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

“ШІ в задачах доступності та самовідновлення”,

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	ШІ в задачах доступності та самовідновлення
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	Журавчак Даниїл Юрійович, доцент кафедри кібербезпеки
Контактна інформація викладачів	danyil.zhuravchak@lnu.edu.ua; https://ami.lnu.edu.ua/employee/zhuravchak-d-yu 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 (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/course/shi-v-zadachakh-dostupnosti-ta-samovidnovlennia
Інформація про дисципліну	Дисципліна “Штучний інтелект у задачах доступності та самовідновлення” є вибірковою дисципліною з спеціальності 125 — кібербезпека та захист інформації для освітньої програми “Технології штучного інтелекту в кібербезпеці”, яка викладається в 3-му семестрі в обсязі 3-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Дисципліна “Штучний інтелект у задачах доступності та самовідновлення” охоплює теоретичні та практичні аспекти використання штучного інтелекту для забезпечення високої доступності систем та їх автоматизованого відновлення після збоїв. Студенти ознайомляться з методами прогнозування збоїв, алгоритмами самовідновлення та інструментами ШІ для аналізу доступності. Курс включає як теоретичні основи, так і практичні завдання з використання технологій ШІ для покращення надійності інформаційних систем.
Мета та цілі дисципліни	Метою викладання дисципліни є формування у студентів знань та навичок щодо використання штучного інтелекту для забезпечення високої доступності інформаційних систем і їхнього самовідновлення після збоїв. Студенти навчаться прогнозувати збої, розробляти алгоритми самовідновлення, а також застосовувати методи машинного навчання для аналізу доступності систем. Окремою метою є формування розуміння щодо використання сучасних інструментів і технологій для підвищення надійності та стабільності кіберсистем.
Література для вивчення дисципліни	**1. Базова література** 1. Russell S., Norvig P. “Artificial Intelligence: A Modern Approach”, 4th Edition, Pearson, 2020.

	2. Rao V., Atchison B. “AIOps: Real-world Applications of Artificial Intelligence for IT Operations”, Manning, 2021. 3. Nash K. “Accelerating AIOps with Machine Learning”, O’Reilly Media, 2020. 4. Goodfellow I., Bengio Y., Courville A. “Deep Learning”, MIT Press, 2021 (оновлене видання). **2. Допоміжна література** 5. Bishop C. M. “Pattern Recognition and Machine Learning”, Springer, 2006. 6. Goodfellow I., Bengio Y., Courville A. “Deep Learning”, MIT Press, 2016. 7. Murphy K. “Machine Learning: A Probabilistic Perspective”, MIT Press, 2012. 8. Sutton R. S., Barto A. G. “Reinforcement Learning: An Introduction”, 2nd Edition, MIT Press, 2018. 9. LeCun Y., Bengio Y., Hinton G. “Deep Learning”, Nature, 2015. 10. Rao V., Atchison B. “AIOps: Real-world Applications of Artificial Intelligence for IT Operations”, Manning, 2021. 11. Nash K. “Accelerating AIOps with Machine Learning”, O’Reilly Media, 2020. 12. Friedrich M. “Mastering AIOps: Automate IT Operations and Reduce Operational Costs”, Packt Publishing, 2021. **3. Інтернет-ресурси** 13. National Institute of Standards and Technology (NIST). “Framework for Improving Critical Infrastructure Cybersecurity”. https://www.nist.gov 14. The Future of Privacy Forum (FPF). “Privacy and Artificial Intelligence”. https://fpf.org. 15. Dynatrace Blog. “AIOps: How AI is Revolutionizing IT Operations”. https://www.dynatrace.com 16. Gartner. “Market Guide for AIOps Platforms”. https://www.gartner.com
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 32 год., з них 16 год. лекцій та 16 год. лабораторних робіт. Самостійної роботи: 48 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: Знання**:** 1. Знати основні принципи забезпечення доступності та самовідновлення систем. a. Розуміти концепції високої доступності, резервування ресурсів та основних підходів до автоматизованого відновлення після збоїв. b. Знати методи штучного інтелекту, які використовуються для прогнозування збоїв і підтримки доступності.

