Силабус освітнього компонента

Програма навчальної дисципліни

Нейронні мережі

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua

Кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Штучний інтелект і бізнес-аналітика", "Теорія інформації і кодування", "Технологія управління безпекою бізнес-процесів, "Агентне моделювання" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Нейронні мережі" є вибірковим освітнім компонентом. Вивчення даної дисципліни спрямовано на засвоєння основ роботи нейронних мереж та їхньої архітектури, вивчення сучасних методів навчання та оптимізації моделей, критичне оцінювання результатів роботи моделей, виявлення їх сильних та слабких сторін, а також розробку та покращення власних рішень в галузі кібербезпеки на основі нейронних мереж.

Мета та цілі дисципліни

Посилити сформовані теоретичні знання та практичні навички розробки, навчання та застосування нейронних мереж для вирішення різноманітних завдань на підставі застосування сучасних програмних продуктів та можливостей штучного інтелекту.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ6. Здатність аналізувати, контролювати та
забезпечувати систему управління доступом до
інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому..

Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Мережева та хмарна безпека.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Розробка інтелектуальних систем на основі моделей нейронних мереж. Огляд принципів побудови інтелектуальних систем, аналіз задач, які ефективно розв'язуються нейронними мережами. Вибір архітектури, збір даних, навчання та інтеграція моделей у реальні застосунки.	2
Тема 2. Нейронні мережі як ключовий інструмент для штучного інтелекту. ЧатGPT та його можливості. Вивчення ролі нейронних мереж у сучасному ШІ. Розгляд трансформерів, великих мовних моделей та принципів роботи ChatGPT. Приклади застосувань: генерація тексту, обробка мови, аналіз даних.	2
Тема 3. Нейронні мережі прямого та зворотного поширення сигналу. Розгляд роботи Feedforward Neural Networks (FNN) та алгоритму зворотного поширення похибки. Архітектури багатошарових персептронів, функції активації та процес оптимізації.	2
Тема 4. Нейронні мережі, що самонавчаються. Огляд самоорганізовних моделей: мереж Кохонена, автоенкодерів та методів кластеризації. Принципи безконтрольного навчання та їх застосування для виявлення структур у даних.	2
Тема 5. Глибинні нейронні мережі. Детальне вивчення глибоких архітектур: CNN, RNN, LSTM, GRU. Особливості навчання, регуляризації та оптимізації. Використання для розпізнавання зображень, мови, сигналів.	2
Тема 6. Радіальні базисні мережі.	2

Принципи роботи RBF-мереж: радіальні функції, центровані нейрони, швидке навчання. Застосування в інтерполяції, класифікації та апроксимації функцій.	
Тема 7. Гібридні нейронні мережі та системи нечіткого логічного виводу. Поєднання нейронних мереж із нечіткою логікою (ANFIS), генетичними алгоритмами та іншими методами ШІ. Використання гібридних підходів для складних задач керування, прогнозування та аналізу.	2
Тема 8. Методи штучного інтелекту в кібербезпеці. Використання нейронних мереж для виявлення аномалій, виявлення вторгнень, класифікації шкідливого ПЗ та аналізу мережевих загроз. Переваги ШІ у прогнозуванні та реагуванні на кіберінциденти.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Моделювання нейронних мереж з використанням одно- та багатошарового персептрона. Ознайомлення з принципами роботи персептрона, реалізація одношарових і багатошарових моделей. Навчання мереж за алгоритмом зворотного поширення помилки, аналіз точності та поведінки моделі на різних наборах даних.	6	0,2
Тема 2. Штучний інтелект: основи користування. Практичне знайомство з інструментами ШІ: інтерфейси, сервіси, моделі. Використання готових моделей для розв'язання базових задач: класифікації, прогнозування, генерації тексту. Основи безпечного та коректного застосування ШІ.	6	0,1
Тема 3. Побудова нейронної мережі в пакеті Statistica Neural Networks. Створення, налаштування та навчання нейронних мереж у середовищі Statistica. Використання вбудованих інструментів для аналізу помилок, вибору архітектури, оптимізації параметрів та оцінки результатів.	4	0,1
Тема 4. Кластеризація та класифікація з використанням нейронної мережі Кохонена. Створення самоорганізовної карти (SOM), навчання без учителя, кластеризація даних. Візуалізація результатів, аналіз структури кластерів і застосування SOM для задач класифікації.	4	0,1
Тема 5. Моделювання радіальних базисних мереж. Побудова RBF-мереж, вибір центрів радіальних функцій, навчання та перевірка моделі. Застосування RBF для задач апроксимації та класифікації, порівняння з персептроном.	4	0,1
Тема 6. Розроблення нечіткої моделі гібридної мережі для розв'язання задачі прогнозування. Створення гібридних нейронно-нечітких систем (ANFIS). Формування нечітких правил, навчання параметрів моделі, побудова системи прогнозування та аналіз її точності.	4	0,1
Тема 7. Застосування методів штучного інтелекту для задач	4	0,1

