Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Голова НМК
_____ Д. М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Методи штучного інтелекту для кібербезпеки»
(назва навчальної дисципліни)

Галузь знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

Спеціальність:_____
(код та найменування спеціальності)

Освітня програма: _____
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

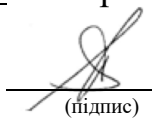
Харків 2023 рік

Робоча програма «Методи штучного інтелекту для кібербезпеки»
(назва дисципліни)

Розробник: Клюшніков І. М., доцент, к.т.н., с.н.с. 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2023 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="11">Галузь знань
10 «Природничі науки»,
11 «Математика та статистика»,
12 «Інформаційні технології»,
15 «Автоматизація та приладобудування»,
16 «Хімічна та біоінженерія»,
17 «Електроніка та телекомунікації»,
19 «Архітектура та будівництво»
(шифр та найменування)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2023/2024</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 64/150</td><td>2-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача освіти – 5</td><td>32 години</td></tr>
<tr><td>Практичні, семінарські[1)]</td></tr>
<tr><td>немає</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 години</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 64/86.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: надання здобувачам освіти необхідних знань, навичок та вмінь з використання різноманітних методів штучного інтелекту для забезпечення кібербезпеки інформаційних систем.

Завдання: формування у здобувачів освіти базових системних понять і навичок, цілісного бачення сучасного рівня основних характеристик апаратного (АЗ), системного та прикладного програмного забезпечення (ПЗ) інформаційних систем, виявлення їх вразливостей та застосування алгоритмів штучного інтелекту (ШІ), які дозволяють виявляти факти несанкціонованого втручання та запобігати порушенню кібербезпеки: принципи, методи й інструментальні засоби розробки засобів виявлення; посилення міждисциплінарних зв'язків, розвиток системного мислення, без яких неможливе ефективне використання інформаційних технологій, а також:

1) придбання знань про основні принципи побудови нейроннх мереж, експертних систем, а також онтологій та баз знань;
2) придбання знань про синтаксис мови програмування SWI-Prolog;
3) придбання знань про основи використання конструктора онтології Protege.

Компетентності, які набуваються:

– здатність вчитися і оволодівати сучасними знаннями;

– здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення;

– здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій;

– здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

Крім того, здобувачі освіти повинні мати:

– знання основ розробки штучних нейромереж, баз знань та онтологій;

– здатність використовувати SWI-Prolog для розроблення експертних систем штучного інтелекту;

– здатність використовувати Protege для розроблення онтології, що використовуються системами штучного інтелекту;

– здатність застосовувати отримані знання та навички в процесі подальшого навчання, при написані курсових і випускних робіт, а також у своїй подальшій професійній діяльності.

Очікувані результати навчання. В результаті вивчення дисципліни здобувачі освіти мають вміти застосовувати підходи та засоби для розв'язання задач забезпечення кібербезпеки із застосуванням методів штучного інтелекту.

Пререквізити – дисципліна є вибірковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки галузі знань 12 «Інформаційні технології».

Кореквізити – Відсутні.

3. Програма навчальної дисципліни

Модуль 1
Змістовий модуль 1

Тема 1. Застосування штучного інтелекту в задачах кібербезпеки
Історія розвитку штучного інтелекту. Напрямки досліджень в галузі штучного інтелекту. Напрямки застосування ШІ в кібербезпеці. Недоліки і проблеми сучасного штучного інтелекту

Тема 2. Базові поняття штучного інтелекту
Математичний нейрон. Активаційна функція. Завдання класифікації чисел. Персептрон. Алгоритм навчання персептрону.

Тема 3. Нейронні мережі
Історія виникнення. Застосування нейромереж. Штучна нейронна мережа. Типи нейронних мереж. Навчання нейромереж.

Тема 4. Експертні системи
Історія виникнення. Поняття експертної системи. Призначення та галузі застосування експертних систем. Архітектура експертної системи. Класифікація експертних систем. Розробка експертних систем. Базові функції.

