ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
05.09.2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Функціональна та кібербезпека систем автоматизації

Назва

Галузь знань 17 – Електроніка, автоматизація та електронні комунікації
Спеціальність 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка (магістратура)
Освітня програма Автоматизація, комп'ютерно-інтегровані технології та робототехніка (освітньо-професійна)
Статус дисципліни обов'язкова, дисципліна професійної підготовки
Факультет Інформаційних технологій
Кафедра Автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

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

Робоча програма складена на основі освітньо-професійної програми підготовки магістрів «Автоматизація та комп'ютерно-інтегровані технології»

Програма складена _____ Людмила КОРЕЦЬКА
Підпис Ім'я, прізвище викладача(ів)

Схвалена на засіданні кафедри Автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

Протокол № 1 від 30 серпня 2024 р.

Зав. кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки _____ Валерій МАРТИНЮК

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, прізвище

Хмельницький 2024

ВСТУП

Мета викладання дисципліни. Дисципліна "Функціональна та кібербезпека систем автоматизації" є однією зі спеціальних професійних дисциплін і займає провідне місце у підготовці магістрів автоматизації та комп'ютерно-інтегрованих систем.

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

Предмет дисципліни. Методи та підходи до забезпечення необхідного рівня функціональної та кібербезпеки 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 та кібербезпеки систем автоматизації.

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:

ІК. 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.

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

ФК12. Здатність застосовувати новітні комп'ютерно-інтегровані технології для забезпечення функціональної та кібербезпеки систем автоматизації.

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 застосовуванням 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.

ПРН16. Розробляти і використовувати пристрої функціональної безпеки на основі програмованих і мережевих системи безпеки.

ФУНКЦІОНАЛЬНА ТА КІБЕРБЕЗПЕКА СИСТЕМ АВТОМАТИЗАЦІЇ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	2
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Денна

Результати навчання. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів (2), застосовувати сучасні підходи і методи моделювання та оптимізації для дослідження та створення ефективних систем автоматизації складними технологічними та організаційно-технічними об'єктами (4), розробляти комп'ютерно-інтегровані системи управління складними технологічними та організаційно-технічними об'єктами, застосовуючи системний підхід із врахуванням нетехнічних складових оцінки об'єктів автоматизації (5), розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційно-технічними об'єктами, розробляти програмно-технічні керуючі комплекси із застосовуванням мережевих та інформаційних технологій, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв, засобів людино-машинного інтерфейсу та з урахуванням технологічних умов та вимог до управління виробництвом (9), розробляти і використовувати спеціалізоване програмне забезпечення та цифрові технології для створення систем автоматизації складними організаційно-технічними об'єктами, професійно володіти спеціальними програмними засобами (10), збирати необхідну інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела, аналізувати і оцінювати її (12), розробляти і використовувати пристрої функціональної безпеки на основі програмованих і мережевих системи безпеки (16).

Зміст навчальної дисципліни. Функціональна безпека: основні поняття та визначення. Аспекти, складові функціональної безпеки АСУТП та «Інтернет-речей» у промисловості. Показники функціональної безпеки Вимоги до функціональної безпеки. Методи забезпечення та життєвий цикл функціональної безпеки. Стандарти функціональної безпеки. Резервування у автоматизованих системах управління. Відповідність вимогам функціональної безпеки за допомогою методології Assurance Case для забезпечення вимогам функціональної безпеки. Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ

Запланована навчальна діяльність: лекції – 18 год., лабораторні заняття – 36 год., самостійна робота – 96 год.; разом – 150 год.
Методи навчання: словесні, наочні, проблемно-пошукові (лекції); пояснювально-ілюстративні, практичні, проблемно-пошукові, частково-пошукові (лабораторні заняття, самостійна робота: індивідуальні завдання), дослідницькі.
Форми і методи оцінювання результатів навчання: захист лабораторних робіт, усне опитування, тестування, підсумковий контрольний захід.
Вид семестрового контролю: іспит.
Навчальні ресурси:
1. Омельянов О. М., Спірін 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 : ННІІТ 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. Савєльєва 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 : ФОП 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 // Вимірювальна 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.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/
6. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: к.т.н., доцент Корецька Людмила Олександрівна

1. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:		
	Денна форма		
	Лекції	Лабораторні роботи	СРС
Тема 1. Функціональна безпека: основні поняття та визначення	2	4	11
Тема 2. Аспекти, складові функціональної безпеки АСУТП та «Інтернет-речей» у промисловості. Показники функціональної безпеки. Вимоги до функціональної безпеки	4		22
Тема 3. Методи забезпечення та життєвий цикл функціональної безпеки. Стандарти функціональної безпеки	2		11
Тема 4. Резервування у автоматизованих системах управління	2	24	11
Тема 5. Відповідність вимогам функціональної безпеки за допомогою методології Assurance Case для забезпечення вимогам функціональної безпеки	2		11
Тема 6. Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ	4	8	22
Підсумкове заняття.	2		8
Разом за семестр:	**18**	**36**	**96**

