

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Декан ФІТ

5

ЗАТВЕРДЖУЮ

Тетяна ГОВОРУЩЕНКО

09.09

2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій

Галузь знань 12 Інформаційні технології
(шифр) (назва)

Спеціальність 126 Інформаційні системи та технології очна денна форма здобуття освіти
(шифр) (назва)

Освітня програма Інформаційні системи та технології

Шифр дисципліни ОСП.06

Статус дисципліни: обов'язкова
(назва)

Факультет інформаційних технологій

Кафедра комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
ОД	1	1	4	Г20	51	17	34			69			+	

Робоча програма складена згідно стандарту вищої освіти зі спеціальності 126 Інформаційні системи та технології для третього рівня вищої освіти, освітньо-наукової програми та навчального плану

Програма складена Олег САВЕНКО
Підпис Ініціали, прізвище викладача(ів)

Схвалена на засіданні кафедри комп'ютерної інженерії та інформаційних систем

Протокол № 2 від 30 08 2024 р.

Зав. кафедри комп'ютерної інженерії та інформаційних систем

Підпис

Ірина ЗАСОРНОВА

Ім'я, прізвище

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Протокол № 1 від 05 09 2024 р.

Голова Вченої ради

Підпис

Тетяна ГОВОРУЩЕНКО

Ім'я, прізвище

Хмельницький 2024

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна "Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій" є дисципліною з циклу поглибленої професійної підготовки в галузі інформаційних технологій.

Мета 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.

Предмет дисципліни. Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій.

Завданнями дисципліни є: 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.

Після вивчення дисципліни студент має досягти таких результатів навчання та набути таких компетентностей та програмних результатів навчання:

Інтегральна. 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.

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК04. 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.

ФК01. Здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у ІСТ та дотичних до них міждисциплінарних напрямках з ІТ та суміжних галузей.

ФК02. 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.

ФК06. Здатність застосовувати сучасні методи дослідження, синтезу, проєктування інформаційних систем і технологій у науковій та науково-педагогічній діяльності.

ФК09. 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.

ПРН01. 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 напрямку, отримання нових знань та/або здійснення інноваційної діяльності.

ПРН02. 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.

ПРН03. 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.

ПРН04. 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 напрямках.

ПРН05. 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.

ПРН09. Застосовувати сучасні програмно-технічні засоби, зокрема для реалізації методів захисту комп'ютерної інформації при проєктуванні інформаційних систем та цифрових сервісів в різних предметних областях.

ПРН13. Аналізувати дані та знання для оптимізації інформаційних систем та цифрових сервісів, забезпечення їх надійності та безпеки.

Анотація дисципліни

ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Тип дисципліни

Рівень вищої освіти

Мова викладання

Семестр

Кількість встановлених кредитів ЄКТС

**Форми навчання, для яких викладається
дисципліна**

Обов'язкова

Третій (освітньо-науковий)

Українська

1

4,0

Очна денна

Результати навчання

Студент, який успішно завершив вивчення дисципліни, повинен отримати такі результати навчання:

ПРН01. 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 напрямку, отримання нових знань та/або здійснення інноваційної діяльності.

ПРН02. 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.

ПРН03. 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.

ПРН04. 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 напрямках.

ПРН05. 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.

ПРН09. Застосовувати сучасні програмно-технічні засоби, зокрема для реалізації методів захисту комп'ютерної інформації при проектуванні інформаційних систем та цифрових сервісів в різних предметних областях.

ПРН13. Аналізувати дані та знання для оптимізації інформаційних систем та цифрових сервісів, забезпечення їх надійності та безпеки.

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.

Запланована навчальна діяльність: лекції - 17 год., лабораторні заняття – 34 год., самостійна робота - 69 год.; разом – 120 год.

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і візуалізації); лабораторні заняття (з використанням методів проблемного навчання), самостійна робота (індивідуальні завдання).

Форми оцінювання результатів навчання: усне опитування, захисти лабораторних робіт

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., & Medzaty, 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. Електронна бібліотека університету. Доступ до ресурсу: <http://library.khmnu.edu.ua/>.

Викладач: д.т.н., проф. Олег САВЕНКО.

2. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні роботи	самостійну роботу
<i>Перший семестр</i>				
<i>Тема 1. Якість інформаційних систем та технологій.</i>	6	8	-	24
<i>Тема 2. Надійність інформаційних систем та технологій.</i>	8	16	-	32
<i>Тема 3. Забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.</i>	3	10	-	13
Разом за 1-ий семестр:	17	34	-	69

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1 Зміст лекційного курсу

Номер лекції	Перелік змістових модулів, тем лекцій, їх анотації	Кількість годин
	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. <i>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. Постановка, проведення та аналіз результатів експериментальних досліджень. 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.</i>	2
2	Лекція 2. Якість інформаційних систем та технологій як предметна область для наукових досліджень <i>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.</i> <i>Аналіз наукових публікацій та напрямів з дослідження якості</i>	2

