**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

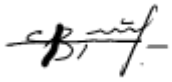
**Львівський національний університет імені Івана Франка**

**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

# «Нейронні мережі 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** | Нейронні мережі в задачах кібербезпеки |
| **Адреса викладання дисципліни** | м. Львів, вул. Університетська 1 |
| **Факультет та кафедра, за якою закріплена дисципліна** | Факультет прикладної математики та інформатики<br>Кафедра кібербезпеки |
| **Галузь знань, шифр та назва спеціальності** | 12 – інформаційні технології<br>125 – кібербезпека та захист інформації |
| **Викладачі дисципліни** | Венгерський Петро Сергійович, професор кафедри кібербезпеки<br>Карпюк Роман Валентинович, старший викладач кафедри кібербезпеки |
| **Контактна інформація викладачів** | petro.venherskyy@lnu.edu.ua; roman.karpiuk@lnu.edu.ua<br>https://ami.lnu.edu.ua/employee/venherskyi<br>https://ami.lnu.edu.ua/employee/karpiuk-r-v<br>Головний корпус ЛНУ ім. І. Франка, каб. 380.<br>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 “Нейронні мережі в задачах кібербезпеки” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми «Технології штучного інтелекту в кібербезпеці», яка викладається в 2-му семестрі в обсязі 5-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| **Коротка анотація дисципліни** | Основним завданням курсу є формування професійних компетентностей майбутніх фахівців в галузі кібербезпеки на базі нейронних мереж та методів машинного навчання для вирішення задач кібербезпеки, пошуку аномалій в журналах подій, спрацюваннях від інструментів SecOps, виявлення шкідливих доменів та шкідливого програмного забезпечення. |
| **Мета та цілі дисципліни** | Метою викладання навчальної дисципліни є визначення сфер кібербезпеки, де доречне застосування нейронних мереж та практичне |

| | |
|---|---|
| | застосування здобутих знань для підвищення ефективності виявлення зловмисних дій атакуючими командами. |
| **Література для вивчення дисципліни** | 1. Brij B. Gupta, Quan Z. Sheng - Machine Learning for Computer and Cyber SecurityPrinciple, Algorithms, and Practices, 2019, 364 p.<br>2. Clarence Chio, David Freeman - Machine Learning and Security: Protecting Systems with Data and Algorithms 1st Edition, 2019, 386 p.<br>3. Ruth J. Innovative - Machine Learning Applications for Cryptography IGI Global, 2024, 313 p.<br>4. Hossain, Eklas - Machine Learning Crash Course for Engineers Springer, 2024, 473 p.<br>5. Aurelien Geron - Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 3rd Edition, 2023, 850 p.<br><br>Допоміжна<br><br>6. https://www.udemy.com/<br>7. https://www.coursera.org/<br>8. RangeForce Platform |
| **Обсяг курсу** | Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год. |
| **Очікувані результати навчання** | У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:<br><br>**знати:**<br><br>• основи формування датасетів і аналізу даних, їх форматування, відкидання «шуму» та підготовки початкової статистичної вибірки для моделей машинного навчання;<br>• різні види алгоритмів машинного навчання, включаючи методи з вчителем (supervised learning) і самонавчання (unsupervised learning):<br>• основи навчання моделей та оцінки їх ефективності;<br>• архітектури нейронних мереж (MLP, CNN, RNN) та їх модифікації;<br>• алгоритми навчання нейронних мереж і методи регуляризації для покращення ефективності моделей;<br>• основні області кібербезпеки, де нейронні мережі можуть надати значні переваги (наприклад, виявлення аномалій, фішингових атак, аналіз трафіку);<br>• розуміння обмежень машинного навчання як компенсуючого інструменту в кібербезпеці;<br>• основи роботи з інструментами Big Data, такими як SIEM-системи, які здатні інтегрувати та обробляти великі обсяги даних з використанням машинного навчання.<br><br>**вміти:** |