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Функціональна безпека: основні поняття та визначення		
1	**Функціональна безпека: основні поняття та визначення** Функціональна безпека: основні стандарти, поняття та визначення. Атрибути надійності, інформаційної та функціональної безпеки. Аналіз ризиків. Структурні схеми надійності. Аналіз дерев відмов. Марківські моделі. Аналіз видів, наслідків та критичності відмов (ЄМЕСА). Модель відмов із загальної причини	2
Тема 2. Аспекти, складові Функціональної безпеки АСУТП та «Інтернет-речей» у промисловості. Показники функціональної безпеки Вимоги до функціональної безпеки		
2	**Функціональна безпека та «Інтернет-речей» у промисловості** Автоматизовані системи та «Інтернет-речей» у промисловості: поняття «Промисловий Інтернет-речей», співвідношення з поняттям «кіберфізична система», класифікація продуктів «Інтернет-речей», співвідношення з поняттями АСУТП, ICS; загрози, уразливості, ризики. Показники функціональної безпеки, надійність автоматизованої системи управління. Вимоги до функціональної безпеки.	2
3	**Вимоги до інформаційної безпеки** Відмінності комп'ютерних систем керування та інших інформаційних систем. Стандарти у сфері інформаційної безпеки комп'ютерних систем управління. Структура вимог щодо інформаційної безпеки. Система менеджменту інформаційної безпеки. Особливості забезпечення інформаційної безпеки комп'ютерних систем керування	2
Тема 3. Методи забезпечення та життєвий цикл функціональної безпеки. Стандарти функціональної безпеки		
4	**Методи забезпечення функціональної безпеки.** Стандарти функціональної безпеки. Життєвий цикл функціональної безпеки. Структура життєвого циклу інформаційної та функціональної безпеки Технічні методи забезпечення функціональної безпеки. Методи захисту від відмов апаратних засобів та систем відповідно до вимог. Методи захисту від програмних відмов, забезпечення відповідно до вимог**.**	2
Тема 4. Резервування у автоматизованих системах управління		
5	**Резервування у автоматизованих системах управління** Класифікація методів резервування. Основні принципи резервування. Характеристики видів резервування. Функціональне, часове та інформаційне резервування у системах автоматизації. Методи підвищення ефективності резервування. Відновлювані і невідоновлювані системи автоматизації та оцінка їх надійності таких систем Резервування нижнього, середнього та верхнього рівнів. Резервування промислових мереж. Резервування бездротових мереж. Протоколи резервування. Оцінка надійності резервованих систем.	2
Тема 5. Відповідність вимогам функціональної безпеки за допомогою методології Assurance Case для забезпечення вимогам функціональної безпеки		
6	**Відповідність вимогам інформаційної та функціональної безпеки за допомогою методології Assurance Case.** Основи методології Assurance Case. Нотація «Мета, аргумент та підтвердження». Нотація структурованих цілей. Інструментальні засоби та база знань Assurance Case. Критика невдалих застосувань Assurance Case	2

	та шляхи покращення оцінювання безпеки.	
Тема 6. Комплексні системи захисту інформації та кібербезпека в системі забезпечення функціональної безпеки АСУ		
7	**Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ** Дублювання функцій. Організація підтримки забезпечення функціональної безпеки в системах SCADA. Розмежування прав доступу в системах функціональної безпеки (оператор, головний оператор, системи автоматичного контролю). Системи реального часу в АСУ ТП. Організація систем реального часу в АСУ ТП. Архітектура систем реального часу	2
8	**Кібербезпека в АСУ ТП** Кібербезпека та інформаційна безпека промислових систем управління. Класифікація видів кібератак на промислові та IoT системи. Зв'язок інформаційної та кібербезпеки АСУ ТП. Засоби та методи зменшення ризиків у системах АСУ ТП. Вразливості існуючих промислових мереж та використовуваних протоколів, можливі сценарії атак, оцінка ризиків для АСУ ТП	2
9	**Підсумкове заняття**	2
	Разом за семестр:	**18**

