Силабус освітнього компонента
Програма навчальної дисципліни

Штучний інтелект і бізнес-аналітика

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Професійна підготовка, Вибіркова

Семестр
3

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: «Нейронні мережі", "Моделювання систем критичної інфраструктури", "Теорія інформації і кодування", "Безпека безперервності бізнес-процесів" та інших у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти формують уявлення про типи завдань, що виникають у галузі аналітики та методи їх вирішення, які допоможуть майбутнім фахівцям з безпеки виявляти, формалізувати та успішно вирішувати практичні завдання аналізу даних, що виникають у процесі їх професійної діяльності з використанням можливостей штучного інтелекту.

Мета та цілі дисципліни

формування системи фундаментальних знань щодо процесу виокремлення, дослідження та моделювання статистичних даних для виявлення невідомих до цього структур та закономірностей із застосуванням можливостей штучного інтелекту.

Формат занять

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

Компетентності

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.
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.
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.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

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.
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.
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.
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.
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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Технології управління безпекою бізнес-процесів, Математичні моделі управління ІТ-проєктами.

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.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Введення в бізнес-аналітику та Data Mining як сучасні напрямки інтелектуального розвитку та аналізу даних.
Тема 2. Бізнес-аналітика та Data Mining: техніки та методики.
Тема 3. Google Anaitics - цифровий пошуковий інструмент для репортингу бізнес-інформації.
Тема 4. Концепції управління даними та попередній аналіз статистичної інформації.
-процесів.
Тема 5. Аналіз часових рядів та виявлення аномалій.
Тема 6. Методи класифікації та кластеризації в бізнес-аналітиці.
Тема 7. Візуалізація та інтерактивні дослідження бізнесу.
Тема 8. Штучний інтелект та аналітика даних: практичні аспекти.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Можливості для бізнес-аналітики та Data Mining в епоху штучного інтелекту.
Тема 2. Аналітичні інструменти в оцінюванні бізнесу.
Тема 3. Використання Google Analitics для аналізу сайтів бізнес-структур.
Тема 4. Формування інформаційного простору для дослідження явищ та процесів.
Тема 5. Пошук та виявлення аномалій в даних за допомогою бібліотеки pandas Python.
Тема 6. Ієрархічні та неієрархічні методи кластерного аналізу.

Тема 7. Робота з Google Public Data Explorer Google Trends.
Тема 8. Хмарні інструменти аналітики даних.

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. Інтелектуальний аналіз даних. Навчально-методичний посібник з лабораторних робіт / Талах М.В. Чернівці: Технодук, 2024. 153 с.
2. Сидорова А. В., Біленко Д. В., Буркіна Н. В. Бізнес-аналітика: навчально-методичний посібник. Вінниця: ДонНУ імені Василя Стуса. 2019. 104 с. [Електронний ресурс]. – Режим доступу: https://r.donnu.edu.ua/bitstream/123456789/105/1/79_%D0%9D%D0%9C%D0%9F_%D0%91%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0.pdf
3. Варенко В.М. Основи аналітики : навч. посіб. / В.М. Варенко. Ліра До, 2022. 248 с.
4. Провост Ф. Data Science для бізнесу. Як збирати, аналізувати і використовувати дані / Ф. Провост, Т. Фоусетт ; пер. з англ. А. Дудченко. – 2-ге вид. Київ : Наш формат, 2020. 400 с. [Електронний ресурс]. – Режим доступу: https://nashformat.ua/pdf-preview/data-science-dlya-biznesu.-yak-zbyraty-analizuvaty-i-vykorystovuvaty-dani-709241?srsltid=AfmBOoo8h8ebyGtMT3MEFWHus55lxzaw0c9uSp3sOHdGY3yVtAGc1cqg
5. Інтелектуальний аналіз даних: Комп'ютерний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки та інформаційні технології», спеціалізацій «Інформаційні системи та технології проектування», «Системне проектування сервісів» / О. О. Сергеєв-Горчинський, Г. В. Іщенко ; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 73 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/53cc4098-de84-4297-862f-d9ae3a586546/content
6. Бхаргава Р. Неочевидне. Як передбачити майбутнє, аналізуючи тренди : пер. з англ К. Дерев'янко. 2-ге вид. Київ : Віват, 2019. – 288 с. [Електронний ресурс]. – Режим доступу: https://books2you.com.ua/biznes-knyhy/zarubizhna-dilova-literatura/neochevydne-yak-peredbachyty-maybutnie-analizuiuchy-trendy-rokhit-bkharhava/
7. How to Do A/B Testing: 15 Steps for the Perfect Split Test. [Електронний ресурс]. – Режим доступу: https://blog.hubspot.com/marketing/how-to-do-a-b-testing

Додаткова література :

1. 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
2. Гороховатський В.О., Творошенко І.С. Методи інтелектуального аналізу та оброблення даних: навч. посібник. Харків: ХНУРЕ, 2021. 92 с. [Електронний ресурс]. – Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/2e55d639-52fd-48d9-b7b7-14989f49f291/content

3. Цифрова економіка : підручник / Т. І. Олешко, Н. В. Касьянова, С. Ф. Смерічевський та ін. Київ : НАУ, 2022. 200 с. [Електронний ресурс]. – Режим доступу: https://dspace.nau.edu.ua/bitstream/NAU/54129/1/%D0%9F%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA%20%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%20%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D0%BA%D0%B0.pdf
4. Семенова К. Д., Тарасова К. І. Бізнес-статистика : Підручник / К. Д. Семенова, К. І. Тарасова. К : ФОП Гуляєва В.М. 2018. 210 с. [Електронний ресурс]. – Режим доступу: http://dspace.oneu.edu.ua/jspui/bitstream/123456789/7578/1/%D0%91%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0.pdf
5. Ковальчук В. В. Інтелектуальний аналіз даних: конспект лекцій. Одеса, ОДЕКУ, 2015. 206 с. [Електронний ресурс]. – Режим доступу: http://eprints.library.odeku.edu.ua/611/5/Kovalchuk_VV_Intelekt_analiz_danykh_ta_syste_analiz_KL_2015.pdf
6. Кузьменко О. Майбутнє аналітики: нові тенденції та технології. [Електронний ресурс]. – Режим доступу: https://www.whitesales.ua/uk/blog/the-future-of-analytics-emerging-trends-and-technologies.

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
Станіслав МІЛЕВСЬКИЙ