Силабус освітнього компонента
Програма навчальної дисципліни

Сучасні моделі та методи штучного інтелекту

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (освітньо-науковий)

Тип дисципліни
Вибіркова

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів.
Детальніше про викладача на сайті кафедри

МІЛОВ Олександр Володимирович

oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна "Сучасні моделі та методи штучного інтелекту" присвячена вивченню основних принципів, алгоритмів та застосувань штучного інтелекту (ШІ) у сфері кібербезпеки. Курс охоплює використання моделей машинного навчання та глибокого навчання для виявлення загроз, аналізу кіберінцидентів, запобігання атакам та автоматизації захисту інформаційних систем. Аспіранти ознайомляться з методами виявлення аномалій, алгоритмами класифікації мережевого трафіку, застосуванням нейронних мереж для ідентифікації шкідливого ПЗ та методами обробки великих обсягів даних у кіберпросторі.

Мета та цілі дисципліни

Метою дисципліни є формування у здобувачів глибоких знань та навичок щодо використання сучасних методів штучного інтелекту для забезпечення кібербезпеки. Курс спрямований на підготовку спеціалістів, здатних застосовувати ШІ для аналізу та протидії кіберзагрозам, розробляти автоматизовані системи захисту та використовувати алгоритми для прогнозування нових видів атак. Навчання здобувачів впроваджувати інноваційні рішення для захисту інформаційних ресурсів та забезпечення стійкості мережевих систем до сучасних кіберзагроз.

Формат занять

Лекції, практичні роботи, самостійна робота, індивідуальне завдання, консультації. Підсумковий контроль – іспит.

Компетентності

ІК Здатність продукувати нові ідеї, розв’язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
ЗК-2. Здатність до абстрактного мислення, аналізу та синтезу, проведення самостійних досліджень.
ЗК-3. Здатність до виявлення, генерування нових ідей, дослідження та вирішення проблем за професійним спрямуванням.
ЗК-4. Здатність працювати в міжнародному науковому просторі, розробляти та управляти науковими проектами.
СК-2. Здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми на основі глибокого осмислення наявних і створення нових цілісних знань, а також професійної практики. Використання моделювання механізмів кібербезпеки.
СК-4. Здатність систематизувати професійні знання в інформаційно-комунікаційних технологіях, моделювання механізмів кібербезпеки.
СК-5. Здатність розробляти та реалізовувати нові конкурентоздатні ідеї в галузі захисту інформації, використовувати методологічні та організаційно-технічні основи забезпечення безпеки.
СК-6. Здатність до розробки технологій та інструментальних засобів аналізу, прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення безпеки інформації.
СК-7. Здатність критично переосмислювати наявні інформаційні технології та відстежувати тенденції їх розвитку.

Результати навчання

РН-1. Вміння формувати і аргументовано відстоювати власну думку з різних проблем філософії науки та методології наукового пізнання, бути критичним і самокритичним.
РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.

