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 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ БЕЗПЕКА ДАНИХ У МАШИННОМУ НАВЧАННІ/ DATA SECURITY IN MACHINE LEARNING

для студентів / for students

галузь знань	**12 – Інформаційні технології / Information Technologies** *(шифр і назва)*
спеціальність	**122 – Комп'ютерні науки / Computer Science** *(шифр і назва спеціальності)*
освітній рівень	**магістр / Master's educational level** *(молодший бакалавр, бакалавр, магістр)*
освітня програма	**Штучний інтелект / Artificial Intelligence** *(назва освітньої програми)*
вид дисципліни	**вибіркова / selective**

Форма навчання	**денна**
Навчальний рік	**2020/2021**
Семестр	**4**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська, англійська/ Ukrainian, English**
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 – 2020

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

ЗАТВЕРДЖЕНО
Завідувач кафедри математичної інформатики

_____ Терещенко В.М.
(підпис)

Протокол № 1 від «28» 08 2020 р.

ЗАТВЕРДЖЕНО
Зав. кафедри теоретичної кібернетики

_____ (Крак Ю.В.)
(підпис) (прізвище та ініціали)

Протокол № 1 від «27» 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: 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 «Безпека даних у машинному навчанні» 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 2 семестрі 2 курсу магістратури в обсязі – 4 *кредитів ECTS*.

У курсі передбачено 2 *змістових частини*, 1 *колоквіум, 3 лабораторні роботи*. Завершується дисципліна іспитом в 4 семестрі.

/

The discipline "Data security in machine learning" 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 « Безпека даних у машинному навчанні» 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 спілкуватися іноземною мовою (ЗК5).
- Здатність до проектування та реалізації систем штучного інтелекту. (СК21.2).

/

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 communicate in a foreign language.
- The ability to design and implement artificial intelligence systems.

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, іспит, лабораторні роботи/* Colloquium, exam, labs	*20%*
РН 1.2	Знати основні інструменти для безпечного навчання/ To know the basic tools for secure learning			
РН 1.3	Знати математичні основи криптографічних алгоритмів/ To know mathematical foundations of cryptographic algorithms			*20%*
РН 1.4	Знати основні криптографічні протоколи для безпечного навчання/ To know the basic cryptographic protocols for secure learning			
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, іспит, лабораторні роботи/* Colloquium, exam, labs	*20%*
РН 2.2	Вміти застосовувати криптографічні засоби для забезпечення інформаційної безпеки в машинному навчанні/ Be able to use cryptographic tools to ensure information security in machine learning			*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, Іспит/Lab, exam*	*5%*
РН3.1	Обгрунтовувати 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 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			*5%*

	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)										
ПРН19.2. Знати, аналізувати, вибирати та кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних у машинному навчанні. / Know, analyze, select and apply qualified means of ensuring information security and data integrity in machine learning.	+	+	+	+	+	+	+	+	+	+

7. Схема формування оцінки/ Mark forming scheme.

7.1. Форми оцінювання студентів/ Student evaluation forms:

- оцінювання впродовж навчального періоду/evaluation in semester:

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

2. Лабораторні роботи 1-3 / Laboratory Works 1-3: РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2, РН2.3, РН3.1, РН4.1, РН4.2 – 45 балів (points)/27 балів (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, РН2.1, РН2.2, РН3.1, РН4.1, РН4.2;
- *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.

- the maximum number of points that can be obtained by a student: 40 points;
-learning outcomes that will be evaluated: РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2, РН3.1, РН4.1, РН4.2;
- form of conducting and types of tasks: written work;

- types of tasks: 3 written tasks (3 theoretical questions);
- to obtain an overall positive grade in the discipline, the grade for the exam must be not less than 24 points;
- a student is not allowed to take the exam if he scored less than 36 points during the semester;
- a students are not allowed to take the exam if they have not completed and defended the abstract during the semester..

