



MLOps у веб-системах

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>F Інформаційні технології</i>
Спеціальність	<i>F3 Комп'ютерні науки</i>
Освітня програма	<i>Технології візуальних обчислень</i>
Статус дисципліни	<i>Вибірковий</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, 2 семестр</i>
Обсяг дисципліни	<i>4 кредитів (120 годин) 30 лек. 14 лаб. 76 СРС</i>
Семестровий контроль/ контрольні заходи	<i>Залік, МКР</i>
Розклад занять	https://schedule.kpi.ua/
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	Лектор: к.т.н., доц. Полягушко Любов Григорівна, liubovpoliagushko@gmail.com Лабораторні: ас. Рудик Володимир Іванович, rudyk.volodymyr@iit.kpi.ua
Розміщення курсу	Засоби Classroom та e-mail.

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Програму навчальної дисципліни «MLOps у веб-системах» складено відповідно до освітньої програми освітньо-професійної програми «Технології візуальних обчислень» другого рівня вищої освіти спеціальності F3 «Комп'ютерні науки».

Метою навчальної дисципліни є підготовка фахівців, здатних забезпечувати повний життєвий цикл моделей машинного навчання у веб-системах – від розробки та версіонування до автоматизованого розгортання, моніторингу та промислової експлуатації, що відповідає сучасним інженерним практикам та потребам ринку праці у сфері MLOps.

У результаті вивчення дисципліни студенти мають продемонструвати:

- Пояснювати принципи MLOps та обґрунтовувати архітектурні рішення для організації повного життєвого циклу ML-проектів у веб-системах.
- Розробляти автоматизовані ML-пайплайни з валідацією даних, версіонуванням моделей та налаштуванням CI/CD для безперервної інтеграції і доставки.
- Контейнеризувати ML-застосунки та розгортати їх з використанням Kubernetes, створювати REST API для інтеграції моделей з веб-додатками.
- Налаштовувати системи моніторингу продуктивності моделей, виявляти дрейф даних і моделей та впроваджувати стратегії безпечного оновлення у виробничому середовищі.

- Проєктувати та супроводжувати надійні ML-системи у промисловому середовищі з дотриманням вимог безпеки та нормативного регулювання.

2. Пререквізити та постреквізити дисципліни

У структурно-логічній схемі навчальна дисципліна «MLOps у веб-системах» розміщена тоді, коли студенти вже прослухали навчальні дисципліни Методи та системи штучного інтелекту, Вступ до інтелектуального аналізу даних, Технології розробки програмного забезпечення, що достатньо для виконання лабораторних робіт з даної дисципліни.

Отримані знання можна використовувати при виконанні магістерської дисертації.

3. Зміст навчальної дисципліни

Розділ 1. Основи MLOps

Тема 1.1. Концептуальні засади MLOps

Тема 1.2. Управління даними в MLOps

Розділ 2. Розробка та версіонування

Тема 2.1. Система контролю версій для ML

Тема 2.2. Безперервна інтеграція та доставка

Розділ 3. Контейнеризація та оркестрація

Тема 3.1. Контейнеризація ML-застосунків

Тема 3.2. Оркестрація та мікросервісна архітектура

Тема 3.3. Обслуговування моделей

Розділ 4. Моніторинг та підтримка

Тема 4.1. Спостережуваність ML-систем

Тема 4.2. Управління життєвим циклом моделей

Розділ 5. Хмарні технології та безпека

Тема 5.1. Хмарні MLOps платформи

Тема 5.2. Безпека та дотримання нормативних вимог

4. Навчальні матеріали та ресурси

Базова:

1. Gift N., Deza A. Practical MLOps: Operationalizing Machine Learning Models. O'Reilly Media, 2021. 368 p.
2. Alla S., Adari S.K. Beginning MLOps with MLFlow: Deploy Models in AWS SageMaker, Google Cloud, and Microsoft Azure. Apress, 2021. 447 p.
3. Hapke H., Nelson C. Building Machine Learning Pipelines: Automating Model Life Cycles with TensorFlow. O'Reilly Media, 2020. 394 p.
4. Chen E. Designing Machine Learning Systems: An Iterative Process for Production-Ready Applications. O'Reilly Media, 2022. 394 p.
5. Lakshmanan V., Robinson S., Munn M. Machine Learning Design Patterns: Solutions to Common Challenges in Data Preparation, Model Building, and MLOps. O'Reilly Media, 2020. 408 p.