РН-3. Вміння читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію. Вміння та навики працювати з сучасними бібліографічними і реферативними базами даних, а також наукометричними платформами (наприклад, Scopus, Web of Science, Web of Knowledge та ін.).
РН-4. Знання, розуміння, вміння та навички використання правил цитування та посилання на використані джерела, правил оформлення бібліографічного списку, розуміння змісту і порядку розрахунків основних кількісних наукометричних показників ефективності наукової діяльності (індекс цитування, індекс Гірша (h-індекс), імпакт-фактор (ІФ, або IF)).
РН-5. Вміння та навички критично сприймати та аналізувати існуючі наукові теорії та ідеї, шукати власні шляхи вирішення проблеми та завдань, проводити критичний аналіз власних матеріалів, генерувати власні нові ідеї, приймати обґрунтовані рішення.
РН-6. Вміння та навички планувати та управляти часом підготовки дисертаційного дослідження, формулювати мету, задачі, об'єкт і предмет дослідження, формувати структуру і розробляти план дослідження, використовувати методи дослідження, створювати обґрунтовані та достовірні нові знання через оригінальні дослідження, якість яких відповідає вимогам сучасного розвитку наукових досліджень на міжнародному рівні.
РН-7. Вміння демонструвати своєчасність та плановість у науковому дослідженні, спроможність управляти науковими проектами.
РН-8. Вміння використовувати кількісні і якісні методи для проведення наукових досліджень.
РН-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження..
РН-10. Володіння предметною базою знань та сучасними техніками дослідження, здатність створювати та інтерпретувати нові знання.
РН-11. Вміння розробляти проекти наукових досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів.
РН-12. Вміння оцінювати конкурентоспроможність отриманих результатів.
РН-13. Вміння узагальнювати і критично оцінювати результати, отримані вітчизняними і зарубіжними дослідниками.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., практичні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Світоглядні та соціокультурні основи науково-технічної діяльності, Іноземна мова для комунікації у науково-педагогічному середовищі, Представлення наукових результатів.

Особливості дисципліни, методи та технології навчання

Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальною та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до штучного інтелекту.
Основні поняття. Історія розвитку. Сфери застосування та вплив штучного інтелекту на різні галузі.
Тема 2. Класичні методи штучного інтелекту.
Експертні системи. Логічні та дедуктивні методи в штучному інтелекті. Пошукові алгоритми.
Тема 3. Машинне навчання: класифікація та основні методи.
Супервізоване навчання: методи регресії, класифікації. Ненаглядне навчання: кластеризація, пошук аномалій. Напівконтрольоване та підкріплювальне навчання.
Тема 4. Нейронні мережі та глибоке навчання.
Основи нейронних мереж. Конволюційні нейронні мережі. Рекурентні нейронні мережі (RNN). Глибоке навчання для ідентифікації шкідливого програмного забезпечення.
Тема 5. Моделі машинного навчання на основі дерев рішень.
Дерева рішень (Decision Trees). Модель випадкових лісів (Random Forest). Моделі підсилення (Gradient Boosting, XGBoost).
Тема 6. Моделі підкріплювального навчання (Reinforcement Learning).
Основи підкріплювального навчання: агент, середовище, нагорода. Моделі Q-навчання (Q-Learning). Актор-критик моделі та методи Deep Q-Learning (DQN).
Тема 7. Глибоке навчання та його роль у кібербезпеці.
Конволюційні нейронні мережі (CNN). Рекурентні нейронні мережі (RNN). Глибоке навчання для ідентифікації шкідливого програмного забезпечення.
Тема 8. Методи обробки природної мови (NLP).
Основи NLP: токенізація, лемматизація, стемінг. Використання глибоких нейронних мереж для NLP. Моделі Word2Vec, GloVe, BERT.
Тема 9. Генетичні та еволюційні алгоритми в кібербезпеці.
Основи еволюційних алгоритмів. Застосування генетичних алгоритмів у штучному інтелекті. Алгоритми ройового інтелекту.
Тема 10. Аналіз великих даних у кібербезпеці за допомогою штучного інтелекту.
Використання ШІ для обробки та аналізу великих даних у реальному часі. Застосування глибоких нейронних мереж для виявлення аномалій у великих масивах даних.
Тема 11. Штучний інтелект та захист об’єктів критичної інфраструктури.
Роль штучного інтелекту у забезпеченні кібербезпеки критичних систем (енергетика, транспорт). Моделі та методи для моніторингу та запобігання загрозам у критичних інфраструктурах. Використання штучного інтелекту для підвищення стійкості систем до атак.
Тема 12. Інтерпретованість та етика ШІ у кібербезпеці.
Інтерпретовані моделі для аналізу результатів кіберзахисту. Етичні питання, пов'язані з використанням штучного інтелекту в кібербезпеці. Проблеми конфіденційності та відповідальності при застосуванні штучного інтелекту.
Тема 13. Штучний інтелкт для автоматизації управління ризиками у кібербезпеці.
Оцінка кіберризиків за допомогою штучного інтелекту. Моделі для прогнозування кіберзагроз. Інтелектуальні системи для керування інцидентами кібербезпеки.
Тема 14. Майбутні перспективи використання штучного інтелекту у кібербезпеці.
Нові технології та підходи у штучному інтелекті для кібербезпеки. Роль квантових обчислень у поєднанні з штучним інтелектом для кіберзахисту. Виклики майбутнього: прогнозування кіберзагроз за допомогою штучного інтелету.

