ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету
інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
05 09 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій

Галузь знань – F Інформаційні технології
Спеціальність – F6 Інформаційні системи і технології
Рівень вищої освіти – Третій (освітньо-науковий)
Освітньо-наукова програма – Інформаційні системи і технології
Обсяг дисципліни – 4 кредити ЄКТС, ***Шифр дисципліни*** – ОФП.06
Мова навчання – українська
Статус дисципліни: обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Комп'ютерної інженерії та інформаційних систем

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	1	4	120	50	16	34			70			+	
Разом ДФН			**4**	**120**	**50**	**16**	**34**			**70**			**1**	

Робоча програма складена на основі освітньо-наукової програми «Інформаційні системи і технології» та навчального плану за спеціальністю F6 Інформаційні системи і технології

Робоча програма складена _____ д-р., техн. наук, проф. Олег САВЕНКО
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Комп'ютерної інженерії та інформаційних систем

Протокол від 18.08.2025 № 1. Зав. кафедри _____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Протокол № 1 від 28 08 2025 р.

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

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувачка кафедри, д-р. філософії, доц.	Комп'ютерної інженерії та інформаційних систем		Ольга ПАВЛОВА
Гарант освітньо-професійної програми, д-р. техн. наук, проф.	Комп'ютерної інженерії та інформаційних систем		Тетяна ГОВОРУЩЕНКО

3. Пояснювальна записка

Дисципліна «Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій» є дисципліною фахової підготовки для здобувачів третього (освітньо-наукового) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-науковою програмою «Інформаційні системи і технології» в межах спеціальності F6 Інформаційні системи і технології.

Пререквізити – вихідна.

Постреквізити – інтелектуальні інформаційні системи і технології (ОФП.04), теорія і проєктування систем Інтернету речей (ОФП.05), педагогічна (викладацька) практика (ОФП.07).

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** здатність продукувати нові ідеї, розв'язувати комплексні науково-прикладні задачі професійної та/або дослідницько-інноваційної діяльності у сфері інформаційних систем та технологій, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення (ІК); здатність до абстрактного мислення, аналізу та синтезу (ЗК01); здатність розв’язувати комплексні науково-прикладні задачі у сфері інформаційних систем і технологій та з дотичних до міждисциплінарних напрямів на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності (ЗК04); здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у ІСТ та дотичних до них міждисциплінарних напрямах з ІТ та суміжних галузей (ФК01); здатність усно і письмово презентувати та обговорювати результати наукових досліджень й інноваційних розробок українською та іноземними мовами, глибоке розуміння наукових текстів іноземними мовами за напрямком досліджень (ФК02); здатність застосовувати сучасні методи дослідження, синтезу, проєктування інформаційних систем і технологій у науковій та науково-педагогічній діяльності (ФК06); здатність аналізувати дані та оцінювати необхідні знання для розв’язання задач оптимізації життєвого циклу інформаційних систем та цифрових сервісів, забезпечення їх надійності та безпеки з використанням математичних методів і методів комп’ютерного моделювання (УК03);

***програмних результатів навчання*:** мати передові концептуальні та методологічні знання з ІСТ і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інноваційної діяльності (ПРН01); вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми ІСТ державною та іноземними мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях (ПРН02); формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень, математичного та/або комп’ютерного моделювання, наявні наукові дані (ПРН03); розробляти та досліджувати концептуальні, математичні і комп’ютерні моделі процесів і систем, використовувати їх для отримання нових знань та/або створення інноваційних продуктів у сфері ІСТ та дотичних міждисциплінарних напрямах (ПРН04); планувати і виконувати експериментальні та/або теоретичні дослідження інформаційних систем і технологій з використанням сучасних методів дослідження, технічних, програмних засобів та з дотриманням норм академічної і професійної етики (ПРН05); застосовувати сучасні програмно-технічні засоби, зокрема для реалізації методів захисту комп’ютерної інформації при проектуванні інформаційних систем та цифрових сервісів в різних предметних областях (ПРН09); аналізувати дані та знання для оптимізації інформаційних систем та цифрових сервісів, забезпечення їх

надійності та безпеки з використанням математичних методів і методів комп'ютерного моделювання (ПРН13).

Мета дисципліни. Формування у здобувачів вищої освіти компетентностей, необхідних для розв'язання складних спеціалізованих задач у сфері інформаційних систем і технологій, розвитку абстрактного і логічного мислення та застосування сучасного математичного апарату, технологій та методів забезпечення надійності та безпеки інформаційних систем та технологій.

Предмет дисципліни. Поняття, теоретичні та практичні основи, технології та методи забезпечення надійності та безпеки інформаційних систем та технологій, що застосовуються для провадження наукової діяльності.

Завдання дисципліни. Надати студентам знання і практичні навички із застосування технологій та методів забезпечення надійності та безпеки інформаційних систем та технологій, які необхідні для подальшої наукової та професійної діяльності. Зокрема: 1) ознайомити студентів з інформаційними технологіями та інформаційними системами в контексті наукових досліджень, їх позиціонування; 2) ознайомити з якістю інформаційних систем та технологій в контексті наукових досліджень; 3) ознайомити з надійністю інформаційних систем та технологій; 4) ознайомити із методами та технологіями забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях; 5) ознайомити студентів з теоретичною базою, що використовується при розв'язуванні наукових задач; 6) виробити у студентів вміння використовувати набуті знання; 7) навчити здійснювати планування та постановку експерименту і обробку його результатів за результатами розроблених інформаційних технологій певного призначення; 8) підготувати студентів до провадження дослідницької та/або інноваційної діяльності в галузі інформаційних технологій; 9) ознайомити студентів з особливості академічної доброчесності при проведенні наукових досліджень.

