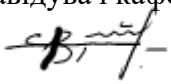
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

“Системи ШІ в задачах захисту інформації”,

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	Системи ШІ в задачах захисту інформації
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	Пелешко Дмитро Дмитрович, професор кафедри кібербезпеки
Контактна інформація викладачів	Dmytro.peleshko@lnu.edu.ua https://ami.lnu.edu.ua/employee/peleshko-d-d 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/admission/specializations
Інформація про дисципліну	Дисципліна “Системи ШІ в задачах захисту інформації ” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми «Технології штучного інтелекту в кібербезпеці», яка викладається в 1-му семестрі в обсязі 6-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів компетентностей з проектування систем глибинного навчання для аналізу і обробки потоків даних в області технологій інформаційної безпеки
Мета та цілі дисципліни	Навчальна дисципліна «Системи ШІ в задачах захисту інформації» є складовою циклу професійної підготовки фахівців другого освітньо-кваліфікаційного рівня “магістр”. Пропонований навчальний курс

	забезпечить студентам здобуття поглиблених теоретичних та практичних знань, умінь та розуміння, що відносяться до областей Neural Network, Data Science, Deep Learning, що дасть їм можливість розв'язувати різноманітні задачі аналізу даних та розроблення систем прийняття рішень на базі таких систем для виконання прикладних завдань чи бізнес-проектів у різних галузях інформаційних технологій, зокрема кібербезпеки, IoT тощо.
Література для вивчення дисципліни	Основна: 1. Christopher M. Bishop, Hugh Bishop Deep Learning: Foundations and Concepts, Springer, 2024, 656 p. 2. Nikhil Buduma, Joe Papa, Nithin Buduma Fundamentals of Deep Learning. Designing Next-Generation Machine Intelligence Algorithms. O'Reilly, 2022, 388 p. 3. Josh Patterson Deep Learning: A Practitioner's Approach. O'Reilly, 2022, 352 p. 4. Dokur, Nadide Artificial Intelligence (AI) Applications in Cyber Security, 2023 5. Stella Chen. (2024) AI (https://www.amazon.com/dp/B0CSTRD7YJ/ref=sspa_dk_detail_1?psc=1&pd_rd_i=B0CSTRD7YJ&pd_rd_w=jZp3g&content-id=amzn1.sym.7446a9d1-25fe-4460-b135-a60336bad2c9&pf_rd_p=7446a9d1-25fe-4460-b135-a60336bad2c9&pf_rd_r=QEP3ATCHPA3WN01P5NZK&pd_rd_wg=68ozJ&pd_rd_r=76970004-cfdb-4a21-a42e-c28d8fae426d&sp_csd=d2lkZ2V0TmFtZT1zcF9kZXRhaWw#detailBullets_feature_div) Допоміжна: 6. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016. 800 p. 7. Charu C. Aggarwal Neural Networks and Deep Learning. Springer International Publishing. 2018. 8. Нікольський Ю. В. Системи штучного інтелекту : навч. посібник. – 2-ге вид., випр. та доп. / Нікольський Ю. В. – Львів : Магнолія-2006, 2013. – 279 с. 9. Засоби штучного інтелекту: навч. посіб. / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2014. — 204 с. : іл. — Бібліогр.: с. 200 (11 назв). — ISBN 978-617-607-692-6 10. Системи штучного інтелекту: навч. посіб. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина ; за наук. ред. В. В. Пасічника ; М-во освіти і науки, молоді та спорту України. — 2-ге вид., виправл. та доповн. — Львів: Магнолія-2006, 2013. — 279 с. : іл. — (Серія «Ком'пютинг»). — Бібліогр.: с. 275—278 (58 назв). — ISBN 978-617-57-40-11-4 11. https://www.udemy.com/ 12. https://www.coursera.org/

Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 116 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • Здатність формулювати та вдосконалювати важливу дослідницьку задачу, для її вирішення збирати необхідну інформацію та формулювати висновки, які можна захищати в науковому контексті. • Здатність використовувати професійно-профільні знання і практичні навички для оптимізації проектування інформаційних систем будь-якої складності, для вирішення конкретних завдань проектування інтелектуальних інформаційних систем з керування об'єктами різної фізичної природи. • Здатність проводити оцінку наявних технологій та на основі аналізу формувати вимоги до розроблення перспективних інформаційних технологій. • Здатність здійснювати ефективну комунікативну діяльність роботи команди зі розроблення проекту інформаційної системи. **вміти:** • використовувати знання та розуміння, що відносяться до базових областей штучного інтелекту і проектування систем підтримки прийняття рішень. • використовуючи методи глибинного машинного навчання, здатність створювати системи підтримки прийняття рішень. • застосовувати засвоєний матеріал для створення прототипів моделей глибинного навчання; • використовувати Python для програмної реалізації моделей глибиного 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 **Курс забезпечує набуття таких компетентностей: ЗК 3, КФ 1-3, КФ 5-8, КФ 11;** **та програмних результатів навчання: РН 2, РН 3, РН 5, РН 10-13, РН 16, РН 17, РН 19-22, РН 24.**
Ключові слова	Пошук аномалій, захист інформації, генеративний ШІ, глибокі нейронні мережі, конволюційні мережі, рекурентні мережі автоенкодери, мережі для стеганозахисту,
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче

Підсумковий контроль, форма	Екзамен у кінці 1 семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисципліни: • Інтелектуальні інформаційні технології
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: • лабораторні роботи, поточне тестування, усне опитування, самостійна робота: 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 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. П**олітика 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 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 участь у лабораторних заняттях		
Критерії оцінювання (8*5 балів)	**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 (16*0.5 балів та 1*2 бали)	**10 балів**	
Підготовка доповіді на конференцію	**2**	
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.	**0.5**	
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 **18 тестових питань в сумі 50 балів**		
Критерії оцінювання вирішення тестів	***50***	

	Відповідь вірна: 4 питання 10 питань 4 питання	 1 3 4
	Відповідь невірна	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	Завдання, год.	Термін виконання
1	**Тема 1.** Основні поняття. Основні математичні операції. Машинне навчання та місце глибокого навчання. Приклади сучасних стартапів і проектів з використанням глибокого навчання. Python. Бібліотеки для проектування систем глибокого навчання.	лекція, самостійна робота	[1-12]	1 12	1 тиждень
	Тема 1. Налаштування програмного середовища, формування енвайромента.	лаб	[1-12]	1	
2	**Тема 2.** Глибокі мережі прямого розповсюдження. Глибокі мережі: в чому краса та складність.	лекція, самостійна робота	[1-12]	3 13	1 тиждень
	Тема 2. Вирішення задач за допомогою глибоких мереж прямого розповсюдження.	лаб.	[1-12]	3	
3-4	**Тема 3.** Регуляризація в глибокому навчанні. Early Stopping. Dropout. Методи ініціалізації в глибокому навчанні. Unsupervised pre-training. Xavier initialization	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 3. Програмна реалізація методів регуляризації при вирішені практичних задач	лаб	[1-12]	4	
5-6	**Тема 4.** Оптимізація в навчанні глибоких моделей. Batch normalization. Метод моментів: Ньютона, Нестерова і Гессе. Адаптивні варіанти градієнтного спуску: Adadelta, Adagrad, RMSProp, Adam	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 4. Дослідження алгоритмів навчання та їх реалізація для вирішення практичних задач	лаб.	[1-12]	4	
7-8	**Тема 5.** Глибокі конволюційні нейронні мережі. Конволюція.	лекція, самостійна	[1-12]	4 13	2 тижні

	Пулінг. Приклад практичної реалізації. Сучасні архітектури згорткових мереж.	робота			
	Тема 5. Вирішення практичних задач в області кібербезпеці на основі конволюційних мереж	лаб.	[1-12]	4	
9-10	**Тема 6.** Автоенкодери і їх навчання. Типи автоенкодерів та їх застосування. Denoising Autoencoder. Sparse Autoencoder. Convolution (Deep) Autoencoder.	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 6. Вирішення задач пошуку аномалій та виявлення шахрайства на базі автоенкодерів	лаб.	[1-12]	4	
11-12	**Тема 7. Тема 8.** Рекурентні нейронні мережі. Processing of sequences. Problem of Long-Term Dependencies, Time-delay neural networks. Backpropagation & RNN, Simple RNN, Deep RNN, Bidirectional RNN.	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 7. Програмна реалізація та вирішення практичних задач захисту інформації на базі рекурсивних та рекурентних глибоких нейронних мереж	лаб.	[1-12]	4	
13-14	**Тема 8.** Рекурентні нейронні мережі. LSTM network. Core Idea Behind LSTMs, Step-by-Step LSTM Walk Through. Phased LSTM, GRU. SRN, Elman network, Jordan network, SCRN, uRNN, SRU.	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 8. Використання моделей стеку LSTM для вирішення задач захисту інформації.	лаб.	[1-12]	4	
15-16	**Тема 9.** Генеративний AI. Варіаційний автоенкоденр, Генеративні мережі, Дифузія.	лекція, самостійна робота	[1-12]	4 13	2 тижні
	Тема 9. Застосування методів генеративного AI, варіаційного автоенкоденра, генеративних мереж та дифузій для вирішення задач в кібербезпеці.	лаб.	[1-12]	4	
	Всього			**180**	