Силабус освітнього компонента
Програма навчальної дисципліни

Нейронні мережі

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
2

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 - 9. Лектор з дисциплін: "Моделювання систем інформаційної безпеки", "Штучний інтелект і бізнес-аналітика", "Стандартизація та сертифікація в галузі інформаційної безпеки", "Технологія 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 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.

КЗ–2. 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 – 32 год., лабораторні роботи – 16 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 та групові проекти.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Розробка інтелектуальних систем на основі моделей нейронних мереж.
Тема 2. Нейронні мережі як ключовий інструмент для штучного інтелекту. Чат GPT та його можливості.
Тема 3. Нейронні мережі прямого та зворотного поширення сигналу.
Тема 4. Нейронні мережі, що самонавчаються.
Тема 5. Глибинні нейронні мережі.
Тема 6. Радіальні базисні мережі.
Тема 7. Гібрідні нейронні мережі та системи нечіткого логічного виводу.
Тема 8. Методи штучного інтелекту в кібербезпеці..

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Моделювання нейронних мереж з використанням одно та башатошарового персептрона.
Тема 2. Штучний інтелект: основи користування.
Тема 3. Побудова нейронної мережі в пакеті Statistica Neural Networks.
Тема 4. Кластеризація та класифікація з використанням нейронної мережі Кохонена.
Тема 5. Моделювання радіальних базисних мереж.
Тема 6. Розроблення нечіткої моделі гібридної мережі для розв'язання задачі прогнозування.
Тема 7. Застосування методів штучного інтелекту для деяких класів задач кіібербезпеки та безпеки мереж.

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. [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

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
Ольга КОРОЛЬ