Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


_____ Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Надійність та відмовостійкість комп'ютерних систем»
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

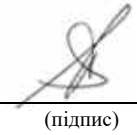
Рівень вищої освіти: ***перший (бакалаврський)***

Силабус введено в дію з 01.09.2025 року

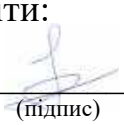
Харків – 2025 р.

Розробник: Клюшніков І. М., доцент, к.т.н., с.н.с. 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)
Протокол № 1 від « 29 » 08 2025 р.

Завідувач кафедри д.т.н., професор  Вячеслав ХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

 Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

Клюшніков Ігор Миколайович
доцент кафедри комп'ютерних систем, мереж і кібербезпеки
кандидат технічних наук, старший науковий співробітник
Викладає дисципліни: «Надійність та функціональна безпека інформаційно-комп'ютерних систем», «Мобільне програмування», «Безпека мобільних систем», «Методи штучного інтелекту для кібербезпеки».
Напрями наукових досліджень: гарантоздатність складних технічних систем, застосування мобільних інтелектуальних систем, сервіс-орієнтовані мобільні системи, штучний інтелект.
Контактна інформація:
e-mail: i.kliushnikov@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	7 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	4,5 кредити ЄКТС / 135 годин (64 аудиторних, з яких: лекції - 32, лабораторні - 32; СРЗ - 71)
Види навчальної діяльності	Лекції та лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	"Дискретна математика", "Основи функціонування комп'ютерів", "Гуманітарна або економічна дисципліна за вибором", "Комп'ютерна схемотехніка"

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – оволодіння методами і навичками оцінювання і забезпечення надійності і функціональної безпеки апаратних і програмних компонентів інформаційно-управляючих систем (ІУС).

Завдання:

вивчити основні поняття і показники надійності, живучості та функціональної безпеки ІУС; вивчити методи і засоби оцінювання надійності та функціональної безпеки апаратних і програмних компонентів ІУС та систем в цілому; вивчити методи і засоби забезпечення надійності та функціональної безпеки ІУС; оволодіти навичками розрахунку показників і розроблення засобів забезпечення виконання вимог до надійності та функціональної безпеки при створенні ІУС.

Компетентності, які набуваються:

а) загальні компетентності:

(КЗ 1) здатність застосовувати знання у практичних ситуаціях.

(КЗ 2) знання та розуміння предметної області та розуміння професії.

(КЗ 3) здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

(КЗ 4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

(КЗ 5) здатність до пошуку, оброблення та аналізу інформації.

б) фахові компетентності:

(КФ 1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

(КФ 2) здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

(КФ 3) здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

(КФ 4) здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

(КФ 6) здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

(КФ 7) здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

(КФ 12) здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

(ПРН 1) застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

(ПРН 3) використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

(ПРН 4) аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

(ПРН 5) адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

(ПРН 7) діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

(ПРН 8) готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

(ПРН 14) вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

(ПРН 19) застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

(ПРН 30) здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

(ПРН 32) здійснювати управління процесами відновлення штатного функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем з використанням процедур резервного копіювання та відновлення даних.

4. Зміст навчальної дисципліни

Змістовний модуль 1. Основні поняття та показники надійності та функціональної безпеки ІКС. Оцінювання надійності.

Тема 1. Загальна характеристика дисципліни. Базові поняття теорії надійності та функціональної безпеки КС.

Предмет, мета вивчення і задачі дисципліни. Структура і зміст дисципліни, а також методичні рекомендації по її вивченню. Місце дисципліни в навчальному процесі. Вимоги до знань і умінь студентів. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Стани (справний, несправний; працездатне, непрацездатний; граничне) і події (несправність, пошкодження, відмова; класифікація відмов, відновлення та

ремонт; схема станів і подій-переходів). Властивості (системний аналіз властивостей; надійність та її складові: безвідмовність, ремонтопридатність, довговічність і збереженість; відмовостійкість і готовність; живучість і безпечність). Системи і елементи в теорії безпечності і надійності (поняття системи і елемента, класифікація та характеристика основних типів систем). Класифікація систем, важливих для безпеки. Стандарти в галузі надійності та функціональної безпеки КС.