Додаткова:

6. MLflow Documentation. URL: <https://mlflow.org/docs/latest/index.html>
7. Kubeflow Documentation. URL: <https://www.kubeflow.org/docs/>
8. TensorFlow Extended (TFX) Guide. URL: <https://www.tensorflow.org/tfx>
9. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. 3rd Edition. O'Reilly Media, 2022. 861 p.
10. Burns B., Beda J. Kubernetes: Up and Running. 2nd Edition. O'Reilly Media, 2019. 318 p.
11. AWS SageMaker Developer Guide. URL: <https://docs.aws.amazon.com/sagemaker/>
12. Google Cloud AI Platform Documentation. URL: <https://cloud.google.com/ai-platform/docs>
13. Azure Machine Learning Documentation. URL: <https://docs.microsoft.com/en-us/azure/machine-learning/>

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

Лекційні заняття

РОЗДІЛ 1. ОСНОВИ MLOPS

Тема 1.1. Концептуальні засади MLOps

Лекція 1. Вступ до MLOps

Огляд еволюція від традиційної розробки програмного забезпечення через DevOps до спеціалізованих практик MLOps. Аналіз основних викликів, що виникають при переході від експериментальних моделей машинного навчання до виробничих систем, включаючи проблеми відтворюваності, масштабованості та підтримки.

Лекція 2. Життєвий цикл проектів машинного навчання у веб-системах

Повний життєвий цикл проекту машинного навчання від ідеї до виведення моделі з експлуатації у виробничому середовищі. Порівнення підходів, орієнтовані на дані, та підходів, орієнтовані на модель, до розробки, аналізуються їх переваги та недоліки в контексті веб-додатків. Методологія управління експериментами та стратегії переходу від прототипування до промислової експлуатації моделей.

Тема 1.2. Управління даними в MLOps

Лекція 3. Версіонування та управління якістю даних

Принципи та інструменти версіонування наборів даних у проектах машинного навчання. Концепції відстеження походження даних та управління даними як основи для забезпечення прозорості та відстежуваності походження даних. Методи перевірки якості даних, виявлення аномалій та забезпечення узгодженості даних між різними середовищами розробки та промислової експлуатації.

РОЗДІЛ 2. РОЗРОБКА ТА ВЕРСІОНУВАННЯ

Тема 2.1. Система контролю версій для машинного навчання

Лекція 4. Версіонування моделей та експериментів

Особливості версіонування коду машинного навчання порівняно з традиційним програмним забезпеченням. Стратегії семантичного версіонування моделей машинного навчання та управління артефактами. Принципи функціонування реєстру моделей як центрального компонента для зберігання та управління версіями моделей, а також методи забезпечення відтворюваності експериментів.

Тема 2.2. Безперервна інтеграція та доставка

Лекція 5. Пайплайни безперервної інтеграції та доставки для машинного навчання

Особливості адаптації практик безперервної інтеграції та безперервного розгортання для проектів машинного навчання. Стратегії автоматизації процесів навчання, перевірки та розгортання моделей. Інструменти та платформи для створення пайплайнів, специфічних для машинного навчання, включаючи інтеграцію з популярними системами контролю версій.

Лекція 6. Тестування в системах машинного навчання

Методології тестування систем машинного навчання на різних рівнях від модульних тестів компонентів до інтеграційного тестування повних пайплайнів. Підходи до тестування якості та узгодженості даних, перевірки продуктивності моделей та їх поведінки у граничних випадках. Методи A/B тестування моделей у виробничому середовищі та стратегії експериментального розгортання.

РОЗДІЛ 3. КОНТЕЙНЕРИЗАЦІЯ ТА ОРКЕСТРАЦІЯ

Тема 3.1. Контейнеризація застосунків машинного навчання

Лекція 7. Docker для машинного навчання

Принципи контейнеризації додатків машинного навчання з урахуванням специфіки залежностей машинного навчання. Стратегії створення оптимізованих образів Docker для різних типів навантажень машинного навчання, включаючи навчання та виведення прогнозів. Методи управління секретами, конфігураціями та постійними даними в контейнеризованих системах машинного навчання.

Тема 3.2. Оркестрація та мікросервісна архітектура

Лекція 8. Kubernetes для навантажень машинного навчання

Можливості Kubernetes для оркестрації навантажень машинного навчання у веб-системах. Специфічні ресурси та оператори для машинного навчання, стратегії автоматичного масштабування на основі метрик систем машинного навчання. Шаблони мікросервісної архітектури для додатків машинного навчання та інтеграція з сервісною мережею для забезпечення надійності та спостережуваності.

Тема 3.3. Обслуговування моделей

Лекція 9. Розгортання та обслуговування моделей у веб-середовищі

Різні підходи до обслуговування моделей, включаючи пакетне виведення прогнозів та виведення в режимі реального часу. Архітектурні шаблони для створення програмних інтерфейсів машинного навчання та інтеграції з веб-додатками. Спеціалізовані сервери моделей та їх можливості, стратегії оптимізації продуктивності виведення прогнозів та розгортання на граничних пристроях для веб-систем.