Результати навчання. Після вивчення дисципліни студент повинен: досконало володіти професійною термінологією та основними поняттями про методи, моделі. концептуальні, математичні, імітаційні та комп'ютерні моделі процесів і систем; розуміти процеси та етапи розроблення інформаційних технологій, фундаментальні, універсальні та прикладні інформаційні технології; вміти позиціонувати інформаційні технології та інформаційні системи в контексті наукових досліджень; здійснювати розроблення систем для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування; знати стандарти з інформаційних технологій, особливості академічної доброчесності при проведенні наукових досліджень; володіти поняттям якості інформаційних систем та технологій і вміти його формалізувати до конкретних вимог; знати основні види показників для оцінювання якості інформаційного середовища та критерії безпеки, достовірності і надійності; знати і вміти застосовувати види, рівні та типи тестування програмного забезпечення інформаційних систем, розуміти місце вразливостей програмного забезпечення в загальній парадигмі інформаційних систем та технологій; вміти розробляти елементи резервування і надмірності в інформаційних системах; здійснювати технічне діагностування компонентів та елементів інформаційних систем; вміти проєктувати системи забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
Перший семестр				
Тема 1. Якість інформаційних систем та технологій.	6	6	-	30
Тема 2. Надійність інформаційних систем та технологій.	6	6	-	28
Тема 3. Забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.	4	6	-	28
Разом за 1-ий семестр:	16	18	-	86

5. Програма навчальної дисципліни
5.1 Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кіль-кість го-дин
	Перший семестр	
	Тема 1. Якість інформаційних систем та технологій.	
1	**Лекція 1. Інформаційні технології та інформаційні системи в контексті наукових досліджень, їх позиціонування, обов'язкові елементи та взаємозв'язок.** *Інформаційні технології в контексті об'єктів для розроблення в наукових дослідженнях. Поняття та складові частини інформаційних технологій. Методи. Моделі. Концептуальні, математичні, імітаційні та комп'ютерні моделі процесів і систем. Процеси та етапи розроблення інформаційних технологій. Фундаментальні, універсальні та прикладні інформаційні технології. Позиціонування інформаційних технологій та інформаційних систем в наукових дослідженнях. Реалізації інформаційних технологій. Системи для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування. Стандарти з інформаційних технологій [1], [2]. Особливості академічної доброчесності при проведенні наукових досліджень.*	2
2	**Лекція 2. Якість інформаційних систем та технологій як предметна область для наукових досліджень** *Ключові аспекти поняття якості інформаційних систем та технологій. Основні види показників для оцінювання якості інформаційного середовища. Критерії для оцінювання якості інформаційного середовища: безпека, достовірність і надійність. Властивості інформації: цілісність, доступність, конфіденційність. Дефекти та вразливості інформаційних систем. Дефектологічні властивості інформаційних систем: дефектогенність, дефектабельність і дефектоскопічність. Вплив інженерії вимог на якість інформаційних систем. Управління якістю інформаційних систем та технологій. Дослідження якості програмного забезпечення та технічних засобів інформаційних систем в контексті розв'язування наукових задач. Моделі якості програмного забезпечення ІС. Характеристики якості. Стандарти якості. Процеси забезпечення якості. Керування якістю. Моделі оцінювання якості. Метрики для оцінювання якості програмних систем. Валідація і верифікація. Формалізоване задання показників якості інформаційних систем та технологій і розроблення згідно них критеріїв для їх якісного та кількісного оцінювання. Побудова оптимізаційної функції з врахуванням показників якості інформаційних систем. Забезпечення якості інформаційних систем та технологій в контексті виконання наукового дослідження.* *Аналіз наукових публікацій та напрямів з дослідження якості інформаційних систем та технологій. Вплив можливостей*	2

	інформаційних систем і загального управління якістю на вартість якості [3]. Детермінанти якості інформаційної системи та якості даних [4]. Наукові дослідження з управління якістю інформаційних систем [5]. Якість даних як критичний фактор успіху для сприйняття користувачами дослідницьких інформаційних систем [6]. Інформаційні технології прогнозування рівня якості програмного забезпечення [7].	
3	**Лекція 3. Наукові дослідження з тестування програмного забезпечення інформаційних систем.** *Види, рівні та типи тестування програмного забезпечення інформаційних систем. Вразливості програмного забезпечення. Організація тестування. Критерії вибору тестів. Планування та документування тестування. Життєвий цикл дефектів Функціональне, нефункціональне тестування інформаційних систем. Тестування методом «чорного ящика» та методом «білого ящика». Документування результатів тестування. Тестові звіти. Автоматизація тестування. Засоби автоматизації тестування. Функціональне тестування Модульне тестування. Інтеграційне тестування. Тестування системи. Приймальні випробування. Нефункціональне тестування. Тестування продуктивності. Безпечне тестування. Тестування зручності використання. Напрями наукових досліджень за видами, рівнями та типами тестування програмного забезпечення інформаційних систем.* *Приклади напрямів наукових досліджень з тестування програмного забезпечення. Про ролі тестувальників програмного забезпечення: пошукове дослідження [8]. Десятиліття досліджень інтелектуального тестування програмного забезпечення: бібліометричний аналіз [9]. Оптимізація автоматизованого тестування програмного забезпечення за допомогою мета-евристичних методів [10]. Оцінювання методів тестування програмного забезпечення: систематичне дослідження [11]. Еволюція стратегій тестування програмного забезпечення та тенденції: аналіз семантичного вмісту програмного забезпечення [12].*	2
	Тема 2. Надійність інформаційних систем та технологій.	
4	**Лекція 4. Проблеми надійності інформаційних систем.** *Теорія надійності. Її місце в науці. Кількісні показники надійності. Показники безвідмовності об'єктів, які не відновлюються. Показники безвідмовності відновлюваних об'єктів. Основні математичні моделі безвідмовності. Показники ремонтопридатності. Основні математичні моделі ремонтопридатності. Комплексні показники надійності. Методи забезпечення надійності інформаційних систем. Поняття структурної схеми надійності. Основні розрахункові співвідношення для показників безвідмовності. Наближені методи розрахунку показників безвідмовної роботи. Розрахунок показників ремонтопридатності. Інтервальні оцінки показників надійності. Загальна постановка завдань статистичної оцінки показників надійності. Точкові та інтервальні оцінки показників надійності. Здійснення перевірки відповідності показників надійності інформаційних систем технічним умовам. Загальна методика перевірки відповідності показників надійності технічним умовам. Перевірка відповідності середнього напрацювання на відмову*	2

