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

“Безпека систем автоматизації та інтернету речей”,

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	Безпека систем автоматизації та інтернету речей
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
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	Євсеєв Сергій Петрович, професор кафедри кібербезпеки
Контактна інформація викладачів	serhii.yevseiev@lnu.edu.ua https://ami.lnu.edu.ua/employee/yevseiev-s-p Головний корпус ЛНУ ім. І. Франка, каб. 380. 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 “Безпека систем автоматизації та інтернету речей” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми «Технології штучного інтелекту в кібербезпеці», яка викладається в 1-му семестрі в обсязі 6-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на визначення інформації, що потребує захисту на об’єктах критичної інфраструктури (ОКІ). Опанування методів та засобів технічного захисту інформації на ОКІ. Ознайомлення з каналами витоку інформації та підстав їх утворення. Оволодіння навичками роботи із засобами та комплексами виявлення закладних пристроїв несанкціонованого отримання інформації. Оволодіння навичками роботи із засобами та комплексами захисту інформації на ОКІ. Засвоєння порядку проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Оволодіння організаційно-технічними заходами щодо захисту інформації на ОКІ.

Мета та цілі дисципліни	Навчальна дисципліна «Безпека систем автоматизації та інтернету речей» є складовою циклу професійної підготовки фахівців другого освітньо-кваліфікаційного рівня “магістр”. Пропонований навчальний курс забезпечить студентам навчання принципам визначення загальних вимог до кіберзахисту об’єктів критичної інфраструктури, встановлення переліку базових заходів з кіберзахисту, які повинні бути впроваджені на об’єкті критичної інфраструктури, на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, визначення порядку та критеріїв віднесення об’єктів до об’єктів критичної інфраструктури.
Література для вивчення дисципліни	Основна: 1. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text 2. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text 3. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text 4. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 06 жовтня 2021 року № 601. 5. Технічні вимоги на створення спеціалізованого програмного забезпечення «Державний реєстр об’єктів критичної інформаційної інфраструктури». Наказ Державної служби спеціального зв’язку та захисту інформації України, 2022, 31 с. 6. Про затвердження Положення про організацію кіберзахисту в банківській системі України: Постанова Правління Національного банку України від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text Допоміжна: 7. ISO/IEC 27001:2024 Information security, cybersecurity and privacy protection — Information security management systems. 8. ISO/IEC 27002:2024 Information security, cybersecurity and privacy protection — Information security controls. 9. ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection — Guidance on managing information security risks /
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 116 год.
Очікувані результати	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:

навчання	**знати:** • здатність критично аналізувати ризики, вразливості та загрози для критичної інфраструктури, а також приймати обґрунтовані рішення на основі отриманих даних; • здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; • здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог; • здатність виявляти і розв’язувати складні завдання, що виникають під час забезпечення безпеки об’єктів критичної інфраструктури; • розуміння важливості етичних питань у сфері кібербезпеки та захисту критичних об’єктів, включаючи конфіденційність, цілісність та законність дій. **вміти:** • оцінювати та аналізувати загрози: використовувати методи аналізу ризиків для виявлення можливих загроз і вразливостей для критичних об'єктів; • впроваджувати стандарти безпеки: застосовувати та адаптувати відповідні стандарти кібербезпеки для захисту об'єктів критичної інфраструктури, забезпечуючи дотримання міжнародних і національних вимог; • розробляти стратегії кіберзахисту: створювати політики та процедури безпеки для забезпечення захисту конфіденційності, цілісності та доступності даних і систем на критичних об’єктах; • застосовувати технічні засоби захисту: налаштовувати міжмережеві екрани, системи виявлення вторгнень (IDS/IPS), шифрування, VPN та інші технології для забезпечення кіберзахисту; • розробляти та впроваджувати плани реагування на інциденти: створювати плани реагування на кіберінциденти, а також заходи для забезпечення безперервності бізнесу і відновлення після атак; • проводити аудит безпеки: виконувати аналіз поточного стану кібербезпеки критичних об'єктів, оцінювати їхню відповідність стандартам і виявляти вразливості; • ідентифікувати та реагувати на інциденти: вміти швидко ідентифікувати кіберінциденти, проводити аналіз і вживати заходи для мінімізації збитків; • організовувати навчальні заходи для співробітників щодо правил і політик кібербезпеки, підвищувати рівень обізнаності про загрози та найкращі практики безпеки; **Курс забезпечує набуття таких компетентностей: ЗК 2, КФ 2, КФ 4-6, КФ 9;** **та програмних результатів навчання: РН 2, РН 6, РН 8-11, РН 16, РН 21, РН 23.**
Ключові слова	Кібербезпека, Захист інформації, Критична інфраструктура, Загрози кібербезпеці, Системи автоматизації, Виявлення аномалій, Безпека IoT, Шифрування даних, Аудит безпеки, Мережева безпека.

Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Екзамен у кінці 1 семестру
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисципліни: • Інтелектуальні інформаційні технології
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, опитування теоретичного матеріалу, контрольна робота (модуль) самостійна робота. Лекції та лабораторні: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод.
Необхідне обладнання	Комп'ютерний клас із вільно-доступним програмним забезпеченням, локальна комп'ютерна мережа, доступ до Internet мережі.
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; • іспит: 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 незарахування 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. П**олітика 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 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 участь у лабораторних заняттях		
Критерії оцінювання (8*5 балів)	**40 балів**	
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.	**5**	
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.	**4-3**	
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 (16*0.5 балів та 1*2 бали)	**10 балів**	
Підготовка доповіді на конференцію	**2**	
Самостійна робота (додаткове опрацювання матеріалу за темами дисципліни поза межами наданого лектором, з додаткових джерел) Самостійна робота студентів, оцінюється під час поточного контролю теми на відповідному лабораторному занятті. Студент додатково опрацював матеріал та аргументовано його викладає.	**0.5**	
Студент не опрацював самостійно додаткових джерел і не володіє матеріалом	**0**	
Загальна максимальна кількість балів за поточний контроль	**50**	
4. Екзамен	**50**	

	Семестровий екзамен як форма підсумкового контролю є обов'язковим для всіх студентів. Екзаменаційний білет містить **18 тестових питань в сумі 50 балів**	
	Критерії оцінювання вирішення тестів	***50***
	Відповідь вірна: 4 питання 10 питань 4 питання	 1 3 4
	Відповідь невірна	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. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.** Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури	лекція, самостійна робота	[1-9]	4 13	2 тижні
	Тема 1. Вивчення загальних вимог до кіберзахисту об'єктів критичної інфраструктури	лаб	[1-9]	4	
3-4	**Тема 2. Критична інфраструктура.** Національна система захисту критичної інфраструктури. Організаційні засади національної системи захисту критичної інфраструктури.	лекція, самостійна робота	[1-9]	4 13	2 тижні
	Тема 2. Критична інфраструктура за регіонами України. Організаційні засади регіону України як складові національної системи захисту критичної інфраструктури.	лаб.	[1-9]	4	
5-6	**Тема 3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури.** Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.	лекція, самостійна робота	[1-9]	4 13	2 тижні
	Тема 3. Складання відомостей про	лаб	[1-9]	4	

	об’єкт критичної інформаційної інфраструктури визначеного регіону України.				
7-8	**Тема 4. Закон України Про критичну інфраструктуру (проект).** Національна система захисту критичної інфраструктури. Організаційні засади національної системи захисту критичної інфраструктури.	лекція, самостійна робота	[1-9]	4 13	2 тижні
	Тема 4. Вивчення особливостей національної система захисту критичної інфраструктури.	лаб.	[1-9]	4	
9-10	**Тема 5. Державний реєстр об’єктів критичної інформаційної інфраструктури.** Спеціалізоване програмне забезпечення Система керування базами даних	лекція, самостійна робота	[1-9]	4 14	2 тижні
	Тема 5. Вивчення особливостей формування Технічних вимог на створення спеціалізованого програмного забезпечення «Державний реєстр об’єктів критичної інформаційної інфраструктури».	лаб.	[1-9]	4	
11-12	**Тема 6 Положення про організацію кіберзахисту в банківській системі України.** Організація інформаційного обміну.	лекція, самостійна робота	[1-9]	4 14	2 тижні
	Тема 6. Дослідження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури банків.	лаб.	[1-9]	4	
13-14	**Тема 7. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури.** Розробка та впровадження профілю кіберзахисту об’єкт критичної інформаційної інфраструктури.	лекція, самостійна робота	[1-9]	4 14	2 тижні
	Тема 7. Методичні рекомендації щодо розробки поточного та цільового профілю кіберзахисту. Методичні рекомендації щодо аналізу поточного та цільового профілю кіберзахисту.	лаб.	[1-9]	4	
15-16	**Тема 8. Класифікація заходів кіберзахисту.** Клас заходів кіберзахисту RS. Клас заходів кіберзахисту RC	лекція, самостійна робота	[1-9]	4 14	2 тижні

	Тема 8. Проведення класифікації заходів кіберзахисту об’єктів критичної інфраструктури.	лаб.	[1-9]	4	
	Всього			**180**	