

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра автоматизації, комп'ютерно-інтегрованих технологій та робототехніки



ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
Тетяна ГОВОРУЩЕНКО
2024 р.

СИЛАБУС

Навчальна дисципліна Функціональна та кібербезпека систем автоматизації

Освітньо-наукова програма Автоматизація, комп'ютерно-інтегровані технології та робототехніка

Рівень вищої освіти другий (магістерський)

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Корецька Людмила Олександрівна
Профайл викладача	https://akit.khmnmu.edu.ua/koreczka-lyudmyla-oleksandrivna/
Е-mail викладача(ів)	koretskal@khmnmu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnmu.edu.ua/course/view.php?id=7973
Навчальний рік	2024-2025
Консультації	Очні: середа, 14.35-15.55, ауд.4-317; онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Статус дисципліни	Форма навчання	Курс	Семестр	Загальний обсяг		Кількість годин						Форма семестрового контролю			
				Кредити ЄКТС	Години	Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС	Курсовий проєкт	Курсова робота	Залік	Іспит
						Разом	Лекції	Лабораторні роботи	Практичні заняття						
О	Д	1	2	5	150	54	18	36			96				+

Анотація дисципліни

Дисципліна "Функціональна та кібербезпека систем автоматизації" є однією з дисциплін професійної підготовки магістрів за ОП Автоматизація, комп'ютерно-інтегровані технології та робототехніка.

Дисципліна викладається для здобувачів другого (магістерського) рівня вищої освіти денної форми навчання спеціальностей галузі електроніка, автоматизація та електронні комунікації. При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема, методи проблемного навчання.

Мета і завдання дисципліни

Метою дисципліни "Функціональна безпека систем автоматизації" є: 1) формування компетентностей, необхідних для розроблення надійних систем автоматизації; 2) Ознайомити студентів із основними напрямками по забезпеченню функціональної безпеки систем автоматизації; 3) ознайомити студентів з теоретичною базою, що використовується при вирішенні задач оцінювання надійності систем автоматизації.

Завдання дисципліни. Надати студентам знання і практичні навички з оцінювання надійності автоматизованих систем; підготувати студентів до ініціювання та автономного провадження дослідницької та інноваційної діяльності в галузі функціональної безпеки систем автоматизації.

Пререквізити: Теорія, моделювання і оптимізація інтелектуальних і складних систем керування; Робототехнічні та інтелектуальні мехатронні пристрої і системи.

Кореквізити: Професійна практика.

Очікувані результати навчання

Після вивчення дисципліни "Функціональна та кібербезпека систем автоматизації" студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

Компетентності, на формування яких спрямовано ОК:

Інтегральна. Здатність розв'язувати складні задачі і проблеми автоматизації та комп'ютерно-інтегрованих технологій у професійній діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або провадження інноваційної діяльності та характеризується комплексністю та невизначеністю умов і вимог.

ЗК4. Здатність працювати в міжнародному контексті.

ФК2. Здатність проектувати та впроваджувати високонадійні системи автоматизації та їх прикладне програмне забезпечення, для реалізації функцій управління та опрацювання інформації, здійснювати захист прав інтелектуальної власності на нові проектні та інженерні рішення

ФК3. Здатність застосовувати методи моделювання та оптимізації для дослідження та підвищення ефективності систем і процесів керування складними технологічними та організаційно-технічними об'єктами.

ФК4. Здатність аналізувати виробничо-технологічні системи і комплекси як об'єкти автоматизації, визначати способи та стратегії їх автоматизації та цифрової трансформації.

ФК8. Здатність розробляти функціональну, технічну та інформаційну структуру комп'ютерно-інтегрованих систем управління організаційно-технологічними комплексами із застосуванням мережевих та інформаційних технологій, програмно-технічних керуючих комплексів, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв та засобів людино-машинного інтерфейсу.

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів.

ПРН4. Застосовувати сучасні підходи і методи моделювання та оптимізації для дослідження та створення ефективних систем автоматизації складними технологічними та організаційно-технічними об'єктами.

ПРН5. Розробляти комп'ютерно-інтегровані системи управління складними технологічними та організаційно-технічними об'єктами, застосовуючи системний підхід із врахуванням нетехнічних складових оцінки об'єктів автоматизації.

ПРН9. Розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційно-технічними об'єктами, розробляти програмно-технічні керуючі комплекси із застосуванням мережевих та інформаційних технологій, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв, засобів людино-машинного інтерфейсу та з урахуванням технологічних умов та вимог до управління виробництвом.

