«Затверджую»

Завідувач кафедри інформаційних технологій
проєктування та прикладної математики
_____ /Олександр ТЕРЕНТЬЄВ./
«____» _____2022 р.
Розробник силабусу
_____ /Людмила ТЕРЕЙКОВСЬКА/

СИЛАБУС
СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ
назва освітньої компоненти (дисципліни)

1) Шифр за ОНП: ОК 24
2) Навчальний рік: 2020/2021
3) Освітній рівень: перший рівень вищої освіти (бакалавр)
4) Форма навчання: денна
5) Галузь знань: 12 «Інформаційні технології»
6) Спеціальність: 125 «Кібербезпека»
8) Компонента спеціальності: обов'язкова
9) Семестр: 7
10) Цикл дисципліни: дисципліна фахової підготовки
11) Контактні дані викладача: к.т.н., доцент Терейковська Л.О., tereikovska.lo@knuba.edu.ua, http://www.knuba.edu.ua/?page_id=97786, https://scholar.google.com/citations?user=u1caKNcAAAAJ&hl=uk, (044) 241-54-02
12) Мова навчання: українська
13) Пререквізити: «Математичний аналіз», «Дискретна математика», «Теорія ймовірностей, ймовірнісні процеси та математична статистика», «Алгоритмізація та програмування», «Цифрова обробка сигналів», «Інженерія програмного забезпечення»
14) Мета курсу: придбання студентами теоретичних знань, практичних навичок та досвіду розробки систем штучного інтелекту.
15) Результати навчання:

№	Програмний результат навчання	Метод перевірки навчального ефекту	Форма проведення занять	Посилання на компетентності
1.	Знання теоретичних засад застосування нейромережевих методів і моделей інформаційної безпеки та/або кібербезпеки та вміння застосовувати нейромережеві методи і моделі інформаційної безпеки та/або кібербезпеки.	Обговорення під час занять, тематичне дослідження	Лекції, лабораторні заняття, курсова робота, самостійна робота, іспит	КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей

				інформаційної безпеки та/або кібербезпеки.
2.	Знання підходів до застосування засобів штучного інтелекту для здійснення процедур управління інцидентами, проведення розслідувань та їх оцінювання. Вміння застосувати засоби штучного інтелекту для здійснення процедур управління інцидентами, проведення розслідувань та їх оцінювання.	Обговорення під час занять, тематичне дослідження	Лекції, лабораторні заняття, курсова робота, самостійна робота, іспит	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
3.	Знання підходів до застосування засобів штучного інтелекту для моніторингу процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. Вміння застосувати засоби штучного інтелекту для моніторингу процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.	Обговорення під час занять, тематичне дослідження	Лекції, лабораторні заняття, курсова робота, самостійна робота, іспит	КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

16) Структура курсу:

Лекції, год	Практичне заняття, год	Лабораторні заняття, год	Курсовий проект/ курсова робота РГР/Контрольна робота	Самостійні робота здобувача, год	Форма підсумкового контролю
40	-	40	курсова робота	100	іспит
Сума годин:					
Загальна кількість (кредитів ECTS)				180 (6,0)	
Кількість годин (кредитів ECTS) аудиторного навантаження:				80 (2,67)	

17) Зміст курсу: (окремо для кожної форми занять – Л/Пр/Лаб/ КР/СРС)

Лекції:

<u>Змістовний модуль 1. Теорія штучного інтелекту</u>

1. Основні поняття штучного інтелекту

1.1. Поняття «штучний інтелект».

1.2. Етапи розвитку штучного інтелекту.

1.3. Основні напрямки досліджень: пошук рішень, доведення теорем, представлення знань, експертні системи, комп'ютерний зір.

1.4. Структура систем із штучним інтелектом.

2. Способи представлення задач та пошук рішень

2.1. Представлення задач у просторі станів.

2.2. Методи випадкового пошуку, пошук «в глибину та ширину».

2.3. Евристичний пошук.

2.4. Пошук рішень в ігрових програмах.

3. Представлення знань

3.1. Знання та їх представлення у системах штучного інтелекту.

3.2. Логічні моделі.
3.3. Продукційні моделі.
3.4. Семантичні мережі.
3.5. Фрейми.

