Силабус освітнього компонента
Програма навчальної дисципліни

Нейронні мережі

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
6

Мова викладання
Українська

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 - 8. Лектор з дисциплін: "Теорія інформації і кодування", "Моделювання інформаційних систем", "Штучний інтелект і бізнес-аналітика", "Технології управління безпекою бізнес-процесів" 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 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

Сформувати базове уявлення, первинні знання, вміння і навички 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. 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.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. 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.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. 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 – 24 год., лабораторні роботи – 12 год., самостійна робота – 84 год.

Передумови вивчення дисципліни (пререквізити)

Безпека смарт-технологій

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 та групові проекти.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Теоретичні основи нейронних мереж.
Тема 2. Чат GPT та його прикладне застосування.
Тема 3. Нейронні мережі прямого поширення.
Тема 4. Нейронні мережі зі зворотними зв'язками.
Тема 5. Мережі із самоорганізацією. Карти Кохонена.
Тема 6. Застосування нейронних мереж в кібербезпеці
.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Перцептрони: архітектура та навчання.
Тема 2. Прикладні аспекти використання нейронних мереж: чат GPT.
Тема 3. Багатошарова нейронна мережа прямого поширення.
Тема 4. Аналітичні рішення на основі самоорганізуючих карт Кохонена.
Тема 5. Застосування методів штучного інтелекту для задач кібербезпеки.
.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

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. Пістунов. Дніпро: НТУ «ДП», 2023. 17 с.
http://pistunovi.inf.ua/NEURONET_LABS.pdf.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

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

Студент 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

28.08.2024 — Завідувач кафедри — Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП — Роман КОРОЛЬОВ