Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра автоматизації, метрології та енергоефективних технологій

«**ЗАТВЕРДЖУЮ**»
Директор навчально-наукового інституту «Українська інженерно-педагогічна академія»

Денис КОВАЛЕНКО

«__» липня 2026 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Надійність та кібербезпека систем керування

(назва навчальної дисципліни)

рівень вищої освіти другий (магістерський)

галузь знань G Інженерія, виробництво та будівництво
(шифр і назва)

спеціальність G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(шифр і назва)

освітня програма Автоматизація та комп`ютерно-інтегровані технології
(шифр і назва)

спеціалізація
(шифр і назва)

вид навчальної дисципліни Обов`язкова
(обов`язкова / за вибором)

інститут Навчально-науковий інститут «Українська інженерно-педагогічна академія»

2026 / 2027 навчальний рік

Програму рекомендовано до затвердження вченою радою навчально-наукового інституту «Українська інженерно-педагогічна академія»

«_29_» ___червня____ 2026 року, протокол №_8_

РОЗРОБНИКИ ПРОГРАМИ: Близниченко Олена Миколаївна, кандидат технічних наук, доцент кафедри АМЕТ

Програму схвалено на засіданні кафедри
Автоматизації, метрології та енергоефективних технологій

Протокол від «_17_» __червня___2026 року № _15_

Завідувач кафедри __Автоматизації, метрології та енергоефективних технологій

(підпис) Геннадій КАНЮК
(прізвище та ініціали)

Програму погоджено з гарантом освітньо-професійної програми
(керівником проектної групи)
Автоматизація та комп'ютерно-інтегровані технології
(назва освітньої програми)

Гарант освітньо-професійної програми
(керівник проектної групи)

(підпис) Геннадій КАНЮК
(прізвище та ініціали)

Програму погоджено науково-методичною комісією
Навчально наукового інституту «Українська інженерно-педагогічна академія»
(назва факультету, для здобувачів вищої освіти якого викладається навчальна дисципліна)

Протокол від «__29__» __червня___2026 року № __8__

Голова науково-методичної комісії Навчально наукового інституту «Українська інженерно-педагогічна академія»

(підпис) Сергій ПЕТРОВ
(прізвище та ініціали)

ВСТУП

Програма навчальної дисципліни «Надійність та кібербезпека систем керування» розроблена відповідно до освітньо-професійної програми підготовки «Автоматизація та комп'ютерно-інтегровані технології»

другий (магістерський)
(назва рівня вищої освіти)

спеціальності G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка

спеціалізації _____

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є формування у здобувачів другого (магістерського) рівня вищої освіти системного розуміння та практичних умінь щодо аналізу, моделювання, проєктування, забезпечення і верифікації надійності, відмовостійкості, функціональної та інформаційної безпеки автоматизованих і кіберфізичних систем керування енергетичних та загальнопромислових об'єктів із застосуванням сучасних математичних методів, теорії надійності, системного аналізу, цифрових технологій та актуальних міжнародних підходів до кіберзахисту промислових систем.

1.2. Основні завдання вивчення дисципліни.

1. **Ознайомлення з основами забезпечення надійності та кібербезпека систем керування:**

- вивчення основних понять і показників надійності, готовності, ремонтопридатності, безвідмовності та відмовостійкості автоматизованих систем керування;
- формування розуміння взаємозв'язку понять *reliability, availability, maintainability, safety, cybersecurity* та *resilience* під час проєктування і експлуатації систем керування;
- вивчення принципів забезпечення функціональної та інформаційної безпеки автоматизованих систем керування технологічними процесами;
- ознайомлення з типовими відмовами, кіберзагрозами та вразливостями SCADA, PLC, DCS, HMI, IIoT і промислових мереж;
- аналіз архітектури промислових мереж, критичних функцій, відмов, вразливих точок та взаємозалежностей, що впливають на надійність і кіберстійкість систем;
- вивчення вимог і підходів міжнародних стандартів та рекомендацій IEC 62443, ISO/IEC 27001, NIST SP 800-82 Rev. 3, NIST Cybersecurity Framework 2.0;
- засвоєння концепцій *defense-in-depth*, *Zero Trust*, сегментації мереж, зон і каналів, керування доступом та моніторингу безпеки.

2. **Опанування методів аналізу надійності, відмов і кіберризиків та проєктування високонадійних і захищених систем керування:**

- вивчення математичних моделей надійності, методів статистичного аналізу відмов і відновлення;
- засвоєння методів побудови структурних схем надійності та марковських моделей;

- формування практичних умінь виконувати аналіз видів і наслідків відмов FMEA/FMECA та аналіз дерев відмов FTA;
- обґрунтування резервування, діагностування, відновлення та інших заходів підвищення відмовостійкості систем керування;
- вивчення методів і алгоритмів оцінювання кіберризиків та визначення рівнів безпеки для компонентів автоматизованих систем керування;
- формування навичок побудови архітектури захищених промислових мереж з урахуванням SCADA, HMI, PLC, IIoT та інших складових АСКТП;
- розроблення технічних рішень щодо сегментації мереж, побудови DMZ, резервування критичних компонентів, керування доступом і забезпечення відновлення;
- формування навичок інтегрованого оцінювання надійності, функціональної безпеки та кіберризиків під час проєктування систем керування.