	інформаційних систем та технологій. Вплив можливостей 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]. Тема 2. Надійність інформаційних систем та технологій.	2
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 ремонтпридатності. Основні математичні моделі ремонтпридатності. 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 ремонтпридатності. 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.	2

	<i>Перевірка відповідності середнього напруження на відмову технічним умовам. Перевірка відповідності середнього часу відновлення технічним умовам. Фактори, що впливають на надійність інформаційних систем.</i> <i>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].</i>	
5	Лекція 5. Проблеми та стратегії резервування і надмірності в інформаційних системах. <i>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.</i> <i>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].</i>	2
6	Лекція 6. Технічне діагностування компонентів та елементів інформаційних систем. <i>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.</i> <i>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].</i>	2

7	Лекція 7. Методології та стратегії забезпечення функційної безпеки. Резилентні системи. <i>Функційна безпека. Методи та стратегії забезпечення функційної безпеки інформаційних систем. Складові частини резилентних систем. Розроблення резилентних 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 безпека та кібербезпека.</i> <i>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].</i> Тема 3. Забезпечення кібербезпеки та захисту інформації в інформаційних системах та технологіях.	2
8	Лекція 8. Методології та наукові напрями кібербезпеки. <i>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.</i> <i>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].</i>	2
9	Лекція 9. Методи захисту інформації при проектуванні інформаційних систем та цифрових сервісів в різних предметних областях. <i>Проектування 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. Проектування 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.</i> <i>Метод виявлення комп'ютерних вірусів на основі інформації з PE-</i>	1

	<i>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 інформаційних системах. Методи ідентифікації аномальних станів для систем виявлення вторгнень [36], [38].</i>	
	Разом за 1-ий семестр:	17

3.2 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.	4
2	Лабораторне заняття 2. Дослідження методів оптимізації автоматизованого тестування програмного забезпечення.	4
3	Лабораторне заняття 3. Дослідження функційної безпеки та надійності інформаційних систем.	4
4	Лабораторне заняття 4. Вразливості інформаційних систем та цифрових сервісів і методи їх виявлення.	4
5	Лабораторне заняття 5. Розроблення інформаційних технологій з елементами надмірності та резервування.	4
6	Лабораторне заняття 6. Розроблення резилентних систем та методів організації їх функціонування.	4
7	Лабораторне заняття 7. Розподілені інформаційні системи для реалізації методів виявлення зловмисного програмного забезпечення в корпоративних мережах.	4
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.	4
9	Лабораторне заняття 9. Підсумкове заняття.	2
	Разом за 1-ий семестр:	34

3.3 Зміст самостійної (індивідуальної) роботи

Обсяг самостійної роботи з дисципліни в 1 семестрі становить 69 годин. Він включає опрацювання лекційного матеріалу, підготовку та виконання лабораторних робіт і їх захисту.

Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Вид самостійної роботи	К-ть годин
<i>Перший семестр</i>		
1	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	4
2	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	4
3	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №2.	4
4	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	4
5	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №3.	4
6	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №3.	4
7	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №4.	4
8	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №4.	4
9	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №5.	4
10	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №5.	4
11	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №6.	4
12	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №6.	4
13	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №7.	4
14	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №7.	4
15	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №8.	4
16	Опрацювання лекційного матеріалу. Самостійне опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №8.	4
17	Опрацювання лекційного матеріалу.	5
Разом за 1-ий семестр:		69

5. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться в основному словесними методами з використанням інформаційних технологій, а також, з використанням методів проблемного навчання і візуалізації. Лабораторні заняття проводяться з використанням інформаційних технологій, методів проблемного навчання і мають за мету – набуття студентами практичних навичок.

6. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять. Семестровий контроль проводиться у формі заліку. При цьому при виведенні остаточної оцінки враховуються результати поточного контролю.

Кожний вид роботи з дисципліни оцінюється за *чотирибальною* шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих *позитивно* з врахуванням коефіцієнта вагомості. Студент, який набрав позитивний середньозважений бал за поточну роботу, отримує залік з відповідним балом.

При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; засвоєння теоретичного матеріалу з тем перевіряється під час проведення лабораторних занять; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни і робочим навчальним планом.

Оцінка, яка виставляється за *лабораторне заняття*, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; вміння студента обґрунтувати прийняті конструктивні рішення. Для виконання програми дисципліни студент повинен отримати вісім позитивних оцінок за лабораторні роботи в семестрі. Пропущене лабораторне заняття студент повинен відпрацювати в лабораторіях кафедри у встановлений викладачем термін.

При *оцінюванні знань* студентів викладач керується такими критеріями.