	технічним умовам. Перевірка відповідності середнього часу відновлення технічним умовам. Фактори, що впливають на надійність інформаційних систем. *Приклади наукових досліджень з надійності інформаційних систем. Надійність інформаційних систем в організаціях як фактор формування організаційної культури [13]. Підвищення безпеки та надійності інформаційних систем за допомогою технології блокчейн: тематичне дослідження щодо впливу та потенціалу [14]. Дослідження методу оцінки надійності системи високої надійності за трьома станами на основі попередньої інформації з багатьох джерел [15]. Моделі надійності систем моніторингу на основі БПЛА з декількома станами: проблеми зниження ефективності місії [16].*	
5	**Лекція 5. Проблеми та стратегії резервування і надмірності в інформаційних системах.** *Резервування. Оцінка надійності резервованих систем без відновлення. Оцінка надійності резервованих систем з відновленням. Перспективи вирішення проблем забезпечення надійності інформаційних систем. Стратегії резервування. Дослідження ефективності резервування.* *Надмірності в інформаційних системах. Забезпечення відмовостійкості та живучості інформаційних систем. Життєвий цикл інформаційних систем. Стратегії використання надмірностей для забезпечення стійкості інформаційних систем. Дослідження ефективності використання надмірності.* *Розроблення інформаційних технологій з елементами надмірності та резервування. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. Використання надмірностей [17]. Стратегія гібридної відмовостійкості для мобільних розподілених систем [18]. Нова адаптивна відмовостійка структура в хмарі [19]. Діагностика несправностей на основі спостерігача та відмовостійке керування для комутованих систем [20]. Оцінка надійності багатокаскадних резервованих систем з урахуванням відмов міжмодульних і мостових комунікацій [21].*	2
6	**Лекція 6. Технічне діагностування компонентів та елементів інформаційних систем. Методології та стратегії забезпечення функційної безпеки. Резилентні системи.** *Технічна діагностика як наука. Технічне діагностування інформаційних систем. Основні поняття і визначення технічної діагностики. Наукові задачі технічної діагностики. Технічне діагностування аналогових об'єктів. Технічна діагностика цифрових об'єктів. Технічні засоби діагностування. Технічне діагностування елементів та компонентів кіберфізичних систем. Дослідження ефективності діагностування інформаційних систем.* *Напрями наукових досліджень в технічному діагностуванні інформаційних систем. Інтелектуальне діагностування комп'ютерних систем [22]. Система технічної діагностики інформаційної мережі промислової безпеки [23]. Адаптивні накопичувальні та діагностичні інформаційні системи підприємств енергетики та промисловості [24]. Значення технічної діагностики для забезпечення надійності промислових систем [25].*	2

	Функційна безпека. Методи та стратегії забезпечення функційної безпеки інформаційних систем. Складові частини резилентних систем. Розроблення резилентнтих систем та методів організації їх функціонування. Фактори зовнішнього впливу на інформаційні системи. Типи зовнішніх впливів. Руйнуючі програмні впливи. Наслідки впливів на елементи та компоненти інформаційних систем. Функційна базпека та кібербезпека. *Відмовостійкість та стійкі системи штучного інтелекту: таксономія, моделі та методи [26]. Моделі надійності та вартості програмного забезпечення з гарантією та життєвим циклом [27]. Безпека, конфіденційність і експертиза в інформаційних системах підприємства [28]. Про комплексну функційну безпеку та кібербезпеку [29].* ***Тема 3. Забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.***	
7	**Лекція 7. Методології та наукові напрями кібербезпеки.** *Кібербезпека в контексті інформаційних систем та технологій. Наукові задачі в предметній області з кібербезпеки. Моделі зловмисника. Методи оцінювання ризиків. Стандарти визначення кібербезпеки об'єктів інформатизації. Кібербезпека критичних систем та критичної інфраструктури.* *Приклади наукових досліджень з кібербезпеки. Виявлення внутрішньої загрози ритму поведінки з усвідомленням часу та адаптацією користувача [30]. Автоматизований і безпечний метод побудови зашифрованого набору даних трафіку для миттєвих повідомлень в Android з низькими накладними витратами на рівні функцій [31]. Збільшення можливостей вбудовування стегозображень за рахунок використання крайових пікселів у просторі помилок передбачення [32]. Кіберризик і кібербезпека: систематичний огляд доступності даних [33].*	2
8	**Лекція 8. Методи захисту інформації при проектуванні інформаційних систем та цифрових сервісів в різних предметних областях.** *Проєктування інформаційних систем із засобами забезпечення стійкості до зловмисного програмного забезпечення. Методи та засоби захисту інформації в корпоративних мережах. Побудова корпоративних мереж із врахуванням стандартів з кібербезпеки. Проєктування розподілених систем виявлення комп'ютерних атак. Розроблення методів виявлення комп'ютерних атак. Інтеграція методів виявлення та розподілених систем в єдиний сенсор. Системи обману для виявлення комп'ютерних атак в корпоративних мережах. Застосування методів виявлення аномалій для побудови систем захисту інформації. Застосування компонентів штучного інтелекту для видобування знань в системах виявлення комп'ютерних атак. Дослідження методів обфускації програмного коду.* *Метод виявлення комп'ютерних вірусів на основі інформації з PE-структури файлів у поєднанні з моделями глибокого навчання [34]. Методи побудови розподілених систем для виявлення комп'ютерних атак [35]. Методи безпеки аутентифікації та авторизації в*	2

	інформаційних системах. Методи ідентифікації аномальних станів для систем виявлення вторгнень [36], [38]. *Лекція 8 може бути замінена одним з сертифікатів курсів Cisco* https://www.netacad.com/catalogs/learn/cybersecurity?category=course , наприклад: https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US	
	Разом за 1-ий семестр:	16