Критерії оцінювання на іспиті / Examination criteria for the exam

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

Умови лабораторних робіт/Laboratory works:

Приклад лабораторної роботи:

Застосувати один з методів федеративного навчання для тренування моделі. Підготувати звіт і вихідний код.

Sample Lab:

Apply one of the methods of federated learning for model training. Prepare report and source code.

Запитання до колоквіуму/Test questions

Приклади завдань:

1. Поняття про вразливості. Приклади.
2. Означення диференційної приватності.
3. Схеми федеративного навчання.

Sample tasks:

1. Vulnarability notion. Examples.
2. Definition of differential privacy.
3. Schemes of federated learning.

7.2. Організація оцінювання / Evaluation organization:

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 1–3: до 4,7,10 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.

/ Terms of evaluation forms:

1. Colloquium: during the semester.;
2. Laboratory Works 1-3: up to 4,7,10 weeks of the training period, respectively.

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. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ / STRUCTURE OF THE DISCIPLINE. THEMATIC PLAN OF LECTURES

№	Назва лекції	Кількість годин		
		Лекції	Лабораторні	Самостійна робота
Частина 1.«Методи безпечного навчання» Part 1. "Methods of secure learning"				
1	**Тема 1.** Вразливості і загрози в машинному навчанні. Приватність даних і цілісність моделей. *Самостійна робота:* Вивчити причини та наслідки загроз і вразливостей на прикладах. / **Theme 1.**Vulnerabilities and threats in machine learning. Data privacy and consistency of models. *Individual work:* Case study of reasons and consequences of vulnerabilities and threats.	1		16
2	**Тема 2.** Диференційна приватність. *Самостійна робота:* Вивчити методи диференційної приватності. / **Theme 2**.Differential privacy. *Individual work:* Study of methods of differential privacy.	2		16
3	**Тема 3.** Федеративне навчання. *Самостійна робота:* Вивчити методи федеративного навчання. / **Theme 3**. Federated learning. *Individual work:* Study methods of federated learning.	2	6	20
Колоквіум / Colloquium.		1		
Частина 2.«Криптографічні інструменти безпечного навчання»/ Part 2. "Cryptographic tools for secure learning"				
4	**Тема 4.** Розподіл секрету і доведення без розголошення. *Самостійна робота:*	2	4	20

	Вивчити методи доведень без розголошення. / **Theme 4.** Secret sharing and zero knoeledge proofs. *Individual work:* Study methods of zero knowledge proofs.			
5	**Тема 5.** Гомоморфне шифрування. *Самостійна робота:* Вивчити методи гомоморфного шифрування. / **Theme 5.** Homomorphic encryption. *Individual work:* Study methods of homomorphic encryption.	2	4	20
ВСЬОГО/ TOTAL		10	14	92

Загальний обсяг ***120*** *годин*, в тому числі / **Total duration** ***120*** *hours*, namely:
Лекції/ Lectures – **10** *годин / hours*,
Лабораторні/Labs – **14** годин / *hours***,**
Консультації / Consultations – **4** *години / hours.*
Самостійна робота / Individual work – **92** *години / 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. J. Katz, Y. Lindell *Introduction to modern cryptography.* CRC Press, 2015.
5. C.Dwork, A.Roth. *The Algorithmic Foundations of Differential Privacy.* Foundations and Trends in Theoretical Computer Science, 2014, Vol. 9, Nos. 3–4, 211–407.
6. V.Mothukuri, R.Parizi, S. Pouriyeh, Y.Huang, A.Dehghantanha, G.Srivastava. *A survey on security and privacy of federated learning.* Future Generation Computer Systems, 2021, Vol. 115, 619-640.

Додаткові / Additional:

7. J.-P.Aumasson *Serious cryptography.* No starch press, 2018.
8. N.Smart *Cryptography made simple*. Springer, 2016.
9. Ian Goodfellow *Deep Learning.* MIT Press, 2017.