4. Розпізнавання образів та навчання

4.1. Основні відомості про розпізнавання образів.
4.2. Геометричний та байесовський методи розпізнавання.
4.3. Рекурентні алгоритми навчання розпізнаванню образів.
4.4. Розпізнавання та навчання на основі моделей нейронних мереж.

5. Мова програмування Пролог та штучний інтелект

5.1. Загальна характеристика Пролог.
5.2. Синтаксис мови програмування Пролог.
5.3. Рішення задач штучного інтелекту на мові Пролог.

Змістовний модуль 2. Нейронні мережі

6. Принципи застосування нейронних мереж

6.1. Передумови застосування нейронних мереж.
6.2. Біологічний прототип штучного нейрону.
6.3. Основні поняття штучних нейронних мереж. Принципи функціонування.
6.4. Поняття синаптичного зв'язку.
6.5. Функція активації. Види активаційних функцій.
6.6. Архітектура нейронної мережі.
6.7. Методи використання нейронних мереж для вирішення практичних задач. Недоліки та переваги.

7. Багатошаровий персептрон

7.1. Структура багатошарового персептрону.
7.2. Функції активації вхідного, вихідного та схованих шарів.
7.3. Огляд методів навчання багатошарового персептрону.
7.4. Вербалізація персептрону.
7.5. Переваги та недоліки персептрону.
7.6. Приклади застосування персептрону для класифікації даних.

8. Алгоритм зворотнього розповсюдження помилки

8.1. Теоретичні основи алгоритму зворотнього розповсюдження помилки.
8.2. Похідна експоненціальної функції.
8.3. Визначення помилки навчання.
8.4. Поняття прямого та зворотнього проходів.
8.5. Розрахунок помилки навчання для вхідного, схованих та вихідного шарів нейронів.
8.6. Корекція вагових коефіцієнтів.
8.7. Приклад використання.

9. Нейронна мережа радіальної базисної функції

9.1. Структура мережі РБФ.
9.2. Теоретичне підґрунтя функціонування мережі РБФ.
9.3. Характеристика нейронних шарів. Особливості функції активації.
9.4. Типові задачі, що вирішуються за допомогою мережі РБФ.
9.5. Особливості навчання. Розрахунок параметрів функції Гауса.
9.6. Порівняння з багатошаровим персептроном.

10. Ймовірнісні нейронні мережі

10.1. Теоретичне підґрунтя функціонування ймовірнісних мереж.
10.2. Структура мережі PNN.
10.3. Характеристика нейронних шарів.
10.4. Особливості функцій активації.

10.5. Математичне забезпечення мережі.
10.6. Поняття запам'ятовування даних.
10.7. Особливості безітераційного навчання.
10.8. Функціонування в режим розпізнавання.
10.9. Порівняння з багатошаровим персептроном.
10.10. Типові сфери застосування.

11. Мережа адаптивної резонансної теорії

11.1. Загальна характеристика мережі адаптивної резонансної теорії.
11.2. Поняття динамічного запам'ятовування та резонансу.
11.3. Математичне забезпечення.
11.4. Структура зв'язків.
11.5. Особливості функцій активації.
11.6. Функціонування мережі адаптивної резонансної теорії в режимі навчання та в режимі розпізнавання.
11.7. Відбір інформативних ознак.
11.8. Переваги та недоліки адаптивної резонансної теорії.
11.9. Приклади практичного застосування. Шляхи розвитку**.**

12. Нейронні мережі, що самонавчаються

12.1. Задача кластеризації даних.
12.2. Принципи функціонування та базова модель нейронної мережі, що самонавчається.
12.3. Структура моделі Ліпмана-Хемінга.
12.4. Математичне забезпечення моделі.
12.5. Визначення параметрів моделі Ліпмана-Хемінга.
12.6. Розрахунок вагових коефіцієнтів.
12.7. Застосування моделі для кластеризації даних.

13. Топографічна карта Кохонена

13.1. Структура нейромережевої моделі типу топографічної карти Кохонена.
13.2. Поняття топографічного шару.
13.3. Особливості лінійної, квадратичної та гексагональної сітки зв'язків.
13.4. Математичне забезпечення моделі.
13.5. Навчання мережі. Принцип «переможець забирає все». Поняття радіусу навчання.
13.6. Особливості сучасних модифікацій. Нейронна мережа типу «пружна карта».
13.7. Приклади застосування карти Кохонена для кластеризації даних.