3. **Моделювання та дослідження процесів надійності і кіберзахисту із застосуванням програмного забезпечення та цифрових технологій:**

- використання MATLAB/Simulink, Python, електронних таблиць та інших програмних засобів для розрахунку показників надійності, моделювання відмов і аналізу відмовостійкості;
- застосування SIEM, IDS/IPS, Wireshark та інших спеціалізованих засобів для аналізу журналів подій, мережевого трафіку, виявлення загроз і аномалій;
- моделювання сценаріїв відмов та кіберінцидентів у промислових мережах;
- аналіз ефективності технічних і програмних засобів захисту, зокрема міжмережевих екранів, VPN, криптографічних механізмів, систем резервного копіювання та моніторингу;
- застосування цифрових технологій для оцінювання надійності, кіберстійкості та ефективності захисних заходів;
- дослідження можливостей використання штучного інтелекту для виявлення аномалій, аналізу даних відмов, журналів подій і підтримки прийняття технічних рішень.

4. **Розвиток практичних навичок проєктування, діагностування, аудиту та забезпечення кіберстійкості систем керування:**

- практичне застосування теоретичних знань під час розроблення фрагментів архітектури високонадійних, відмовостійких і захищених промислових систем;
- виконання розрахунково-аналітичних і проєктних завдань з оцінювання надійності, резервування, діагностування та кіберзахисту;
- розроблення моделей загроз, карт активів, зон і каналів, а також обґрунтування заходів захисту відповідно до IEC 62443;
- розроблення алгоритмів виявлення інцидентів, аналізу журналів подій, локалізації наслідків, реагування та відновлення;
- формування навичок підготовки планів резервування, аварійного відновлення та забезпечення безперервності функціонування систем керування;
- проведення аудиту надійності та інформаційної безпеки, оцінювання відповідності вимогам ISO/IEC 27001, IEC 62443 та внутрішнім політикам підприємства;
- виконання розрахунково-аналітичних і групових проєктних завдань у межах практичної та самостійної роботи з розроблення, впровадження, тестування та оцінювання систем забезпечення надійності й кібербезпеки.

5. **Розвиток критичного мислення, дослідницьких і проєктних компетентностей:**

- стимулювання здобувачів до самостійного аналізу сучасних підходів, методів і технологій забезпечення надійності, відмовостійкості, функціональної та кібербезпеки систем керування;
- формування здатності критично оцінювати ризики, результати моделювання, технічні рішення та наслідки відмов і кіберінцидентів;
- розвиток умінь обґрунтовувати вибір архітектури, методів резервування, діагностування, моніторингу, захисту та відновлення систем;
- розвиток навичок роботи з міжнародними стандартами, нормативними документами, науково-технічною літературою, програмним кодом і спеціалізованими інформаційними ресурсами;
- формування здатності документувати результати досліджень і технічні рішення, дотримуючись норм академічної доброчесності, професійної етики та правових норм щодо інтелектуальної власності;
- розвиток науково-дослідницьких умінь у сфері надійності, функціональної безпеки, кібербезпеки та кіберстійкості автоматизованих і кіберфізичних систем керування.

1.3. Кількість кредитів

4

1.4. Загальна кількість годин

120

1.5. Характеристика навчальної дисципліни	
Обов’язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	1-й
Семестр	
2-й	2-й
Лекції	
22 год.	6 год.
Практичні, семінарські заняття	
10 год.	2 год.
Лабораторні заняття	
0 год.	0 год.
Самостійна робота	
88 год.	112 год.
у тому числі індивідуальні завдання	
0 год.	0 год.

1.6. Перелік компетентностей, що формує дана дисципліна

ЗК1. Здатність проведення досліджень на відповідному рівні.

ЗК2. Здатність генерувати нові ідеї (креативність).

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 проєктні та інженерні рішення.

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

ФК7. Здатність застосовувати спеціалізоване програмне забезпечення та цифрові технології для розв’язання складних задач і проблем автоматизації та комп’ютерно-інтегрованих технологій.

1.7. Перелік результатів навчання, що формує дана дисципліна

ПРН02. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів.

ПРН07. Аналізувати виробничо-технічні системи у енергетичній та загальнопромислових галузях як об’єкти автоматизації і визначати стратегію їх автоматизації та цифрової трансформації.

ПРН08. Застосовувати сучасні математичні методи, методи теорії автоматичного керування, теорії надійності та системного аналізу для дослідження та створення систем автоматизації складними технологічними та організаційно-технічними об’єктами.