	2. Ознайомитися з концепціями AIOps: a. Знати основи використання AIOps для автоматизації управління IT-операціями, аналізу журналів подій та виявлення аномалій. Уміння**:** 1. Аналізувати та прогнозувати збої: a. Уміти використовувати алгоритми машинного навчання для прогнозування можливих відмов та забезпечення безперервної роботи систем. 2. Розробка та реалізація рішень для самовідновлення: a. Застосовувати принципи самовідновлення та використовувати алгоритми для автоматизації процесу відновлення після збоїв. Навички**:** 1. Робота з інструментами AIOps: a. Використовувати інструменти та алгоритми для моніторингу доступності систем, виявлення аномалій та автоматизованого реагування на збої. 2. Практичне застосування методів штучного інтелекту: a. Вміти інтегрувати алгоритми ШІ для підвищення надійності та стабільності інформаційних систем.
Ключові слова	AIOps, доступність, самовідновлення, штучний інтелект (ШІ), машинне навчання, автоматизація IT-операцій, прогнозування збоїв, відновлення систем, кіберстійкість, аномалії, алгоритми самонавчання, моніторинг систем, надійність, хмарні технології, високий рівень доступності, аналіз журналів подій, автоматизоване реагування, безперервна робота, IT інфраструктура, операційна ефективність.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік в кінці 3 семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисципліни: • Кібербезпека. • Штучний інтелект. • IT моніторинг та менеджмент • Журналювання подій • ITIL
Навчальні методи та тех.-ніки, які будуть використовуватися під час викладання курсу	Лекції — інформаційно-рецептивний метод для викладу теоретичних знань. Практичні заняття — практичне застосування набутих знань, включаючи використання інструментів ШІ для аналізу загроз. Самостійна робота — виконання індивідуальних завдань та підготовка рефератів. Воркшопи — обговорення етичних кейсів, робота у групах над практичними завданнями.
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 упродовж семестру за 100-бальною шкалою. Бали нараховуються за такими видами робіт з наступним співвідношенням: • робота під час лабораторних занять: 50% семестрової оцінки; максимальна кількість балів 50; • самостійна робота: 30% семестрової оцінки; максимальна кількість балів 30; • контрольна робота: 20% семестрової оцінки; максимальна кількість балів 20. Підсумкова максимальна кількість балів 100. **Академічна доброчесність:** очікується, що роботи студентів будуть оригінальними дослідженнями чи міркуваннями. Списування та втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в написанні завдань є підставою для її незарахуваннння викладачем, незалежно від масштабів плагіату чи обману. Жодні форми порушення академічної доброчесності не толеруються. **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 робіт, 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. **Політика виставлення балів.** Враховуються бали, набрані при поточному контролі та бали за виконання лабораторних робіт. 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. **Оцінювання роботи на лабораторних заняттях:** студенти на 8 лабораторних заняттях виконують різноманітні вправи та завдання. У підсумку максимальна кількість балів студента за роботу на лабораторних заняттях - 50. Бали оцінювання роботи на лабораторних заняттях нараховуються за наступним співвідношенням: 3-4 – студент в повному обсязі володіє навчальним матеріалом, має повне розуміння досліджуваної проблеми, надає правильні відповіді на запитання по темі, має свої ідейні міркування щодо реалізації даної проблеми; 1-2 – студент не достатньо розуміє приведені ним результати, вагається та надає неточні/не конкретні відповіді на запитання по темі; 0 - студент безвідповідально відносився до виконання роботи, студент виявляє нульовий рівень компетентності та зовсім не засвоїв розглянутий матеріал. Також за запропоновані новітні методи, активність і креативність під час лабораторних занять студент може набрати додаткових 9 балів.

	Оцінювання самостійної роботи: студенти самостійно виконують завдання для 8 домашніх робіт. У підсумку максимальна кількість балів студента за самостійну роботу - 30. Бали оцінювання самостійної роботи нараховуються за наступним співвідношенням: 3-4 – робота цілком і повністю відображає індивідуальне завдання студента, містить правильні висновки, ілюстрований (за потреби) відповідними графіками, студент має повне розуміння розглянутої теми, надає правильні відповіді на запитання по темі; 2 – робота в достатній мірі відображає індивідуальне завдання студента, містить допустимі висновки, ілюстрований (за потреби) відповідними графіками, які частково відображають суть виконаного завдання, присутні неточності та незначні помилки у відповідях на запитання по темі; 1 – звіт містить загальні формулювання завдання, висновки нечіткі, необхідні ілюстрації відсутні, студент не досить добре розуміє розглянутий матеріал, надає неточні/не конкретні відповіді на запитання по темі; 0 - робота відсутня/не відповідає темі, студент зовсім не засвоїв розглянутий матеріал. **Оцінювання контрольної роботи:** 10 тестових теоретичних питань (по 1 балу за кожне) та 2 практичних завдання (по 5 балів кожне). Бали оцінювання практичного завдання залікової (контрольної) роботи нараховуються за наступним співвідношенням: 5 – студент в повному обсязі володіє навчальним матеріалом, має повне розуміння досліджуваної проблеми, надає правильні відповіді на запитання по темі, має свої ідейні міркування щодо реалізації даної проблеми; 3-4 – студент достатньо розуміє розглянутий матеріал, демонструє достатній рівень обґрунтування результатів (або з несуттєвими недоліками); 2 – студент не достатньо розуміє приведені ним результати, вагається та надає неточні/не конкретні відповіді на запитання по темі; 1 – студент погано розуміє приведені результати, у більшості надає помилкові відповіді на питання по роботі; 0 - студент безвідповідально відносився до виконання завдання, студент виявляє нульовий рівень компетентності та зовсім не засвоїв розглянутий матеріал. **Критерії оцінювання результатів неформальної освіти:** Нарахування балів відбувається за публікацію студентом тез доповідей на конференціях, наукових статей, за участь студента у діяльності наукових гуртків, семінарів, круглих столів, конкурсів, участь у заходах неформальної освіти, за отримання сертифікатів про проходження навчання на різних освітніх платформах (Coursera, Prometheus тощо). Кількість балів визначається відсотком покриття результатів відповідної активності до вимог результатів навчання з навчальної дисципліни.
Питання до контрольної роботи.	**Основи доступності та самовідновлення** • Що таке доступність систем і чому вона важлива в IT? • Які методи резервування ресурсів використовуються для забезпечення доступності? • Приклади впровадження концепції самовідновлення в інформаційних системах. **AIOps та його роль у забезпеченні доступності**