Оцінку „зараховано”, за шкалою ECTS – A (див. шкалу оцінок), отримує студент за глибоке і повне опанування змісту навчального матеріалу, в якому він легко орієнтується, понятійного апарату, за уміння зв’язувати теорію з практикою, вирішувати практичні завдання, висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає грамотний, логічний виклад відповіді (як в усній, так і в письмовій формі), якісне зовнішнє оформлення. Студент повинен набути практичних навичок із застосування розглянутих методів в наукових та експериментальних дослідженнях. Оцінка "відмінно" виставляється студенту, який глибоко засвоїв навчальний матеріал та вміє його раціонально застосувати, знає методики та продемонстрував вміння самостійно освоювати інші методи, які не розглядалися в лекційному матеріалі. Студент не повинен вагатися при видозміні запитання, повинен робити детальні та узагальнюючі висновки.

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

Оцінку „зараховано”, за шкалою ECTS – C, отримує студент за правильну відповідь з однією суттєвою помилкою.

Оцінки „зараховано”, за шкалою ECTS – D, заслуговує студент, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, що справляється з виконанням

практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент слабо знає структуру курсу, допускає помилки у відповіді, засвоїв і набув практичних навичок у застосуванні навчального матеріалу, але допустив неточності. Вагається при відповіді на видозмінене запитання, разом з тим студент володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.

Оцінки „зараховано”, за шкалою ECTS – E, заслуговує студент за неповне опанування матеріалу, але отримані знання і набуті практичні навички із застосування навчального матеріалу.

Оцінка „незараховано”, за шкалою ECTS – FX, виставляється, коли студент має розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекидає їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткових знань з курсу.

Оцінка „незараховано”, за шкалою ECTS – F, виставляється студенту за повне незнання і нерозуміння навчального матеріалу або відмову від відповіді і передбачає повторне навчання студента з дисципліни.

Кожний вид роботи оцінюється за чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважене значення з усіх оцінок за лабораторні роботи.

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

Навчання студентів у семестрі за вибраними коефіцієнтами									
Аудиторна робота				Самостійна робота				Форма семестрового контролю	
1 семестр									
Лабораторні роботи №:								Залік	
1	2	3	4	5	6	7	8		
1								+	

Примітка: ВК – ваговий коефіцієнт.

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

Для переходу від вітчизняної оцінки до оцінки за шкалою ECTS необхідно знайти середньоарифметичну оцінку за вітчизняною шкалою, помножити її на відповідний ваговий коефіцієнт і, додавши всі складові, отримаємо суму балів, які визначають конкретну оцінку ECTS.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ECTS

Оцінка ECTS	Інституційна шкала балів	Інституційна оцінка	Критерії оцінювання
A	4,75–5,00	5	Відмінно – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навичок
B	4,25–4,74	4	Добре – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	Добре – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	Задовільно – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	Задовільно – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання

FX	2,00– 2,99	2	Незараховано	<i>Незадовільно</i> – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00– 1,99	2		<i>Незадовільно</i> – необхідна серйозна подальша робота і повторне вивчення дисципліни

7. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ СТУДЕНТІВ

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 ремонтпридатності. Основні математичні моделі ремонтпридатності.
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 резилентних 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. Проектування 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. Проектування 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 РЕ-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.

8. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

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

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.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. ДСТУ ISO/IEC 2382:2017 (ISO/IEC 2382:2015, IDT) Інформаційні технології. Словник термінів.
2. ДСТУ ISO/IEC 25001:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQaRE). Планування та керування (ISO/IEC 25001:2014, 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., & Medzaty, 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. Boukhelif 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. Janićić 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>

Додаткова література

1. ДСТУ ISO/IEC TR 24774:2016 Інженерія систем і програмних засобів. Керування життєвим циклом. Настанови щодо опису процесу (ISO/IEC TR 24774:2010, IDT).
2. ДСТУ ISO/IEC 15026-4:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 4. Гарантування в життєвому циклі (ISO/IEC 15026-4:2012, IDT)
3. ДСТУ ISO/IEC 15026-3:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 3. Рівні цілісності системи (ISO/IEC 15026-3:2015, IDT)

4. ДСТУ ISO/IEC/IEEE 16326:2015 Розроблення систем та програмного забезпечення. Процеси життєвого циклу. Керування проектами (ISO/IEC/IEEE 16326:2009, IDT)

5. ДСТУ ISO/IEC 15026-2:2018 Інженерія систем і програмних засобів. Гарантії стосовно систем і програмних засобів. Частина 2. Сценарій гарантування (ISO/IEC 15026-2:2011, IDT)

6. ДСТУ ISO/IEC 16085:2016 Інженерія систем і програмних засобів. Процеси життєвого циклу. Керування ризиками (ISO/IEC 16085:2006, IDT)

7. ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT)

8. ДСТУ ISO/IEC 30111:2016 Інформаційні технології. Методи захисту. Процеси оброблення вразливостей (ISO/IEC 30111:2013, IDT)

9. ДСТУ ISO/IEC 33001:2016 Інформаційні технології. Оцінювання процесу. Поняття та термінологія (ISO/IEC 33001:2015, IDT)

Інформаційні ресурси

Електронний університет:

1. Модульне середовище для навчання MOODLE. Доступ до ресурсу: <https://msn.khmnu.edu.ua>.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/page_lib.php.