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

ПРН11. Дотримуватись норм академічної доброчесності, знати основні правові норми щодо захисту інтелектуальної власності, комерціалізації результатів науково-дослідної, винахідницької та проєктної діяльності.

1.8. Пререквізити

Освітні компоненти першого семестру магістерської підготовки, що передують вивченню дисципліни: «Основи наукових досліджень та авторського права», «Програмування та цифрові технології в автоматизованих системах керування», «Сучасні методи та алгоритми систем автоматичного керування», «Проєктування та технології кіберфізичних виробничих систем», «Моделювання та оптимізація систем керування». Також необхідні базові знання з теорії ймовірностей і математичної статистики, теорії автоматичного керування, програмування, комп’ютерних мереж та архітектури систем автоматизації, сформовані на першому (бакалаврському) рівні вищої освіти.

2. Тематичний план навчальної дисципліни

Розділ 1. Надійність, відмовостійкість та функціональна безпека систем керування

Тема 1. Основні поняття та показники надійності систем керування

Зміст: Надійність як комплексна властивість технічних і програмно-технічних систем. Безвідмовність, довговічність, ремонтопридатність, збережуваність, готовність. Відмова, пошкодження, дефект, критичність. Показники MTTF, MTBF, MTTR, availability. Життєвий цикл і забезпечення надійності автоматизованих систем. Взаємозв’язок dependability, reliability, safety, security і resilience.

Тема 2. Імовірнісно-статистичні моделі відмов і оцінювання показників надійності

Зміст: Інтенсивність відмов, функція надійності, імовірність безвідмовної роботи. Експоненціальний і Вейбуллівський закони розподілу. Аналіз даних про відмови та відновлення. Оцінювання параметрів і довірчих інтервалів. Програмна реалізація розрахунків і візуалізація показників надійності.

Тема 3. Структурні методи та марковські моделі надійності

Зміст: Послідовні, паралельні та комбіновані структури. Reliability Block Diagrams (RBD). Резервування: активне, пасивне, гаряче, тепле, холодне. Загальні відмови та залежності. Марковські моделі станів для оцінювання надійності, готовності та ремонтопридатності. Аналіз варіантів архітектури систем керування.

Тема 4. Аналіз видів, наслідків і критичності відмов. Діагностування та прогнозування

Зміст: FMEA та FMECA відповідно до IEC 60812. Аналіз дерев відмов (FTA). Формування переліку відмов, причин, наслідків і заходів зниження ризику. Діагностичне покриття, виявлення та локалізація несправностей. Предиктивна діагностика на основі даних. Планування технічного обслуговування.

Тема 5. Відмовостійкі архітектури та функціональна безпека автоматизованих систем

Зміст: Принципи fail-safe, fault-tolerant і graceful degradation. Резервування контролерів, каналів зв'язку, живлення, серверів і даних. Безпечний стан, діагностування та відновлення. Основи функціональної безпеки та оцінювання ризику небезпечних відмов. Баланс між продуктивністю, надійністю, безпекою та вартістю.

Розділ 2. Кібербезпека, кіберстійкість та захист промислових систем керування

Тема 6. Загрози та вразливості OT/ICS, SCADA, PLC, DCS, HMI та IIoT

Зміст: Особливості операційних технологій та промислових систем керування. Поверхня атаки, типові вразливості й кіберзагрози. Модель порушника. Атаки на PLC, HMI, SCADA, промислові протоколи й IIoT. Вплив кіберінцидентів на технологічний процес, надійність, безпеку та безперервність виробництва. MITRE ATT&CK for ICS.

Тема 7. Оцінювання кіберризиків та проєктування архітектури захисту за IEC 62443

Зміст: Ідентифікація активів, загроз, вразливостей та наслідків. Оцінювання і оброблення ризику. IEC 62443-3-2: система під розглядом, zones and conduits, цільові рівні безпеки. IEC 62443-3-3: фундаментальні вимоги та системні вимоги. Defense-in-depth. Принципи сегментації та DMZ для промислових мереж.

Тема 8. Технічні та програмні засоби кіберзахисту систем керування

Зміст: Керування ідентифікацією та доступом, мінімальні привілеї, багатофакторна автентифікація з урахуванням обмежень OT. Захист промислових мереж, міжмережеві екрани, VPN, криптографічний захист, TLS і PKI. Безпечне конфігурування, керування оновленнями та вразливостями, резервне копіювання. IDS/IPS, SIEM, журнали подій і моніторинг аномалій.

Тема 9. Виявлення інцидентів, реагування, відновлення та кіберстійкість

Зміст: Життєвий цикл кіберінциденту: підготовка, виявлення, аналіз, локалізація, усунення, відновлення та післяінцидентний аналіз. Плани реагування для OT/ICS. Резервування й відновлення конфігурацій PLC/SCADA, резервні копії та аварійні режими. Безперервність і кіберстійкість. Метрики ефективності захисту, навчальні сценарії та tabletop exercises.