РОЗДІЛ 4. МОНІТОРИНГ ТА ПІДТРИМКА

Тема 4.1. Спостережуваність систем машинного навчання

Лекція 10. Моніторинг продуктивності та якості моделей

Метрики для моніторингу систем машинного навчання у виробничому середовищі, включаючи бізнес-метрики, технічні показники та метрики якості моделей. Методи виявлення дрейфу даних та дрейфу моделі, їх вплив на продуктивність системи. Інструменти та платформи для збору, зберігання та візуалізації метрик систем машинного навчання.

Лекція 11. Логування та трасування в системах машинного навчання

Принципи структурованого логування для додатків машинного навчання з урахуванням специфіки відстеження експериментів та виведення прогнозів. Методи розподіленого трасування для складних пайплайнів машинного навчання та мікросервісних архітектур. Вимоги до аудиту систем машинного навчання, дотримання нормативних вимог та логування із збереженням конфіденційності в контексті захисту персональних даних.

Тема 4.2. Управління життєвим циклом моделей

Лекція 12. Стратегії оновлення та відкату моделей

Методи керування моделями в промисловій експлуатації, включаючи стратегії поступового розгортання нових версій. Підходи поступового розгортання та синьо-зеленого розгортання для систем машинного навчання, їх переваги та недоліки. Механізми автоматичного повернення до попередньої версії при погіршенні якості моделі та процедури аварійного відновлення сервісів машинного навчання.

РОЗДІЛ 5. ХМАРНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

Тема 5.1. Хмарні платформи MLOps

Лекція 13. Керовані сервіси машинного навчання та архітектурні рішення

Можливості провідних хмарних платформ для MLOps, включаючи AWS SageMaker, Azure Machine Learning та Google AI Platform. Переваги керованих сервісів порівняно з рішеннями на власній інфраструктурі в контексті різних типів організацій та проектів. Безсерверні підходи до машинного навчання та стратегії вибору оптимальної архітектури для конкретних веб-додатків.

Тема 5.2. Безпека та дотримання нормативних вимог

Лекція 14. Забезпечення безпеки пайплайнів машинного навчання

Специфічні загрози безпеці для систем машинного навчання, включаючи змагальні атаки, крадіжку моделей та отруєння даних. Методи захисту даних та моделей на всіх етапах життєвого циклу. Вимоги регулювання та дотримання нормативних вимог для систем машинного навчання у різних галузях, включаючи Загальний регламент захисту даних та інші нормативні акти щодо захисту персональних даних.

Лекція 15. Проведення модульної контрольної роботи

Лабораторні заняття

Лабораторна робота №1. Налаштування базового MLOps середовища	2 год.
Лабораторна робота №2. Розробка ML-пайплайну з валідацією	2 год.

Лабораторна робота №3. Автоматизація з GitHub Actions	2 год.
Лабораторна робота №4. Створення ML API та контейнеризація	2 год.
Лабораторна робота №5. Моніторинг та метрики	3 год.
Лабораторна робота №6. A/B тестування та управління версіями моделей	3 год.

6. Самостійна робота студента

*Самостійна робота студента складає 76 години та передбачає:
підготовку до аудиторних занять – 66 год.,
підготовку до МКР – 4 год.,
підготовку до заліку – 6 год.*

Теми для самостійного опрацювання:

Тема 1.1: Концептуальні засади MLOps

Основні відмінності між традиційним DevOps та MLOps підходами та причини виникнення потреби у спеціалізованих практиках для машинного навчання.

Тема 1.2: Управління даними в MLOps

Концепція відстеження походження даних як засіб забезпечення прозорості та відстежуваності в пайплайнах машинного навчання та інструменти для її реалізації.

Тема 2.1: Система контролю версій для машинного навчання

Відмінності семантичного версіонування моделей машинного навчання від версіонування традиційного програмного забезпечення та принципи, які слід використовувати.

Тема 2.2: Безперервна інтеграція та доставка

Специфічні етапи пайплайну безперервної інтеграції та доставки для проекту машинного навчання порівняно з традиційним веб-додатком.

Тема 3.1: Контейнеризація застосунків машинного навчання

Основні виклики контейнеризації додатків машинного навчання та методи оптимізації розміру образів Docker для різних типів навантажень машинного навчання.

Тема 3.2: Оркестрація та мікросервісна архітектура

Переваги використання операторів Kubernetes для навантажень машинного навчання порівняно зі стандартними ресурсами.

Тема 3.3: Обслуговування моделей

Доцільність використання пакетного виведення прогнозів замість обслуговування в режимі реального часу та архітектурні компроміси цього підходу.

Тема 4.1: Спостережуваність систем машинного навчання

Відмінності між дрейфом даних та дрейфом моделі і найефективніші стратегії моніторингу для кожного типу.

Тема 4.2: Управління життєвим циклом моделей

Критерії для автоматичного повернення до попередньої версії моделі та методи уникнення хибнопозитивних спрацьовувань.