ПРН10. Розробляти і використовувати спеціалізоване програмне забезпечення та цифрові технології для створення систем автоматизації складними організаційно-технічними об'єктами, професійно володіти спеціальними програмними засобами.

ПРН12. Збирати необхідну інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела, аналізувати і оцінювати її.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема практичного заняття*	Тема лабораторної роботи*	Самостійна робота студентів		
				Зміст	Год.	Література
1-2	Функціональна безпека: основні поняття та визначення		Оцінка потенційної небезпеки виробничих процесів	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	11	[2-5, 8]
3-4	Функціональна		Резервування у	Опрацювання лекційного	11	[2-5, 8]

	безпеку та «Інтернет-речей» у промисловості		системах автоматизації: модулі введення, давачі	матеріалу. Підготовка до захисту лабораторної роботи №1. Підготовка до лабораторної роботи №2.		
5-6	Вимоги до інформаційної безпеки		Резервування у системах автоматизації: модулі виведення	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2. Підготовка до лабораторної роботи №3.	11	[2, 9-11]
7-8	Методи забезпечення функціональної безпеки		Резервування у системах автоматизації: процесорні модулі	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Підготовка до лабораторної роботи №4.	11	[2-5, 8]
9-10	Резервування у автоматизованих системах управління		Резервування у системах автоматизації: джерела живлення	Підготовка до тестування за темами 1-4. Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4. Підготовка до лабораторної роботи №5.	11	[4-8]
11-12	Резервування нижнього, середнього та верхнього рівнів		Організація резервування промислових мереж	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Підготовка до лабораторної роботи №6.	11	[4-8]
13-14	Відповідність вимогам інформаційної та функціональної безпеки за допомогою методології Assurance Case			Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Підготовка до лабораторної роботи №7 (частина 1).	11	[9-11]
15-16	Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ		Оцінка надійності систем автоматизації із резервуванням (частина 1)	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7 (частина 2).	11	[9-11]
17-18	Підсумкове заняття		Оцінка надійності систем автоматизації із резервуванням (частина 2)	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Підготовка до підсумкового контрольного заходу.	8	

Примітка: * Послідовність проведення занять визначається розкладом (може не відповідати нумерованим тижням)

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. До практичних занять студент має підготуватися за відповідною темою і проявляти активність. Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ.

Критерії оцінювання результатів навчання.

Кожний вид роботи з дисципліни оцінюється за **чотирибальною** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; засвоєння теоретичного матеріалу з тем перевіряється тестовим контролем; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни і робочим навчальним планом.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота	Самостійна, індивідуальна робота	Семестр. контроль (іспит)
2 семестр		
Лабораторні роботи №:	Тестовий контроль	Підсумковий контрольний захід
1-8	Т 1-4	
ВК: 0,4	0,2	0,4

Умовні позначення: ТК – тестовий контроль; Т – тема дисципліни; ВК – ваговий коефіцієнт.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20. На тестування відводиться 20 хвилин. Тестування проводиться з використанням модульного середовища для навчання MOODLE.

Оцінювання здійснюється за чотирибальною шкалою.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту, наведена у таблиці.

Сума балів за тестове завдання	1–11	12–14	15–18	19–20
Оцінка	2	3	4	5

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна шкала балів	Інституційна оцінка	Критерії оцінювання
A	4,75-5,00	5	Зараховано Відмінно – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навичок. Добре – повне знання навчального матеріалу з кількома незначними помилками. Добре – в загальному правильна відповідь з двома-трьома суттєвими помилками. Задовільно – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією. Задовільно – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
B	4,25-4,74	4	
C	3,75-4,24	4	
D	3,25-3,74	3	
E	3,00-3,24	3	
FX	2,00-2,99	2	Незараховано Незадовільно – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни Незадовільно – необхідна серйозна подальша робота і повторне вивчення дисципліни.
F	0,00-1,99	2	