Тема 10. Комплексне проєктування, аудит і нормативно-правова відповідність високонадійних та захищених систем керування

Зміст: Інтеграція вимог до надійності, функціональної та інформаційної безпеки у життєвому циклі системи. Архітектурні компроміси та оцінювання залишкового ризику. Аудит і оцінювання відповідності вимогам ISO/IEC 27001, IEC 62443 та внутрішнім політикам. Документування проєктних рішень, захист інтелектуальної власності, академічна доброчесність під час використання науково-технічних джерел, програмного коду та інструментів ШІ.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Надійність, відмовостійкість та функціональна безпека систем керування												
Тема 1. Основні поняття та показники надійності систем керування	12	2	2	0	0	8	12	2	0	0	0	10
Тема 2. Імовірнісно-статистичні моделі відмов і оцінювання показників надійності	12	2	0	0	0	10	12	0	0	0	0	12
Тема 3. Структурні методи та марковські моделі надійності	12	2	2	0	0	8	12	0	0	0	0	12
Тема 4. Аналіз видів, наслідків і критичності відмов. Діагностування та прогнозування	12	2	2	0	0	8	12	0	0	0	0	12
Тема 5. Відмовостійкі архітектури та функціональна безпека автоматизованих систем	12	2	0	0	0	10	12	0	0	0	0	12
Разом за розділом 1	60	10	6	0	0	44	60	2	0	0	0	58
Розділ 2. Кібербезпека, кіберстійкість та захист промислових систем керування												
Тема 6. Загрози та вразливості OT/ICS, SCADA, PLC, DCS, HMI та IIoT	12	2	0	0	0	10	12	0	0	0	0	12
Тема 7. Оцінювання кіберризиків та проектування архітектури захисту за IEC 62443	12	4	2	0	0	6	12	2	0	0	0	10
Тема 8. Технічні та програмні засоби кіберзахисту систем керування	12	2	0	0	0	10	12	0	0	0	0	12
Тема 9. Виявлення інцидентів, реагування, відновлення та кіберстійкість	12	2	0	0	0	10	12	0	0	0	0	12
Тема 10. Комплексне проектування, аудит і нормативно-правова відповідність високонадійних та захищених систем керування	12	2	2	0	0	8	12	2	2	0	0	8
Разом за розділом 2	60	12	4	0	0	44	60	4	2	0	0	54
Усього годин	120	22	10	0	0	88	120	6	2	0	0	112

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин ДФН	Кількість годин ЗФН
1	**Розрахунок показників надійності та готовності системи керування.** Визначення MTTF, MTBF, MTTR, коефіцієнта готовності, аналіз результатів та оцінювання впливу відмов на функціонування системи. Основні ПРН: ПРН02, ПРН08, ПРН10.	2	0
2	**Структурний аналіз надійності та резервування систем керування.** Побудова RBD, аналіз послідовних, паралельних і комбінованих структур, порівняння активного та пасивного резервування, використання марковських моделей. Основні ПРН: ПРН02, ПРН08, ПРН10.	2	0
3	**Аналіз видів, наслідків і критичності відмов методами FMEA/FMECA та FTA.** Ідентифікація відмов, причин і наслідків, оцінювання критичності, формування заходів з діагностування, резервування та відновлення. Основні ПРН: ПРН02, ПРН07, ПРН08.	2	0
4	**Оцінювання кіберризиків та проєктування архітектури захисту АСКТП відповідно до IEC 62443.** Ідентифікація активів, загроз і вразливостей, формування зон і каналів (*zones and conduits*), визначення заходів сегментації та використання DMZ. Основні ПРН: ПРН02, ПРН07, ПРН10.	2	0
5	**Комплексне проєктування високонадійної та кіберстійкої архітектури системи керування.** Поєднання резервування критичних компонентів, сегментації мережі, моніторингу, реагування на кіберінциденти, резервного копіювання та відновлення. Основні ПРН: ПРН02, ПРН07, ПРН08, ПРН10, ПРН11.	2	2
	Разом	10	2

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин ДФН	Кількість годин ЗФН
1	Опрацювання термінології *dependability, reliability, availability, maintainability, safety, security, resilience*. Аналіз основних показників надійності автоматизованих систем, MTTF, MTBF, MTTR та коефіцієнта готовності.	8	10
2	Статистичний аналіз даних про відмови та відновлення. Побудова функції надійності та функції інтенсивності відмов. Опрацювання експоненціального та Вейбуллівського розподілів, оцінювання параметрів та довірчих інтервалів.	10	12
3	Побудова структурних схем надійності та марковських моделей. Аналіз послідовних, паралельних і комбінованих структур. Порівняння варіантів резервування та показників готовності.	8	12
4	Опрацювання методів FMEA/FMECA та FTA. Формування переліку відмов, причин, наслідків, критичності та заходів	8	12

