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 таінформатики
Львівського національного університету імені Івана Франка
(Протокол №9/24 від 29 серпня 2024 р.)

Завідувач кафедри .

Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни
“Системна інтеграція технологій безпеки”,
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	Системна інтеграція технологій безпеки
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	Брич Тарас Богданович, кандидат тех. наук доцент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактнаінформація викладачів	taras.brych@lnu.edu.ua https://ami.lnu.edu.ua/employee/brych-t-b
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 “ Системна інтеграція технологій безпеки” є вибірковою дисципліною зі спеціальності 125 – кібербезпека та захист інформації для освітньої програми Технології штучного інтелекту в кібербезпеці, яка викладається в 3-му семестрі другого (магістерського) рівня освіти в обсязі 3 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області системної розбудови технологій безпеки, розвитку системи знань про адмініструванні систем захисту інформації, розуміння основних принципів протидії кіберзагрозам, розбудови та організації роботи SOC.
Мета та цілідисципліни	Метою курсу є формування у студентів знань для створення, організації роботи, забезпечення персоналом, повноважень, інструментарію та ресурсів для адміністрування системами захисту інформації.
Література для вивчення дисципліни	Основна література 1. *Kathryn Knerler, Ingrid Parker, Carson Zimmerman.* 11 Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation.. 2022. 452 p. 2. Cybersecurity and Infrastructure Security Agency (CISA), “CISA Insider Threat Mitigation,” November 2021. [Online]. Available: https://www.cisa.gov/insider-threat- mitigation. 3. European Union - Horizon 2020 Programme Framework, “General Data Protection Regulation (GDPR) Compliance Guidelines,” November 2021. [Online]. Available: https://gdpr.eu/. 4. National Institute of Standards and Technology (NIST), “Security and Privacy Controls for Information Systems and Organizations,” December 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. 5. Google Cloud, Deloitte, “Future of the SOC: SOC People: Skills not Tiers,” 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/ about-deloitte/Deloitte_and_Chronicle_Future_of_the_SOC-Skills_Before_Tiers.pdf. Додаткова література 6. C. Crowley, “Common and Best Practices for Security Operations Centers: Resultsof the 2019 SOC Survey,” 2019. [Online]. Available: https://www.sans.org/media/ analyst-program/common-practices-security-operations-centers-results-2019-soc- survey-39060.pdf.

	7. S. K. White, “IT Asset Management (ITAM): A Centralized Approach to ManagingIT Systems and Assets,” CIO, 11 September 2019. [Online]. Available: https://www. cio.com/article/3437476/it-asset-management-itam-a-centralized-approach-to- managing-it-systems-and-assets.html. 8. MITRE ATT&CK – https://attack.mitre.org/matrices/enterprise/ 9. FIRST is the global Forum of Incident Response and Security Teams – https://www.first.org/
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 24 год., з них 8 год. лекцій та 16 год. лабораторних робіт. Самостійної роботи: 66 год.
Очікуваніре-зультатинав-чання	У результаті вивчення навчальної дисципліни студент має набути такихкомпетентностей: **знати:** сервіси безпеки; повноваження SOC; функції SOC; адміністрування локальних мереж; системи управління інформаційною безпекою – ISMS; **вміти:** організовувати ефективне функціонування оперативних центрів кібербезпеки (SOC); застосувати сучасні стратегії розбудови SOC; проводити пріоритезацію завдань та відповідний підбір інструментів - необхідного ПЗ для їх виконання; аналізувати роботу SOC з метою покращення продуктивності та розширення функціональності.
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, локальні мережі, IDS, IPS, DLP, NGFW, EDR\XDR, SIEM, SOAR, SOC.
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 базових знань з: - Основи кібербезпеки - Організація IT на підприємстві - Безпека комп'ютерних мереж - Менеджмент інформаційної безпеки - Оцінка ризиків в кібербезпеці
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Модульний контроль Лабораторні роботи
Необхідне обладнання	Комп’ютери, доступ до мережі Internet.

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 підсумкової контрольної роботи. 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 балів)	**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 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**
	Студент не опрацював самостійно додаткових джерел і не володіє матеріалом — **0**
	Загальна максимальна кількість балів за поточний контроль — **50**
	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	**Тема 1 Системи управління інформаційною безпекою - ISMS (Information Security Management Systems.** (Захист від шкідливих програм - Antimalware Protection. Запобігання проникненню на основі хоста - Host-Based Intrusion Prevention. Безпека додатків. Профілювання мережі та серверів. Загальна система оцінки вразливості – CVSS. Системи управління інформаційною безпекою – ISMS.)	лекція, самостійна робота лаб,	[7, 8, 9]	1 4 8	1 тиждень
2	**Тема 2. Безпечне управління пристроями, мобільними пристроями, конфігураціями.** (Identity Manager-и. Mobile Device Management-и. Configuration management tools. Patch Management tool.)	лекція, лаб, самостійна робота	[5,6, 9]	1 4 10	1 тиждень
3	**Тема 3. Створення SOC відповідно вимог та потреб організації.** (Активи, які необхідно захищати, повноваження. Роль та функції SOC. Ситуаційна обізнаність. Правове,	лекція, самостійна робота	[1, 2, 6]	1 8	1 тиждень

	нормативне середовище. Технічне середовища систем і даних. Загрози.)				
4	**Тема 4. Вимоги до персоналу SOC – підбір, навчання.** (Підбір, навчання, заохочення персоналу. План зміни кадрів. Розрахунок кількості аналітиків.)	лекція, самостійна робота	[1, 2, 6]	1 8	1 тиждень
5	**Тема 5. Пріоритети реагування на інциденти. Аналіз кіберзагроз.** (Обробка інцидентів. Виявлення та аналіз. Зберігання даних. Дії після інциденту. Реагування на інциденти в хмарі. Полювання на загрози - кіберрозвідка. Red Teaming. Blue teams. Purple teaming. Deception в практиці SOC. Аналіз шкідливих програм. Цифрова криміналістика.)	лекція, самостійна робота	[1, 2, 6, 3, 5]	1 8	1 тиждень
6	**Тема 6. Вибір необхідних даних для збереження та аналізу.** (Планування збору даних. Моніторинг та захист хосту. Моніторинг мережі. Моніторинг складових системи у хмарі. Стратегії підбору інструментів збору даних.)	лекція, лаб, самостійна робота	[3, 7, 8, 9]	1 4 8	1 тиждень
7	**Тема 7. Підбір необхідних інструментів аналітиків SOC.** (Інтеграція інструментів. Інформація про безпеку та керування подіями. Аналітика поведінки користувача. Автоматизація безпеки, координація та реагування. Захист інструментів і даних SOC.)	лекція, лаб, самостійна робота	[3, 4, 6, 8, 9]	1 2 8	1 тиждень
8	**Тема 8. Вимірювання продуктивності роботи SOC. Робота з інформацією галузі кібербезпеки.** (Програма SOC Metrics. Використання зовнішньої організації для вимірювання SOC. Вибір показників.)	лекція, лаб, самостійна робота	[3, 4, 6, 8, 9]	1 2 8	1 тиждень