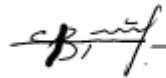


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено

На засіданні кафедри кібербезпеки
факультету прикладної математики
та інформатики
Львівського національного університету
імені Івана Франка
(Протокол № 9/24 від 29 серпня 2024 р.)

Завідувач кафедри



Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни

“Машинне навчання та адаптивний інтелект”,

**що викладається в межах ОПІ Технології штучного інтелекту в
кібербезпеці другого (магістерського) рівня вищої освіти для
здобувачів з спеціальності 125 – кібербезпека та захист
інформації**

| | |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Назва дисципліни | Машинне навчання та адаптивний інтелект |
| Адреса викладання дисципліни | м. Львів, вул. Університетська 1 |
| Факультет та кафедра, за якою закріплена дисципліна | Факультет прикладної математики та інформатики Кафедра кібербезпеки |
| Галузь знань, шифр та назва спеціальності | 12 – інформаційні технології 125 – кібербезпека та захист інформації |
| Викладачі дисципліни | Винокурова Олена Анатоліївна, професор кафедри кібербезпеки |
| Контактна інформація викладачів | olena.vynokurova@lnu.edu.ua ; https://ami.lnu.edu.ua/employee/vynokurova Головний корпус ЛНУ ім. І. Франка, каб. 260. м. Львів, вул. Університетська, 1 |
| Консультації з питань навчання по дисципліні відбуваються | Консультації в день проведення лекцій/лабораторних занять (а також за розкладом консультацій кафедри). |
| Сторінка курсу | https://ami.lnu.edu.ua/admission/specializations |
| Інформація про дисципліну | Дисципліна “Машинне навчання та адаптивний інтелект” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми «Технології штучного інтелекту в кібербезпеці», яка викладається в 2-му семестрі в обсязі 3-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| Коротка анотація дисципліни | Основним завданням курсу є формування професійних компетентностей майбутніх фахівців в галузі кібербезпеки на базі методів штучного інтелекту та машинного навчання, організації систем ідентифікації, аутентифікації і авторизації користувачів на базі штучного інтелекту та набуття навиків розробці і застосування моделей машинного навчання при вирішенні практичних задач в кібербезпеці. |

| | |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Мета та цілі дисципліни | Метою викладання навчальної дисципліни є вивчення теоретичних основ методів машинного навчання, реалізації методів машинного навчання та адаптивного інтелекту для вирішення практичних задач. |
| Література для вивчення дисципліни | <ol style="list-style-type: none"> 1. Gareth James , Daniela Witten , Trevor Hastie , Robert Tibshirani An Introduction to Statistical Learning: with Applications in Python Springer, 2023, 607 p. 2. Anitha S. Pillai and Roberto Tedesco Machine Learning and Deep Learning in Natural Language Processing, CRC Press, 2024, 245 p. 3. Ruth J. Innovative Machine Learning Applications for Cryptography IGI Global, 2024, 313 p. 4. Hossain, Eklas Machine Learning Crash Course for Engineers Springer, 2024, 473 p. 5. Yuxi (Hayden) Liu, Sebastian Raschka, Vahid Mirjalili Machine Learning with PyTorch and Scikit-Learn, Packt Publishing, 2022, 774 p. <p>Допоміжна</p> <ol style="list-style-type: none"> 6. Субботін, С. О., Олійник А. О. Нейронні мережі: навчальний посібник. Запоріжжя: ЗНТУ, 2014. 132 с. 7. В. Д. Дмитрієнко, О. Ю. Заковоротний, В. І. Носков, М. В. Мезенцев Основи нейрокомп'ютерингу. Х.: НТМТ, 2014, 140 с. 8. https://www.udemy.com/ 9. https://www.coursera.org/ |
| Обсяг курсу | Загальний обсяг: 90 годин. Аудиторних занять: 32 год., з них 16 год. лекцій та 16 год. лабораторних робіт. Самостійної роботи: 58 год. |
| Очікувані результати навчання | <p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p>знати:</p> <ul style="list-style-type: none"> • процес створення пайплайну моделей машинного навчання – від збору даних до розгортання моделей на сервері • основи формування датасетів і предобробки даних, їх перетворення та підготовки для моделей машинного навчання; • алгоритми машинного навчання з вчителем і самонавчання; • основи навчання моделей та оцінки їх ефективності; • програмні засоби для реалізації моделей машинного навчання; • теоретичний та практичний матеріал згідно програми курсу. <p>вміти:</p> <ul style="list-style-type: none"> • вибирати і використовувати оптимальні методи машинного навчання і програмні засоби для вирішення практичних; • використовувати на практиці теоретичні основи алгоритмів машинного навчання; • застосовувати засвоєний матеріал для створення прототипів моделей машинного навчання; |