5.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кіль-кість годин
	Перший семестр	
1	***Лабораторне заняття 1.*** *Дослідження якості інформаційних систем та технологій і реалізація методів їх оцінювання на основі відомих та удосконалених метрик.*	2
2	***Лабораторне заняття 2.*** *Дослідження методів оптимізації автоматизованого тестування програмного забезпечення.*	2
3	***Лабораторне заняття 3.*** *Дослідження функційної безпеки та надійності інформаційних систем.*	2
4	***Лабораторне заняття 4.*** *Вразливості інформаційних систем та цифрових сервісів і методи їх виявлення.*	2
5	***Лабораторне заняття 5.*** *Розроблення інформаційних технологій з елементами надмірності та резервування.*	2
6	***Лабораторне заняття 6.*** *Розроблення резилентних систем та методів організації їх функціонування.*	2
7	***Лабораторне заняття 7.*** *Розподілені інформаційні системи для реалізації методів виявлення зловмисного програмного забезпечення в корпоративних мережах.*	2
8	***Лабораторне заняття 8.*** *Застосовування сучасних програмно-технічних засобів, зокрема спеціалізованих, для реалізації методів захисту інформації при проектуванні інформаційних систем та цифрових сервісів в корпоративній інфраструктурі.*	2
9	***Лабораторне заняття 9.*** *Підсумкове заняття.*	2
	Разом за 1-ий семестр:	18

Лабораторне заняття 4 може бути замінене сертифікатом з курсу Cisco:
https://www.netacad.com/courses/cyberops-associate?courseLang=en-US

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

Обсяг самостійної роботи з дисципліни становить 86 годин. Він включає опрацювання лекційного матеріалу, підготовку до виконання лабораторних робіт, підготовку до поточного контролю. Для студентів доступна сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідне навчально-методичне забезпечення.

Номер тижня	Вид самостійної роботи	К-ть годин
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	5
2	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	5
3	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №2.	5
4	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	5
5	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №3.	5
6	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №3.	5
7	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №4.	5
8	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №4.	5
9	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №5.	5
10	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №5.	5
11	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №6.	5
12	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №6.	5
13	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №7.	5
14	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №7.	5
15	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №8.	5
16	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №8.	5
17	Опрацювання лекційного матеріалу.	6
	Разом за 1-ий семестр:	86

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, інформаційно-комунікаційних технологій); лабораторні заняття (з використанням інструктування, демонстрування, розв'язування типових і прикладних задач, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання лабораторних робіт, поточного та підсумкового контролю, виконання індивідуальних завдань), з використанням інформаційно-комп'ютерних технологій.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних лабораторних занять, , в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– оцінювання результатів захисту лабораторних робіт (опитування теоретичного матеріалу, розв'язування задач);

– тестування;

– оцінювання індивідуального домашнього завдання.

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, 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), активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час лабораторних занять та тестування.

Здобувач вищої освіти, виконуючи самостійну роботу або індивідуальну 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 повинен повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності не допускаються.

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**	**Самостійна робота**	**Семестровий контроль**
Лабораторні заняття №:								Тестовий контроль	ІДЗ	Залік
1*	2	3	4	5	6	7	8	Т 1-3	Т 1-2	
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	6-10	18-30	За рейтингом
24-40								**6-10**	**18-30**	**60-100***

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**»;

Т – тема навчальної дисципліни.

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 дотримання вимог при оформленні.

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 результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 25 тестових завдань, кожне з яких є рівнозначним.

Відповідно до таблиці структурування видів робіт за тестовий контроль здобувач залежно від кількості правильних відповідей може отримати від 6 до 10 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	1-13	14-16	17-18	19-20	21-22	23-25
Відсоток правильних відповідей	0-59	60-65	66-72	73-82	83-89	90-100
Кількість балів	-	6	7	8	9	10

На тестування відводиться 40 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити

тестування письмово, записуючи правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів виконання індивідуального домашнього завдання (ІДЗ).

Виконане та оформлене відповідно до вимог, визначених Методичними рекомендаціями, індивідуальне домашнє завдання (ІДЗ) комплексно оцінюється викладачем з урахуванням таких критеріїв: самостійність виконання; правильність розв'язання поставлених задач; обґрунтованість вибору методів розв'язання; повнота пояснень та аргументованість відповідей; якість оформлення та дотримання вимог до структури і змісту роботи.

Результат виконання здобувачем вищої освіти кожного ІДЗ оцінюється відповідно до таблиці **Критеріїв оцінювання навчальних досягнень здобувача вищої освіти** з урахуванням рівня досягнення запланованих програмних результатів навчання та сформованих компетентностей. За підсумками захисту присвоюється відповідна сума балів (мінімальний позитивний бал – 18 бали, максимальний – 30 балів).

У разі, якщо здобувач вищої освіти виявив рівень знань і виконання ІДЗ, що нижчий ніж 60 відсотків від максимальної кількості балів, встановленої Робочою програмою для цієї структурної одиниці, завдання не зараховується. У такому випадку студент має повторно опрацювати зміст завдання, усунути помилки та здати на перевірку доопрацьоване ІДЗ у терміни, погоджені з викладачем.

