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 “Інтелектуальні інформаційні технології”, 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 р.

Назва дисципліни	**Інтелектуальні інформаційні технології**
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
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	Кирик Мар'ян Іванович, доктор технічних наук, професор кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	marian.kyryk@lnu.edu.ua; https://ami.lnu.edu.ua/employee/kyryk-m-i
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/department/kiberbezpeky
Інформація про дисципліну	Дисципліна "Інтелектуальні інформаційні технології" є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається в 2-му семестрі другого (магістерського) рівня освіти в обсязі 4-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області штучного інтелекту та машинного навчання, одержання студентами теоретичних знань та практичних навиків використання інтелектуальних інформаційних технологій, застосування основних технологій та методів штучного інтелекту у кібербезпеці, для аналізу великих даних, виявлення загроз і аномалій, інтеграції для покращення безпеки мереж і систем.
Мета та цілі дисципліни	Метою навчальної дисципліни "Інтелектуальні інформаційні технології" є підготовка висококваліфікованих та конкурентоспроможних фахівців на ринку праці, які володіють компетентностями необхідними для ефективного розв'язування практичних проблем у сфері захисту інформації; розробці, використанні та впровадженні сучасних технологій штучного інтелекту для забезпечення інформаційної та кібербезпеки шляхом навчання принципам і методам застосування штучного інтелекту у системах захисту, а також у контексті захисту IT-інфраструктур, включаючи IoT та хмарні середовища.
Література для вивчення дисципліни	*Основна* 1. Omar M. Machine Learning for Cybersecurity. Innovative Deep Learning Solutions. Springer, 2022 – 48p. 2. Субботін С.О. Нейронні мережі : теорія та практика : навчальний посібник. Житомир : Вид.О.О. Євенок, 2020. 184 с 3. Шаховська Н. Б. Системи штучного інтелекту: навч. посібник / Н. Б. Шаховська, Р. М. Камінський, О. Б. Вовк. Львів: Видавництво Львівської політехніки, 2018. 392 с. 4. Нейронні мережі – шлях до глибинного навчання [Електронний ресурс] – URL: https://codeguida.com/post/739.

	5. Cisco systems. Навчальні матеріали мережних академій Cisco за курсом Network Security https://www.netacad.com/courses/cybersecurity/network-security/ *Додаткова* 6. Wu Bolun, Zou Futai. Code Vulnerability Detection Based on Deep Sequence and Graph Models: A Survey // Security and Communication Network, Volume 2022, Article ID 1176898, 11 p. 7. Anitha S. Pillai and Roberto Tedesco Machine Learning and Deep Learning in Natural Language Processing, CRC Press, 2024, 245 p. *Рекомендовані онлайн курси* 8. Udemy: Mastering Machine Learning and intro' to Deep Learning 9. Coursera: Deep Learning Specialization
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 112 год., з них 32 години лекцій та 32 годин лабораторних занять. Самостійної роботи: 56 годин.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей. **знати:** • принципи роботи штучного інтелекту та машинного навчання • основні технології та методи штучного інтелекту, які застосовуються у кібербезпеці; • методологічні підходи до побудови систем штучного інтелекту • теоретичний та практичний матеріал згідно програми курсу. **вміти:** • вибирати і використовувати оптимальні методи машинного навчання і програмні засоби для вирішення практичних задач; • розробляти та налаштувати системи з підтримкою штучного інтелекту, зокрема в IDS/IPS та брандмауерах; • інтегрувати та оптимізувати інструменти штучного інтелекту для покращення безпеки мереж і систем; • використовувати сучасні інформаційні системи та технології, методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків; • застосувати методи та засоби штучного інтелекту. Курс забезпечує набуття таких компетентностей: ЗК 1-4, КФ1-3, КФ8, КФ11; та програмних результатів навчання: РН4, РН11, РН12, РН14, РН19, РН23, РН24.
Ключові слова	Інтелектуальні інформаційні технології, штучний інтелект, машинне навчання, нейронні мережі, великі дані, Інтернет речей, хмарні технології
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Екзамен у кінці семестру. Формат екзамену: письмовий тестовий.
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисциплін " Системи ШІ в задачах захисту інформації", "Безпека систем автоматизації та Інтернету речей".
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Лекції з мультимедійними презентаціями; лабораторні заняття у вигляді виконання практичних завдань (у тому числі командних); самостійне опрацювання навчальних матеріалів, розміщених у хмарних сховищах; обговорення тем та консультації в середовищі Microsoft Teams, індивідуальні завдання.