	зниження ризику. Аналіз методів технічного діагностування та прогнозування відмов.		
5	Аналіз відмовостійких архітектур PLC/SCADA/DCS, загальних причин відмов, принципів *fail-safe*, *fault-tolerant*, *graceful degradation* та функціональної безпеки автоматизованих систем.	10	12
6	Аналіз актуальних загроз і вразливостей OT/ICS, SCADA, PLC, DCS, HMI та IIoT за NIST SP 800-82 Rev. 3 і MITRE ATT&CK for ICS. Формування моделі порушника для обраного об’єкта.	10	12
7	Опрацювання IEC 62443-3-2 та IEC 62443-3-3. Побудова карти активів, визначення зон і каналів, оцінювання кіберризиків, обґрунтування цільових рівнів безпеки та архітектури захисту.	6	10
8	Аналіз технічних і програмних засобів кіберзахисту OT: сегментація, DMZ, IAM, багатофакторна автентифікація, VPN, TLS, PKI, резервне копіювання, IDS/IPS, SIEM.	10	12
9	Аналіз сценарію кіберінциденту в АСКТП. Розроблення заходів виявлення, локалізації, реагування, відновлення та післяінцидентного аналізу. Оцінювання кіберстійкості системи.	10	12
10	Підготовка комплексного технічного обґрунтування високонадійної та захищеної системи керування з використанням міжнародних стандартів. Оформлення джерел, програмного коду та результатів використання ШІ з дотриманням академічної доброчесності й прав інтелектуальної власності.	8	8
	Разом	88	112

Орієнтовні теми аналітичних оглядів у межах самостійної роботи

1. Поняття і класифікація видів та методів несанкціонованого доступу.
2. Визначення і модель зловмисника.
3. Організація захисту інформації в автоматизованих системах.
4. Класифікація способів захисту інформації в комп’ютерних системах.
5. Фізичні методи захисту інформації.
6. Законодавчі методи захисту інформації.
7. Управління доступом в АСКТП.
8. Криптографічні методи захисту інформації в промислових мережах.
9. Види умисних загроз безпеці інформації в АСК.
10. Безпека оптоволоконних каналів в SCADA-системах.
11. Інформаційні витоки через слабкострумові лінії.
12. Приховування інформації криптографічним методом.
13. Стеганографічні методи приховування інформації.
14. Захист SCADA-систем: сучасні підходи.
15. Типи кібератак на PLC та інші компоненти АСКТП.
16. Протоколи безпечного обміну в АСК: аналіз вразливостей.
17. Надійність промислових мереж: оцінка і підвищення.
18. SIEM-системи: функціонал, налаштування, приклади.
19. Виявлення вторгнень у системи управління: IDS/IPS-рішення.
20. Захист PLC-контролерів: апаратні та програмні методи.
21. Кібербезпека енергетичних АСК.

22. Загрози і контрзаходи в IIoT.
23. Оцінка ризиків безпеки на виробництві: методики.
24. IEC 62443: аналіз вимог до кіберзахисту.
25. Порівняння стандартів ISO/IEC 27001 та NIST SP800-82.
26. Захист HMI-панелей в автоматизованих системах.
27. Методика тестування вразливостей у SCADA.
28. Категоризація інцидентів кібербезпеки в АСК.
29. Digital Twin у кіберзахисті.
30. Концепція Zero Trust в промислових мережах.
31. Атаки ransomware на об'єкти автоматизації: профілактика.
32. Анонімність і аудит у кіберфізичних системах.
33. Використання ШІ для виявлення аномалій в АСКТП.
34. Захист інформації в хмарних рішеннях для автоматизації.
35. Безпека бездротових каналів зв'язку у вбудованих системах.
36. Соціальна інженерія як загроза персоналу в АСКТП.
37. MITRE ATT&CK для SCADA: огляд та застосування.
38. Побудова SOC для промислових об'єктів.
39. Етичне хакерство і пентест в системах управління.
40. Юридичні аспекти відповідальності за кіберінциденти.

6. Індивідуальні завдання

Не передбачено навчальним планом

7. Методи навчання

Під час вивчення дисципліни застосовуються студентоцентроване, проблемно-орієнтоване, проєктне та дослідницьке навчання; пояснювально-ілюстративний, проблемний, частково-пошуковий і дослідницький методи; кейс-метод; аналіз реальних і модельних відмов та кіберінцидентів; розрахунково-аналітичні й проєктні завдання; побудова та аналіз структурних схем надійності, FMEA/FMECA, FTA і марковських моделей; моделювання сценаріїв відмов та кіберінцидентів; аналіз і проєктування архітектури OT/ICS відповідно до IEC 62443; робота з міжнародними стандартами та нормативними документами; аналіз журналів подій і мережевого трафіку; командне обговорення та обґрунтування технічних рішень; методи дистанційного навчання в Moodle.

Для розрахунків, моделювання та аналізу можуть застосовуватися MATLAB/Simulink, Python, електронні таблиці, Wireshark та інші доступні спеціалізовані програмні засоби.