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 залік виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

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
C	73-82		

			навчання та/або професійної діяльності за фахом
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. Наукові задачі в галузі інформаційних технологій. Методи оптимізації для розв'язування наукових задач. Відмінності між інженерною та науковою задачами.
2. Моделі інформаційних технологій та оптимізаційні методи, як їх основа.
3. Якість інформаційних систем та технологій.
4. Інформаційні технології в контексті об'єктів для розроблення в наукових дослідженнях.
5. Концептуальні, математичні, імітаційні та комп'ютерні моделі процесів і систем.
6. Системи для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування.
7. Стандарти з інформаційних технологій.
8. Основні види показників для оцінювання якості інформаційного середовища.
9. Критерії для оцінювання якості інформаційного середовища: безпека, достовірність і надійність.
10. Властивості інформації: цілісність, доступність, конфіденційність.
11. Дефекти та вразливості інформаційних систем.
12. Дефектологічні властивості інформаційних систем: дефектогенність, дефектабельність і дефектоскопічність.
13. Управління якістю інформаційних систем та технологій.
14. Дослідження якості програмного забезпечення та технічних засобів інформаційних систем в контексті розв'язування наукових задач.
15. Моделі якості програмного забезпечення ІС.
16. Стандарти якості.
17. Валідація і верифікація.
18. Формалізоване задання показників якості інформаційних систем та технологій і розроблення згідно них критеріїв для їх якісного та кількісного оцінювання.
19. Побудова оптимізаційної функції з врахуванням показників якості інформаційних систем.
20. Забезпечення якості інформаційних систем та технологій в контексті виконання наукового дослідження.
21. Аналіз наукових публікацій та напрямів з дослідження якості інформаційних систем та технологій. Вплив можливостей інформаційних систем і загального управління якістю на вартість якості.
22. Детермінанти якості інформаційної системи та якості даних.
23. Наукові дослідження з управління якістю інформаційних систем.
24. Якість даних як критичний фактор успіху для сприйняття користувачами дослідницьких інформаційних систем.
25. Інформаційні технології прогнозування рівня якості програмного забезпечення.

26. Наукові дослідження з тестування програмного забезпечення інформаційних систем.
27. Види, рівні та типи тестування програмного забезпечення інформаційних систем.
28. Вразливості програмного забезпечення.
29. Функціональне, нефункціональне тестування інформаційних систем.
30. Автоматизація тестування. Засоби автоматизації тестування.
31. Напрями наукових досліджень за видами, рівнями та типами тестування програмного забезпечення інформаційних систем.
32. Про ролі тестувальників програмного забезпечення: пошукове дослідження.
33. Десятиліття досліджень інтелектуального тестування програмного забезпечення: бібліометричний аналіз.
34. Оптимізація автоматизованого тестування програмного забезпечення за допомогою мета-евристичних методів.
35. Оцінювання методів тестування програмного забезпечення: систематичне дослідження.
36. Еволюція стратегій тестування програмного забезпечення та тенденції: аналіз семантичного вмісту програмного забезпечення.
37. Проблеми надійності інформаційних систем.
38. Теорія надійності. Її місце в науці. Кількісні показники надійності.
39. Показники безвідмовності об’єктів, які не відновлюються. Показники безвідмовності відновлюваних об’єктів.
40. Основні математичні моделі безвідмовності.
41. Показники ремонтопридатності. Основні математичні моделі ремонтопридатності.
42. Методи забезпечення надійності інформаційних систем.
43. Надійність інформаційних систем в організаціях як фактор формування організаційної культури.
44. Підвищення безпеки та надійності інформаційних систем за допомогою технології блокчейн: тематичне дослідження щодо впливу та потенціалу.
45. Дослідження методу оцінки надійності системи високої надійності за трьома станами на основі попередньої інформації з багатьох джерел.
46. Моделі надійності систем моніторингу на основі БПЛА з декількома станами: проблеми зниження ефективності місії.
47. Проблеми та стратегії резервування і надмірності в інформаційних системах.
48. Перспективи вирішення проблем забезпечення надійності інформаційних систем.
49. Надмірності в інформаційних системах. Забезпечення відмовостійкості та живучості інформаційних систем. Дослідження ефективності використання надмірності.
50. Розроблення інформаційних технологій з елементами надмірності та резервування. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. Використання надмірностей.
51. Стратегія гібридної відмовостійкості для мобільних розподілених систем.
52. Адаптивна відмовостійка структура в хмарі.
53. Діагностика несправностей на основі спостерігача та відмовостійке керування для комутованих систем.
54. Оцінка надійності багатокаскадних резервованих систем з урахуванням відмов міжмодульних і мостових комунікацій.
55. Технічне діагностування компонентів та елементів інформаційних систем.
56. Технічна діагностика як наука. Технічне діагностування інформаційних систем.
57. Наукові задачі технічної діагностики.
58. Технічне діагностування елементів та компонентів кіберфізичних систем.
59. Дослідження ефективності діагностування інформаційних систем.
60. Напрями наукових досліджень в технічному діагностуванні інформаційних систем. Інтелектуальне діагностування комп'ютерних систем.

