiley&SonsInc., 2006.
4. N.Smart *Cryptography made simple*. Springer, 2016.
5. О.Вербіцький *Вступ до криптології.* ВНТЛ, 1998.

Додаткові / Additional:

6. J. Katz, Y. Lindell *Introduction to modern cryptography*. CRC Press, 2015.
7. A. Narayanan, J. Bonneau, Ed. Felten, A. Miller, S. Goldfeder *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton University Press, 2016.
8. C. Paar, J. Pelzl *Understanding cryptography.* Springer, 2010.