	• Що таке AIOps і як він використовується для управління IT-операціями? • Які ключові переваги AIOps для підвищення надійності систем? • Як AIOps допомагає в прогнозуванні збоїв? **Методи штучного інтелекту в задачах доступності** • Які алгоритми машинного навчання можуть використовуватися для прогнозування збоїв? • Як аналіз журналів подій допомагає у виявленні аномалій? • Наведіть приклади інструментів, що використовуються для автоматизації процесу відновлення. **Практичні аспекти впровадження самовідновлювальних рішень** • Які кроки необхідно виконати для впровадження рішення з самовідновлення? • Як можна оцінити ефективність відновлювальних заходів? • Приклади використання хмарних технологій для забезпечення безперервної роботи. **Моніторинг та аналіз даних для забезпечення доступності** • Які основні метрики використовуються для оцінки доступності системи? • Як аналіз даних допомагає у визначенні причин збоїв? • Роль автоматизованого моніторингу в забезпеченні безперервної роботи.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	**Тема 1. Основи конфіденційності та етики у кібербезпеці** - Визначення конфіденційності, цілісності та доступності (CIA-триада). - Етичні принципи у кібербезпеці.	Лекція, самостійна робота	[1, 3, 5, 7]	2 8	1 тиждень
	Тема 1. Основи конфіденційності та етики у кібербезпеці - Практичні завдання щодо аналізу конфіденційності та етичних аспектів у кібербезпеці.	лаб	[1, 3, 5, 7]	2	
2	**Тема 2 Персонально ідентифікована інформація (PII) та її захист** - Поняття PII, основні методи захисту персональних даних.	лекція, самостійна робота	[1, 2, 5, 6]	2 8	1 тиждень
	Тема 2. Персонально ідентифікована інформація (PII) та її захист - Практичні завдання щодо	лаб.	[1, 2, 5, 6]	2	

	ідентифікації PII та використання інструментів захисту.				
3	**Тема 3. Регуляції захисту даних** - Міжнародні та національні стандарти захисту даних (GDPR, ISO27001, Держспецзв'язок).	лекція, самостійна робота	[3, 4, 6, 7]	2 8	1 тиждень
	Тема 3. Регуляції захисту даних - Лабораторні завдання з аналізу дотримання стандартів та регуляцій конфіденційності.	лаб	[3, 4, 6, 7]	2	
4	**Тема 4 Етичні аспекти використання штучного інтелекту (ШІ) у кібербезпеці** - Потенційні ризики, пов'язані з ШІ, та етичні стандарти.	лекція, самостійна робота	[5, 7, 9, 10]	2 8	1 тиждень
	Тема 4. Етичні аспекти використання штучного інтелекту (ШІ) у кібербезпеці - Лабораторні завдання з оцінки етичних ризиків при використанні ШІ.	лаб.	[5, 7, 9, 10]	2	
5	**Тема 5. Захист даних у хмарних середовищах** - Архітектура даних та специфіка захисту у хмарах.	лекція, самостійна робота	[4, 6, 8, 11]	2 8	1 тиждень
	Тема 5. Захист даних у хмарних середовищах - Лабораторні завдання з аналізу ризиків і методів захисту даних у хмарах.	лаб.	[4, 6, 8, 11]	2	
6	**Тема 6. Методи оцінювання ризиків у кібербезпеці** - Якісна та кількісна оцінка ризиків, процес управління ризиками.	лекція, самостійна робота	[2, 4, 8, 12]	2 6	1 тиждень
	Тема 6. Методи оцінювання ризиків у кібербезпеці - Лабораторні завдання з проведення оцінки ризиків за допомогою різних методів.	лаб.	[2, 4, 8, 12]	2	
7	**Тема 7 Машинне навчання для забезпечення конфіденційності** - Алгоритми виявлення загроз та аналіз аномалій для забезпечення конфіденційності.	лекція, самостійна робота	[5, 6, 9, 12]	2 3	1 тиждень
	Тема 7. Машинне навчання для забезпечення конфіденційності - Лабораторні завдання з використання алгоритмів машинного навчання для ідентифікації загроз.	лаб.	[5, 6, 9, 12]	2	

8	**Тема 8. Комплаєнс та його роль у забезпеченні конфіденційності даних** - Основні заходи комплаєнсу, приклади інструментів для дотримання конфіденційності.	лекція, самостійна робота	[4, 7, 9, 11]	2 3	1 тиждень
	Тема 8. Комплаєнс та його роль у забезпеченні конфіденційності даних - Лабораторні завдання з оцінки політик комплаєнсу та управління конфіденційністю.	Лаб.	[4, 7, 9, 11]	2	1 тиждень
	Всього			**90**	