61. Система технічної діагностики інформаційної мережі промислової безпеки.
62. Адаптивні накопичувальні та діагностичні інформаційні системи підприємств енергетики та промисловості.
63. Значення технічної діагностики для забезпечення надійності промислових систем.
64. Методології та стратегії забезпечення функційної безпеки.
65. Резилентні системи. Складові частини резилентних систем. Розроблення резилентнтих систем та методів організації їх функціонування.
66. Функційна безпека. Методи та стратегії забезпечення функційної безпеки інформаційних систем.
67. Фактори зовнішнього впливу на інформаційні системи. Типи зовнішніх впливів. Руйнуючі програмні впливи. Наслідки впливів на елементи та компоненти інформаційних систем.
68. Відмовостійкість та стійкі системи штучного інтелекту: таксономія, моделі та методи.
69. Моделі надійності та вартості програмного забезпечення з гарантією та життєвим циклом.
70. Безпека, конфіденційність і експертиза в інформаційних системах підприємства.
71. Про комплексну функційну безпеку та кібербезпеку.
72. Методології та наукові напрями кібербезпеки.
73. Наукові задачі в предметній області з кібербезпеки.
74. Методи оцінювання ризиків.
75. Стандарти визначення кібербезпеки об’єктів інформатизації.
76. Кібербезпека критичних систем та критичної інфраструктури.
77. Виявлення внутрішньої загрози ритму поведінки з усвідомленням часу та адаптацією користувача.
78. Автоматизований і безпечний метод побудови зашифрованого набору даних трафіку для миттєвих повідомлень в Android з низькими накладними витратами на рівні функцій.
79. Збільшення можливостей вбудовування стегозображень за рахунок використання крайових пікселів у просторі помилок передбачення.
80. Кіберризик і кібербезпека: систематичний огляд доступності даних.
81. Методи захисту інформації при проектуванні інформаційних систем та цифрових сервісів в різних предметних областях.
82. Проєктування інформаційних систем із засобами забезпечення стійкості до зловмисного програмного забезпечення.
83. Методи та засоби захисту інформації в корпоративних мережах.
84. Побудова корпоративних мереж із врахуванням стандартів з кібербезпеки.
85. Проєктування розподілених систем виявлення комп’ютерних атак.
86. Розроблення методів виявлення комп’ютерних атак.
87. Інтеграція методів виявлення та розподілених систем в єдиний сенсор.
88. Системи обману для виявлення комп’ютерних атак в корпоративних мережах.
89. Застосування методів виявлення аномалій для побудови систем захисту інформації.
90. Застосування компонентів штучного інтелекту для видобування знань в системах виявлення комп’ютерних атак.
91. Дослідження методів обфускації програмного коду.
92. Метод виявлення комп’ютерних вірусів на основі інформації з PE-структури файлів у поєднанні з моделями глибокого навчання.
93. Методи побудови розподілених систем для виявлення комп’ютерних атак.
94. Методи безпеки аутентифікації та авторизації в інформаційних системах.
95. Методи ідентифікації аномальних станів для систем виявлення вторгнень.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни забезпечений необхідною навчально-методичною літературою. Викладачами дисципліни підготовлено і видано методичний посібник:

Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій : лабораторний практикум з дисципліни для здобувачів третього (освітньо-наукового) рівня вищої освіти спеціальності 126 «Інформаційні системи та технології» / О. С. Савенко, Д. О. Денисюк, А. О. Нічепорук, М. В. Капустян. Хмельницький : ХНУ, 2024. 57 с.

Підготовлені і розміщенні в модульному середовищі університету: презентації лекцій, методичні матеріали до виконання практичних занять з розв'язування задач та завдання, варіанти ІДЗ.

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, доступ до мережі Інтернет, робота з презентаціями.

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі.

13. Рекомендована література:

Основна література

1. ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) Інформаційні технології. Словник термінів.
2. ДСТУ ISO/IEC 15288:2005 Інформаційні технології. Процеси життєвого циклу системи (ISO/IEC 15288:2002, IDT).
3. Alzoubi, Haitham & Alshurideh, Muhammad & Akour, Iman & Al Shraah, Ata & Ahmed, Gouher. (2021). Impact of information systems capabilities and total quality management on the cost of quality. 24. 1-11.
4. Thorsten Knauer & Nicole Nikiforow & Sebastian Wagener, 2020. "Determinants of information system quality and data quality in management accounting," Journal of Management Control: Zeitschrift für Planung und Unternehmenssteuerung, *Springer*, vol. 31(1), pages 97-121, April.
5. Piattini, M., García-Rodríguez de Guzmán, I. & Pérez-Castillo, R. Special issue on quality management for information systems. *Software Qual J* **28**, 891–894 (2020). https://doi.org/10.1007/s11219-020-09516-z
6. Azeroual O, Saake G, Abuosba M, Schöpfel J. Data Quality as a Critical Success Factor for User Acceptance of Research Information Systems. *Data*. 2020; 5(2):35. https://doi.org/10.3390/data5020035
7. Hovorushchenko, T., Voichur, Y., & Medzatyi, D. (2023). Information technology for prediction of software quality level. *Radioelectronic and Computer Systems, 0*(3), 238-254. doi:https://doi.org/10.32620/reks.2023.3.19
8. Raluca Florea, Viktoria Stray, Dag I.K. Sjøberg, On the roles of software testers: An exploratory study, *Journal of Systems and Software*, Volume 204, 2023, 111742, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2023.111742. (https://www.sciencedirect.com/science/article/pii/S0164121223001371)
9. Boukhlif M, Hanine M, Kharmoum N. A Decade of Intelligent Software Testing Research: A Bibliometric Analysis. *Electronics*. 2023; 12(9):2109. https://doi.org/10.3390/electronics12092109

10. Khari, M.; Mishra, D.; Acharya, B.; Crespo, R. Optimization of Automated Software Testing Using Meta-Heuristic Techniques; *Springer International Publishing*: Berlin/Heidelberg, Germany, 2022.

11. Mitchell Mayeda, Anneliese Andrews, Chapter Two - Evaluating software testing techniques: A systematic mapping study, Editor(s): Ali R. Hurson, Advances in Computers, Elsevier, Volume 123, 2021, Pages 41-114, ISSN 0065-2458, ISBN 9780128241219, https://doi.org/10.1016/bs.adcom.2021.01.002.

(https://www.sciencedirect.com/science/article/pii/S0065245821000279)

12. F. Gurcan et al.: Evolution of Software Testing Strategies and Trends: Semantic Content Analysis. Received 21 September 2022, accepted 29 September 2022, date of publication 4 October 2022, date of current version 11 October 2022. Digital Object Identifier 10.1109/ACCESS.2022.3211949 https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3044013/Evolution_of_Software_Testing_Strategies_and_Trends_Semantic_Content_Analysis_of_Software_Research_Corpus_of_the_Last_40_Years.pdf?sequence=1

13. Tworek, Katarzyna. (2020). Reliability of information systems in organizations as a factor shaping organizational culture. *Argumenta Oeconomica*. 2020. 259-274. 10.15611/aoe.2020.2.11.