Тема 5. Бази знань
Підходи до подання знань. Вербально-дедуктивне визначення знань. Дані та знання. Зв’язки між інформаційними одиницями. Проблема винятків. Властивості та моделі знань. Неоднорідність знань. Області і рівні знань. Моделі знань.

Тема 6. Інтелектуальні мультиагентні системи
Інтелектуальні агенти та мультиагентні системи. Архітектура мультиагентних систем. Колективна поведінка агентів. Координація поведінки агентів у мультиагентній системі.

Тема 7. Нечітка логіка
Історія виникнення. Теорія нечітких множин. Методи побудови функцій приналежності нечітких множин. Нечіткі оператори. Нечіткі множини в системах керування. Практичне застосування нечіткої логіки.

Тема 8. Онтології
Поняття про онтології. Елементи онтологій. Типи властивостей. Редактори онтологій.

Модульний контроль

Змістовий модуль 2

Тема 9. Кібербезпека і штучний інтелект
Основні тренди в забезпеченні кібербезпеки. Аспекти кібербезпеки. Штучний інтелект та кібербезпека. Існуючи рішення застосування ШІ для кібербезпеки.

Тема 10. Онтології в кібербезпеці.
Вступ до інженерії знань в кібербезпеці. Таксономія кібербезпеки. Верхні онтології. Онтології предметної галузі для кібербезпеки. Мережеві онтології.

Тема 11. Безпека систем машинного навчання
Вразливості алгоритмів машинного навчання. Модель загроз. Отруєння даними. Захист від отруєння. Атаки під час тестування та захист від них. Ворожа маніпуляція даними.

Тема 12. Прогнозування використання вразливостей
Введення в байєсовські мережи і класифікатори. Прогнозування експлойтів. Моделі прогнозування. Аналіз вразливостей та експлойтів. Ворожа маніпуляція даними.

Тема 13. Застосування штучного інтелекту для виявлення мережевих атак
Введення в бінарні класифікатори. Навчання бінарного класифікатора виявленню мережевих атак. Алгоритм виявлення мережевих атак. Схеми об’єднання бінарних класифікаторів.

Тема 14. Системи виявлення кібератак
Мережеві системи виявлення вторгнень: розгортання та методологія застосування. Машинне навчання в виявленні вторгнень: застосування нечіткої логіки та штучних нейронних мереж.

Тема 15. Аналіз вразливостей мобільних застосунків з використанням штучного інтелекту
Структура пакетів мобільних застосунків під Android. Методи виявлення шкідливого коду під Android. Підготовка наборів даних. Визначення вразливостей з допомогою машин опорних векторів та його переваги.

Тема 16. Кібербезпека для штучного інтелекту
Штучний інтелект як об’єкт для кібератак. Види атак на ШІ. Модель загроз. Методи забезпечення кібербезпеки ШІ.

