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
“Виявлення вразливостей коду на основі методів глибинного навчання”,
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	Виявлення вразливостей коду на основі методів глибинного навчання
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	Трушевський Валерій Миколайович, кандидат фіз.-мат. наук, доцент кафедри кібербезпеки (лекції) Щербина Микола Юрійович, асистент кафедри кібербезпеки (лабораторні заняття)
Контактна інформація викладачів	valeriy.trushevsky@lnu.edu.ua https://ami.lnu.edu.ua/en/employee/v-m-trushevskyy; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
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/course/vyiavlennia-vrazlyvostey-kodu-na-osnovi-metodiv-hlybynnoho-navchannia
Інформація про дисципліну	Дисципліна “Виявлення вразливостей коду на основі методів глибинного навчання” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається у 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 у галузі виявлення вразливостей коду програмного забезпечення на основі методів штучного інтелекту. Розглядаються основні типи вразливостей програмного забезпечення та технології тестування для їх виявлення, типи нейронних мереж та методи глибинного навчання у застосуванні до виявлення вразливостей.
Мета та цілі дисципліни	Метою курсу є вивчення основних типів вразливостей програмного забезпечення та технологій їх виявлення, що базуються на методах штучного інтелекту.
Література для вивчення дисципліни	*Основна* 1. Bishop Christopher M., Bishop H. Deep Learning. Foundations and Concepts. Springer, 2024 – 649p. 2. Brown B. Cyber Security Program and Policy Using NIST Cybersecurity Framework, 2023. – 169 p. 3. Simon J. D. Prince. Understanding Deep Learning, 2023. – 544 p.

	4. Cai W., Chen J., Yu J., Gao L. A software vulnerability detection method based on deep learning with complex network analysis and subgraph partition // Information and Software Technology, Volume 164, December 2023. 5. Kohnfelder K. Designing Secure Software, 2021. – 312 p. 6. Omar M. Machine Learning for Cybersecurity. Innovative Deep Learning Solutions. Springer, 2022 – 48p. 7. Zagane M., Kamel Abdi M., Alenezi M. Deep Learning for Software Vulnerabilities Detection Using Code Metrics // IEEE Access, V.8, 2020, 9p. 8. 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. *Додаткова* 9. Deogun D. Secure By Design First Edition, 2019. – 410 p. 10. Трушевський В.М., Шинкаренко Г.А., Щербина Н.М. Метод скінченних елементів і штучні нейронні мережі. Теоретичні аспекти і застосування. Львів, Вид. центр ЛНУ ім. Івана Франка, 2014 – 396 с. *Рекомендовані онлайн курси* 11. Udemy: Principles of Secure Coding 12. Udemy: Mastering Machine Learning and intro' to Deep Learning 13. Coursera: Deep Learning Specialization
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:** - вимоги до безпеки програмного забезпечення; - основні типи вразливостей; - засоби автоматизованого тестування для виявлення вразливостей; - основні типи ШНМ та методи їх навчання; - методи глибинного навчання; - основні практики OWASP; - тестування безпеки; **вміти:** - виявляти ризики безпеки у коді та зовнішніх залежностях за допомогою методів глибинного навчання; - застосовувати шаблони атак для виявлення вразливостей; - визначати заходи протидії загрозам; - запобігати вразливостям конфіденційності; - проводити code review для виявлення потенційних вразливостей системи; - застосовувати основні принципи OWASP на практиці.

Ключові слова	Безпека програмного забезпечення, безпечний код, вразливості, ризики, статичні та динамічні аналізатори коду, загрози, OWASP, штучна нейронна мережа (ШНМ), глибинне навчання, персептрон, багатошаровий персептрон, рекурентна ШНМ, глибинна ШНМ, згорткова ШНМ, градієнтний метод, метод зворотного поширення похибки, National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE)
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 таких дисциплін: 1) Дискретна математика; 2) Програмування; 3) Основи кібербезпеки; 4) Основи криптології; 5) Прикладна криптологія.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Індивідуальні завдання
Необхідне обладнання	Лабораторія з обладнаними робочими станціями, з'єднаними в комп'ютерну мережу. IDE для програмування мовою C++, C#, Python або Java.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. 70 балів нараховують за виконання 7 лабораторних завдань та 30 балів – за оволодіння теоретичним матеріалом курсу (2 модульні контролі по 15 балів) **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.

Критерії оцінювання знань студентів	Бали рейтингу	Макс. к-сть балів
1. Бали поточної успішності за виконання індивідуальних завдань		
Критерії оцінювання (7*10 бали)	**70 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.	**10**	
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.	**9-5**	
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. Модульний контроль		
Критерії оцінювання (2*15)	**30**	
Протягом семестру проводиться **2 модульних контролі**. Кожен модуль складається з **15 тестових питань**.		
***Критерії оцінювання вирішення тестів (15*1 бали)*:**	**15**	
Відповідь вірна	**1**	
Відповідь невірна	**0**	
Загальна кількість балів по завершенні вивчення дисципліни	**100**	

Питання до модульних контролів

1. Основні елементи безпеки та вразливості програмного забезпечення.
2. Типові моделі атак програмного забезпечення. Пошук вразливостей.
3. Основні стратегії уникнення вразливостей. Шаблони атак для виявлення вразливостей. Вразливості спричинені людським фактором.
4. Оцінка функціональності програмного забезпечення. Виявлення ризиків безпеки у коді та зовнішніх залежностях.
5. Моделювання та ранжування загроз. Визначення заходів протидії загрозам.
6. Використання OWASP Threat Dragon для моделювання загроз, Microsoft Threat Modeling Tool.
7. Типові помилки програмування та методи їх усунення. Переповнення буферу. Рекомендації щодо запобігання вразливостей.