8. Методи контролю

Поточний контроль здійснюється шляхом усного та письмового опитування, експрес-опитування, тестування, оцінювання результатів практичних занять, перевірки завдань для самостійної роботи, розрахунково-аналітичних завдань, аналізу кейсів, комп'ютерного моделювання та виконання контрольної роботи, передбаченої навчальним планом.

Під час поточного контролю оцінюються правильність застосування методів аналізу надійності та кібербезпеки, коректність розрахунків і моделей, здатність аналізувати відмови та кіберризики, обґрунтовувати технічні рішення, застосовувати міжнародні стандарти та інтерпретувати отримані результати.

Підсумковий контроль — семестровий екзамен.

9. Схема нарахування балів

для підсумкового семестрового контролю при проведенні семестрового екзамену

Поточний контроль, самостійна робота, індивідуальні завдання												Екзамен	Сума
Змістовий модуль 1					Змістовий модуль 2					Контрольна робота, передбачена навчальним планом	Разом		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	20	60	40	100
4	4	4	4	4	4	4	4	4	4				

Оцінювання результатів опрацювання кожної теми здійснюється за результатами поточного контролю, який залежно від змісту теми та форми навчання може включати усне або письмове опитування, тестування, виконання практичного, розрахунково-аналітичного або самостійного завдання, аналіз кейсу, моделювання та обґрунтування технічного рішення.

Для допуску до складання семестрового екзамену здобувач вищої освіти повинен набрати не менше 20 балів під час поточного контролю та виконати контрольну роботу, передбачену навчальним планом.

Критерії оцінювання навчальних досягнень

За результатами опрацювання кожної теми здобувач може отримати від 0 до 4 балів:

4 бали — здобувач повністю володіє теоретичним матеріалом, правильно застосовує методи аналізу надійності та кібербезпеки, аргументовано обґрунтовує технічні рішення, правильно виконує розрахунки та інтерпретує результати;

3 бали — матеріал засвоєно в цілому правильно, завдання виконано з незначними неточностями, які не впливають на загальний результат;

2 бали — основні положення засвоєно, однак є суттєві неточності у розрахунках, аналізі або обґрунтуванні технічних рішень;

1 бал — знання фрагментарні, завдання виконано частково, здобувач потребує суттєвого коригування результатів;

0 балів — завдання не виконано або виконано на рівні, що не демонструє досягнення відповідних результатів навчання.

Контрольна робота — максимум 20 балів.

Екзамен — максимум 40 балів.

Критерії оцінювання контрольної роботи

Контрольна робота оцінюється максимально у **20 балів**. Під час оцінювання враховуються правильність застосування теоретичних положень, коректність розрахунків і моделей, обґрунтованість технічних рішень, уміння аналізувати отримані результати та формулювати висновки.

Кількість балів	Критерії оцінювання
18–20 балів	Роботу виконано повністю та правильно. Здобувач демонструє системне розуміння питань надійності, відмовостійкості, функціональної та кібербезпеки систем керування; коректно застосовує математичні методи, методи аналізу надійності, FMEA/FMECA, FTA, RBD, підходи оцінювання кіберризиків та положення відповідних стандартів. Розрахунки, моделі й технічні рішення є обґрунтованими, результати правильно інтерпретовані, висновки логічні та аргументовані. Допускаються лише поодинокі несуттєві неточності.
14–17 балів	Роботу виконано переважно правильно. Здобувач володіє основним теоретичним матеріалом, правильно застосовує більшість методів і підходів, але допускає окремі неточності у розрахунках, побудові моделей, використанні термінології або обґрунтуванні технічних рішень. Висновки загалом правильні, однак можуть бути недостатньо повними.
10–13 балів	Основні завдання виконано, здобувач демонструє базове розуміння матеріалу, однак має суттєві прогалини у застосуванні методів аналізу надійності або кібербезпеки. У розрахунках, моделях чи оцінюванні ризиків наявні помилки, частина технічних рішень недостатньо обґрунтована. Висновки частково відповідають отриманим результатам.
1–9 балів	Роботу виконано фрагментарно. Теоретичні знання несистемні, методи та нормативні підходи застосовано некоректно або лише частково. Наявні суттєві помилки у розрахунках, аналізі, моделюванні та інтерпретації результатів. Висновки відсутні або не обґрунтовані.
0 балів	Роботу не виконано, не подано у встановлений термін без поважної причини або подана робота не демонструє досягнення визначених результатів навчання.

Критерії оцінювання семестрового екзамену

Семестровий екзамен оцінюється максимально у **40 балів**. Під час оцінювання враховуються повнота та правильність відповідей, рівень володіння понятійно-термінологічним апаратом, здатність застосовувати методи аналізу надійності та кібербезпеки, обґрунтовувати технічні рішення, аналізувати проблемні ситуації та формулювати професійні висновки.

