ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Ім'я, ПРІЗВИЩЕ

09 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Функціональна та кібербезпека систем автоматизації
Назва дисципліни

Галузь знань – G Інженерія, виробництво та будівництво
Спеціальність – G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Рівень вищої освіти –Другий (магістерський)
Освітньо-професійна програма – Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Обсяг дисципліни – 5 кредитів ЄКТС, ***Шифр дисципліни*** – ОФП.05
Мова навчання – українська
Статус дисципліни: обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	1	2	5	150	50	16	34			100				+
Разом ДФН			**5**	**150**	**50**	**16**	**34**			**100**				**1**

Робоча програма складена на основі освітньо-професійної програми «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» за спеціальністю G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»

Робоча програма складена _____ канд. техн. наук, доцент Людмила КОРЕЦЬКА
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

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

Протокол від 01.09.2025 №1 Зав. кафедри _____ Людмила КОРЕЦЬКА
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Автоматизації, комп'ютерно-інтегрованих технологій та робототехніки		Людмила КОРЕЦЬКА
Гарант освітньо-професійної програми, д-р. техн. наук, проф.	Автоматизації, комп'ютерно-інтегрованих технологій та робототехніки		Валерій МАРТИНЮК

3. Пояснювальна записка

Дисципліна «Функціональна та кібербезпека систем автоматизації» є однією із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів другого (магістерського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка» в межах спеціальності G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка».

Пререквізити – теорія, моделювання і оптимізація інтелектуальних і складних систем керування (ОФП.01), проєктування та моделювання робототехнічних систем (ОФП.02).

Постреквізити – переддипломна практика (ОФП.06), кваліфікаційна робота (ОФП.07).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** здатність розв'язувати складні задачі і проблеми автоматизації, комп'ютерно-інтегрованих технологій та робототехніки 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 (ІК); здатність працювати в міжнародному контексті (ЗК.04); 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 (ФК.02); здатність застосовувати методи моделювання та оптимізації для дослідження та підвищення ефективності систем і процесів керування складними технологічними та організаційно-технічними об'єктами (ФК.03); здатність аналізувати виробничо-технологічні системи і комплекси як об'єкти автоматизації, визначати способи та стратегії їх автоматизації та цифрової трансформації (ФК.04); 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 (ФК.08); здатність застосовувати новітні комп'ютерно-інтегровані технології для забезпечення функціональної та кібербезпеки систем автоматизації (УК.03).

***програмних результатів навчання*:** створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів (ПРН02); застосовувати сучасні підходи і методи моделювання та оптимізації для дослідження та створення ефективних систем автоматизації складними технологічними та організаційно-технічними об'єктами (ПРН04); розробляти комп'ютерно-інтегровані системи управління складними технологічними та організаційно-технічними об'єктами, застосовуючи системний підхід із врахуванням нетехнічних складових оцінки об'єктів автоматизації (ПРН05); 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 (ПРН09); розробляти і використовувати спеціалізоване програмне забезпечення та цифрові технології для створення систем автоматизації складними організаційно-технічними об'єктами, професійно володіти спеціальними програмними засобами (ПРН10); збирати необхідну інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела, аналізувати і оцінювати її (ПРН12); розробляти і використовувати пристрої функціональної безпеки на основі програмованих і мережевих систем безпеки (ПРН15).

Мета дисципліни. Метою дисципліни "Функціональна та кібербезпека систем автоматизації" є: 1) формування компетентностей, необхідних для розроблення надійних систем автоматизації; 2) ознайомлення студентів із основними напрямками по забезпеченню функціональної та кібербезпеки систем автоматизації; 3) ознайомлення 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 функціонування автоматизованих систем; підготувати студентів до ініціювання та автономного провадження дослідницької та інноваційної діяльності в галузі функціональної та кібербезпеки систем автоматизації.

Результати навчання. Після вивчення дисципліни студент повинен: Пояснювати принципи функціональної та кібербезпеки систем автоматизації та їх значення для надійності виробничих процесів; ідентифікувати загрози та вразливості у програмно-технічних комплексах і визначати заходи їх усунення; застосовувати методи аналізу надійності, ризиків та відмов для оцінювання рівня функціональної безпеки; проєктувати архітектуру безпечних систем автоматизації, враховуючи вимоги стандартів і нормативних документів (IEC 61508, IEC 62443 тощо); розробляти та впроваджувати заходи кіберзахисту в комп'ютерно-інтегрованих системах управління; моделювати процеси забезпечення безпеки з використанням сучасних програмних засобів та технологій; проводити тестування і валідацію систем безпеки, оцінювати ефективність реалізованих рішень; готувати аналітичні висновки та рекомендації щодо підвищення рівня функціональної та кібербезпеки систем автоматизації.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	лекції	**лабораторні заняття**	**СРС**
Тема 1. Функціональна безпека: основні поняття та визначення	2	4	12
Тема 2. Аспекти, складові функціональної безпеки АСУТП та «Інтернет-речей» у промисловості	4		24
Тема 3. Методи забезпечення та життєвий цикл функціональної безпеки. Стандарти функціональної безпеки	2		12
Тема 4. Резервування у автоматизованих системах управління	2	20	16
Тема 5. Відповідність вимогам функціональної безпеки за допомогою методології Assurance Case для забезпечення вимогам функціональної безпеки	2		12
Тема 6. Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ	4	10	24
Разом:	**16**	**34**	**100**

5. Програма навчальної дисципліни

5.1 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 та шляхи покращення оцінювання безпеки.	2
	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
	Разом за семестр:	**16**

