Силабус освітнього компонента
Програма навчальної дисципліни

Безпека мереж для штучного інтелекту

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Вибіркова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
7

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЄЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».
Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна спрямована на формування у студентів знань і практичних навичок щодо забезпечення безпеки мережевої інфраструктури, яка підтримує роботу систем штучного інтелекту. Розглядаються особливості організації захищеного обміну даними, методи протидії мережевим загрозам, атакам на алгоритми та моделі ШІ, а також використання сучасних технологій шифрування, IDS/IPS та політик безпеки. Значна увага приділяється питанням захисту розподілених і хмарних систем, що застосовуються для навчання та розгортання моделей, а також міжнародним стандартам і практичним підходам до управління безпекою в цій сфері.

Мета та цілі дисципліни

Формування у студентів системного розуміння принципів і методів забезпечення безпеки мережевої інфраструктури для систем штучного інтелекту, набуття навичок практичного застосування сучасних технологій захисту даних, протидії атакам та управління ризиками.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації – критично для захисту даних моделей і обчислювальних процесів.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих

загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи кібербезпеки, Основи програмування, Комп'ютерні мережі.

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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до безпеки мереж для ШІ. Розгляд особливостей сучасних мережевих технологій, що забезпечують роботу систем штучного інтелекту, та специфічних викликів у сфері кібербезпеки.	2
Тема 2. Загрози для інфраструктури ШІ. Аналіз основних загроз: атак на навчальні дані, моделі та канали зв'язку; проблеми конфіденційності й цілісності даних.	2
Тема 3. Мережеві атаки на системи ШІ. Типові атаки (DoS/DDoS, перехоплення трафіку, ін'єкції), їхній вплив на моделі ШІ та методи протидії.	2
Тема 4. Захист каналів зв'язку та даних у системах ШІ. Методи шифрування, автентифікації та захищеного обміну даними між елементами мережевої інфраструктури.	2
Тема 5. Використання IDS/IPS для моніторингу систем ШІ. Застосування систем виявлення та запобігання вторгнень у мережах, що обслуговують моделі штучного інтелекту.	2
Тема 6 Захист розподілених і хмарних систем ШІ. Питання безпеки при використанні хмарних платформ, контейнеризації та мікросервісної архітектури для навчання та розгортання моделей.	2
Тема 7. Атаки на алгоритми ШІ та методи захисту. Аналіз атак типу adversarial examples, отруєння даних та методів підробки моделей; способи побудови стійких моделей.	2
Тема 8. Політики та стандарти безпеки для мереж ШІ. Розгляд міжнародних стандартів (NIST, ISO/IEC), принципів розробки політик безпеки та практичних підходів до їхнього впровадження у сфері ШІ.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз мережевих загроз для систем ШІ. Вивчення основних векторів атак, типових вразливостей і потенційних ризиків у мережах, що обслуговують моделі штучного інтелекту.	6	0,1
Тема 2. Конфігурація захищеного обміну даними. Налаштування шифрування каналів зв'язку та реалізація механізмів автентифікації між сервісами ШІ.	6	0,1
Тема 3. Використання IDS/IPS для захисту систем ШІ. Практична робота з встановлення та налаштування систем виявлення і запобігання вторгнень; аналіз сповіщень та подій.	6	0,1
Тема 4. Аудит безпеки розподілених систем ШІ. Оцінка вразливостей хмарних та локальних середовищ, що використовуються для тренування та розгортання моделей.	6	0,1
Тема 5. Захист від мережевих атак (DoS/DDoS). Моделювання атак та застосування контрзаходів для забезпечення стійкості мережевої інфраструктури ШІ.	4	0,1
Тема 6. Захист даних у навчанні моделей ШІ. Впровадження заходів для запобігання отруєння даних та атак типу adversarial examples.	4	0,1