Лекція 1 «Вступ. Основні поняття надійності і безпечності».

Самостійна робота: Опрацювання матеріалу лекції. Властивості надійності. Ризики критичних відмов та методи їх визначення.

Тема 2. Показники надійності та функціональної безпеки КС.

Загальна характеристика показників надійності КС (поняття і класифікація). Одиничні показники надійності (показники безвідмовності, загальний закон надійності, експонентний закон; показники ремонтопридатності; загальна характеристика показників довговічності і зберігання). Закони розподілу випадкових величин в надійності. Комплексні показники надійності (коефіцієнти готовності, оперативної готовності та технічного використання). Загальна характеристика показників відмовостійкості (класифікація, спеціальні показники відмовостійкості). Загальна характеристика показників живучості та безпечності (класифікація, спеціальні показники живучості та безпечності).

Лекція 2 «Показники надійності».

Лекція 3 «Показники живучості і безпечності».

Самостійна робота: Опрацювання матеріалу лекцій. Показники надійності (довговічності і збереженості), живучості та безпечності.

Тема 3. Оцінювання надійності невідновлюваних КС.

Класифікація методів забезпечення надійності і безпеки (загальна характеристика методів забезпечення надійності при розробці, виробництві і експлуатації; особливості забезпечення надійності апаратних і програмних засобів). Оцінювання надійності нерезервованих невідновлювальних систем (структурна схема надійності, урахування режимів роботи і умов експлуатації, послідовність розрахунку безвідмовності). Оцінювання надійності невідновлювальних резервованих систем. Методи резервування (основні поняття теорії резервування, класифікація методів резервування; паралельне резервування, мажоритарну резервування, резервування заміщенням). Оцінювання надійності систем з послідовно-паралельним з'єднанням елементів. Надійність мажоритарних систем з одно- і багатоярусної структурою. Особливості оцінювання адаптивних систем. Надійність систем при резервуванні заміщенням (облік режимів роботи резерву; ковзне резервування; порівняльний аналіз безвідмовності резервованих систем).

Лекція 4 «Оцінювання надійності невідновлювальних комп’ютерних систем. Нерезервовані системи».

Лекція 5 «Оцінювання надійності невідновлювальних резервованих комп'ютерних систем. Постійне резервування», Лекція 6 «Оцінювання надійності невідновлювальних резервованих комп'ютерних систем. Мажоритарне резервування»ю

Лекція 7 «Оцінювання надійності невідновлювальних резервованих комп'ютерних систем. Динамічне резервування. Резервування заміщенням».

Лабораторна робота 1 «Дослідження методів постійного резервування і розрахунок надійності невідновлювальних КС», Лабораторне заняття 2 «Дослідження методів динамічного резервування і розрахунок надійності невідновлювальних КС».

Самостійна робота: Інструментальні засоби оцінювання надійності та функційної безпечності КС. Опрацювання матеріалу лекції. Підготовка до захисту лабораторних робіт.

Тема 4. Оцінювання надійності відновлюваних КС.

Оцінювання надійності відновлюваних нерезервованих систем (основні співвідношення для розрахунку безвідмовності, ремонтопридатності і готовності). Оцінювання надійності відновлюваних резервованих систем (особливості відновлюваних резервованих систем, поняття про марковські випадкові процесі в теорії надійності; методика оцінки надійності (аналіз станів, граф переходів, рівняння Колмогорова-Чепмена в диференціальному і алгебраїчному вигляді і особливості їх аналізу, розрахунок показників готовності і оперативної готовності). Використання інструментальних засобів для оцінювання.