	8. Виявлення поширених веб-вразливостей. Запобігання вразливостям конфедиційності. 9. Тестування безпеки. Code review для виявлення потенційних вразливостей системи. Концепції статичного та динамічного аналізу коду. 10. Виявлення проблем в коді використовуючи PyLint Tool, засоби автоматизованого тестування. Використання OWASP Zed Attack Proxy (ZAP). 11. OWASP: Основні типи вразливостей. 12. Багатошаровий та одношаровий персептрон. 13. Основні типи нейронних мереж та методів навчання. 14. Архітектура глибинних ШНМ. 15. Рекурентні ШНМ. 16. Навчання ШНМ на основі методу градієнтного спуску. 17. Навчання ШНМ на основі зворотного поширення помилки. 18. Регуляризація навчання ШНМ. 19. Згорткові нейронні мережі. 20. Трансформери ШНМ. 21. ШНМ на основі графів. 22. Генеративні змагальні мережі (Generative Adversarial Networks).
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. Вимоги до безпеки програмного забезпечення** (Термінологія та основні елементи безпеки програмного забезпечення. Вразливості програмного забезпечення. Типові моделі атак. Виправлення вразливостей хешу пароля. Визначення основних вимог безпеки програмного забезпечення. Пошук вразливостей. Злам хешу пароля та захист від цього)	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
2	**Тема 2. Стратегії уникнення вразливостей.** (Основні стратегії уникнення вразливостей. Оцінка функціональності програмного забезпечення. Виявлення ризиків безпеки у коді та зовнішніх залежностях. Шаблони атак для виявлення вразливостей. Вразливості спричинені людським фактором)	лекція, самостійна робота		2 4	1 тиждень
		лаб.	[1-6]	2	
3-4	**Тема 3. Тестування безпеки програмного забезпечення.** (Тестування безпеки. Code review для виявлення потенційних вразливостей системи. Концепції статичного та динамічного аналізу коду, NVD, CVE, CWE. Аналіз на основі глибинного навчання. Виявлення проблем в коді використовуючи PyLint Tool, засоби автоматизованого тестування. Використання OWASP Zed Attack Proxy (ZAP))	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	

5-6	**Тема 4. Основні вразливості OWASP** (Порушення контролю доступу, криптографічні вразливості, вразливості ін'єкцій, вразливості небезпечного дизайну, вразлива конфігурація веб-аплікацій, помилки ідентифікації та автентифікації, порушення цілісності програмного забезпечення даних, помилки логування та моніторінгу безпеки, підробка запитів сервера)	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	
7-8	**Тема 5. Основи теорії ШНМ.** **(**Моделі нейронів, активаційні функції, класифікація та архітектура нейронних мереж, одношаровий та багатошаровий персептрон, рекурентні мережі, методи навчання з вчителем та без, цільова функція, градієнтний метод, глибинне навчання**)**	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	
9	**Тема 6. Глибинні нейронні мережі (Deep Neural Networks).** (Базисні функції, багатошарові мережі, функції активації, глибинні мережі, методи навчання, загальна архітектура, функції помилки)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
10	**Тема 7. Навчання ШНМ на основі методу градієнтного спуску.** (Функція помилки, оптимізація градієнтного спуску, збіжність, нормалізація даних)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
11	**Тема 8. Навчання ШНМ на основі зворотного поширення помилки.** (Оцінка градієнтів, нейронні мережі прямого поширення, Jacobian matrix, Hessian matrix, автоматична диференціація)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
12	**Тема 9. Регуляризація навчання ШНМ.** (Індуктивне зміщення, квадратична регуляризація, криві навчання, спільне використання параметрів, залишкові з'єднання)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
13	**Тема 10. Згорткові нейронні мережі (Convolutional Networks).** (Загальна архітектура, принципи роботи, застосування CNN до виявлення вразливостей у програмному коді)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
14	**Тема 11. Трансформери ШНМ.** (Коефіцієнти уваги, обробка трансформерів, самоувага, маштабована самоувага, багатостороння увага, шари трансформерів, обробка природньої мови, моделі мовних трансформерів, мультимодальні трансформери)	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
15	**Тема 12. ШНМ на основі графів.** **(**Машинне навчання на графах. Властивості графів, класифікація графів, мережі на графах, геометричне глибинне навчання**)**	лекція, самостійна робота	[1-6]	2 3	1 тиждень
		лаб.	[1-6]	2	
16	**Тема 13. Генеративні змагальні мережі (Generative Adversarial Networks).**	лекція, самостійна робота	[1-6]	2 3	1 тиждень

	(Функція втрат, змагальне навчання на практиці, CycleGAN)	лаб.	[1-6]	2	