14. Adi Nugroho Susanto Putro, Sabil Mokodenseho, Nur Alim Hunawa, Muhatir Mokoginta, Evelin Ragil Marjoni. Enhancing Security and Reliability of Information Systems through Blockchain Technology: A Case Study on Impacts and Potential. *West Science Information System and Technology*. Vol. 1, No. 01, August 2023, pp. 35~43

15. Huang J, Huang Z, Zhan X. 2023. Research on three-state reliability evaluation method of high reliability system based on multi-source prior information. *PeerJ Computer Science* 9:e1439 https://doi.org/10.7717/peerj-cs.1439

16. I Kliushnikov, V Kharchenko, H Fesenko, E Zaitseva, V. Levashenko. Reliability Models of Multi-state UAV-based Monitoring Systems: Mission Efficiency Degradation Issues. *2023 International Conference on Information and Digital Technologies (IDT)* 2023. – IEEE, P.299-306.

17. Стецюк М. В. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. – *Кваліфікаційна наукова праця на правах рукопису*. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2022. https://nauka.khmnu.edu.ua/wp-content/uploads/dysertacziya-1.pdf

18. Wu, Y.; Liu, D.; Chen, X.; Ren, J.; Liu, R.; Tan, Y.; Zhang Z. MobileRE: A replicas prioritized hybrid fault tolerance strategy for mobile distributed system. *Journal of Systems Architecture*, 2021, vol 118, N102217. https://doi.org/10.1016/j.sysarc.2021.102217

19. Rawat, A.; Sushil, R.; Agarwal, A.; Sikander, A.; Bhadoria, R.S. A New Adaptive Fault Tolerant Framework in the Cloud. *IETE Journal of Research*, 2021, pp 113 117. DOI: 10.1080/03772063.2021.1907231

20. Du, D.; Xu, S.; Cocquempot V. Observer Based Fault Diagnosis and Fault Tolerant Control for Switched Systems. *Series: Studies in Systems, Decision and Control. Springer: Singapore*, 2021; vol 280, p 81. DOI 10.1007/978 981 15 9073 3

21. Kharchenko, V., Kovalenko, A., Ruchkov, E., Babeshko, I. (2021). Reliability Assessment of Multi-cascade Redundant Systems Considering Failures of Intermodular and Bridge Communications. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Theory and Engineering of Dependable Computer Systems and Networks. DepCoS-RELCOMEX 2021. *Advances in Intelligent Systems and Computing*, vol 1389. Springer, Cham. https://doi.org/10.1007/978-3-030-76773-0_18

22. Поморова, Оксана Вікторівна. Теоретичні основи, методи та засоби інтелектуального діагностування комп'ютерних систем : автореф. дис ... д-ра техн. наук :

05.13.13 / Оксана Вікторівна Поморова; Нац. ун-т "Львівська політехніка".– Львів : 2007.– 33 с.

23. Repp, P. (2017). The system of technical diagnostics of the industrial safety information network. *Journal of Physics: Conference Series.* 803. 012127. 10.1088/1742-6596/803/1/012127.

24. Sobchuk, V., Barabash, O., Musienko, A., and Svynchuk, O., "Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors", *in E3S Web of Conferences*, 2021, vol. 250. doi:10.1051/e3sconf/202125008002.

25. D. Lj. Branković, Z. N. Milovanović and V. Z. Janičić Milovanović. The Importance of Technical Diagnostics for Ensuring the Reliability of Industrial Systems. *A chapter in Reliability and Maintainability Assessment of Industrial Systems*, 2022, pp 143-187 from Springer http://www.springer.com/9783030936235 DOI: 10.1007/978-3-030-93623-5_8

26. Moskalenko, V.; Kharchenko, V.; Moskalenko, A.; Kuzikov, B. Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods. *Algorithms* 2023, 16, 165. https://doi.org/10.3390/a16030165

27. Shrivastava AK, Sharma R, Pham H. Software reliability and cost models with warranty and life cycle. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. 2023;237(1):166-179. doi:10.1177/1748006X221076273

28. B. B. Gupta & Dharma P. Agrawal (2021) Security, privacy and forensics in the enterprise information systems, *Enterprise Information Systems*, 15:4, 445-447, DOI: 10.1080/17517575.2020.1791364

29. Wu JX. On integrated security and safety. Security and Safety 2022; **1**: E2022002. https://doi.org/10.1051/sands/2022002

30. Song, S., Gao, N., Zhang, Y. *et al.* BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. *Cybersecurity* **7**, 2 (2024). https://doi.org/10.1186/s42400-023-00190-9

31. Xu, K., Cheng, G. F3l: an automated and secure function-level low-overhead labeled encrypted traffic dataset construction method for IM in Android. *Cybersecurity* **7**, 1 (2024). https://doi.org/10.1186/s42400-023-00185-6

32. Habiba Sultana, A.H.M. Kamal, Tasnim Sakib Apon, Md. Golam Rabiul Alam, Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space, *Cyber Security and Applications*, Volume 2, 2024, 100028, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100028.
(https://www.sciencedirect.com/science/article/pii/S2772918423000164)

33. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract*. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

34.Nguyen, V.T.; Hien, V.T.; Tuan, L.D.; Tiep, M.V.; Anh, N.H.; Vuong, P.T. A Computer Virus Detection Method Based on Information from PE Structure of Files Combined with Deep Learning Models. Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2020. *Communications in Computer and Information Science*. Dang, T.K., Küng, J., Takizawa, M., Chung, T.M. Eds.; Springer, Singapore, 2020; vol 1306, pp 120–129. https://doi.org/10.1007/978 981 33 4370 2_9

35. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773

36. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень: Автореф. дис. ... докт. техн. наук: 05.13.21/НАУ. – К., 2019. – 42с.

37. Савенко О.С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти – Національний університет «Львівська політехніка», Львів, 2019. https://lpnu.ua/sites/default/files/2020/dissertation/1500/dysertaciyasavenkaos.pdf

38. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024(1), 152-175. doi:https://doi.org/10.32620/reks.2024.1.13

39. Kashtalian, A., Lysenko, S., Sachenko, A., Savenko, B., Savenko, O., & Nicheporuk, A. (2025). Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*, *2025*(1), 264-297. doi:https://doi.org/10.32620/reks.2025.1.18

40. Kashtalian, A., Lysenko, S., Kysil, T., Sachenko, A., Savenko, O., & Savenko, B. (2025). Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*, *24*(1), 35-51. https://doi.org/10.47839/ijc.24.1.3875

Додаткова література

1. ДСТУ. Надійність техніки. Терміни та визначення. ДСТУ 2860 94.

