Силабус освітнього компонента
Програма навчальної дисципліни

Основи розподіленого штучного інтелекту для кібербезпеки

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
Професійна підготовка, Вибіркова

Семестр
2

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

Загальна інформація

Анотація

Навчальна дисципліна "Основи розподіленого штучного інтелекту для кібербезпеки" спрямована на вивчення базових концепцій, методів і підходів до застосування технологій розподіленого штучного інтелекту (ШІ) для підвищення ефективності систем кібербезпеки. Студенти ознайомляться з архітектурою розподілених систем ШІ, основними принципами організації взаємодії між компонентами таких систем та їх застосуванням для виявлення, аналізу та попередження кіберзагроз.

Мета та цілі дисципліни

Метою дисципліни є формування у студентів глибоких теоретичних знань і практичних навичок у застосуванні технологій розподіленого штучного інтелекту для вирішення завдань кібербезпеки. Основна увага приділяється вивченню принципів створення, впровадження та використання розподілених інтелектуальних систем для автоматизації процесів виявлення, аналізу і протидії кіберзагрозам.

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.
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
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.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до 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

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
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.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки 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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
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., практичні заняття – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Основи кібербезпеки, Комп'ютерні мережі, Основи машинного навчання для кібербезпеки.

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

Теми лекційних занять

Тема 1. Вступ до розподіленого штучного інтелекту.
Історія розвитку та основні концепції розподіленого штучного інтелекту. Огляд застосувань РШІ у різних галузях, зокрема в кібербезпеці.
Тема 2. Архітектури розподілених систем ШІ.
Модель клієнт-сервер, однорангові мережі та мультиагентні системи. Принципи проектування розподілених систем для обробки великих даних та їх роль у кібербезпеці.
Тема 3. Мультиагентні системи та їх застосування у кібербезпеці.
Поняття агентів, типи агентів та їх взаємодія. Роль мультиагентних систем у захисті від кіберзагроз, координація та співпраця між агентами.
Тема 4. Методи та алгоритми машинного навчання для кібербезпеки.
Алгоритми класифікації, кластеризації та регресії. Використання машинного навчання для виявлення аномалій та атак.
Тема 5. Глибоке навчання та його застосування у кібербезпеці.
Архітектура нейронних мереж та основи глибокого навчання. Застосування глибоких нейронних мереж для аналізу кіберзагроз та інцидентів.
Тема 6. Технології обробки великих даних у кібербезпеці.
Основи технологій обробки великих даних (Big Data), розподілені бази даних, Hadoop, Spark. Використання обробки великих даних для виявлення кібератак та управління кіберзагрозами.
Тема 7. Безпека та захист розподілених систем штучного інтелекту.
Загрози безпеці в розподілених ШІ-системах, атаки на мультиагентні системи. Методи захисту, шифрування та автентифікація в розподілених системах ШІ.
Тема 8. Кіберзагрози та кіберзахист за допомогою штучного інтелекту.
Аналіз типів кіберзагроз (DDoS-атаки, фішинг, шкідливе програмне забезпечення). Використання інструментів ШІ для моніторингу та захисту від кіберзагроз.
Тема 9. Автоматизація процесів реагування на кіберзагрози за допомогою ШІ.
Використання ШІ для автоматизації виявлення, аналізу та реагування на інциденти кібербезпеки. Системи автоматизованого аналізу інцидентів та реагування в реальному часі.
Тема 10. Перспективи розвитку розподіленого штучного інтелекту у кібербезпеці.
Сучасні тенденції та інновації в сфері РШІ та кібербезпеки. Майбутнє інтеграції ШІ та кіберзахисту: прогнози і виклики.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вступ до програмування розподілених систем ШІ.
Налаштування середовища для роботи з розподіленими системами. Створення базової програми для розподіленого обчислення з використанням мови програмування.
Тема 2. Застосування методів машинного навчання для виявлення аномалій.
Використання алгоритмів класифікації для виявлення аномалій у кіберданих.
Тема 3 Розробка моделі виявлення загроз за допомогою обробки великих даних.
Реалізація системи виявлення аномалій з використанням аналізу великих даних у кібербезпеці.
Тема 4. Захист розподілених систем від атак.
Реалізація та тестування методів шифрування та автентифікації в розподілених системах.
Тема 5. Автоматизація реагування на кіберзагрози за допомогою ШІ.
Створення системи автоматизованого виявлення та реагування на кіберінциденти.
Тема 6. Моделювання кіберзагроз у розподіленій системі.
Оцінка ефективності захисту від загроз за допомогою розподілених агентів та алгоритмів ШІ.
Тема 7. Інтеграція ШІ для захисту IoT-систем.
Розробка та тестування алгоритмів ШІ для виявлення аномалій у IoT-мережах.
Тема 8. Оцінка ефективності засобів ШІ у кібербезпеці.

Проведення тестування ефективності різних методів ШІ у виявленні та попередженні кібератак. Порівняння результатів роботи різних підходів та моделей.

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. Russell, Stuart, Norvig, Peter. "Artificial Intelligence: A Modern Approach" https://www.amazon.com/Artificial-Intelligence-Modern-Approach-3rd/dp/0136042597
2. Wooldridge, M. "An Introduction to MultiAgent Systems" https://www.wiley.com/en-us/An+Introduction+to+MultiAgent+Systems%2C+2nd+Edition-p-9780470519462
3. Goodfellow, Ian, Bengio, Yoshua, Courville, Aaron. "Deep Learning" https://www.deeplearningbook.org/
4. Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" https://www.wiley.com/en-us/Applied+Cryptography%3A+Protocols%2C+Algorithms%2C+and+Source+Code+in+C%2C+20th+Anniversary+Edition-p-9781119096726
5. Collins, Michael. "Big Data Analytics" https://www.amazon.com/Big-Data-Analytics-Michael-Collins/dp/1493219929

Додаткова література :

6. Stallings, William. "Cryptography and Network Security: Principles and Practice" https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- практичні заняття: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% 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