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 “Мережева безпека та виявлення вторгнень”, 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	**Мережева безпека та виявлення вторгнень**
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 "Мережева безпека та виявлення вторгнень" є вибірковою дисципліною з 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 4,5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області мережевої безпеки, використання методів та інструментів захисту мережі та підключених до неї пристроїв від несанкціонованого доступу, методів захисту конфіденційності даних та захисту цілісності інформації у мережах, підготовка фахівців, здатних аналізувати, обирати, застосовувати методи та засоби забезпечення мережевої безпеки та виявлення вторгнень.
Мета та цілі дисципліни	Метою навчальної дисципліни "Мережева безпека та виявлення вторгнень" є формування знань з мережевої безпеки, використання методів та інструментів захисту мережі та підключених до неї пристроїв від несанкціонованого доступу, методів захисту конфіденційності даних у мережах, виявлення та запобігання вторгненням.
Література для вивчення дисципліни	*Основна* 1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с. 2. Ходаківський І.В. Безпека інформаційних систем та мереж. Навчальний посібник. Київ: Видавництво ЦНЛ, 2020. – 280 с. 3. Cisco systems. Навчальні матеріали мережних академій Cisco за курсом Network Security https://www.netacad.com/courses/cybersecurity/network-security/ 4. Cisco systems. Навчальні матеріали мережних академій Cisco за курсом CCNA Cybersecurity Operations https://www.netacad.com/courses/cybersecurity/cyberops-associate/ 5. AWS Cloud Security. https://aws.amazon.com/security/

	Додаткова 6. R. Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco, CA, USA:No Starch Press, 2013. 376p. 7. Технології захисту локальних мереж на основі обладнання CISCO: навч.посіб. /Т.І. Коробейнікова, С.М. Захарченко. – Львів: Видавництво Львівська політехніка, 2021. – 232 с. 8. Kaufman, C., Perlman, R., and Speciner, M.: Network Security, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2002. 9. Gilman, Evan and Barth, Doug. Zero trust networks. O'Reilly Media, Incorporated, 2017.
Обсяг курсу	Загальний обсяг: 135 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 годин лабораторних занять. Самостійної роботи: 71 година.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей. **знати:** • теоретичні та практичні підходи до організації мережевої безпеки; • протоколи безпеки та особливості роботи систем виявлення та запобігання вторгненням; • методи розробки і впровадження систем мережевої безпеки; • основні програмні та апаратні засоби виявлення та запобігання вторгненням. **вміти:** • здійснювати аналіз мережевої безпеки та усувати можливі шляхи несанкціонованого доступу; • ідентифікувати можливі загрози чи атаки; • планувати та реалізувати відповідні заходи, щодо безпеки інформаційно-комунікаційних систем та мереж; • проектувати системи захисту і безпеки мереж з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію та технічне обслуговування.
Ключові слова	Мережева безпека, мережеві атаки, міжмережеві екрани, IPS, IDS, сигнатури, списки контролю доступу (ACL), технологія VPN, протокол IPSec, політика безпеки.
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	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.
Необхідне обладнання	Комп'ютер, мережа Internet, проектор. Програмне забезпечення Cisco Packet Tracer, Oracle VM VirtualBox, мережеве обладнання.
Критерії оцінювання	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:

(окремо для кожного виду навчальної діяльності)

• лабораторні роботи: 50% семестрової оцінки;
• самостійна робота: 10% семестрової оцінки;
• модульний контроль: 40% 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 лабораторних робіт, самостійній роботі та бали модульного 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 лабораторних робіт		
Критерії оцінювання (5*10 балів)	**50 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.	**10-9**	
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	**8-5**	

	незначні помилки.	
	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 бали)	**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	**40**
	Критерії оцінювання (2*20 балів)	**40**
	Протягом семестру проводиться **2 модульних контролі**. Кожен модуль містить **20 тестових питань.**	
	Критерії оцінювання вирішення тестів (20*1 бал):	
	Відповідь вірна	**1**
	Відповідь невірна	**0**
	Загальна кількість балів по завершенні вивчення дисципліни	**100**
Питання до модульних контролів	1. Який тип атаки може відключити комп'ютер, змушуючи його надлишково використовувати пам'ять або перевантажувати процесор? 2. Який метод намагається отримати пароль шляхом перебору усіх можливих комбінацій? 3. Який нетехнічний метод кіберзлочинець використовуватиме для збору конфіденційної інформації з організації? 4. Яка служба визначає, до яких ресурсів користувач може отримати доступ та які операції може виконувати користувач? 5. Назвіть важливу характеристику черв'яків (worms) 6. Який тип мережевої загрози призначений для перешкоджання доступу до ресурсів авторизованих користувачів? 7. Яке рішення потрібно запропонувати, щоб забезпечити безпечний канал зв'язку між віддалено розташуваними користувачами і компанією 8. Яка мета атаки мережевої розвідки? 9. У чому перевага SSH у порівнянні з Telnet при віддаленому керуванні маршрутизатором? 10. Назвіть найбільш ефективні способи захисту від шкідливих програм	