| | |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> використовувати Python для програмної реалізації моделей машинного навчання, їх тестування та оцінки, а також визначати тип задачі машинного навчання: регресії, класифікації та кластеризації і розв'язувати поставлену проблему на основі здобутих знань та навиків <p>Курс забезпечує набуття таких компетентностей: ЗК 2-4, КФ 1, КФ 3, КФ 11;</p> <p>та програмних результатів навчання: РН 4, РН 13, РН 19, РН 21-24.</p> |
| Ключові слова | Методи машинного навчання, адаптивний інтелект, навчання з вчителем, самонавчання, ансамблеві методи, методи огортання моделей в api, Python, Pytorch, Tensorflow |
| Формат курсу | Очний Проведення лекцій, лабораторних робіт і консультацій. |
| Теми | Теми подані у Схемі курсу нижче |
| Підсумковий контроль, форма | Екзамен у кінці 2 семестру |
| Пререквізити | Для вивчення курсу студенти потребують базові знання з дисципліни: <ul style="list-style-type: none"> Інтелектуальні інформаційні технології Системи ІІІ в задачах захисту інформації |
| Навчальні методи та техніки, які будуть використовуватися під час викладання курсу | Презентації, лекції, лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, опитування теоретичного матеріалу, самостійна робота. Лекції та лабораторні: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод. |
| Необхідне обладнання | Комп'ютерний клас із вільно-доступним програмним забезпеченням, локальна комп'ютерна мережа, доступ до Internet мережі. |
| Критерії оцінювання (окремо для кожного виду навчальної діяльності) | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: <ul style="list-style-type: none"> лабораторні заняття, самостійна робота студентів: 50% семестрової оцінки; максимальна кількість балів 50 екзамен: 50% семестрової оцінки; максимальна кількість балів 50 |

Підсумкова максимальна кількість балів 100.

Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади мож-ли-вої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.

Політика виставлення балів. Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнь на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.

Жодні форми порушення академічної доброчесності не толеруються.

| Критерії оцінювання знань студентів | Бали рейтингу | Макс. к-сть балів |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|
| 1. Бали поточної успішності за участь у лабораторних заняттях | | |
| Критерії оцінювання (8*5 бали) | 40 балів | |
| Студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань. Правильно вирішив усі тестові завдання. | 5 | |
| Студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань. | 4-3 | |

| | | |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| | Студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань. | 2-1 |
| | Студент не володіє матеріалом. | 0 |
| | 2. Самостійна робота студентів (СРС) | |
| | Критерії оцінювання (8 * 0.5 балів + 1*6 балів) | 10 балів |
| | Самостійна робота підготовка доповіді на конференцію | 6 |
| | Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел) Самостійна робота студентів, оцінюється під час поточного контролю теми на відповідному практичному занятті. Студент додатково опрацював матеріал та аргументовано його викладає. <i>Оцінюється додатковим балом за кожну лабораторну роботу.</i> | 1 |
| | Студент не опрацював самостійно додаткових джерел і не володіє матеріалом | 0 |
| | Загальна максимальна кількість балів за поточний контроль | 50 |
| | 4. Екзамен | 50 |
| | Семестровий екзамен як форма підсумкового контролю є обов'язковим для всіх студентів. Екзаменаційний білет містить 2 теоретичні питання по 15 балів та 1 практична задача з реалізацією 20 балів | |
| | Критерії оцінювання відповіді на теоретичні питання (2*15 балів): | 30 |
| | Відповідь написано в повному обсязі, аргументовано, глибоко та всебічно розкрито зміст теоретичного питання. | 15 |
| | Відповідь в основному розкриває зміст теоретичного питання, не вистачає достатньої глибини та аргументації, допущено окремі несуттєві неточності та незначні помилки. | 14-11 |
| | Відповідь в цілому розкриває основний зміст питання але без глибокого всебічного аналізу, обґрунтування та аргументації, допущено окремі суттєві неточності та помилки. | 10-6 |
| | Відповідь не повна, фрагментарна без аргументації та обґрунтування. | 5-1 |
| | Відповідь не надана | 0 |
| | Критерії оцінювання програмної реалізації поставленої задачі (20 балів): | 20 |
| | Програмна реалізація вирішує задачу | 20 |
| | Програмна реалізація не вирішує задачу | 0 |
| | Загальна кількість балів по завершенні вивчення дисципліни | 100 |
| Опитування | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу. | |