Лекція 8 «Оцінювання надійності відновлюваних комп'ютерних систем».

Лабораторна робота 3 «Дослідження надійності відновлюваних КС з використанням апарату марковських процесів».

Самостійна робота: 10 годин.

Інструментальні засоби оцінювання надійності та функційної безпечності КС. Опрацювання матеріалу лекції. Підготовка до захисту лабораторної роботи. Підготовка до модульного контролю.

Модульний контроль 1.

Змістовний модуль 2. Методи діагностування та оцінювання стану апаратних і програмних засобів КС. Методи оцінювання та забезпечення функціональної безпеки КС.

Тема 5. Методи діагностування апаратних засобів КС.

Основні поняття технічної діагностики (об'єкти, процеси, засоби і системи контролю і діагностування; властивості - достовірність контролю і достовірність функціонування, контролепридатність; логічна модель і помилки контролю і діагностування). Структурна організація систем контролю і діагностування (структурні схеми робочого, тестового і комбінованого контролю і діагностування; основні елементи структур - перетворювачі вхідних впливів і вихідних реакцій, формувач очікуваних реакцій, блок аналізу, генератор

тестових впливів). Показники ефективності систем контролю і діагностування (показники достовірності контролю і діагностування, повнота контролю, глибина діагностування; оперативність контролю і діагностування; складність і надійність засобів контролю і діагностування). Класифікація методів контролю і діагностування (ознаки класифікації, загальна характеристика методів робочого і тестового контролю). Методи робочого контролю і діагностування (контроль дублюванням, мажоритарний контроль, контроль за модулем, програмно-логічні методи контролю, оцінка характеристик). Методи тестового контролю і діагностування (метод таблиць несправностей, методики отримання тестів перевірки працездатності і пошуку дефектів, псевдовипадкове тестування, сигнатурний аналіз, вбудовані засоби тестування невідновлювальних систем, принципи апаратно-програмної реалізації систем тестового діагностування).

Лекція 9 «Основи діагностування комп'ютерних систем. Базові поняття»ю

Лекція 10 «Основи діагностування комп'ютерних систем. Методи контролю та діагностування».

Лабораторна робота 4 «Розробка тестів для контролю і діагностування цифрових схем КС».

Самостійна робота: Методи он-лайн контролю мікропроцесорних систем. Опрацювання матеріалу лекцій. Підготовка до захисту лабораторної роботи.

Тема 6. Методи оцінювання надійності і функціональної безпечності програмних засобів КС.

Особливості оцінювання надійності та функціональної безпечності програмних засобів КС (поняття надійності програмних засобів, класифікація та аналіз дефектів, показники надійності програмних засобів). Моделі якості. Огляд та вимоги стандартів IEC25010, IEC25010, ISO 13849-1 та інш. Загальна характеристика моделей надійності програмних засобів (класифікація, аналіз основних моделей - метрик Холстеда, моделі Джелінского-Моранді, Шумана та ін.). Вибір і верифікація моделей надійності (матриця припущень, процедури вибору і комплексування моделей). Застосування методик і інструментальних засобів. Огляд і аналіз методів забезпечення надійності програмних компонентів.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали інструменти): комп'ютерне та мультимедійне обладнання.

Лекція 12 «Оцінювання надійності та функціональної безпечності програмних засобів КС. Моделі якості».

Лекція 13 «Загальна характеристика моделей надійності програмнихзасобів. Аналіз методів забезпечення надійності програмних компонентів».

Лабораторна робота 5 «Дослідження моделей надійності програмних засобів КС».

Самостійна робота: Моделі надійності (SRGM) програмних засобів. Опрацювання матеріалу лекції. Підготовка до захисту лабораторної роботи.

Тема 7. Методи оцінювання функціональної безпеки КС.

