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 "Технології комп'ютерного зору в задачах кібербезпеки", 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	Технології комп'ютерного зору в задачах кібербезпеки
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
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/admission/specializations
Інформація про дисципліну	Дисципліна "Технології комп'ютерного зору в задачах кібербезпеки"є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається у 3-му семестрі другого (магістерського) рівня освіти в обсязі 3 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).

Коротка анотація дисципліни	Цей курс спрямований на надання студентам базових компетентностей у застосуванні технологій комп'ютерного зору для вирішення ключових задач кібербезпеки. Студенти ознайомляться з основними принципами роботи систем комп'ютерного зору, методами обробки зображень і відео, а також їх використанням для виявлення загроз та аномалій. Сстуденти будуть вивчати алгоритми розпізнавання облич, методи аналізу відео та інструменти, такі як OpenCV.
Мета та цілі дисципліни	Метою курсу є надання студентам базових знань та навичок для застосування технологій комп'ютерного зору у вирішенні завдань кібербезпеки. Студенти вивчатимуть основні принципи роботи з обробкою зображень та відео для виявлення загроз, розпізнавання облич, а також використання біометричних технологій. Особлива увага приділяється практичним аспектам, зокрема застосуванню інструментів, таких як OpenCV, для аналізу відеоданих та автоматизації процесів виявлення аномалій у системах кібербезпеки.
Література для вивчення дисципліни	Основна: 1. Szeliski, R. Computer Vision: Algorithms and Applications. Springer, 2022. 2. Tchakounté, F., Atemkeng, M. Global Perspectives on the Applications of Computer Vision in Cybersecurity. IGI Global, 2024. 3. Jain, A. K., Ross, A. A., Nandakumar, K. Introduction to Biometrics: Second Edition. Springer, 2020. 4. Khan, S., Rahmani, H., Shah, S. A. A., Bennamoun, M. A Guide to Convolutional Neural Networks for Computer Vision. Morgan & Claypool, 2020. Додаткова: 5. Forsyth, D. A., Ponce, J. Computer Vision: A Modern Approach. Pearson, 2011. 6. Bradski, G., Kaehler, A. Learning OpenCV 3: Computer Vision in C++ with the OpenCV Library. O'Reilly Media, 2016. 7. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016. 8. Jain, A. K., Ross, A. A., Nandakumar, K. Introduction to Biometrics. Springer, 2011.
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 24 год., з них 8 год. лекцій та 16 год. лабораторних робіт. Самостійної роботи: 66 год.

Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **Знати:** 1. Основи роботи систем комп'ютерного зору та їх застосування в кібербезпеці. 2. Основні методи обробки зображень та відео для виявлення аномалій. 3. Принципи використання біометричних технологій для ідентифікації користувачів. 4. Підходи до аналізу відеоданих для моніторингу та захисту систем. **Вміти:** 1. Використовувати базові бібліотеки комп'ютерного зору (OpenCV) для обробки зображень. 2. Реалізовувати прості системи для розпізнавання облич та ідентифікації користувачів. 3. Аналізувати відеопотоки для виявлення потенційних загроз у кібербезпеці. 4. Інтегрувати елементи комп'ютерного зору у системи кібербезпеки.
Ключові слова	Обробка зображень, біометричні системи, розпізнавання облич, аномалії у відео, комп'ютерний зір, захист даних, ідентифікація користувачів, автоматизація кібербезпеки, OpenCV, TensorFlow, виявлення загроз, машинне навчання, глибоке навчання, моніторинг відеопотоків.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці 3 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. Комп'ютери повинні мати середовища для програмування на Python з встановленими бібліотеками OpenCV, TensorFlow та іншим програмним забезпеченням для роботи з комп'ютерним зором.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: лабораторні роботи: 40% семестрової оцінки; самостійна робота: 10% семестрової оцінки; модульний контроль: 50% семестрової оцінки 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. **Політика 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	**50**	
Підсумкове модульне тестування містить **25 тестових питань по 2 бали**		
Критерії оцінювання відповіді на тестові питання (25*2 бали):	**50**	
Відповідь правильна	**2**	

	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	Вступ до курсу "Технології комп’ютерного зору в кібербезпеці". Основні цілі та принципи використання комп'ютерного зору у кібербезпеці.	Лекція Лабораторна Самостійна робота	[1-4]	2 2 6	1 тиждень
2	Практична робота з OpenCV: обробка зображень і відео для аналізу загроз.	Лабораторна Самостійна робота	[1-4]	2 10	1 тиждень
3	Основи обробки зображень і відео для кібербезпеки. Алгоритми виявлення загроз.	Лекція Лабораторна Самостійна робота	[1-4]	2 2 10	1 тиждень
4	Виявлення аномалій у відео за допомогою комп'ютерного зору.	Лабораторна Самостійна робота	[1-4]	2 10	1 тиждень
5	Біометричні технології: ідентифікація користувачів та захист даних.	Лекція Лабораторна Самостійна робота.	[1-4]	2 2 10	1 тиждень
6	Автоматизація процесів моніторингу та виявлення загроз за допомогою комп'ютерного зору.	Лабораторна Самостійна робота	[1-4]	2 10	1 тиждень

7	Використання глибокого навчання у комп'ютерному зорі для кібербезпеки.	Лекція Лабораторна Самостійна робота	[1-4]	2 2 10	1 тиждень
8	Підсумкове тестування. Оцінювання здобутих знань та навичок в кінці курсу.	Лабораторна	[1-4]	2	1 тиждень