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 "Оцінки похибок при застосуванні методів машинного навчання", що викладається в межах ОПП Технології штучного інтелекту в кібербезпеці другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека та захист інформації

Львів - 2024

Назва дисципліни	Оцінки похибок при застосуванні методів машинного навчання
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	Венгерський Петро Сергійович, доктор фіз.-мат. наук, Грицишин Остап Орестович, асистент кафедри кібербезпеки
Контактна інформація викладачів	https://ami.lnu.edu.ua/employee/venherskyi petro.venherskyy@lnu.edu.ua https://ami.lnu.edu.ua/employee/hrytsyshyn-o-o ostap.hrytsyshyn@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/лабораторних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/otsinky-pokhybok-pry-zastosuvanni-metodiv-mashynnoho-navchannia
Інформація про дисципліну	Дисципліна “Оцінки похибок при застосуванні методів машинного навчання” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається у 1-му семестрі другого (магістерського) рівня освіти в обсязі 4 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).

Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області оцінки похибок при застосуванні методів машинного навчання. У процесі вивчення курсу студенти опанують ключові методи оцінки ефективності моделей, зокрема ROC-криві, точність, повноту, F-міру, та зможуть ідентифікувати та вирішувати проблеми перенавчання. Окрім того, курс охоплює основи роботи з регресійними та лінійними моделями, особливості їх застосування в кібербезпеці та інших сферах, а також аналіз розмірів вибірки для підвищення якості навчання моделей.
Мета та цілі дисципліни	Метою курсу є вивчення принципів оцінки похибок при застосуванні методів машинного навчання, а також набуття знань щодо аналізу ефективності та надійності моделей. Студенти вивчатимуть різні методи оцінки класифікації, виявлення перенавчання та вибору оптимального розміру вибірки. Курс спрямований на розвиток вміння застосовувати отримані знання на практиці для покращення точності та надійності моделей машинного навчання в різних сферах, зокрема в кібербезпеці та аналізі даних.
Література для вивчення дисципліни	Основна: 1. Методи штучного інтелекту в кібербезпеці [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря 2. Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. – Електронні текстові дані (1 файл: 19,9 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022 – 82 с. 3. Goodfellow, I., Bengio, Y., Courville, A. (2020). Deep Learning. MIT Press. 4. Murphy, K. P. (2022). Probabilistic Machine Learning: An Introduction. MIT Press. Додаткова: 5. Flach, P. (2020). Machine Learning: The Art and Science of Algorithms that Make Sense of Data. 2nd Edition, Cambridge University Press. 6. Schölkopf, B., & Smola, A. (2020). Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond. MIT Press.
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 год.

Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** ● класи задач, які розв'язуються методами машинного навчання; ● базові принципи роботи регресійних та лінійних моделей; ● основи побудови систем машинного навчання з можливістю навчання; ● методи оцінки класифікаторів (точність, повнота, F-міра); ● принципи побудови ROC-кривих для оцінки якості моделі; ● методи боротьби з перенавчанням, включаючи DropOut; ● критерії вибору оптимального розміру вибірки для навчання моделей; **вміти:** ● оцінювати якість моделей машинного навчання за допомогою ROC-кривих; ● проводити розрахунки точності, повноти та F-міри для класифікаторів; ● застосовувати методи запобігання перенавчанню в нейронних мережах; ● використовувати підходи до вибору адекватного розміру вибірки для ефективного навчання; ● аналізувати та інтерпретувати результати моделей машинного навчання в різних галузях, таких як кібербезпека та аналіз даних; ● ідентифікувати та вирішувати проблеми, пов'язані з похибками моделей машинного навчання.
Ключові слова	Машинне навчання, похибка класифікації, оцінка моделей, ROC-крива, точність, повнота, F-міра, регресійна модель, лінійна класифікація, узагальнений персептрон, перенавчання, DropOut, зворотне розповсюдження похибки, машина Больцмана, кібербезпека, розмір вибірки, оптимізація моделей, нейронні мережі, системи з можливістю навчання.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче

Підсумковий контроль, форма	Залік у кінці семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, модульний контроль, лабораторні роботи
Необхідне обладнання	Лабораторія з обладнаними робочими станціями, з'єднаними в комп'ютерну мережу. IDE для програмування мовою C++, C#, Python або Java.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються наступним чином: ● Модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів — 50. ● Лабораторні роботи, самостійна робота, активність на заняттях: 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 можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні 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. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані на лабораторних заняттях, самостійній роботі та бали підсумкового

тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень 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 виконання 5-ти індивідуальних завдань		
Критерії оцінювання (5*8 балів)	**40 балів**	
Студент в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час захисту індивідуальних завдань, глибоко та всебічно розкриває зміст теоретичних питань. Реалізоване програмне забезпечення пройшло перевірку на плагіат та повністю виконує умову завдання.	**8**	
Студент достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час захисту індивідуальних завдань, в основному розкриває зміст теоретичних питань. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації. Реалізоване програмне забезпечення містить окремі несуттєві неточності та незначні помилки.	**7-5**	
Студент не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час захисту індивідуального завдання, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності, програмна реалізація завдання частково виконана.	**4-1**	
Студент не виконав лабораторне завдання та не володіє матеріалом.	**0**	
2. Самостійна робота студентів (СРС)		
Критерії оцінювання (5*2 балів)	**10 балів**	
Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел) Самостійна робота студентів, оцінюється під час захисту відповідних лабораторних робіт. Студент додатково опрацював матеріал, підготував доповідь та аргументовано його викладає.	**2**	
Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**	

	3. Модульний контроль	
	Критерії оцінювання (2*25 балів)	**50 балів**
	Протягом семестру проводиться **2 модульних контролі**. Кожен модуль містить **25 тестових питань.**	
	Критерії оцінювання відповіді на тестові питання (25*1 бал):	**25**
	Відповідь правильна	**1**
	Відповідь не надана або неправильна	**0**
	Загальна кількість балів по завершенні вивчення дисципліни	**100**
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.	

Схема курсу

№	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1-2	**Тема 1. Застосування методів в кібербезпеці** Розгляд застосування методів машинного навчання для виявлення та запобігання кіберзагрозам. у кібербезпеці.	лекція, самостійна робота	[1-4]	4 6	2 тижні
		лабораторна	[1-4]	4	
3	**Тема 2. Регресійні моделі** Побудова та використання регресійних моделей у машинному навчанні. Методи оцінки похибок.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	
4	**Тема 3. Використання лінійних моделей для класифікації** Методи класифікації, які базуються на лінійних моделях. Порівняння ефективності.	лекція, самостійна робота	[1-4]	2 4	1 тиждень

		лабораторна	[1-4]	2	
5-6	**Тема 4. Базові можливості машинного навчання** Основи та можливості машинного навчання: підхід до розв'язання задач.	лекція, самостійна робота	[1-4]	4 6	2 тижні
		лабораторна	[1-4]	4	
7	**Тема 5. Системи із можливістю навчання** Розгляд систем, що можуть навчатися на даних і покращувати свої рішення з часом.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	
8	**Тема 6. Узагальнені персептрони** Математичні моделі та їх використання у класифікації та регресії.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	
9-10	**Тема 7. Метод зворотного розповсюдження похибок** Алгоритм оптимізації нейронних мереж через зворотне розповсюдження.	лекція, самостійна робота	[1-4]	4 6	2 тижні
		лабораторна	[1-4]	4	
11	**Тема 8. Машина Больцмана** Архітектура нейронних мереж і застосування машини Больцмана у задачах навчання.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	
12	**Тема 9. Складнощі розв’язання задач на основі систем із можливістю навчання**	лекція, самостійна робота	[1-4]	2 4	1 тиждень

	Аналіз обмежень і труднощів систем навчання.				
		лабораторна	[1-4]	2	
13	**Тема 10. ROC-криві** Побудова та аналіз ROC-кривих для оцінки класифікаторів.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	
14	**Тема 11. Оцінка класифікатора - точність, повнота, F-міра** Методи оцінки продуктивності класифікаторів.	лекція, самостійна робота	[1-4]	2 3	1 тиждень
		лабораторна	[1-4]	2	
15	**Тема 12. Перенавчання та метод DropOut** Методи боротьби з перенавчанням та використання DropOut для покращення моделей.	лекція, самостійна робота	[1-4]	2 3	1 тиждень
		лабораторна	[1-4]	2	
16	**Тема 13. Розмір вибірки для машинного навчання** Визначення оптимального розміру вибірки для ефективного навчання моделей.	лекція, самостійна робота	[1-4]	2 4	1 тиждень
		лабораторна	[1-4]	2	