Особливості оцінювання функціональної безпечності КС. Огляд та вимоги стандартів IEC61508, IEC26262, IEC15408, ISO 13849 та інші. Класифікація і огляд методів оцінювання. Аналіз сутності та приклади застосування методів ХМЕСА, ХТА, ХІТ, ХВD. Особливості оцінювання функціональної безпечності КС з використанням марковських випадкових процесів. Урахування фактору кібербезпеки.

Лекція 13 «Оцінювання функціональної безпечності КС. Класифікація і огляд методів оцінювання»ю

Лекція 14 «Аналіз сутності та приклади застосування методів ХМЕСА, ХТА, ХІТ, ХВD та функціональної безпечності методів на основі марковських випадкових процесів».

Лабораторна робота 6 «Оцінка функційної безпечності та надійності з використанням ХМЕСА».

Самостійна робота: Оцінка функційної безпечності та надійності з використанням дерев відмов і атак. Опрацювання матеріалу лекцій. Підготовка до захисту лабораторної роботи.

Тема 8. Методи забезпечення функціональної безпеки та надійності КС.

Загальна послідовність та зміст етапів забезпечення надійності та функціональної безпеки при створенні та використанні КС. Поняття про оптимальне резервування та обмеження при проектуванні надійних і безпечних КС. Принципи одиничної відмови, незалежності та диверсності та їх впровадження. Методи і технології багатоверсійного проектування. Перспективні технології забезпечення функціональної безпеки та надійності КС. Підведення підсумків дисципліни.

Обов’язкові предмети та засоби (обладнання, устаткування, матеріали інструменти): комп’ютерне та мультимедійне обладнання.

Лекція 15 «Способи забезпечення надійності та функціональної безпеки при створенні та використанні КС».

Лекція 16 «Принципи одиничної відмови, незалежності та диверсності та їх впровадження. Методи і технології багатоверсійного проектування».

Лабораторна робота 7 «Дослідження методів побудови структури КС для забезпечення заданої надійності при мінімальній вартості».

Лабораторна робота 8 «Дослідження методів побудови структури КС для забезпечення максимальної надійності при обмеженнях на вартість системи».

Самостійна робота: Типові архітектури та технології проектування відмовостійких та безпечних КС. Опрацювання матеріалу лекцій. Підготовка до захисту лабораторної роботи. Виконання індивідуального завдання. Підготовка до модульного контролю.

Модульний контроль 2.

5. Індивідуальні завдання

Розрахунково-графічне завдання за індивідуальним варіантом. Тема «Розрахунок готовності та оптимальне резервування компонентів КС» (за темою 8, змістовного модуля 2; 8 годин самостійної роботи).

6. Методи навчання

Словесні (пояснення, розповідь, проблемний виклад), наочні (ілюстрування, демонстрація, презентація), практичні (лабораторні).

7. Методи контролю

Проведення поточного контролю під час проведення лабораторних занять, письмовий модульний контроль, підсумковий контроль, семестровий контроль у письмово-усній формі на екзамені.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1,2			
Виконання і захист лабораторних робіт	0…5	3	0…15
Модульний контроль	0…25	1	0…25
Змістовий модуль 3,4			
Виконання і захист лабораторних робіт	0...5	5	0…25
Виконання і захист розрахунково-графічного завдання	0...10	1	0…10
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається із двох теоретичних та одного практичного запитання, максимальна кількість балів за кожне теоретичне запитання, складає 34 балів, а за практичне – 32 балів.

Таблиця 2 – Шкали оцінювання: бальна та традиційна

Сума балів	Оцінка за традиційною шкалою
	Іспит
90-100	Відмінно
75-89	Добре
60-74	Задовільно
0-59	Незадовільно

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60 – 74). Показати мінімум знань та умінь. Показати позитивні результати по лабораторним роботам 1 – 5, розрахунково-графічному завданню та семінару.

Знати основні поняття і показники надійності та функціональної безпеки КС; методи оцінювання надійності апаратних і програмних компонентів і комп'ютерних систем в цілому; методи забезпечення надійності та функціональної безпеки КС на різних етапах життєвого циклу.