Теми практичних занять

Лабораторні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Моделі машинного навчання для класифікації мережевих атак.
Тема 2. Використання нейронних мереж для ідентифікації шкідливого програмного забезпечення.
Тема 3. Генетичні алгоритми та їх застосування.

Тема 4. Виявлення та аналіз атак на основі поведінкових моделей.
Тема 5. Використання еволюційних алгоритмів для оптимізації кіберзахисту.
Тема 6. Інтелектуальна система для аналізу вразливостей у програмному забезпеченні.
Тема 7. Застосування алгоритмів ройового інтелекту.
Тема 8. Аналіз реальних кіберзагроз та інцидентів за допомогою штучного інтелекту.

Самостійна робота

Самостійна робота аспіранта є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам 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. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» / Уклад. : А.С. Савченко, О. О. Синельніков. – К. : НАУ, 2017. – 190 с. URL: https://drive.google.com/file/d/1KeXV8EApf0Vc3qXV0UAw577ES2ZcWpUx/view?usp=sharing
2. Руденко О. Г., Бодянський Є. В. Штучні нейронні мережі: Навчальний посібник. — Харків: ТОВ "Компанія СМІТ", 2006. — 404 с. URL: https://f.eruditor.link/file/260293/
3. Кононюк А.Ю. Нейроні мережі і генетичні алгоритми – К.:«Корнійчук», 2008. – 446 с. URL: https://pdf.lib.vntu.edu.ua/books/2016/Kononyk_2008_470.pdf
4. Математичний апарат штучного інтелекту в електроенергетичних системах: підручник / В.В.Кирик. - Київ: КПІ ім. Ігоря Сікорського, вид-во "Політехніка". - 2019.-224 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/34259dab-7eaa-4b78-86d9-4a000d90b2be/content
5. Bishop C. M. - Pattern Recognition and Machine Learning. Springer, 2006. URL: https://drive.google.com/file/d/1kEd_Wc7_7q9nc_cUj-MbiNnKYZo9c0Xx/view?usp=sharing
6. Goodfellow I., Bengio Y., Courville A. - Deep Learning. MIT Press, 2016. URL: https://books.google.com.ua/books?id=Np9SDQAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
7. Mitchell T. - Machine Learning. McGraw-Hill Education, 1997. URL: https://www.cin.ufpe.br/~cavmj/Machine%20-%20Learning%20-%20Tom%20Mitchell.pdf

Додаткова література

8. Нікітіна Л. О. Моделі та методи штучного інтелекту у комп'ютерних іграх. /Л. О. Нікітіна, С. О. Нікітін. - Х.: «Друкарня Мадрид», 2018.-102 с. URL: http://library.kpi.kharkov.ua/files/new_postupleniya/motmet.pdf
9. Стратегія розвитку штучного інтелекту в Україні: монографія/ За ред. А.І. Шевченка. Київ: Інституту проблем штучного інтелекту Міністерства освіти і науки України і Національної академії наук України, 2023. 305 с. [Електронний ресурс]. – Режим доступу: https://jai.in.ua/archive/2023/ai_mono.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні роботи: 20% семестрової оцінки;
•самостійна робота: 30% семестрової оцінки;
•індивідуальне завдання: 20% семестрової оцінки;
•іспит: 30% 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

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

28.08.2024 — Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП
Олександр МІЛОВ