<table>
<tr><td>Необхідне обладнання</td><td>Комп’ютер, мережа Internet, проектор. Програмне забезпечення Cisco Packet Tracer, Oracle VM VirtualBox, мережеве обладнання.</td></tr>
<tr><td>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</td><td>
Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:
• тестування, усне опитування, лабораторні завдання: 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 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 при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов’язково враховуються присутність на заняттях та активність студента під час практичного 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.
<table>
<tr><th>Критерії оцінювання знань студентів</th><th>Бали рейтингу</th><th>Макс. к-сть балів</th></tr>
<tr><td colspan="3">1. Бали поточної успішності за участь у лабораторних заняттях</td></tr>
<tr><td>Критерії оцінювання (10*4 балb)</td><td colspan="2">40 балів</td></tr>
<tr><td>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.</td><td colspan="2">5</td></tr>
<tr><td>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</td><td colspan="2">4-3</td></tr>
</table>
</td></tr>
</table>

	та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.	
	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 (10*1 балу)	**10 балів**
	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 лабораторному занятті. Студент додатково опрацював матеріал та аргументовано його викладає. Оцінюється додатковим балом за кожне практичне заняття.	**1**
	Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**
	Загальна максимальна кількість балів за поточний контроль	**50**
	2. Екзамен	**50**
	Семестровий екзамен як форма підсумкового контролю є обов'язковим для всіх студентів. Екзаменаційний білет містить **4 тести по 2 бали, 4 тести по 3 бали та 5 теоретичних питань по 6 балів**	
	Критерії оцінювання відповіді на теоретичні питання (5*6 балів):	**30**
	Відповідь написано в повному обсязі, аргументовано, глибоко та всебічно розкрито зміст теоретичного питання.	**6**
	Відповідь в основному розкриває зміст теоретичного питання, не вистачає достатньої глибини та аргументації, допущено окремі несуттєві неточності та незначні помилки.	**5**
	Відповідь в цілому розкриває основний зміст питання але без глибокого всебічного аналізу, обґрунтування та аргументації, допущено окремі суттєві неточності та помилки.	**4-3**
	Відповідь не повна, фрагментарна без аргументації та обґрунтування.	**2-1**

	Відповідь не надана	**0**
	Критерії оцінювання вирішення тестів (4*3 бали):	**12**
	Відповідь вірна	**3**
	Відповідь невірна	**0**
	Критерії оцінювання вирішення тестів (4*2 бали):	**8**
	Відповідь вірна	**2**
	Відповідь невірна	**0**
	Загальна кількість балів по завершенні вивчення дисципліни	**100**
Питання до екзаменів.	1. Що таке штучний інтелект (AI) та які основні його компоненти? 2. Які основні типи машинного навчання існують, і в чому їх відмінності? 3. Опишіть основні етапи процесу машинного навчання від збору даних до оцінки моделі. 4. Які переваги та обмеження мають традиційні брандмауери в порівнянні з брандмауерами, що використовують AI? 5. Поясніть, як AI може використовуватися для виявлення загроз у системах виявлення та запобігання вторгнень (IDS/IPS). 6. Які алгоритми використовуються для виявлення аномалій у мережевому трафіку за допомогою AI? 7. Які методи обробки природної мови (NLP) використовуються для боротьби з фішингом? 8. Які основні методи виявлення та запобігання фішингу з використанням AI? 9. Які є підходи до інтеграції AI у хмарні середовища для покращення безпеки? 10. Опишіть, як нейронні мережі можуть бути використані для виявлення складних загроз у кібербезпеці. 11. Які основні виклики та ризики застосування AI у кібербезпеці? 12. Як AI може допомогти у захисті Інтернету речей (IoT) від кібератак ? 13. Які алгоритми використовуються для розпізнавання шкідливого програмного забезпечення з AI? 14. Які методи використання AI для автоматизації реагування на інциденти? 15. Як AI може бути використаний для покращення аналізу поведінкових даних у кібербезпеці? 16. Що таке системи з підтримкою штучного інтелекту, і як вони відрізняються від традиційних систем? 17. Які інструменти та платформи використовуються для аналізу великих даних у кібербезпеці? 18. Опишіть основи роботи систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) з AI. 19. Які переваги та обмеження має автоматизація реагування на інциденти за допомогою AI? 20. Які методи AI використовуються для виявлення поліморфних та метаморфних вірусів?	