	11. Які існують методи забезпечення конфіденційності? 12. Які рішення мережевої безпеки можна використовувати для зниження ризику DoS-атак 13. Яка служба дозволить поставити у відповідність веб-адресі конкретну IP-адресу веб-сервера призначення 14. Які рішення мережевої безпеки можна використовувати для зниження ризику DoS-атак? 15. Які заходи безпеки маршрутизатора потрібно підтримувати для захисту граничного маршрутизатора на периметрі мережі? 16. Назвіть перевагу використання фаєрвола зі збереженням стану в порівнянні з проксі-сервером 17. Назвіть недоліки використання IDS. 18. Назвіть спільні характеристики систем IDS та IPS. 19. У чому недолік механізму виявлення загроз на основі шаблонів (signatures)? 20. Які протоколи IPsec використовуються для забезпечення цілісності даних? 21. Які твердження справедливі щодо стандартних списків ACL? 22. Які можливості у розширених списків ACL?
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. Основи мережевої безпеки** Загрози безпеці та вразливості. Фізична безпека. Типи шкідливого програмного забезпечення. Мережеві атаки. Нейтралізація мережевих атак. Захист мережевого обладнання	лекція, самостійна робота	[1-6]	2 4	1 тиждень
		лаб.	[1-6]	2	
2	**Тема 2. Забезпечення мережевої безпеки. Безпека мережевих пристроїв.** Забезпечення мережевої безпеки. Безпечний доступ до пристроїв. Присвоєння адміністративних ролей.	лекція, самостійна робота		2 5	1 тиждень
		лаб.	[1-6]	2	
3-4	**Тема 3. Безпека бездротових мереж.** Переваги бездротового зв'язку. Бездротові технології. Принципи роботи WLAN. Загрози WLAN. Безпека WLAN.	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	
5-6	**Тема 4. Моніторинг та керування мережевим обладнанням.** Безпечне управління та звітність. Використання системного журналу Syslog для безпеки мережі. Використання SNMP для безпеки мережі.	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	
7-8	**Тема 5. Захист мережі за допомогою списків контролю доступу ACL.** Призначення ACL. Рекомендації щодо створення ACL. Типи ACL для IPv4. ACL-	лекція, самостійна робота	[1-6]	4 8	2 тижні

	списки IPv6. Використання списків контролю доступу ACL для управління мережевим трафіком	лаб.	[1-6]	4	
9	**Тема 6. Технології міжмережевого екрану.** Типи міжмережевих екранів. Зональні міжмережеві екрани. Налаштування зонального брандмауера (ZPF)	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
10	**Тема 7. Системи виявлення та запобігання вторгненням.** Характеристики IDS та IPS. Впровадження мережевих IPS. IPS на основі хоста. Мережеві IPS. Аналізатори портів.	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
11	**Тема 8. IPS сигнатури.** Характеристики IPS сигнатури. Сигналізація IPS сигнатур. Дії сигнатур IPS. Управління та моніторинг IPS. Глобальна кореляція IPS	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
12	**Тема 9. Безпека в хмарі AWS.** Переваги використання хмар. Безпека в AWS Cloud. Принципи проектування безпеки. Модель розподіленої відповідальності.	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
13-14	**Тема 10. Безпека доступу та хмарні ресурси.** Налаштування безпеки доступу до ресурсів хмари. Основи IAM (Identity and Access Management). Автентифікація та авторизація. Служби аутентифікації та керування доступом.	лекція, самостійна робота	[1-6]	4 8	2 тижні
		лаб.	[1-6]	4	
15	**Тема 11. Захист хмарної інфраструктури.** Трирівнева структура веб-застосунку. Використання груп безпеки AWS. Використання списків управління доступом мережі AWS.	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
16	**Тема 12. Інциденти мережевої безпеки.** Виявлення та реагування на інциденти. Обробка інцидентів. CSIRT (A Computer Security Incident Response Team). NIST 800-61r2. Сервіси AWS, які підтримують фазу виявлення та визначення. Сервіси AWS, які підтримують фазу вирішення та відновлення **(**Машинне навчання на графах. Властивості графів, класифікація графів, мережі на графах, геометричне глибинне навчання**)**	лекція, самостійна робота	[1-6]	2 5	1 тиждень
		лаб.	[1-6]	2	
ВСЬОГО				**135**	