| | |
|---|---|
| | • вибирати оптимальні методи для вирішення різних задач у кібербезпеці, таких як пошук аномалій, класифікація загроз чи аналіз трафіку;<br>• практично застосовувати алгоритми машинного навчання та нейронних мереж у реальних задачах кібербезпеки;<br>• використовувати SIEM для збору, аналізу даних і створення вибірок для навчання моделей;<br>• будувати кореляційні правила та автоматизувати реагування на інциденти з використанням машинного навчання;<br>• оцінювати ефективність моделей на основі метрик якості, таких як точність, повнота, F1-міра тощо;<br>• оптимізувати моделі за допомогою налаштування гіперпараметрів, застосування методів регуляризації та інших технік покращення продуктивності.<br><br>**Курс забезпечує набуття таких компетентностей: ЗК 1-4, КФ 1, КФ 3, КФ 5-7, КФ 11;**<br><br>**та програмних результатів навчання: РН 4, РН 13, РН 16, РН 20-22, РН 24.** |
| **Ключові слова** | Методи машинного навчання, нейроні мережі SIEM, кібербезпека, аномалія, DensityFunction, RandomForest, ML, класифікатор, датасет, аналіз, MLP, CNN, RNN |
| **Формат курсу** | Очний<br><br>Проведення лекцій, лабораторних робіт і консультацій. |
| **Теми** | Теми подані у Схемі курсу нижче |
| **Підсумковий контроль, форма** | Екзамен у кінці 2 семестру |
| **Пререквізити** | Для вивчення курсу студенти потребують базові знання з дисципліни:<br><br>• Інструменти SecOps<br>• Мережева безпека<br>• Системи ШІ в задачах захисту інформації<br>• Оцінки похибок при застосуванні методів машинного навчання |
| **Навчальні методи та техніки, які будуть використовуватися під час** | Презентації, лекції, лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, опитування теоретичного матеріалу, самостійна робота, платформа RangeForce. |

<table>
<tr><td>викладання курсу</td><td></td></tr>
<tr><td>Необхідне обладнання</td><td>Комп’ютерний клас із вільно-доступним програмним забезпеченням, локальна комп’ютерна мережа, доступ до Internet мережі.</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:<br><br>• поточне тестування, лабораторні роботи, самостійна робота студентів: 50% семестрової оцінки; максимальна кількість балів 50<br><br>• екзамен: 50% семестрової оцінки; максимальна кількість балів 50<br><br>Підсумкова максимальна кількість балів 100.<br><br>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.<br><br>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.<br><br>Політика виставлення балів. Враховуються бали набрані при виконанні лабораторних робіт, 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.<br><br>Жодні форми порушення академічної доброчесності не толеруються.<br><br>
<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 бали)</td><td colspan="2">40 балів</td></tr>
</table>
</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | 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. | **4** |
| | | 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. | **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 (10 * 1 бал)** | **10 балів** |
| | | **Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел)**<br><br>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 лабораторне заняття.* | **1** |
| | | Студент не опрацював самостійно додаткових джерел і не володіє матеріалом | **0** |
| | | **3. Екзамен** | **50** |
| | | **Семестровий екзамен як форма підсумкового контролю є обов'язковим для всіх студентів.**<br><br>Екзаменаційний білет містить **2 теоретичні питання по 15 балів та 5 тестів по 4 бали** | |