	21. Як AI може допомогти у виявленні та захисті від нових та невідомих загроз? 22. Опишіть роль AI у моніторингу та управлінні безпекою в хмарних середовищах. 23. Які особливості захисту IoT-пристроїв з використанням AI? 24. Як алгоритми кластеризації можуть використовуватися для виявлення аномалій у кібербезпеці? 25. Які методи використовуються для захисту даних при використанні AI у кібербезпеці? 26. Як AI може бути інтегрований у систему управління безпекою підприємства? 27. Опишіть приклади успішного впровадження AI у системи кібербезпеки. 28. Які етичні та правові питання пов'язані з використанням AI у кібербезпеці? 29. Як використовуються техніки глибинного навчання (deep learning) для захисту від кіберзагроз? 30. Які сучасні тренди у розвитку інтелектуальних технологій для кібербезпеки, і як вони вплинуть на майбутнє галузі?
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. Інтелектуальні інформаційні технологій у кібербезпеці.** Огляд інтелектуальних інформаційних технологій. Визначення та основні поняття штучного інтелекту, машинного навчання, нейронних мереж та аналізу великих даних. Роль інтелектуальних інформаційних технологій у кібербезпеці	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
2	**Тема 2. Основи штучного інтелекту та машинного навчання у кібербезпеці.** Основні концепції штучного інтелекту та машинного навчання. Типи машинного навчання: навчання з учителем, без учителя, з підкріпленням. Використання машинного навчання для автоматизації процесів кібербезпеки.	лекція, самостійна робота		2 4	1 тиждень
		лаб.	[1-6]	2	
3-4	**Тема 3. Системи виявлення та запобігання вторгнень (IDS/IPS).** Основи роботи IDS/IPS та їх еволюція. Застосування штучного інтелекту у виявленні аномалій та нових загроз. Використання класифікаційних та кластеризаційних алгоритмів у IDS/IPS.	лекція, самостійна робота	[1-6]	4 6	2 тижні
		лаб.	[1-6]	4	
5-6	**Тема 4. Використання штучного інтелекту в міжмережевих екранах.** Традиційні брандмауери та їх обмеження. Інтеграція AI для динамічного налаштування правил брандмауера.	лекція, самостійна робота	[1-6]	4 6	2 тижні
		лаб.	[1-6]	4	

	Використання AI для глибокого аналізу мережевих пакетів (DPI).				
7	**Тема 5. Використання штучного інтелекту для виявлення та запобігання фішингу.** Використання алгоритмів обробки природної мови (NLP) для аналізу фішингових атак. Застосування AI для автоматизації захисту від фішингу	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
8-9	**Тема 6. Аналіз великих даних.** Великі дані (Big Data) та їх значення в кібербезпеці. Методи збору та аналізу великих даних за допомогою штучного інтелекту. Використання великих даних для прогнозування атак. Інструменти та платформи для аналізу великих даних.	лекція, самостійна робота	[1-6]	4 6	2 тижні
		лаб.	[1-6]	4	
10-11	**Тема 7. Нейронні мережі та їх застосування у виявленні загроз.** Архітектура та типи нейронних мереж. Застосування глибоких нейронних мереж для виявлення складних загроз. Використання нейронних мереж для аналізу поведінки користувачів та систем.	лекція, самостійна робота	[1-6]	4 6	2 тижні
		лаб.	[1-6]	4	
12	**Тема 8. Інтернет речей (IoT).** Використання штучного інтелекту для виявлення вразливостей та атак на IoT-пристрої. Алгоритми штучного інтелекту для аналізу даних IoT та виявлення аномалій.	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
13	**Тема 9. Хмарні технології.** Переваги використання хмар. Безпека у хмарних середовищах. Методи штучного інтелекту для виявлення загроз у віртуальних машинах та контейнерах. Інтеграція штучного інтелекту з хмарними платформами для покращення безпеки.	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
14	**Тема 10. Розпізнавання та блокування шкідливого програмного забезпечення.** Технології виявлення шкідливого ПЗ за допомогою штучного інтелекту. Статичний та динамічний аналіз ПЗ з використанням штучного інтелекту.	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
15	**Тема 11. Комп'ютерний зір.** Методи комп'ютерного зору: обробка зображень, відеоаналіз.	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
16	**Тема 12. Робототехніка та автономні системи.** Інтелектуальні контролери та автономні системи. Застосування у промисловості та побуті.	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
ВСЬОГО				**120**	