Кількість балів	Критерії оцінювання
36–40 балів	Здобувач демонструє повні, системні та глибокі знання змісту дисципліни; вільно володіє термінологією; правильно пояснює принципи забезпечення надійності, відмовостійкості, функціональної та кібербезпеки; обґрунтовано застосовує математичні методи, FMEA/FMECA, FTA, RBD, марковські моделі, методи оцінювання кіберризиків та положення IEC 62443, ISO/IEC 27001, NIST. Правильно розв’язує практичні та аналітичні завдання, аргументує прийняті рішення та формулює обґрунтовані висновки.

Кількість балів	Критерії оцінювання
30–35 балів	Здобувач демонструє достатньо повні та системні знання, правильно розкриває основні питання дисципліни та застосовує відповідні методи. Допускає незначні неточності у термінології, розрахунках, інтерпретації стандартів або обґрунтуванні окремих технічних рішень, які не змінюють загальної правильності відповіді.
20–29 балів	Здобувач володіє основними положеннями дисципліни та демонструє досягнення мінімально необхідних результатів навчання, але знання мають недостатньо системний характер. Допускаються суттєві неточності у поясненні методів, виконанні розрахунків, аналізі відмов, оцінюванні кіберризиків або застосуванні нормативних вимог. Практичні завдання виконуються частково, висновки потребують додаткового обґрунтування.
1–19 балів	Знання здобувача є фрагментарними та недостатніми для підтвердження сформованості передбачених результатів навчання. Основні поняття, методи та стандарти відтворюються з істотними помилками; практичні та аналітичні завдання не виконуються або виконуються переважно неправильно; технічні рішення не обґрунтовані.
0 балів	Здобувач не приступив до виконання екзаменаційних завдань або надані відповіді не демонструють знань і вмінь, передбачених результатами навчання дисципліни.

Використання технологій штучного інтелекту

Під час вивчення навчальної дисципліни використання технологій штучного інтелекту (ШІ) здійснюється відповідно до Політики використання технологій штучного інтелекту Харківського національного університету імені В. Н. Каразіна.

У межах дисципліни застосовуються такі моделі використання ШІ.

1. Модель «ШІ заборонено».

Використання технологій штучного інтелекту не допускається під час виконання контрольних заходів, спрямованих на перевірку індивідуальних знань і сформованості компетентностей здобувача освіти, зокрема під час усного опитування, контрольної роботи, семестрового екзамену та інших видів оцінювання, для яких викладачем установлено обмеження щодо використання ШІ.

2. Модель «ШІ як асистент».

Під час підготовки до практичних занять, виконання завдань для самостійної роботи, аналітичних оглядів та інших письмових робіт дозволяється використання технологій ШІ для:

- пошуку та систематизації інформації;
- добору та первинного аналізу наукових джерел;
- пояснення складних понять;
- удосконалення структури тексту;
- перевірки граматики, стилю та оформлення;
- генерації ідей, плану роботи або прикладів.

Фінальний текст роботи, висновки, аналіз, інтерпретація результатів та прийняті технічні рішення повинні бути самостійно підготовлені здобувачем освіти.

3. Модель «ШІ як інструмент».

Під час виконання окремих практичних, проєктних або дослідницьких завдань використання технологій штучного інтелекту може бути складовою навчальної діяльності.

У таких випадках здобувачі освіти можуть використовувати генеративні моделі ШІ для:

- аналізу та підготовки даних;
- генерації, аналізу й оптимізації програмного коду;
- аналізу даних про відмови та кіберінциденти;
- виявлення аномалій;
- порівняння результатів роботи різних моделей ШІ;
- створення візуалізацій і схем;
- аналізу великих масивів даних;
- проведення навчальних і дослідницьких експериментів із застосуванням сучасних інструментів штучного інтелекту.

Усі результати, отримані за допомогою ШІ, підлягають критичному аналізу, перевірці та доопрацюванню здобувачем освіти.

Декларування використання ШІ.

У разі використання технологій штучного інтелекту здобувач освіти зобов'язаний зазначити:

- назву сервісу або моделі ШІ;
- дату використання;
- характер отриманої допомоги (пошук інформації, генерація ідей, аналіз даних, генерація або аналіз програмного коду, редагування тексту, створення візуалізацій тощо).

За вимогою викладача здобувач освіти повинен надати використані запити (*prompts*) або пояснити спосіб використання інструментів ШІ.

Недекларованe використання технологій штучного інтелекту або подання згенерованого ШІ матеріалу як власного результату навчальної діяльності розглядається як порушення принципів академічної доброчесності відповідно до внутрішніх нормативних документів Харківського національного університету імені В. Н. Каразіна.

Неформальна освіта

На 2026/2027 навчальний рік окремі зовнішні курси, результати яких автоматично конвертуються у фіксовану кількість балів з дисципліни, не визначені.

Визнання результатів навчання, здобутих у неформальній та/або інформальній освіті, здійснюється відповідно до чинного Порядку визнання результатів навчання, отриманих у неформальній освіті, у Харківському національному університеті імені В. Н. Каразіна.