14. Згорткові нейронні мережі (CNN)

14.1. Загальна характеристика мережі CNN.
14.2. Процедура згортки в мережі CNN.
14.3. Процедура субдискретизації в мережі CNN.
14.4. Порівняльна характеристика багатошарового персептрону та CNN.
14.5. Математичне забезпечення мережі CNN.
14.6. Особливості застосування мережі CNN для розпізнавання зображень.

15. Рекурентні нейронні мережі

15.1. Загальні положення в області рекурентних нейронних мереж.
15.2. Мережі асоціативної пам'яті.
15.3. Рекурентні нейронні мережі на основі багатошарового персептрону.

16. Сучасні модифікації рекурентних нейронних мереж

16.1. Необхідність модифікації класичних RNN.
16.2. Мережі LSTM та GRU.
16.3. Програмна реалізація LSTM.

Змістовний модуль 3. Нейромережеві технології

17. Технологія створення навчальної вибірки для нейронних мереж

17.1. Загальні принципи створення навчальної вибірки для нейронних мереж.
17.2. Визначення параметрів навчальних прикладів.
17.3. Оцінка терміну створення навчальної вибірки.
17.4. Особливості формування маркованих та немаркованих прикладів.
17.5. Застосування експертних знань для створення навчальних прикладів.

18. Визначення доцільності застосування типу нейромережевої моделі

18.1. Загальні обмеження на застосування нейронних мереж для вирішення практичних задач.
18.2. Підходи до визначення доцільності застосування типу нейромережевої моделі.
18.3. Класифікація вимог до нейромережевих моделей.
18.4. Основні характеристики різних типів нейромережевих моделей.
18.5. Розробка критеріїв визначення доцільності.
18.6. Приклади визначення доцільності застосування нейромережевої моделі для вирішення практичних задач.

19. Застосування нейромережевих систем для аналізу зображень

19.1. Визначення допустимих видів та найбільш ефективного виду нейромережевої моделі для аналізу зображень.
19.2. Визначення множини вхідних та вихідних параметрів моделі.
19.3. Визначення архітектурних параметрів нейромережевої моделі для аналізу зображень.
19.4. Розрахунок вагових коефіцієнтів.
19.5. Технологія застосування моделі для аналізу зображень.

20. Застосування нейромережевих систем для розпізнавання мережевих вторгнень

20.1. Визначення допустимих видів та найбільш ефективного виду нейромережевої моделі для розпізнавання мережевих вторгнень.
20.2. Визначення множини вхідних та вихідних параметрів.
20.3. Визначення архітектурних параметрів нейромережевої моделі для розпізнавання мережевих вторгнень.
20.4. Розрахунок вагових коефіцієнтів.
20.5. Технологія застосування нейромережевої моделі для розпізнавання мережевих вторгнень.

Практичні заняття: немає.

Лабораторні заняття:

1. Реалізація багатошарового персептрону.
2. Реалізація ймовірнісної нейронної мережі.
3. Реалізація модулю розпізнавання рукописних цифр за допомогою багатошарового персептрону.
4. Розпізнавання двовимірних кольорових об’єктів за допомогою CNN.

Курсова робота:

1. Інтелектуальний модуль розпізнавання мережевої кібератаки типу neptune на базі ДШП з одним вихідним нейроном.
2. Інтелектуальний модуль розпізнавання мережевої кібератаки типу portsweep на базі PNN.
3. Інтелектуальний модуль розпізнавання мережевої кібератаки типу smurf на базі ДШП з двома вихідними нейронами.
4. Інтелектуальний модуль розпізнавання мережевої кібератаки типу rootkit на базі PNN.
5. Інтелектуальний модуль розпізнавання мережевої кібератаки типу Pod на базі ДШП з одним вихідним нейроном.
6. Інтелектуальний модуль розпізнавання мережевої кібератаки типу perl на базі PNN.
7. Інтелектуальний модуль розпізнавання мережевої кібератаки типу teardrop на базі ДШП з двома вихідними нейронами.
8. Інтелектуальний модуль розпізнавання мережевої кібератаки типу loadmodule на базі PNN.