Схема курсу

| Тиж. | Тема, план, короткі тези | Форма діяльності (заняття) | Література | Завдан-ня, год. | Термін виконанн-я |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|------------|-----------------|-------------------|
| 1-2 | Тема 1. Вступ до машинного навчання та адаптивного інтелекту. Методи машинного навчання з вчителем. Лінійна та поліноміальна регресія | лекція, самостійна робота | [1-9] | 2 7 | 1 тиждень |
| | Тема 1. Вирішення задач за допомогою лінійної та поліноміальної регресії. | лаб | [1-9] | 2 | |
| 3-4 | Тема 2. Методи машинного навчання з вчителем. Задача класифікації. K-NN, Naïve Bayes, SVM, Logistic regression. | лекція, самостійна робота | [1-9] | 2 7 | 1 тиждень |
| | Тема 2. Вирішення задач за допомогою методів K-NN, Naïve Bayes, SVM, Logistic regression. | лаб. | [1-9] | 2 | |
| 5-6 | Тема 3. Методи самонавчання. Задача кластеризації. DBSCAN, K-means, fuzzy c-means, методи ієрархічної кластеризації. | лекція, самостійна робота | [1-9] | 2 7 | 1 тиждень |
| | Тема 3. Вирішення практичних задач на основі методів DBSCAN, K-means, fuzzy c-means, методи ієрархічної кластеризації. | лаб | [1-9] | 2 | |
| 7-8 | Тема 4. Методи зменшення розмірності. PCA, SVD, t-SNE | лекція, самостійна робота | [1-9] | 2 7 | 1 тиждень |
| | Тема 4. Вирішення практичних задач зменшення розмірності на основі методів PCA, SVD, t-SNE та візуалізація результатів | лаб. лаб. | [1-9] | 2 7 | |
| 9-10 | Тема 5. Пошук аномалій в даних на базі методів кластеризації та ізоляційних дерев | лекція, самостійна робота | [1-9] | 2 7 | 1 тиждень |
| | Тема 5. Вирішення задачі пошуку аномалій на базі методів кластеризації та ізоляційних дерев | лаб. | [1-9] | 2 | |
| 11-12 | Тема 6. Ансамблеєві методи. Stacking, bagging, boosting. Алгоритми машинного навчання Adaboost, Catboost, XGboost, LightGBM | лекція, самостійна робота | [1-5] | 2 7 | 1 тиждень |
| | Тема 6. Вирішення задач регресії та класифікації на базі методів Adaboost, Catboost, XGboost, LightGBM | лаб. | [1-9] | 2 | |
| 13-14 | Тема 7. Нейронні мережі. Архітектури, алгоритми навчання, регуляризація. | лекція, самостійна робота | [1-9] | 2 8 | 1 тиждень |
| | Тема 7. Вирішення задач | лаб. | [1-9] | 2 | |

| | | | | | |
|-------|---------------------------------------------------------------------------------------------------------|---------------------------|-------|-----------|-----------|
| | класифікації, регресії та прогнозування на базі нейронних мереж. | | | | |
| 15-16 | Тема 8. Основи розгортання моделей. Flask і Fastapi. Огортання моделей машинного навчання в API. | лекція, самостійна робота | [1-9] | 2 8 | 1 тиждень |
| | Тема 8. Практичне використання Flask і Fastapi та огортання моделей машинного навчання в API. | лаб. | [1-9] | 2 | |
| | Всього | | | 90 | |