2.2 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кількість годин
1	Лабораторна робота №1. Оцінка потенційної небезпеки виробничих процесів	4
2	Лабораторна робота №2. Резервування у системах автоматизації: модулі введення, давачі	4
3	Лабораторна робота №3. Резервування у системах автоматизації: модулі виведення	4
4	Лабораторна робота №4. Резервування у системах автоматизації: процесорні модулі	4
5	Лабораторна робота №5. Резервування у системах автоматизації: джерела живлення	4
6	Лабораторна робота №7. Оцінка надійності систем автоматизації із резервуванням	8
7	Лабораторна робота №7. Визначення ризиків кібербезпеки на основі теорії нечітких множин	4
8	Лабораторна робота №8. Розробка кіберзахищеної автоматизованої системи	4
	Разом за семестр	**36**

2.3 Зміст самостійної (індивідуальної) роботи

Самостійна робота студентів денної форми навчання полягає у систематичному опрацюванні програмного матеріалу, підготовці до виконання і захисту лабораторних робіт, тестування з теоретичного матеріалу, тощо.

Номер тижня	Вид самостійної роботи	К-ть годин
1-2	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	11
3-4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1. Підготовка до лабораторної роботи №2.	11
5-6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2. Підготовка до лабораторної роботи №3.	11
7-8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Підготовка до лабораторної роботи №4.	11
9-10	Підготовка до тестування за темами 1-4. Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4. Підготовка до лабораторної роботи №5.	11
11-12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Підготовка до лабораторної роботи №6.	11
13-14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Підготовка до лабораторної роботи №7.	11
15-16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Підготовка до лабораторної роботи №8.	11
17-18	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8. Підготовка до підсумкового контрольного заходу.	8
	Разом за семестр:	**96**

3. МЕТОДИ НАВЧАННЯ

Лекції проводяться, в основному, з використанням словесних, наочних, проблемно-пошукових методів; лабораторні заняття проводяться пояснювально-ілюстративними методами, практичними, проблемно-пошуковими та частково-пошуковими методами; самостійна робота передбачає виконання індивідуальних завдань із залученням практичних, дослідницьких, частково-пошукових методів.

4. ФОРМИ І МЕТОДИ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Поточний контроль здійснюється під час лекційних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни. Семестровий контроль проводиться у формі іспиту (підсумкового контрольного заходу). При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

Перед вивченням дисципліни, як правило, проводиться вхідний контроль знань з дисциплін, що їй передують і забезпечують. При цьому необхідно встановити рівні та критерії сформованості знань щодо змісту навчальних елементів. Такими рівнями є:

Ознайомчо-орієнтовний (ОО) – особа має орієнтовне уявлення щодо понять, які вивчаються, здатна: програмувати основні елементи програмних систем різними мовами програмування, обирати сучасні методології та технології проєктування програмного забезпечення, обґрунтовано використовувати сучасні середовища розроблення програмного забезпечення для розроблення програмних систем.

Понятійно-аналітичний (ПА) – особа має чітке уявлення щодо навчального об'єкту, здатна перенести раніше засвоєнні знання на типові ситуації.

Продуктивно-синтетичний (ПС) – особа має глибоке розуміння щодо навчального об'єкту, здатна здійснювати синтез, генерувати нові ідеї та уявлення, переносити раніше засвоєні знання на нетипові, нестандартні ситуації.

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. Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

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.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку „відмінно”, за шкалою ECTS – A, отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв’язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із проєктування та програмної реалізації програмних систем. Оцінка "відмінно" виставляється студенту, який глибоко засвоїв основні принципи проєктування програмних систем та вміє їх раціонально застосувати, знає методики та вміє ними користуватися при розробленні програмного забезпечення. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

Оцінку „добре”, за шкалою ECTS – B, отримує студент за повне засвоєння навчального матеріалу, володіння понятійним апаратом, орієнтування у вивченому матеріалі, свідоме використання знань для вирішення практичних завдань, грамотний виклад відповіді, але у змісті і формі відповіді мали місце окремі неточності (похибки), нечіткі формулювання закономірностей тощо. Відповідь студента повинна будуватись на основі самостійного мислення.

Оцінку „добре”, за шкалою ECTS – C, отримує студент за правильну відповідь з однією-двома суттєвими помилками.

Оцінки "задовільно", за шкалою ECTS – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок у проєктуванні та реалізації програмних систем, але припустився неточностей. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки "задовільно", за шкалою ECTS – E, заслуговує студент за неповне опанування програмного матеріалу, але отримані знання і набуті практичні навички із проєктування та розроблення програмного забезпечення.

Оцінка „незадовільно”, за шкалою ECTS – FX, виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань.

Як правило, оцінка "незадовільно", за шкалою ECTS – F, виставляється студенту, який не може продовжити навчання без додаткових знань з курсу.

На основі результатів поточного контролю і підсумкового контрольного заходу виставляється підсумкова семестрова оцінка. На основі аналізу контролю знань викладач удосконалює

курс лекцій, звертаючи особливу увагу на ті розділи, чи теми, з яких було найбільше неточних відповідей, що свідчить про методичні чи інші недоліки при висвітленні вказаних тем або розділів.

