



Силабус освітнього компонента

Програма навчальної дисципліни



Нейронні мережі

Шифр та назва спеціальності

К4 – Управління інформаційною безпекою

Інститут

ІНІ комп'ютерних наук та інформаційних технологій (320)

Спеціалізація

-

Кафедра

Кібербезпеки (328)

Освітня програма

Управління інформаційною безпекою

Тип дисципліни

Вибіркова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна

Семестр

6

Мова викладання

Українська

Викладачі, розробники

**АКСЬОНОВА Ірина Вікторівна**

Iryna.Aksonova@khpі.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 вибіркоvim освітнім компонентом. Вивчення даної дисципліни спрямовано на розуміння та активне використання основних понять, моделей і методів побудови нейронних мереж для вирішення практичних завдань розпізнавання образів, прийняття рішень, класифікації та прогнозування, застосування методів штучного інтелекту для задач кібербезпеки.

Мета та цілі дисципліни

Сформуванню базових уявлень, первинних знань, вмінь і навичок студентів з теоретичних та практичних основ використання нейронних мереж на підставі сучасних програмних заходів для дослідження різноманітних процесів та застосування штучного інтелекту для вирішення задач кібербезпеки.

Формат занять

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

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.

СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.

РН17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 12 год., лабораторні роботи – 24 год., самостійна робота – 84 год.

Передумови вивчення дисципліни (пререквізити)

Основи математичного моделювання систем безпеки.

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 проекти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Теоретичні основи нейронних мереж. Розгляд біологічних прототипів, математичних моделей нейронів, архітектур нейронних мереж та основних алгоритмів навчання.	2
Тема 2. Чат GPT та його прикладне застосування. Огляд архітектури трансформерів, принципів роботи мовних моделей, можливостей ChatGPT у вирішенні прикладних завдань.	2
Тема 3. Нейронні мережі прямого поширення. Вивчення багатшарових перцептронів, функцій активації, алгоритму зворотного поширення помилки.	2
Тема 4. Нейронні мережі зі зворотними зв'язками. Особливості рекурентних мереж, LSTM та GRU, застосування для аналізу послідовних даних.	2
Тема 5. Мережі із самоорганізацією. Карти Кохонена. Принципи конкурентного навчання, побудова та інтерпретація карт Кохонена, їх використання для кластеризації.	2
Тема 6. Застосування нейронних мереж в кібербезпеці. Використання штучних нейронних мереж для виявлення вторгнень, класифікації шкідливого ПЗ та аналізу аномалій у кіберсистемах.	2
Загальна кількість годин	12

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Перцептрони: архітектура та навчання. Вивчення будови одношарового перцептрона, реалізація алгоритму навчання та аналіз здатності до розпізнавання простих образів.	4	0,1

Тема 2. Прикладні аспекти використання нейронних мереж: чат GPT. Ознайомлення з принципами роботи великих мовних моделей, використання ChatGPT для вирішення прикладних завдань та аналіз обмежень.	4	0,1
Тема 3. Багатошарова нейронна мережа прямого поширення. Реалізація багатошарового перцептрона з використанням бібліотек Python, експерименти з різними функціями активації та параметрами навчання.	4	0,1
Тема 4. Аналітичні рішення на основі самоорганізуючих карт Кохонена. Розробка та тестування карт Кохонена для кластеризації даних, візуалізація результатів та інтерпретація отриманих груп.	6	0,1
Тема 5. Застосування методів штучного інтелекту для задач кібербезпеки. Практичні приклади використання нейронних мереж для виявлення шкідливого трафіку, аналізу вторгнень та побудови систем захисту.	6	0,2
Загальна кількість годин	24	$\sum_{i=1}^n a_i = 0,6$

Контрольні роботи

За наявності

Теми контрольних робіт

Вагові
коефіцієнти b

Тема 1. Архітектури та алгоритми навчання нейронних мереж. У контрольній роботі розглядаються основні архітектури нейронних мереж — від багатошарових перцептронів до рекурентних і згорткових моделей. Аналізуються принципи роботи алгоритму зворотного поширення помилки, методи оптимізації, роль функцій активації. Особлива увага приділяється практичним прикладам застосування цих архітектур для обробки текстів, зображень та часових рядів.	0,4
Загалом	$\sum_{i=1}^m b_i = 0,4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу, підготовка до лабораторних занять, контрольних робіт та заліку.

Опрацювання теоретичного матеріалу

Теми самостійного вивчення	Кількість годин
Тема 1. Історія розвитку нейронних мереж та штучного інтелекту. Основні етапи становлення технологій, ключові наукові прориви.	8
Тема 2. Функції активації та їх роль у навчанні нейронних мереж. Порівняння лінійних та нелінійних функцій, вплив на точність і швидкість збіжності.	8

Тема 3. Регуляризація та методи запобігання перенаванчання. Dropout, L1/L2-регуляризація, нормалізація даних.	8
Тема 4. Рекурентні нейронні мережі (RNN) та їх модифікації (LSTM, GRU). Особливості роботи з послідовними даними.	8
Тема 5. Глибокі згорткові нейронні мережі (CNN). Архітектура, сфери застосування, приклади у комп'ютерному баченні.	8
Тема 6. Адаптивні методи оптимізації в нейронних мережах. SGD, Adam, RMSprop та порівняння їх ефективності.	8
Тема 7. Трансформери та механізм уваги (Attention). Основи архітектури, відмінності від класичних моделей, практичні застосування.	8
Тема 8. Generative Adversarial Networks (GANs). Механізм змагання генератора і дискримінатора, приклади генерації зображень та текстів.	8
Тема 9. Нейронні мережі у системах кібербезпеки. Методи виявлення аномалій, аналіз мережевого трафіку, прогнозування атак.	10
Тема 10. Етичні та соціальні аспекти використання нейронних мереж. Проблеми упередженості, конфіденційності даних та відповідальності за прийняті рішення.	10
Загальна кількість годин	84

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.

<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.

<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.

<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.

https://library.krok.edu.ua/media/library/category/navchalni-posibniki/trotsko_0001.pdf

Додаткова література

5. Добровська Л. М. Теорія та практика нейронних мереж : навч. посіб. / Л. М. Добровська, І. А. Добровська. Київ: НТУУ «КПІ» Вид-во «Політехніка», 2015. 396 с.

<https://ela.kpi.ua/server/api/core/bitstreams/c4dbb86a-d617-44df-9b7a-5b6e9f91cebf/content>

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.

<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. Пістунів. Дніпро: НТУ «ДП», 2023. 17 с.

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
0,6	0,4		

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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (Π , K , I ,...) 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

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

розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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
Роман КОРОЛЬОВ