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
“Задачі класифікації трафіку IoT”,
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	Задачі класифікації трафіку IoT
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	Костяк Марина Юріївна, доцент кафедри кібербезпеки, доктор техн. наук Ребець Андрій Ігорович, асистент
Контактна інформація викладачів	maryna.kostiak@lnu.edu.ua https://ami.lnu.edu.ua/employee/kostiak-m-yu andrii.rebets@lnu.edu.ua https://ami.lnu.edu.ua/employee/rebets-a
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/admission/specializations
Інформація про дисципліну	Дисципліна “Задачі класифікації трафіку IoT” є вибірковою дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається в 1-му семестрі другого (магістерського) рівня освіти в обсязі 4 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в забезпеченні безпеки мереж IoT пристроїв, розвиток системи знань про особливості та риси мережевого трафіку IoT, його аналіз та класифікація з метою застосування у кібербезпеці.
Мета та цілі дисципліни	Метою курсу є формування у студентів знань про інформаційну безпеку IoT пристоїв та мереж. SMT/SAT розв’язники в задачах кібербезпеки. Перевірка аномалій програмного коду. Створення експлойтів. Перевірка безпеки мережі. Виділення рис для класифікації на основі потоку пакетів пристроїв Інтернету речей. Мультигрупова класифікація на основі нейронних мереж. Використання результатів класифікації з точки зору кібербезпеки.
Література для вивчення дисципліни	1. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: І.В. Стьопочкіна, О.М. Новіков. – Київ : КПІ ім. Ігоря Сікорського, 2022 – 82 с. 2. Коваленко А.А., Оборін О.О., Покора К.В. Метод виявлення аномального трафіку в IoT// Проблеми інформатизації : десята міжнародна науково-технічна конференція. Черкаси – Баку – Бельсько-Бяла – Харків, 2022, т.2, с.4. 3. Parimala, V. K. (Ed.). (2024). Anomaly Detection - Recent Advances, AI and ML Perspectives and Applications.IntechOpen.DOI: 10.5772/intechopen.110988. ISBN: 978-1-83769-027-5. 4. Kuchuk, N., Kovalenko, A., Ruban, I., Shyshatskyi, A., Zakovorotnyi, O. And Sheviakov, I. (2023), “Traffic Modeling for the Industrial Internet of NanoThings”, 2023 IEEE 4th KhPI Week on Advanced Technology, KhPI Week 2023 - Conference Proceedings, 194480, doi:

	http://dx.doi.org/10.1109/KhPIWeek61412.2023.10312856 5. Chatterjee, A., & Ahmed, B. S. (2022). IoT Anomaly Detection Methods and Applications: A Survey. Internet of Things, 100568. Elsevier BV.
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** – засоби ідентифікації та вимірювань (сенсори) в IoT; – технології передачі даних IoT; – методи перевірки безпеки мережі; – методи перевірки аномалій мережевого трафіку IoT; – основи аналізу мережевого трафіку і виявлення аномалій; – методи класифікації трафіку за допомогою машинного навчання; – використання результатів класифікації трафіку для кібербезпеки. **вміти:** – розрізняти засоби ідентифікації та вимірювань (сенсори) в IoT; – застосовувати методи перевірки безпеки мережі; – застосовувати методи перевірки аномалій мережевого трафіку IoT; – аналізувати мережевий трафік для виявлення аномалій; – застосовувати методи класифікації трафіку за допомогою машинного навчання; – використовувати результатів класифікації трафіку для кібербезпеки
Ключові слова	Інтернет речей, безпека мережі, машинне навчання, штучний інтелект
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисциплін "Основи кібербезпеки", "Безпека комп'ютерних мереж", "Менеджмент інформаційної безпеки".
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Лабораторні роботи
Необхідне обладнання	Комп’ютери, комп’ютерні системи та мережі. Віртуальні машини. Інтернет ресурси.

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.