Модульний контроль

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1					
Тема 1. Застосування штучного інтелекту в задачах кібербезпеки	9	2	-	2	5
Тема 2. Базові поняття штучного інтелекту	9	2	-	2	5
Тема 3. Нейронні мережи	9	2	-	2	5
Тема 4. Експертні системи	9	2	-	2	5
Тема 5. Бази знань	9	2	-	2	5
Тема 6. Інтелектуальні мультиагентні системи	9	2	-	2	5
Тема 7. Нечітка логіка	11	2	-	4	5
Тема 8. Онтології	6	1		-	5
Модульний контроль	1	1			
Разом за змістовим модулем 1	72	16	-	16	40
Змістовий модуль 2					
Тема 9. Кібербезпека і штучний інтелект	12	2	-	4	6
Тема 10. Онтології в кібербезпеці	8	2	-	-	6
Тема 11. Безпека систем машинного навчання	14	2	-	6	6
Тема 12. Прогнозування використання вразливостей	8	2	-	-	6
Тема 13. Застосування штучного інтелекту для виявлення мережевих атак	8	2	-	-	6
Тема 14. Системи виявлення кібератак	14	2	-	6	6
Тема 15. Аналіз вразливостей мобільних застосунків з використанням штучного інтелекту	7	2	-	-	5
Тема 16. Кібербезпека для штучного інтелекту	6	1		-	5
Модульний контроль	1	1			
Разом за змістовим модулем 2	78	16		16	46
Контрольний захід	-	-	-	-	-
Усього годин за дисципліною	**150**	**32**	**-**	**32**	**86**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Реалізація логічних функції математичним нейроном	2
2	Класифікація чисел з допомогою персептрону	2
3	Класифікація друкованих літер з допомогою персептрону	2
4	Класифікація рукописних літер з допомогою персептрону	2
5	Реалізація логічних функції двошаровим персептроном	2
6	Реалізація діагностичної нейромережи	2
7	Реалізація математичних функцій нейросимулятором	4
8	Створення онтологій шкідливого коду	4
9	Створення бази знань кіберзагроз	6
10	Створення нейромережи засобами Mathlab Simulink	6
	Разом	**32**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Забезпечення кібербезпеки інформаційних систем	5
2	Тест Тьюринга	5
3	Рекурентні нейромережи	5
4	Основи логіки предикатів	5
5	Основи мови Prolog	5

6	Програмні середовища для створення мультиагентних систем	5
7	Методи обробки нечітких знань	5
8	Основні можливості редактору онтологій Protege	5
9	Існуючі засоби кіберзахисту на основі ШІ	6
10	Типи властивостей в редакторі онтологій Protege	6
11	Типи атак на системи машинного навчання	6
12	Байесовські мережи	6
13	Бінарні класифікатори	6
14	Методи нечіткої логіки	6
15	Структура застосунків для Android	5
16	Застосування ШІ для кіберакак	5
	Разом	**86**

9. Індивідуальні завдання

Індивідуальні завдання не передбачені.

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів освіти за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

12.1. Розподіл балів, які отримують здобувачі освіти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Лабораторні заняття	0...5	7	0...35
Модульний контроль	0…25	1	0…25
Змістовий модуль 2			
Лабораторні заняття	0...5	3	0...15
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Білет для іспиту складається з двох теоретичних питань (25 балів за кожне питання), практичного завдання (25 балів) та тесту (25 балів).

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувачів освіти протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та завдання. Пройти тестування з модульних контролів.

Добре (75 – 89). Твердо знать мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основній та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор».

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=8281.

14. Рекомендована література

Базова

1. AI in Cybersecurity. Intelligent Systems Reference Library / ed. By L.F. Sikos. – Springer, 2019. – vol.151– 215 p.

2. Artificial Intelligence and Cybersecurity. Governance and Policy Challenges. – Centre for European Policy Studies (CEPS), 2021. – 122 p.

3. The NICE Cyber Security Framework Cyber Security Intelligence and Analytics / Izzat Alsmadi. – Springer, 2019. – 366 p.

4. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – Одеса: ОНАЗ ім. О.С. Попова, 2019. − 320 с.
5. Методи та системи штучного інтелекту: навчальний посібник / А.С. Савченко, О. О. Синельніков. – К. : НАУ, 2017. – 190 с.

Допоміжна

1. Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare / ed. by Thomas A. Johnson. – CRC Press, 2017. - 346 p.
2. Системи штучного інтелекту в плануванні, моделюванні та управлінні : підручник / Л.С. Ямпольський, Б.П. Ткач, О.І. Лісовиченко. – К. : ДП «Вид. дім «Персонал», 2017. – 544 с.

15. Інформаційні ресурси

1. A free, open-source ontology editor and framework for building intelligent systems [Ел. ресурс]. URL: https://protege.stanford.edu.
2. SWI-prolog [Ел. ресурс]. URL: https://www.swi-prolog.org.