9. Інтелектуальний модуль розпізнавання мережевої кібератаки типу land на базі ДШП з одним вихідним нейроном.
10. Інтелектуальний модуль розпізнавання мережевої кібератаки типу buffer_overflow на базі PNN.
11. Інтелектуальний модуль розпізнавання мережевої кібератаки типу back на базі ДШП з двома вихідними нейронами.
12. Інтелектуальний модуль розпізнавання мережевої кібератаки типу warezmaster на базі PNN.
13. Інтелектуальний модуль розпізнавання мережевої кібератаки типу guess_passwd на базі ДШП з одним вихідним нейроном.
14. Інтелектуальний модуль розпізнавання мережевої кібератаки типу multihop на базі PNN.
15. Інтелектуальний модуль розпізнавання мережевої кібератаки типу ftp_write на базі ДШП з двома вихідними нейронами.
16. Інтелектуальний модуль розпізнавання мережевої кібератаки типу phf на базі PNN.
17. Інтелектуальний модуль розпізнавання мережевої кібератаки типу imap на базі ДШП з одним вихідним нейроном.
18. Інтелектуальний модуль розпізнавання мережевої кібератаки типу imap на базі PNN.
19. Інтелектуальний модуль розпізнавання мережевої кібератаки типу phf на базі ДШП з двома вихідними нейронами.
20. Інтелектуальний модуль розпізнавання мережевої кібератаки типу ftp_write на базі PNN.
21. Інтелектуальний модуль розпізнавання мережевої кібератаки типу multihop на базі ДШП з одним вихідним нейроном.
22. Інтелектуальний модуль розпізнавання мережевої кібератаки типу guess_passwd на базі PNN.
23. Інтелектуальний модуль розпізнавання мережевої кібератаки типу warezmaster на базі ДШП з двома вихідними нейронами.
24. Інтелектуальний модуль розпізнавання мережевої кібератаки типу back на базі PNN.
25. Інтелектуальний модуль розпізнавання мережевої кібератаки типу buffer_overflow на базі ДШП з одним вихідним нейроном.
26. Інтелектуальний модуль розпізнавання мережевої кібератаки типу land на базі PNN.
27. Інтелектуальний модуль розпізнавання мережевої кібератаки типу loadmodule на базі ДШП з двома вихідними нейронами.
28. Інтелектуальний модуль розпізнавання мережевої кібератаки типу teardrop на базі PNN.
29. Інтелектуальний модуль розпізнавання мережевої кібератаки типу perl на базі ДШП з одним вихідним нейроном.
30. Інтелектуальний модуль розпізнавання мережевої кібератаки типу Pod на базі PNN.
31. Інтелектуальний модуль розпізнавання мережевої кібератаки типу rootkit на базі ДШП з двома вихідними нейронами.
32. Інтелектуальний модуль розпізнавання мережевої кібератаки типу smurf на базі PNN.
33. Інтелектуальний модуль розпізнавання мережевої кібератаки типу portsweep на базі ДШП з одним вихідним нейроном.

Самостійна робота студента (СРС):

1. Загальна характеристика мережі Коско.
2. Задача встановлення асоціації між невідомим вхідним образом та еталонним образом в мережі Коско.
3. Математичне забезпечення мережі Коско.
4. Структура зв'язків в мережі Коско.
5. Особливості функцій активації в мережі Коско.
6. Порівняння мережі Коско з мережею Хопфілда.
7. Визначення параметрів мережі Коско.
8. Функціонування мережі Коско в режимі навчання та в режимі розпізнавання.
9. Приклади практичного застосування мережі Коско.
10. Шляхи розвитку мережі Коско.
11. Особливості розпізнавання змісту текстової інформації.

12. Нестабільність кількості вхідних параметрів в мережах, призначених для розпізнавання змісту тексту.
13. Загальна характеристика семантичних нейронних мереж.
14. Структура зв'язків в семантичних нейронних мережах.
15. Особливості функцій активації в семантичних нейронних мережах.
16. Приклади практичного застосування семантичних нейронних мереж.
17. Шляхи розвитку семантичних нейронних мереж.