Тема 7. Моніторинг та аналіз трафіку ШІ-систем. Збір, нормалізація та аналіз мережевого трафіку для виявлення аномалій і потенційних загроз.	4	0,1
Тема 8. Розробка політик безпеки для мереж ШІ. Створення внутрішніх стандартів і правил безпеки для забезпечення захищеної роботи моделей та інфраструктури.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи безпеки мереж для систем ШІ. Перевірка знань про мережеві технології для ШІ, специфіку кіберзагроз для інфраструктури ШІ та базові методи захисту даних і каналів зв'язку.	0,1
Тема 2. Захист і моніторинг мережевих систем ШІ. Оцінка навичок виявлення та протидії мережевим атакам на системи ШІ, використання IDS/IPS, захист хмарних і розподілених систем, а також стійкість алгоритмів ШІ до атак та впровадження політик безпеки.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи кібербезпеки для ШІ. Вивчення базових принципів безпеки в мережах, що обслуговують моделі штучного інтелекту.	8
Тема 2. Типи мережевих атак на системи ШІ. Аналіз DoS/DDoS, ін'єкцій, перехоплення трафіку та інших атак, специфічних для ШІ.	8
Тема 3. Методи шифрування та автентифікації для ШІ. Використання криптографічних протоколів і автентифікаційних механізмів для захисту даних та каналів зв'язку.	7
Тема 4. Використання IDS/IPS у мережах ШІ. Застосування систем виявлення та запобігання вторгнень для контролю безпеки мереж ШІ.	7
Тема 5. Захист хмарних і розподілених систем ШІ. Особливості безпеки при використанні хмарних платформ, контейнеризації та мікросервісів.	7
Тема 6. Атаки на алгоритми ШІ та їх протидія. Вивчення adversarial examples, отруєння даних, підробки моделей та методів побудови стійких алгоритмів.	7
Тема 7. Моніторинг та аналіз мережевого трафіку для ШІ. Методи збору, аналізу та інтерпретації даних для виявлення потенційних загроз.	7
Тема 8. Політики безпеки для мереж ШІ. Розробка та впровадження політик безпеки відповідно до міжнародних стандартів (NIST, ISO/IEC).	7
Тема 9. Конфіденційність та цілісність даних у ШІ. Принципи забезпечення захисту навчальних даних та моделей від несанкціонованого доступу та модифікації.	7
Тема 10. Аудит безпеки та тестування на проникнення в системах ШІ. Оцінка ефективності заходів захисту, тестування на проникнення та виявлення вразливостей у мережах для ШІ.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1 Russell, S., Norvig, P. Artificial Intelligence: A Modern Approach (4th ed.). Pearson, 2021.
ISBN-13: 978-0134610993
https://www.amazon.com/Artificial-Intelligence-Modern-Approach-Global/dp/1292401133?utm_source=chatgpt.com
2. Chio, C., Freeman, D. Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media, 2018.
ISBN-13: 978-1491979907
https://www.amazon.com/Machine-Learning-Security-Protecting-Algorithms/dp/1491979909?utm_source=chatgpt.com
3. Cisco Press. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (2nd ed.). Pearson, 2024.
ISBN-13: 978-0138221263
https://www.ciscopress.com/store/ccnp-and-ccie-security-core-scor-350-701-official-cert-9780138221263?utm_source=chatgpt.com
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
http://monograph.com.ua/pctc/catalog/view/64/52/231-1
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Додаткова література

1. Papernot, N., McDaniel, P., Goodfellow, I. Practical Black-Box Attacks against Machine Learning. ACM, 2017.
https://arxiv.org/abs/1602.02697?utm_source=chatgpt.com
2. Sharma, D. Artificial Intelligence for Cyber Security and Industry 4.0. CRC Press, 2023.
ISBN-13: 978-0367466664
https://www.amazon.com/Artificial-Intelligence-Cyber-Security-Applications/dp/3031285808?utm_source=chatgpt.com
3. Kaushik, K. Next-Generation Cybersecurity: AI, ML, and Blockchain. Springer, 2023.
ISBN-13: 978-9819712496
https://link.springer.com/book/10.1007/978-981-97-1249-6?utm_source=chatgpt.com
4. Papernot, N., McDaniel, P. Adversarial Machine Learning. Cambridge University Press, 2019.
ISBN-13: 978-1107043466
https://www.amazon.com/Adversarial-Machine-Learning-Anthony-Joseph/dp/1107043468?utm_source=chatgpt.com

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Сергій ЄВСЕЄВ