5.2 Зміст лабораторних занять

№ п/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	4
7	Лабораторна робота №7. Визначення ризиків кібербезпеки на основі теорії нечітких множин	4
8	Лабораторна робота №8. Розробка кіберзахищеної автоматизованої системи	4
9	Узагальнююче заняття	2
	Разом:	**34**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до підготовці до виконання і захисту лабораторних робіт, контрольних робіт. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	**6**
2	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1.	**6**
3	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №2.	6
4	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2.	6
5	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №3.	6
6	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №4.	6
8	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4.	6
9	Підготовка до контрольної роботи за темами 1-4. Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №5.	10
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5.	6
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №6.	6
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6.	6
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №7.	6
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7.	6
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №8.	6
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8.	6
	Разом:	**100**

На самостійне опрацювання студентів виносяться визначені у методичних рекомендаціях лабораторних занять питання з кожної теми з відповідних тем. Керівництво самостійною роботою та контроль за виконанням індивідуального завдання здійснюється викладачем згідно з розкладом консультацій у позаурочний час.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); лабораторні заняття: з використанням методів комп'ютерного моделювання, методів проєктної діяльності, тренінгових вправ, аналіз проблемних ситуацій, пояснення, дискусія; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабраторних робіт, поточного та підсумкового контролю), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– усне опитування перед допуском до лабораторного заняття;
– оцінювання результатів захисту лабораторних робіт;
– оцінювання контрольних робіт (практичних завдань за темами).

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття

(наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, якісно підготувати звіт, захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами контрольної роботи.

Здобувач вищої освіти, виконуючи самостійну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах, які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Незадовільно (недостатній)	Здобувач вищої освіти виявив 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» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**	
Лабораторні роботи №:								Контрольна робота:	Іспит	Разом балів
1	2	3	4	5	6	7	8	КР1		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100***
24-40								**12-20**	**24-40**	

Примітки: *За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; повнота відповіді та знання методики проєктування систем автоматизації із підвищеною функціональною та кібербезпекою, розрахунку надійнойсті таких систем.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання контрольної роботи

Контрольна робота передбачає відповідь на 2 теоретичних питання та виконання одного практичного завдання. При оцінюванні контрольної роботи враховуються: повнота відповіді та якість виконання. Кожне питання оцінюється 6 балами, практичне завдання оцінюється – 8 балами, загальна сума балів на позитивну оцінку становить від 12 до 20.

Розподіл балів при оцінюванні завдань контрольної роботи

Кількість правильних відповідей	1	2	3
Відсоток правильних відповідей	**30**	**60**	**100**
Кількість отриманих балів	0	12	20

При отриманні негативної оцінки контрольну роботу слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	4	5	6
Теоретичне питання № 2	4	5	6
Практичне завдання (2 задачі)	16	22	28
Разом:	**24**		**40**

***Примітка.** *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.*

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

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 киберфізичних 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

11. Навчально-методичне забезпечення

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

1. Корецька Л.О. Функціональна та кібербезпека систем автоматизації. Лабораторний практикум : Методичні рекомендації для здобувачів другого (магістерського) рівня вищої освіти спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка». Хмельницький : ХНУ, 2024. 68 с.

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп’ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, програма Siemens Logo! Soft Comfort, доступ до мережі Інтернет, робота з презентаціями.

13. 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

1. 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.
2. 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).
3. 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).

4. 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).

5. 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).

6. 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.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=7973
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

ФУНКЦІОНАЛЬНА ТА КІБЕРБЕЗПЕКА СИСТЕМ АВТОМАТИЗАЦІЇ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість призначених кредитів ЄКТС	5,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: Після вивчення дисципліни студент повинен: Пояснювати принципи функціональної та кібербезпеки систем автоматизації та їх значення для надійності виробничих процесів; ідентифікувати загрози та вразливості у програмно-технічних комплексах і визначати заходи їх усунення; застосовувати методи аналізу надійності, ризиків та відмов для оцінювання рівня функціональної безпеки; проєктувати архітектуру безпечних систем автоматизації, враховуючи вимоги стандартів і нормативних документів (IEC 61508, IEC 62443 тощо); розробляти та впроваджувати заходи кіберзахисту в комп'ютерно-інтегрованих системах управління; моделювати процеси забезпечення безпеки з використанням сучасних програмних засобів та технологій; проводити тестування і валідацію систем безпеки, оцінювати ефективність реалізованих рішень; готувати аналітичні висновки та рекомендації щодо підвищення рівня функціональної та кібербезпеки систем автоматизації.

Зміст навчальної дисципліни. Функціональна безпека: основні поняття та визначення; аспекти, складові функціональної безпеки АСУТП та «Інтернет-речей» у промисловості; 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

Пререквізити: теорія, моделювання і оптимізація інтелектуальних і складних систем керування (ОФП.01), проєктування та моделювання робототехнічних систем (ОФП.02).

Постреквізити – переддипломна практика (ОФП.06), кваліфікаційна робота (ОФП.07).

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС

Форми (методи) навчання: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); лабораторні заняття: з використанням методів комп'ютерного моделювання, методів проєктної діяльності, тренінгових вправ, аналіз проблемних ситуацій, пояснення, дискусія; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабраторних робіт, поточного та підсумкового контролю), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання захисту лабораторних робіт; контрольної роботи

Вид семестрового контролю: іспит –2 семестр

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. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=7973
8. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/

Викладачі: канд. техн. наук, доцент Корецька Л.О.