Вміти аналізувати вимоги до надійності та функціональної безпеки, виходячи з вимог технічних завдань на розроблення системи; розраховувати показники надійності, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів оцінювання; вибирати елементну базу, методи і об'єм резервування відповідно до вимог.

Добре (75 – 89). Твердо знати мінімум. Показати позитивні результати по лабораторним роботам 1 – 8 (не нижче 3), отримати бали по розрахунково-графічному завданню (не нижче 5).

Знати основні поняття і показники надійності та функціональної безпеки КС; методи оцінювання надійності та функціональної безпеки апаратних і програмних компонентів і КС в цілому; методи забезпечення надійності та функціональної безпеки КС на різних етапах життєвого циклу.

Вміти аналізувати вимоги до надійності та функціональної безпеки, виходячи з вимог технічних завдань на розроблення системи; розраховувати показники надійності та функціональної безпеки системи, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів оцінювання; вибирати елементну базу, методи і об'єм резервування відповідно до вимог.

Відмінно (90 – 100). Здати всі лабораторні роботи з оцінкою «добре» або «відмінно». Виконати у повному обсязі розрахунково-графічне завдання.

Знати основні поняття і показники надійності, відмовостійкості, живучості та надійності та функціональної безпеки КС; методи і засоби оцінювання надійності та безпеки апаратних і програмних компонентів і комп'ютерних систем в цілому; методи і засоби забезпечення надійності та безпеки комп'ютерних систем на різних етапах життєвого циклу; перспективні напрями розвитку та впровадження засобів забезпечення відмовостійкості та безпеки.

Вміти аналізувати вимоги до надійності та функціональної безпеки, виходячи з вимог стандартів та технічних завдань на розроблення системи; розраховувати показники надійності і надійності та функціональної безпеки системи, базуючись на електричних схемах і програмному забезпеченні систем з використанням відповідних методів і засобів оцінювання; приймати рішення щодо забезпечення вимог до надійності шляхом прийняття відповідних проектних рішень, вибору елементної бази, видів резервування, методів контролю і діагностування.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Характер курсу передбачає необхідність відвідування занять. Здобувачі освіти, які за певних обставин не можуть відвідувати заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувані освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувана освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi- dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Сторінка дисципліни у системі дистанційного навчання «Ментор». URL: https://mentor.khai.edu/enrol/index.php?id=9772.

11. Рекомендована література

Базова

1. Основи діагностики цифрових систем. Підручник/ За ред. Харченка В.С., Ілюшка В.М. Харків: Міністерство освіти та науки, 2007. 360 с.

2. Основи надійності цифрових систем. Підручник/ За ред. Харченка В.С., Жихарева В.Я. Харків: Міністерство освіти та науки, 2006. 342 с.

3. Харченко В.С., Скляр В.В., Тарасюк О.М. Методи моделювання та оцінки якості та надійності програмного забезпечення. Навчальний посібник. - Харків: ХАІ, 2008. 221 с.

4. Харченко В.С., Тарасенко В.В., Ушаков О.О. Відмовостійкі вбудовані цифрові системи на ПЛІС. Навчальний посібник. Харків: ХАІ, 2012. 189 с.

5. Відмовобезпечні інформаційно-керуючі системи на програмованій логіці/За ред. Харченко В.С., Скляра В.В. НАКУ «ХАІ», НВП «Радій», 2013. 291 с.

6. Харченко В.С., Лисенко І.В., Тарасюк О.М. Надійність та відмовостійкість комп'ютерних систем. Посібник до лабораторних робіт. Харків: ХАІ, 2013. 98 с.

Допоміжна

1. Аналіз, синтез і проектування цифрових систем керування: навч. посібник / С. М. Єсаулов, О. Ф. Бабічева; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. 150 с.