18) Основна література:

1. Корченко О. Методологія розроблення нейромережевих засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем: [Монографія] / О. Корченко, І. Терейковський, А. Білощицький. К. : ТОВ «Наш Формат». - 2016. – 246 с.
2. Міхайленко В. М. Нейромережеві моделі та методи розпізнавання фонем в голосовому сигналі в системі дистанційного навчання : [Монографія] / В. М. Міхайленко, Л. О. Терейковська, І. А . Терейковський., Б. Б. Ахметов. - К. : ЦП "Компринт", 2017.- 252 с.
3. Руденко О.Г. Штучні нейронні мережі. Навч. посіб. / О.Г. Руденко, Є.В. Бодянський. – Харків: ТОВ "Компанія СМІТ", 2006. – 404 с.
4. Tereykovska L., Tereykovskiy I., Aytkhozhaeva E., Tynymbayev S., Imanbayev A. Encoding of neural network model exit signal, that is devoted for distinction of graphical images in biometric authenticate systems // News of the national academy of sciences of the republic of Kazakhstan series of geology and technical sciences. Volume 6, Number 426 (2017), 217 – 224.
5. Bapiyev I. M., Aitchanov B. H., Tereikovskyi I. A., Tereikovska L. A., Korchenko A. A. Deep neural networks in cyber attack detection systems // International Journal of Civil Engineering and Technology (IJCIET) Volume 8, Issue 11, November 2017, pp. 1086–1092.
6. H. Zhengbing, I. Tereykovskiy, L. Tereykovska, V. Pogorelov. Determination of structural parameters of multilayer perceptron designed to estimate parameters of technical systems // Intelligent Systems and Applications, 2017, 10, P. 57-62

19) Додаткові джерела:

1. Oleksandr Oksiiuk, Liudmyla Tereikovska and Ihor Tereikovskiy. Determination of expected output signals of the neural network model intended for image recognition // 4th International Scientific-Practical Conference «Problems of Infocommunications Science and Technology» October 10 - 13, 2017, Ukraine, Kharkiv.
2. Hu, Z., Tereykovskiy, I., Zorin, Y., Tereykovska, L., Zhibek, A. Optimization of convolutional neural network structure for biometric authentication by face geometry // Advances in Intelligent Systems and Computing. 2018. Volume 754, pp 567-577.
3. Akhmetov, B., Tereikovskyi, I., Tereikovska, L., Adranova, A. Neural Network User Authentication by Geometry of the Auricle // Recent Developments in Data Science and Intelligent Analysis of Information Proceedings of the XVIII International Conference on Data Science and Intelligent Analysis of Information, June 4–7, 2018, Kyiv, Ukraine. Pages 11-19.
4. Tereikovskyi I. A., Chernyshev D. O., Tereikovska L.A., Mussiraliyeva Sh. Zh., Akhmed G. Zh. The Procedure For The Determination Of Structural Parameters Of A Convolutional Neural Network To Fingerprint Recognition. Journal of Theoretical and Applied Information Technology. 30th April 2019. Vol.97. No 8. Pages 2381-2392.
5. Tereikovskyi I., Tereikovska L., Korystin O., Mussiraliyeva S., Sambetbayeva A. (2020) User Keystroke Authentication and Recognition of Emotions Based on Convolutional Neural Network. In: Hu Z., Petoukhov S., He M. (eds) Advances in Artificial Systems for Medicine and Education III. AIMEE 2019. Advances in Intelligent Systems and Computing, vol 1126, pp 283-292.
6. http://library.knuba.edu.ua/
7. http://org2.knuba.edu.ua/course/view.php?id=2574

20) Система оцінювання навчальних досягнень (розподіл балів):

Поточне оцінювання			Підсумковий контроль (іспит)	Сума
Змістовні модулі				
1	2	3		
15	30	15	40	100

21) Умови допуску до підсумкового контролю:

- відвідування лекцій;
- виконання лабораторних робіт;
- дотримання термінів виконання лабораторних робіт;
- дотримання умов академічної доброчесності.

22) Політика щодо академічної доброчесності: розуміння здобувачами вищої освіти етичного кодексу університету та норм академічної доброчесності (вимог щодо оригінальності текстів та допустимого відсотку співпадінь)

23) Посилання на сторінку електронного навчально-методичного комплексу дисципліни:

https://teams.microsoft.com/_#/school/files/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9?threadId=19%3A2fc7c17ef76447b69962c010f7fa1f0d%40thread.tacv2&ctx=channel

http://org2.knuba.edu.ua/course/view.php?id=2574