Питання для підсумкового контролю з дисципліни

1. Основні протоколи передачі даних та автентифікації, які використовуються в «Автоматизованих системах».
2. Основні поняття у сфері функціональної безпеки.
3. Основні засоби забезпечення функціональної безпеки (архітектура, принципи побудови).
4. Принципи проектування систем безпеки об'єктів автоматизації.
5. Класифікація та приклади систем автоматизації, приклади загроз, уразливостей, ризиків.
6. Основні ризики та проблеми функціональної безпеки систем автоматизації.
7. Рівні безпеки SIL.
8. Атрибути надійності, інформаційної та функціональної безпеки.
9. Структурні схеми надійності.
10. Поняття дерева відмови.
11. Аналіз видів, наслідків та критичності відмов (СМЕСА).
12. Як виглядає модель відмов із загальної причини
13. Методи резервування в АСУ ТП
14. Основні принципи резервування
15. Резервування нижнього рівня АСУ ТП.
16. Резервування середнього рівня АСУ ТП.
17. Резервування верхнього рівня АСУ ТП.
18. Резервування промислових мереж
19. Протоколи резервування
20. Оцінка надійності резервованих систем
21. Організація підтримки забезпечення функціональної безпеки в системах SCADA.
22. Дублювання функцій.
23. Розмежування прав доступу в системах функціональної безпеки (оператор, головний оператор, системи автоматичного контролю).
24. Системи реального часу в АСУ ТП.
25. Організація систем реального часу в АСУ ТП.
26. Архітектура систем реального часу
27. Стандарти функціональної безпеки.
28. Життєвий цикл функціональної безпеки.
29. Структура життєвого циклу інформаційної та функціональної безпеки
30. Технічні методи забезпечення функціональної безпеки.
31. Методи захисту від відмов апаратних засобів та систем відповідно до вимог.
32. Методи захисту від програмних відмов, забезпечення відповідно до вимог.
33. Структура вимог щодо інформаційної безпеки
34. Особливості забезпечення інформаційної безпеки комп'ютерних систем керування
35. Технологічний процес та Інтернет речей.
36. Основні визначення системи забезпечення інформаційної безпеки
37. Особливості побудови системи забезпечення інформаційної безпеки для об'єктів критичної інформаційної інфраструктури на промислових об'єктах.
38. Принципи проектування безпечної інфраструктури об'єктів АСУ ТП.
39. Критерії оцінки безпеки, основних загроз, ризиків та проблем, структури та особливостей побудови моделі загроз.
40. Методи та засоби забезпечення безпеки мережної інфраструктури об'єктів АСУ ТП.
41. Приклади інцидентів інформаційної безпеки в АСУ ТП (kill-chain, скомпрометована інфраструктура, наслідки).
42. Методи забезпечення безпеки інформації при аваріях.
43. Захист інформації АСУ ТП від несанкціонованого доступу.
44. Методи безпечного управління змінами у ПЗ та мережному обладнанні об'єктів АСУ ТП.
45. Вразливості існуючих промислових мереж та використовуваних протоколів
46. Можливі сценарії атак, оцінка ризиків для АСУ ТП
47. Класифікація загроз інформаційної безпеки
48. Оцінка вразливості системи
49. Основні способи несанкціонованого доступу
50. Основні напрями та цілі використання криптографічних методів захисту інформації
51. Технічні заходи забезпечення інформаційної безпеки АСУ
52. Організаційні заходи забезпечення інформаційної безпеки АСУ

Рекомендована література

1. Омелянов О. М., Спирін А. В., Твердохліб І. В. Безпека праці та життєдіяльності : навчальний посібник. Вінниця : ВНАУ, 2020. 334 с.
2. Основи надійності та діагностики інформаційних систем : навчальний посібник / В. Вишнівський та ін. Київ : ННІТ ДУТ, 2020. 184 с.
3. Новацький А. О. Мікропроцесорні та мікроконтролерні системи : підручник. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2020. 361 с.
4. Савельєва О. С. Надійність технічних систем : конспект лекцій. Одеса : Од. політехніка, 2021. 109 с.
5. Автоматика протиаварійного управління електроенергетичних систем : підручник / Є. І. Сокол та ін. Харків : ФОРМ Бровін О.В., 2020. 216 с.
6. Основи теорії надійності технічних систем / О. М. Павлюк та ін. Львів : Львів. політехніка, 2021. 208 с.
7. Савенко О.С. Підвищення функціональної безпеки протипожежного контуру автоматизованої системи / О.С. Савенко, Л.О. Корецька, Д.М. Хома // Вимірjувальна та обчислювальна техніка в технологічних процесах. – 2022. –№2. – С. 88-95»
8. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок та ін. Київ : КУБГ, 2019. 218 с.

Інформаційні ресурси

1. Модульне середовище для навчання. Доступ до ресурсу: <https://msn.khmnu.edu.ua/>.
2. Електронна бібліотека університету Доступ до ресурсу : <http://library.khmnu.edu.ua/>
3. Репозитарій ХНУ. Доступ до ресурсу: <https://elar.khmnu.edu.ua/home>

Розробник:



к.т.н., доц. Людмила КОРЕЦЬКА

Погоджено:

Зав. каф. АКІТта Р:



д.т.н., проф. Валерій МАРТИНЮК

Гарант ОП:



д.т.н., проф. Валерій МАРТИНЮК