Аналогічно вносяться корективи в методичні посібники для лабораторних робіт, детальніше розглядаються принципові питання при виконанні лабораторних робіт та їх захисті.

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

Аудиторна робота	Самостійна, індивідуальна робота	Семестровий контроль (іспит)
І семестр		
Лабораторні роботи №:	Контроль:	Підсумковий контрольний захід
1-8	ТК Т 1-8	
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.

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

Тестування проводиться з використанням модульного середовища для навчання MOODLE. Правильні відповіді студент реєструє в он-лайн режимі в модульному середовищі MOODLE. Викладач виставляє результати тестування згідно журналу оцінок модульного середовища MOODLE.

Підсумкова семестрова оцінка за національною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення усіх оцінок до електронного журналу. Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС наведені у наступній таблиці.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

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

5. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

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 (ЄМЕСА).
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. Основні ризики та проблеми кібербезпеки в промисловому Інтернеті речей.
36. Основні поняття в галузі кібербезпеки АСУ ТП та Інтернету речей.
37. Основні загрози, ризики та вразливості у сфері кібербезпеки АСУ ТП та критичної інформаційної інфраструктури.
38. Технологічний процес та Інтернет речей.
39. Основні визначення системи забезпечення інформаційної безпеки та особливості побудови системи забезпечення інформаційної безпеки для об'єктів критичної інформаційної інфраструктури на промислових об'єктах.
40. Основні засоби забезпечення кібербезпеки (архітектура, принципи побудови).
41. Принципи проектування безпечної інфраструктури об'єктів АСУ ТП.
42. Основні ризики та проблеми кібербезпеки АСУ ТП.
43. Критерії оцінки безпеки, основних загроз, ризиків та проблем, структури та

особливостей побудови моделі загроз.

44. Методи та засоби забезпечення безпеки мережної інфраструктури об'єктів АСУ ТП.

45. Приклади інцидентів інформаційної безпеки в АСУ ТП (kill-chain, скомпрометована інфраструктура, наслідки).

46. Методи забезпечення безпеки інформації при аваріях.

47. Захист інформації АСУ ТП від несанкціонованого доступу.

48. Методи безпечного управління змінами у ПЗ та мережному обладнанні об'єктів АСУ ТП.

49. Різниця між кібератакою та кіберфізичною атакою.

50. Протоколи зв'язку та автентифікації для кіберфізичних систем та «Інтернет-речей»

51. Класифікація видів кібератак на промислові та IoT системи

52. Вразливості існуючих промислових мереж та використовуваних протоколів

53. Можливі сценарії атак, оцінка ризиків для АСУ ТП

6. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Функціональна та кібербезпека систем автоматизації» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Омельянов О. М., Спірін 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 : ННІІТ 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. Савєльєва 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 : ФОП 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 // Вимірювальна 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.

9. Васильківський І. С., Федінець В. О., Юсик Я. П. Виконавчі пристрої систем автоматизації. Львів: Львівська політехніка, 2020. 220 с.

Додаткова

10. ДСТУ EN 61508-1:2019. Функціональна безпека електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT). Чинний від 2019-09-01. Вид. офіц. Київ, 2019.

11. EN 61508-2:2019 Функціональна безпека електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 2. Вимоги до електричних, електронних, програмованих електронних систем, пов'язаних з безпекою (EN 61508-2:2010, IDT; IEC 61508-2:2010, IDT).

12. ДСТУ EN 61508-3:2019 Функціональна безпека електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 3. Вимоги до програмного

забезпечення (EN 61508-3:2010, IDT; IEC 61508-3:2010, IDT).

13. ДСТУ EN 61508-4:2019 Функціональна безпека електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 4. Визначення та скорочення (EN 61508-4:2010, IDT; IEC 61508-4:2010, IDT).

14. ДСТУ EN 61508-5:2019 Функціональна безпека електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 5. Приклади методів для визначення рівнів повноти безпеки (EN 61508-5:2010, IDT; IEC 61508-5:2010, IDT).

15. ДСТУ EN 61511-1:2022 Функціональна безпека. Системи приладів безпеки для сектору переробної промисловості. Частина 10. Структура, визначення, вимоги до системного, апаратного та прикладного програмування (EN 61511-1:2017/A1:2017, IDT; IEC 61511-1:2016/A1:2017, IDT). Зміна № 1:2022.

8. ІНФОРМАЦІЙНІ РЕСУРСИ

Електронний університет:

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі тестові завдання для поточного та семестрового контролю знань).
2. Електронна бібліотека університету