| | |
|---|---|
| | <table><tr><td>Критерії оцінювання відповіді на теоретичні питання (2*15 балів):</td><td>30</td></tr><tr><td>Відповідь написано в повному обсязі, аргументовано, глибоко та всебічно розкрито зміст теоретичного питання.</td><td>15</td></tr><tr><td>Відповідь в основному розкриває зміст теоретичного питання, не вистачає достатньої глибини та аргументації, допущено окремі несуттєві неточності та незначні помилки.</td><td>14-11</td></tr><tr><td>Відповідь в цілому розкриває основний зміст питання але без глибокого всебічного аналізу, обґрунтування та аргументації, допущено окремі суттєві неточності та помилки.</td><td>10-6</td></tr><tr><td>Відповідь не повна, фрагментарна без аргументації та обґрунтування.</td><td>5-1</td></tr><tr><td>Відповідь не надана</td><td>0</td></tr><tr><td>Критерії оцінювання вирішення тестів (5*4 бали):</td><td>20</td></tr><tr><td>Відповідь вірна</td><td>4</td></tr><tr><td>Відповідь невірна</td><td>0</td></tr><tr><td>Загальна кількість балів по завершенні вивчення дисципліни</td><td>100</td></tr></table><br><br>**Додаткові бали / або зарахування певних тем** можна отримати за результатами **неформального та/або інформального навчання за** тематикою даної дисципліни. Визнання та зарахування результатів такого навчання відбувається у відповідності до наданих документів про неформальне та/або інформальне навчання.<br><br>Жодні форми порушення академічної доброчесності не толеруються. |
| **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.** Вступ до нейронних мереж. Основні архітектури (MLP, CNN, RNN). Застосування в кібербезпеці. | лекція, самостійна робота | [1-5] | 2<br>7 | 1 тиждень |
| | **Тема 1.** Практичне застосування MLP, CNN, RNN для виявлення аномалій. | лаб | [1-5] | 2 | |
| 2 | **Тема 2.** Навчання нейронних мереж. Backpropagation, оптимізація, регуляризація. | лекція, самостійна робота | [1-5] | 2<br>7 | 1 тиждень |
| | **Тема 2.** Реалізація навчання та оптимізації нейронних мереж для класифікації загроз. | лаб. | [1-5] | 2 | |
| 3-5 | **Тема 3.** Рекурентні нейронні мережі (RNN, LSTM, GRU). Застосування в аналізі кіберзагроз. | лекція, самостійна робота | [1-5] | 6<br>21 | 3 тижні |
| | **Тема 3.** Застосування RNN, LSTM, GRU для виявлення аномалій у трафіку мережі. | лаб | [1-5] | 6 | |
| 6-7 | **Тема 4.** Конволюційні нейронні мережі (CNN). Аналіз мережевого трафіку та зображень. | лекція, самостійна робота | [1-5] | 4<br>14 | 2 тижні |
| | **Тема 4.** Використання CNN для виявлення шкідливого коду у файлах та мережевому трафіку. | лаб. | [1-5] | 4 | |
| 8-9 | **Тема 5.** Нейронні мережі для обробки текстів. NLP у кібербезпеці. | лекція, самостійна робота | [1-5] | 4<br>7 | 2 тижні |
| | **Тема 5.** Використання NLP для фільтрації спаму та аналізу фішингових атак. | лаб. | [1-5] | 4 | |
| 10-13 | **Тема 6.** Генеративні моделі (GANs, VAEs) у кібербезпеці. | лекція, самостійна робота | [1-5] | 8<br>14 | 4 тижні |
| | **Тема 6.** Генерація атак та виявлення аномалій з використанням GANs, VAEs. | лаб. | [1-5] | 8 | |
| 14 | **Тема 7.** Захист нейронних мереж від атак (adversarial attacks). | лекція, самостійна робота | [1-5] | 2<br>8 | 1 тиждень |
| | **Тема 7.** Реалізація захисту нейронних мереж від атак на основі вразливостей. | лаб. | [1-5] | 2 | |
| 15-16 | **Тема 8.** Розгортання нейронних мереж у кібербезпеці: інструменти та платформи. | лекція, самостійна робота | [1-5] | 4<br>8 | 2 тижні |

| | | | | | |
|---|---|---|---|---|---|
| | **Тема 8.** Практичне розгортання моделей у середовищах SIEM. Docker та Kubernetes. | лаб. | [1-5] | 4 | |
| | **Всього** | | | **150** | |