Силабус освітнього компонента
Програма навчальної дисципліни

ЗАХИСТ ТА АТАКА НА ДАНІ ЗА ДОПОМОГОЮ ШІ

Шифр та назва спеціальності
122 – Комп'ютерні науки.

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма
Комп'ютерні науки. Штучний інтелект та управління проєктами

Кафедра
Програмної інженерії та інтелектуальних технологій управління

Рівень освіти
бакалавр

Тип дисципліни
Вибіркова

Семестр
6

Мова викладання
Українська

Викладачі, розробники

ШМАТКО Олександр Віталійович
oleksandr.shmatko@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри програмної інженерії та інтелектуальних технологій управління НТУ «ХПІ».

Загальна інформація, кількість публікацій, основні курси тощо.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Цей курс пропонує поглиблене вивчення методологій і технологій на перетині штучного інтелекту (ШІ), кібербезпеки та науки про дані. Він зосереджується на тому, як ШІ можна використовувати як для захисту даних від складних кіберзагроз, так і для атак на системи даних, щоб краще зрозуміти вразливості. Навчальна програма збалансовано поєднує теоретичні знання з практичним застосуванням, включаючи етичні міркування та новітні галузеві стандарти.

Мета та цілі дисципліни

Метою курсу "Захист та атака на дані за допомогою штучного інтелекту" є надання студентам глибокого та детального розуміння того, як технології штучного інтелекту (ШІ) можуть бути застосовані як для підвищення безпеки даних, так і для виявлення вразливостей в інформаційних системах. Цей курс покликаний надати студентам знання та навички, необхідні для розробки передових заходів безпеки на основі штучного інтелекту, а також для критичного аналізу та використання вразливостей даних за допомогою методів штучного інтелекту.
Поєднуючи практичне навчання з теоретичними основами, курс має на меті виховати покоління професіоналів з кібербезпеки, які вміють використовувати ШІ для подвійної мети - захисту цифрових активів та етичного проникнення в системи даних для підвищення їхньої безпеки. Після закінчення курсу студенти отримають всебічне розуміння взаємодії між ШІ та кібербезпекою, будуть готові орієнтуватися в складних умовах цифрового ландшафту за допомогою інноваційних рішень та сильного етичного компасу. .

Формат занять

Лекції, практичні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

Здатність застосовувати принципи і методи побудови та використання мережевих технологій.
Здатність застосовувати методи та засоби захисту програмного забезпечення та даних від несанкціонованого доступу в умовах супроводження та експлуатації програмних систем і комплексів

Результати навчання

Розуміти загальні принципи та моделі побудови комп'ютерних мереж.
Застосовувати основні механізми та методи безпеки мереж і програмних систем.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 56 год.

Передумови вивчення дисципліни (пререквізити)

Для вивчення дисципліни необхідно володіти хорошими знаннями в області інформаційних технологій, інформаційної безпеки та інформатики. Необхідні знання розподілених систем, комп'ютерних мереж, криптографії та структур даних.

Особливості дисципліни, методи та технології навчання

Методи викладання та навчання:
інтерактивні лекції з презентаціями, дискусії, лабораторні заняття, командна робота, кейс-метод, метод зворотного зв'язку з боку студентів, проблемне навчання.
Форми оцінювання:
письмові індивідуальні завдання до лабораторних робіт (CAS), оцінювання знань на лабораторних заняттях (CAS), експрес-опитування (CAS), онлайн-тести (CAS), підсумковий/семестровий контроль у формі семестрового екзамену, відповідно до графіку навчального процесу (FAS).

Програма навчальної дисципліни

Теми лекційних занять

Тема 1: Вступ до ШІ в кібербезпеці
Огляд технологій ШІ в кібербезпеці. Етичні міркування в ШІ
Тема 2: Вразливості даних та зловживання штучним інтелектом
Розуміння вразливостей даних. Методи ШІ для експлуатації даних
Тема 3: Машинне навчання для виявлення загроз
Контрольоване та неконтрольоване навчання для кібербезпеки. Виявлення аномалій за допомогою машинного навчання
Тема 4: ШІ в оборонних стратегіях безпеки
Проектування протоколів безпеки на основі ШІ. Впровадження систем виявлення вторгнень на основі ШІ
Тема 5: Атаки на системи ШІ
Розуміння та використання вразливостей систем ШІ. Суперечливий ШІ та машинне навчання
Тема 6: ШІ для безпечного управління даними
ШІ в шифруванні та безпечному зберіганні даних. Машинне навчання із збереженням конфіденційності
Тема 7: Нові тенденції та майбутні напрямки
Останні досягнення в галузі ШІ та кібербезпеки. Майбутні загрози та роль ШІ в боротьбі з ними.

Теми практичних занять

Практичні заняття не передбачені.

Теми лабораторних робіт

Лабораторна робота 1. Дослідження проблеми змагального навчання.
Лабораторна робота 2. Дослідження зловмисної атаки на ResNet18
Лабораторна робота 3. Дослідження методів атак та класів. Нецільова атака.
Лабораторна робота 4. Дослідження методів атак та класів. Нецільова атака.
Лабораторна робота 5. Дослідження локального згладжування градієнтів: захист від локальних зловмисних атак

Самостійна робота

Самостійна робота студентів не передбачена планом

Література та навчальні матеріали

1. Rangaraju S. Ai sentry: Reinventing cybersecurity through intelligent threat detection //EPH-International Journal of Science And Engineering. – 2023. – Т. 9. – №. 3. – С. 30-35.
2. Muneer S. M., Alvi M. B., Farrakh A. Cyber Security event detection using machine learning technique //International Journal of Computational and Innovative Sciences. – 2023. – Т. 2. – №. 2. – С. 42-46.
3. Das R. Practical AI for cybersecurity. – CRC Press, 2021..
4. Prasad R. et al. Artificial intelligence and machine learning in cyber security //Cyber Security: The Lifeline of Information and Communication Technology. – 2020. – С. 231-247.
5. Kamhoua C. A. et al. (ed.). Game theory and machine learning for cyber security. – John Wiley & Sons, 2021.
6. Misra S., Tyagi A. K. (ed.). Artificial intelligence for cyber security: methods, issues and possible horizons or opportunities. – Springer Nature, 2021. – Т. 972.
7. Dasgupta P., Collins J. B., Mittu R. (ed.). Adversary-Aware Learning Techniques and Trends in Cybersecurity. – Springer, 2021..

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
20% залік: семестровий екзамен, відповідно до графіку навчального процесу
80% поточне оцінювання:

- 50% оцінювання завдань на лабораторних роботах;
- 30% проміжний контроль (2 модульні контрольні роботи)

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	Дата погодження, підпис 27.08.2023	Завідувач кафедри Андрій КОПП
	Дата погодження, підпис 27.08.2023	Гарант ОП Марина ГРИНЧЕНКО