П**олітика виставлення балів.** Враховуються бали набрані при виконанні індивідуальних завдань, самостійній роботі та бали підсумкового модульного контролю. 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 бали)	**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.	**2-1**
	Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**
	3. Модульний контроль	**50**
	Підсумкова контрольна робота містить **5 теоретичних питань по 10 балів**	
	Критерії оцінювання відповіді на теоретичні питання (5*10 балів):	**50**
	Відповідь написано в повному обсязі, аргументовано, глибоко та всебічно розкрито зміст теоретичного питання.	**10**
	Відповідь в основному розкриває зміст теоретичного питання, не вистачає достатньої глибини та аргументації, допущено окремі несуттєві неточності та незначні помилки.	**8-9**
	Відповідь в цілому розкриває основний зміст питання але без глибокого всебічного аналізу, обґрунтування та аргументації, допущено окремі суттєві неточності та помилки.	**5-7**
	Відповідь не повна, фрагментарна без аргументації та обґрунтування.	**2-4**
	Відповідь не надана	**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
1-2	**Тема 1. SMT/SAT розв'язники в задачах кібербезпеки.** (Поняття і особливості SAT/SMT розв'язників. Застосування SAT розв'язників для задач кібербезпеки. Застосування SMT розв'язників для задач кібербезпеки).	лекція, самостійна робота	[1-5]	4 6	2 тижні
		лаб.	[1-5]	4	
3-4	**Тема 2. Перевірка аномалій програмного коду. Створення експлойтів.** (Статичний аналіз коду. Оптимізаційні компілятори і їхнє застосування. Класифікація вразливостей програмного коду. Властивості коректності програмного коду. Формальна і неформальна перевірка програмного коду. Системи генерації експлойтів.)	лекція, самостійна робота		4 8	2 тижні
		лаб.	[1-5]	4	

5-6	**Тема 3. Перевірка безпеки мережі.** (Застосування розв'язника Z3 для перевірки захищеності мережі. Визначення векторів атаки на мережу. Графи атак. Пошук валідної політики захисту. Формалізація задачі SAT. Методика аналізу захищеності мережі із використанням SAT/SMT - розв'язників)	лекція, самостійна робота	[1-5]	4 6	2 тижні
		лаб.	[1-5]	4	
7-8	**Тема 4. Постановка задачі класифікації трафіку IoT.** (Основні методи класифікації трафіку. Системи виявлення та попередження вторгнень. Категоризація IoT загроз. Категоризація систем виявлення вторгнень. IoT ботнети та методи їхнього виявлення.)	лекція, самостійна робота	[1-5]	4 6	2 тижні
		лаб.	[1-5]	4	
9-10	**Тема 5. Виділення рис для класифікації на основі потоку пакетів пристроїв Інтернету речей.** (Збір даних. Векторна модель для обробки даних. Попередня обробка даних та вибір атрибутів для тренування класифікатора. Аналіз результатів.)	лекція, самостійна робота	[1-5]	4 6	2 тижні
		лаб.	[1-5]	4	
11	**Тема 6. Аналіз потоку пакетів.** (Загальні принцип аналізу потоку пакетів. Методи та засоби аналізу пакетів. Перевірка та аналіз результату.)	лекція, самостійна робота	[1-5]	2 4	1 тиждень
		лаб.	[1-5]	2	
12-13	**Тема 7. Вибір методу машинного навчання.** (Огляд та класифікація методів машинного навчання. Прикладне застосування машинного навчання в задачах аналізу трафіку)	лекція, самостійна робота	[1-5]	4 6	2 тижні
		лаб.	[1-5]	4	
14	**Тема 8. Мультигрупова класифікація на основі нейронних мереж.** (Огляд та порівняння класифікаторів даних. Метричні та статистичні класифікатори. Класифікація даних за допомогою нейронних мереж. Алгоритму побудови класифікатора даних з використанням нейронної мережі).	лекція, самостійна робота	[1-5]	2 4	1 тиждень
		лаб.	[1-5]	2	

15-16	**Тема 9. Використання результатів класифікації з точки зору кібербезпеки.** (Аналізу та перевірка результатів класифікації. Застосування класифікації даних для категоризації подій в системах безпеки. Виправлення неточностей класифікації для зменшення кількості хибних спрацювань.)	лекція, самостійна робота	[1-5]	4 10	2 тижні
		лаб.	[1-5]	4	