До результатів неформальної освіти можуть належати результати проходження онлайн-курсів, участі у тренінгах, семінарах, практикумах, майстер-класах та інших формах навчання, зміст і результати яких відповідають змісту та результатам навчання цієї дисципліни.

Визнання результатів здійснюється за умови:

- документального підтвердження успішного проходження відповідного навчання (сертифікат, свідоцтво або інший документ);
- встановлення відповідності отриманих результатів навчання змісту дисципліни та передбаченим результатам навчання;
- підтвердження здатності здобувача застосовувати отримані знання та вміння під час виконання відповідних навчальних і практичних завдань.

Рішення щодо визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, приймається відповідно до процедури та вимог, установлених чинними нормативними документами Харківського національного університету імені В. Н. Каразіна.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
0-49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Василевський О. М., Ігнатенко О. Г. Нормування показників надійності технічних засобів : навчальний посібник. Вінниця : ВНТУ, 2013. 160 с.

2. Дзюба Л. Ф., Меньшикова О. В., Кусій М. І. Надійність технічних систем і техногенний ризик : навчальний посібник. Львів : ЛДУБЖД, 2018. 145 с.

3. Новицький А. В., Ружило З. В., Банний О. О., Бистрий О. М., Сиволапов В. А. Надійність машин та обладнання. Частина 1. Оцінка та забезпечення надійності машин та обладнання : навчальний посібник. Київ : НУБіП України, 2023. 211 с.

4. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека : навчальний посібник / за заг. ред. Ю. Я. Бобала, І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.

5. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту : навчальний посібник. Львів : Новий Світ-2000, 2020. 678 с.

6. Тарнавський Ю. А. Технології захисту інформації : підручник. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.

7. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки : навчальний посібник. Вінниця : ВНТУ, 2013. 221 с.

Допоміжна література

8. **ISO/IEC 27001:2022.** Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

9. **ISO 31000:2018.** Risk management — Guidelines.

10. **IEC 60812:2018.** Failure modes and effects analysis (FMEA and FMECA).

11. **IEC 61025:2006.** Fault tree analysis (FTA).

12. **IEC 61078:2016.** Reliability block diagrams.

13. **IEC 61165:2006.** Application of Markov techniques.

14. **IEC 61508-1:2010.** Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements.

15. **IEC 62443-2-1:2024.** Security for industrial automation and control systems — Part 2-1: Security program requirements for IACS asset owners.

16. **IEC 62443-3-2:2020.** Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design.

17. **IEC 62443-3-3:2013.** Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels.

18. **IEC 62443-4-2:2019.** Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components.

19. **Stouffer K., Pease M., Tang C. et al.** Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

20. **Pascoe C., Quinn S., Scarfone K.** The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. Gaithersburg, MD: National Institute of Standards and Technology, 2024.

21. **Rose S., Borchert O., Mitchell S., Connelly S.** Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology, 2020.

22. **Cybersecurity and Infrastructure Security Agency.** Cross-Sector Cybersecurity Performance Goals. Version 1.0.1. Washington, DC: CISA, 2023.

23. **MITRE Corporation.** MITRE ATT&CK® for ICS. Knowledge Base of Adversary Tactics and Techniques for Industrial Control Systems.

24. **Локазюк В. М., Савченко Ю. Г.** Надійність, контроль, діагностика і модернізація ПК : навчальний посібник. Київ : Видавничий центр «Академія», 2004. 376 с.**11.**

Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

25. Система дистанційного навчання Харківського національного університету імені В. Н. Каразіна. Moodle Каразінського університету

26. IEC 60812:2018. *Failure modes and effects analysis (FMEA and FMECA).* Офіційна сторінка IEC 60812:2018

27. IEC 61025:2006. *Fault tree analysis (FTA).* Офіційна сторінка IEC 61025:2006

28. IEC 61078:2016. *Reliability block diagrams.* Офіційна сторінка IEC 61078:2016

29. IEC 61165:2006. *Application of Markov techniques.* Офіційна сторінка IEC 61165:2006

30. IEC 61508-1:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements.*Офіційна сторінка IEC 61508-1:2010

31. IEC 62443-3-2:2020. *Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design.*Офіційний ресурс IEC 62443-3-2

32. IEC 62443-3-3:2013. *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels.* Офіційний ресурс IEC 62443-3-3

33. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Офіційна сторінка ISO/IEC 27001:2022

34. NIST. *Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3.* NIST SP 800-82 Rev. 3

35. NIST. *The NIST Cybersecurity Framework (CSF) 2.0.* Ресурс містить сам Framework, Quick Start Guides, профілі, мапінги та відеоматеріали. NIST Cybersecurity Framework 2.0

36. NIST. *Zero Trust Architecture. NIST SP 800-207.* Офіційний ресурс для теми Zero Trust. NIST SP 800-207 Zero Trust Architecture

37. MITRE ATT&CK®. *ICS Matrix.* Офіційна база тактик і технік атак для industrial control systems. MITRE ATT&CK for ICS