кібербезпеки та безпеки мереж. Використання моделей ШІ для виявлення аномалій, аналізу мережевого трафіку, класифікації шкідливих дій. Оцінка ефективності, вибір алгоритму та практичне налаштування моделі для кіберзахисних систем.		
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи нейронних мереж та базові архітектури штучного інтелекту. Інтелектуальні системи на основі нейронних мереж; роль нейронних мереж у ШІ; принципи роботи ChatGPT та трансформерів; мережі прямого та зворотного поширення; самонавчальні мережі та алгоритми безконтрольного навчання.	0,1
Тема 2. Глибокі, спеціалізовані та гібридні нейронні мережі. Методи ШІ у кібербезпеці. Глибинні нейронні мережі: CNN, RNN, LSTM; радіально-базисні мережі; гібридні нейронно-нечіткі системи; використання нейронних мереж у завданнях кібербезпеки та виявлення аномалій.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Трансформери та сучасні архітектури глибокого навчання. BERT, GPT, Vision Transformers — принципи роботи та сфери застосування.	8
Тема 2. Конволюційні нейронні мережі нового покоління. ResNet, EfficientNet, MobileNet, DenseNet — оптимізація, пропускні зв'язки, параметри.	8
Тема 3. Рекурентні моделі та моделювання послідовностей. LSTM, GRU, Temporal Convolutional Networks, attention-механізми.	7
Тема 4. Генеративні моделі. Autoencoders, Variational Autoencoders (VAE), Generative Adversarial Networks (GANs).	7
Тема 5. Навчання з підкріпленням (Reinforcement Learning). Q-learning, Deep Q-Networks, політики, застосування в робототехніці й іграх.	7
Тема 6. Інтерпретованість та пояснюваність нейронних мереж (Explainable AI). SHAP, LIME, CAM, Grad-CAM — пояснення рішень моделей.	7
Тема 7. Методи регуляризації та стабілізації навчання. Dropout, Batch Normalization, Layer Normalization, Weight Decay, Data Augmentation.	7

Тема 8. Оптимізація нейронних мереж. Adam, RMSProp, Learning Rate Schedulers, warm restarts, early stopping.	7
Тема 9. Розгортання моделей ШІ та MLOps. ONNX, TensorRT, Docker, Kubernetes, CI/CD, моніторинг моделей у продакшні.	7
Тема 10. Етичні аспекти та безпека штучного інтелекту. Байдужість моделей, упередження даних, атаки на ШІ (adversarial attacks), відповідальне використання.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Субботін С. О. Нейронні мережі : теорія та практика: навч. посіб. / С. О. Субботін. Житомир : Вид. О. О. Євенок, 2020. 184 с. [Електронний ресурс]. – Режим доступу : https://eir.zp.edu.ua/server/api/core/bitstreams/2abb401b-9ee6-4afc-a92a-2de5c332d12f/content
2. Ткаліченко С.В. Штучні нейронні мережі: Навчальний посібник. Кривий Ріг: Державний університет економіки і технологій, 2023. 150 с. [Електронний ресурс]. – Режим доступу : https://dspace.duet.edu.ua/jspui/handle/123456789/892
3. Терейковський І. А., Бушуєв Д. А., Терейковська Л. О. Штучні нейронні мережі: базові положення: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 123 с. [Електронний ресурс]. – Режим доступу : https://ela.kpi.ua/server/api/core/bitstreams/9fee52b6-83fc-4e99-8541-c2767f634c7c/content.
4 Троцько В.В. Методи штучного інтелекту: навчально-методичний і практичний посібник. Київ: Університет економіки та права «КРОК», 2020 86 с. [Електронний ресурс]. – Режим доступу : https://library.krok.edu.ua/media/library/category/navchalni-posibniki/trotsko_0001.pdf.

Додаткова література

5. Інтеллектуальні методи в управлінні: навчальний посібник / Л. В. Дранишников. Кам'янське: ДДТУ, 2018. 416 с. [Електронний ресурс]. – Режим доступу : https://www.dstu.dp.ua/Portal/Data/3/19/3-19-b7.pdf
6. Методи штучного інтелекту в кібербезпеці: Практикум [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна Київ : КПІ ім. Ігоря Сікорського, 2022. 18 с. [Електронний ресурс]. – Режим доступу : https://ela.kpi.ua/handle/123456789/47605
7. Нейронні мережі в моделюванні економічних систем: метод. рекомендації до виконання практичних робіт для студентів спеціальності 051 «Економіка» / уклад. І.М. Пістунов. Дніпро: НТУ «ДП», 2023. 17 с. [Електронний ресурс]. – Режим доступу : http://pistunovi.inf.ua/NEURONET_LABS.pdf

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.

Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Ольга КОРОЛЬ