Тема 5.1: Хмарні платформи MLOps

Критерії вибору між керованими сервісами машинного навчання та рішеннями на власній інфраструктурі для конкретного проекту.

Тема 5.2: Безпека та дотримання нормативних вимог

Найкритичніші типи змагальних атак для моделей машинного навчання у веб-системах та методи захисту від них.

Тема 5.3: Перспективи розвитку MLOps

Вплив федеративного навчання на традиційні практики MLOps та нові виклики для веб-систем.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- Відвідування лекцій та лабораторних занять, а також відсутність на них, не оцінюється.
- При захисті лабораторних робіт студент має продемонструвати розроблений програмний код та результати його виконання на тестах, як заздалегідь підготованих, так і запропонованих викладачем. У випадку дистанційної форми навчання захист відбувається на відповідній конференції шляхом демонстрації екрана.
- Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.
- Норми етичної поведінки Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

1. **Поточний контроль.** Семестровий рейтинг (виконання робіт в семестрі) оцінюється у 100 балів. Розподіл балів наведено в таблиці:

Види робіт	Бали
Лабораторна робота №1. Налаштування базового MLOps середовища	15
Лабораторна робота №2. Розробка ML-пайплайну з валідацією	15
Лабораторна робота №3. Автоматизація з GitHub Actions	15
Лабораторна робота №4. Створення ML API та контейнеризація	15
Лабораторна робота №5. Моніторинг та метрики	15
Лабораторна робота №6. А/В тестування та управління версіями моделей	15
Модульна контрольна робота	10
Всього	100

Критерії оцінювання заходів поточного контролю:

- 90–100% від максимуму – повне виконання, коректний код, вичерпні відповіді
- 70–89% – виконано з незначними недоліками
- 50–69% – виконано з помилками та неточностями
- 10–49% – часткове виконання, суттєві помилки
- 0% – не виконано або не захищено

За несвоєчасне подання лабораторної роботи (після встановленого терміну) нараховується штраф у розмірі 20% від отриманої оцінки.

Модульна контрольна робота оцінюється у 10 балів і проводиться у формі тесту з 20 питань по 0,5 бала кожне. Відповідь на кожне питання оцінюється як правильна (0,5 бала) або неправильна (0 балів). За несвоєчасне виконання МКР нараховується штраф у розмірі 20% від отриманої оцінки.

2. **Календарний контроль** проводиться двічі на семестр як моніторинг поточного стану виконання вимог програми:

Критерій	Перший календарний контроль	Другий календарний контроль
Термін календарного контролю	Тиждень 6-7	Тиждень 12-13
Умови отримання позитивної оцінки	≥ 24 бали	≥ 45 балів

3. **Умови допуску до заліку:** відсутність заборгованостей з лабораторних робіт 1 - 6.

Студенти, які виконали умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань.

Зі студентами, які виконали умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими студентами, хто бажає підвищити свою рейтингову оцінку, під час заліково-екзаменаційної сесії проводиться семестровий контроль у вигляді заліку. При цьому попередній рейтинг скасовується і студенти отримують рейтингову оцінку за результатами заліку («жорсткий» підхід).

4. **Семестровий контроль** – залік.

Відповідь на заліку оцінюється у 100 балів. Залікова робота складається з одного теоретичного питання та одного практичного завдання. Ваговий бал теоретичного питання – 50 балів, завдання – 50 балів.

Теоретична частина оцінюється таким чином:

- правильна чітко викладена, повна відповідь – (не менше 90% потрібної інформації) – 45-50 балів;
- достатньо повна відповідь (не менше 75% потрібної інформації) – 38-44 бали;
- неповна відповідь (не менше 60% потрібної інформації) – 30-37 балів;
- незадовільна відповідь – 0 балів.

Практичне завдання оцінюється таким чином:

- повне, безпомилкове розв'язування завдання – 45-50 балів;
- повне, розв'язування завдання із несуттєвими невідповідностями – 38-44 бали;
- завдання виконане з певними недоліками – 30-37 балів;
- завдання не виконано – 0 балів.

5. Рейтингова оцінка за освітній компонент за бажанням студента визначається одним з таких способів:

- 1) кількість балів, отриманих за поточний контроль, або
- 2) результат виконання залікової контрольної роботи (тоді не враховуються бали, отримані в семестрі).

Таблиця переведення рейтингових балів у оцінку за університетською шкалою:

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено доцентом каф. ЦТЕ, к.т.н., доц. Полягушко Любов'ю Григорівною

Ухвалено кафедрою ЦТЕ (протокол № 22 від 17.06.2026)

Погоджено Методичною комісією НН ІАТЕ КПІ ім. Ігоря Сікорського (протокол № 9 від 26.06.26)