2. Харченко В.С., Скляр В.В., Конорєв Б,М. та ін Оцінка та забезпечення якості програмних засобів космічних систем. Національне космічне агентство України, НАКУ «ХАІ», Сертцентр АСУ, 2013. 294 с.

3. Основи цифрових систем. Підручник / За ред. Вдячного М.П., Харченка В.С. Харків: Міністерство освіти і науки, 2004. 351 с.

4. Методи системного аналізу у комп'ютерній інженерії та радіоелектроніці: підручник / За ред. С.Ю. Даншиної, В.С. Харченка. Х.: Нац. аерокосм. ун «Харк. авіац. ін-т», 2013. 312 с.

5 . Видання ХАІ з проектів MASTAC (2009-2010), SAFEGUARD (2011-2013), GREENCO (2014-2015), SEREIN (2015-2018), ALIOT (2019).

6. Кустов В.Ф. Основи теорії надійності та функційної безпечності систем залізничної автоматики: Навчальний посібник. Харків: УкрДАЗТ, 2008. 218 с

12. Інформаційні ресурси

1. Бабчук С.М. Надійність комп’ютерних систем і мереж, 2017. URL: http://194.44.112.13/chytalna/5417/index.html#p=1.

2. Вишнівський В.В. Основи надійності та діагностики телекомунікаційних систем, 2016. URL: http://www.dut.edu.ua/uploads/l_1092_31009342.pdf

3. The First 50 Years of Software Reliability Engineering: A History of SRE withFirst Person AccountsJames J. Cusick, PMP, New York, 2017. URL: https://arxiv.org/ftp/arxiv/papers/1902/1902.06140.pdf/

4. Operating System Reliability from the Quality of Experience Viewpoint: An Exploratory Study. URL: https://www.researchgate.net/publication/236332149_Operating_System_Reliability_from_the_Quality_of_Experience_Viewpoint_An_Exploratory_Study

5. Advances in System Reliability Engineering. URL: https://www.elsevier.com/books/advances-in-system-reliability-engineering/ram/978-0-12-815906-4

6. Safety Assessment for Facilities and Activities. IAEA Safety Standards, 2017. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf

7. Joint safety and security modeling for risk assessment in cyber physical systems, 2018. URL: https://tel.archives-ouvertes.fr/tel-01318118/document

8. Systems-Theoretic Safety Assessment of Robotic Telesurgical Systems, 2016. URL: https://www.researchgate.net/publication/275588035_Systems-Theoretic_Safety_Assessment_of_Robotic_Telesurgical_Systems/download.

9. ISO 13849-1:2023. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design URL: https://www.iso.org/standard/73481.html.

10. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. URL: https://dnaop.com/html/2273/doc-ДСТУ_2860-94.

11. ДСТУ 2863-94. Надійність техніки. Програма забезпечення надійності. Загальні вимоги. URL: https://dnaop.com/html/43857/doc-ДСТУ_2863-94.

12. ДСТУ 2389-94. Технічне діагностування та контроль технічного стану. Терміни та визначення. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjfodWqkrmCAxWLcvEDHTjVAugQFnoECBYQAQ&url=http%3A%2F%2Favionics.nau.edu.ua%2Ffiles%2Fdoc%2F%25D0%25A2%25D0%25B5%25D1%2580%25D0%25BC%25D0%25B8%25D0%25BD%25D1%258B%2520%25D0%25B8%25D0%25B7%2520%25D0%2594%25D0%25A1%25D0%25A2%25D0%25A3%25202389-94.doc&usg=AOvVaw1YV_iRGpe3yjBABcERMpEr&opi=89978449

13. Функційна безпека. Частина 6. Життєвий цикл інформаційної та функціональної безпеки. URL: https://tk185.appau.org.ua/61508/publications-iec-61508/funktsiina-bezpeka-chastyna-6-zhyttievyi-tsykl-informatsiinoi-ta-funktsionalnoi-bezpeky/