2. ДСТУ ISO/IEC 2382 14:2005 Інформаційні технології. Словник термінів. Частина 14. Безвідмовність, ремонтопридатність і готовність.

3. ДСТУ ISO/IEC 13335 1:2004 Інформаційні технології. Методи захисту. Керування інформацією й безпекою технології комунікацій. Частина 1. Поняття й моделі для інформації й керування безпекою технології комунікацій.

4. ДСТУ ISO/IEC 2382 18:2005 Інформаційні технології. Словник термінів. Частина 18. Розподілене оброблення даних.

Інформаційні ресурси

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8861
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Третій (доктор філософії)
Мова викладання	Українська
Семестр	1
Кількість призначних кредитів ЄКТС	4,0
Форми здобуття освіти, для яких викладається дисципліна	Очна денна

Результати навчання. Після вивчення дисципліни студент повинен: досконало володіти професійною термінологією та основними поняттями про методи, моделі. концептуальні, математичні, імітаційні та комп'ютерні моделі процесів і систем; розуміти процеси та етапи розроблення інформаційних технологій, фундаментальні, універсальні та прикладні інформаційні технології; вміти позиціонувати інформаційні технології та інформаційні системи в контексті наукових досліджень; здійснювати розроблення систем для одержання, обробки, зберігання, відображення та/або реєстрації даних про технічний стан конструкцій, систем, елементів, їх властивості та/або функціонування; знати стандарти з інформаційних технологій, особливості академічної доброчесності при проведенні наукових досліджень; володіти поняттям якості інформаційних систем та технологій і вміти його формалізувати до конкретних вимог; знати основні види показників для оцінювання якості інформаційного середовища та критерії безпеки, достовірності і надійності; знати і вміти застосовувати види, рівні та типи тестування програмного забезпечення інформаційних систем, розуміти місце вразливостей програмного забезпечення в загальній парадигмі інформаційних систем та технологій; вміти розробляти елементи резервування і надмірності в інформаційних системах; здійснювати технічне діагностування компонентів та елементів інформаційних систем; вміти проєктувати системи забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.

Зміст навчальної дисципліни. Інформаційні технології та інформаційні системи в контексті наукових досліджень, їх позиціонування, обов'язкові елементи та взаємозв'язок. Якість інформаційних систем та технологій в контексті наукових досліджень. Надійність інформаційних систем та технологій. Забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.

Пререквізити – вихідна.
Постреквізити – інтелектуальні інформаційні системи і технології (ОФП.04), теорія і проєктування систем Інтернету речей (ОФП.05), педагогічна (викладацька) практика (ОФП.07).

Запланована навчальна діяльність: лекцій – 32 год., практичних занять – 34 год., самостійної роботи – 86 год.; разом – 120 год.
Форми (методи) навчання: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, інформаційно-комунікаційних технологій); лабораторні заняття (з використанням інструктування, демонстрування, розв'язування типових і прикладних задач, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: усне опитування, захисти лабораторних робіт, тестування, оцінювання індивідуального домашнього завдання

Вид семестрового контролю: залік

Навчальні ресурси:

1. Alzoubi, Haitham & Alshurideh, Muhammad & Akour, Iman & Al Shraah, Ata & Ahmed, Gouher. (2021). Impact of information systems capabilities and total quality management on the cost of quality. 24. 1-11.
2. Hovorushchenko, T., Voichur, Y., & Medzatyi, D. (2023). Information technology for prediction of software quality level. *Radioelectronic and Computer Systems, 0*(3), 238-254. doi:https://doi.org/10.32620/reks.2023.3.19
3. Khari, M.; Mishra, D.; Acharya, B.; Crespo, R. Optimization of Automated Software Testing Using Meta-Heuristic Techniques; Springer International Publishing: Berlin/Heidelberg, Germany, 2022.
4. Tworek, Katarzyna. (2020). Reliability of information systems in organizations as a factor shaping organizational culture. Argumenta Oeconomica. 2020. 259-274. 10.15611/aoe.2020.2.11.
5. I Kliushnikov, V Kharchenko, H Fesenko, E Zaitseva, V. Levashenko. Reliability Models of Multi-state UAV-based Monitoring Systems: Mission Efficiency Degradation Issues. 2023 International Conference on Information and Digital Technologies (IDT) 2023. – IEEE, P.299-306.
6. Стецюк М. В. Методи та засоби забезпечення відмовостійкості та живучості спеціалізованих інформаційних технологій в умовах впливів зловмисного програмного забезпечення. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Хмельницький національний університет, Хмельницький, 2022. https://nauka.khmnu.edu.ua/wp-content/uploads/dysertacziya-1.pdf
7. Kharchenko, V., Kovalenko, A., Ruchkov, E., Babeshko, I. (2021). Reliability Assessment of Multi-cascade Redundant Systems Considering Failures of Intermodular and Bridge Communications. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Theory and Engineering of Dependable Computer Systems and Networks. DepCoS-RELCOMEX 2021. Advances in Intelligent Systems and Computing, vol 1389. Springer, Cham. https://doi.org/10.1007/978-3-030-76773-0_18
8. Поморова, Оксана Вікторівна. Теоретичні основи, методи та засоби інтелектуального діагностування комп'ютерних систем : автореф. дис ... д-ра техн. наук : 05.13.13 / Оксана Вікторівна Поморова; Нац. ун-т "Львівська політехніка".– Львів : 2007.– 33 с.
9. Repp, P. (2017). The system of technical diagnostics of the industrial safety information network. Journal of Physics: Conference Series. 803. 012127. 10.1088/1742-6596/803/1/012127.
10. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773
11. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8861
12. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
13. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

Викладач: д-р. техн. наук, проф. Олег Савенко