СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Методи і засоби надійності програмного забезпечення»

Ступінь освіти	Доктор філософії
Освітньо-наукова	Інженерія програмного забезпечення
Тривалість викладання	Осінній семестр
Кількість кредитів	6 кредитів ЄКТС (180год)
Заняття:	3 семестр (5, 6 чв.)
лекції:	3 год./тижд.
практичні заняття:	2 год./тижд.
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/user/index.php?id=7192

Консультації: за окремим розкладом, що попередньо погоджений зі здобувачами освіти.
Онлайн-консультації: MS Teams, електронна пошта.

Інформація про викладача:

Викладач:
Бердник Михайло Геннадійович
д-р техн. наук, доц., професор каф. ПЗКС
Посилання на профіль:
Сторінка кафедри ПЗКС:
https://pzks.nmu.org.ua/ua/teachers/berdnikmg.php
Orcid ID:
https://orcid.org/0000-0003-4894-8995
Scopus ID:
https://www.scopus.com/authid/detail.uri?authorId=57196469717
Google Scholar:
https://scholar.google.com.ua/citations?view_op=list_works&hl=uk&user=WsH6aBMAAAAJ

1. Анотація курсу

Дисципліна спрямована на формування теоретичних знань і практичних навичок, необхідних майбутнім фахівцям для ефективного створення високонадійного програмного забезпечення. Під час вивчення дисципліни опрацьовуються методи забезпечення надійності та безпеки комп'ютерних систем, їх діагностики, як засобу підвищення надійності систем. Розглядаються способи технічного та програмного забезпечення надійності програмних систем. У проблематиці надійності програмних систем розроблено велику кількість математичних моделей надійності, які є функціями помилок, що залишились в програмних системах, інтенсивності відмов або частоти виникнення дефектів у програмних системах. На їх основі здійснюється оцінка надійності комп'ютерних систем. Відповідні навички теорії надійності комп'ютерних систем студенти використовують в результаті виконання різноманітних практичних завдань у своїй

професійній діяльності. В рамках вивчення курсу розглядаються такі питання: критерії надійності програмних систем, найбільш поширені закони розподілу часу, аналіз надійності складних систем, методи аналізу надійності систем, математичні моделі функціонування елементів і систем, технології розробки надійних програмних систем.

2. Мета та завдання навчальної дисципліни

Мета дисципліни – формування у здобувачів вищої освіти умінь та компетентностей щодо фундаментальних теоретичних положень і практичних аспектів забезпечення надійності, якості та безпеки програмного забезпечення та інформаційних систем, їх діагностики, як засобу підвищення надійності систем. Розглядаються способи технічного та програмного забезпечення надійності. Основними завданнями є вивчення теоретичних основ математичних методів теорії надійності, засвоєння здобувачами понять про методи моделювання, оцінки та оптимізації надійності технічних систем, отримання досвіду з аналізу показників надійності функціональних систем.

Завдання курсу:

– опанування теоретико-понятійної бази курсу;

– ознайомлення здобувачів з теоретичними основами математичних методів забезпечення надійності та безпеки комп'ютерних систем;

– засвоєння здобувачами понять про методи діагностики, як засобу підвищення надійності систем;

– засвоєння здобувачами понять та визначень теорії методів моделювання та оптимізація комп'ютерних і кіберфізичних систем і мереж;

– засвоєння здобувачами теоретичних основ математичних методів теорії надійності;

– засвоєння здобувачами понять про методи моделювання, оцінки та оптимізації надійності технічних систем;

–отримання досвіду з аналізу показників надійності функціональних систем.

3. Результати навчання

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

Пропонувати нові ефективні методи і моделі розроблення, впровадження, супроводу та забезпечення якості програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.

Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.

Формулювати та вирішувати задачі оптимізації, адаптації, прогнозування, керування та прийняття рішень щодо процесів, засобів та ресурсів розробки, впровадження, супроводу та експлуатації програмного забезпечення.

Розробляти, досліджувати та вдосконалювати програмні системи на основі моделей та засобів інтелектуальної обробки даних розподілених і масштабованих систем з урахуванням вимог до надійності їх структурно-алгоритмічного забезпечення.

Дисциплінарні результати навчання сформовано на основі ПРН освітньо-наукової програми «Інженерія програмного забезпечення» третього (освітньо-наукового) рівня вищої освіти (РН03, РН06, РН09, РН14).

4. Структура курсу

Вид заняття	Внесок в загальну оцінку, %
ЛЕКЦІЇ	**52**
Тема 1. Інформаційні технології, інформаційні системи та програмне забезпечення в контексті наукових досліджень, їх позиціонування, обов'язкові елементи та взаємозв'язок. Програмні системи в контексті об'єктів для розроблення в наукових дослідженнях. Концептуальні, математичні, імітаційні та комп'ютерні моделі процесів і систем. Позиціонування інформаційних систем та програмного забезпечення в наукових дослідженнях. Постановка, проведення та аналіз результатів експериментальних досліджень. Програмне забезпечення для обробки, зберігання, відображення даних. Стандарти з інформаційних технологій [1], [2]. Особливості академічної доброчесності при проведенні наукових досліджень.	
Тестова контрольна робота №1	**6**
Тема 2. Якість інформаційних систем, технологій та програмного забезпечення, як предметна область для наукових досліджень. Наукові аспекти поняття якості інформаційних систем, технологій та програмного забезпечення. Основні види показників для оцінювання якості інформаційного середовища. Критерії для оцінювання якості інформаційного середовища: безпека, достовірність і надійність. Дефекти та вразливості інформаційних систем та програмного забезпечення як їх складової. Вплив інженерії вимог на якість інформаційних систем та програмного забезпечення. Моделі якості програмного забезпечення. Характеристики якості. Стандарти якості. Процеси забезпечення якості. Керування якістю. Моделі оцінювання якості. Метрики для оцінювання якості програмних систем. Валідація і верифікація. Побудова оптимізаційної функції з врахуванням показників якості програмного забезпечення в інформаційних системах. Забезпечення якості програмного забезпечення в контексті виконання наукового дослідження. Аналіз наукових публікацій та напрямів з дослідження якості інформаційних систем, технологій та програмного забезпечення. 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].	
Тестова контрольна робота №2	**8**
Тема 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	

програмного забезпечення. 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. Порівняння витрат і ефективності різних методів тестування. Інструментальні засоби автоматизованого тестування. Напрями наукових досліджень за видами, рівнями та типами тестування програмного забезпечення. 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].	
Тестова контрольна робота №3	**8**
Тема 4. Моделі надійності та якості програмних систем. Методології управління якістю. Моделі якості програмних систем. Модель якості за Мак Колом. Модель якості за Боемом. Модель Ваттса. Модель Дьюча та Вілліса. Модель COQUALMO (Constructive Quality Model). Модель якості FURPS. Модель якості ISO 9126. Модель QEST. Схема GDQA. Стандартні показники якості. Методології управління якістю (Kaizen, LEAN/ Six Sigma, ISO, Zero Defect Programs, Total Quality Management, Quality Circle, Taguchi Methods та ін.). Root-Cause аналіз: основні цілі, методи та техніки (Five Whys, Fishbone diagram, Brainstorming, Affinity diagrams). Приклади напрямів наукових досліджень з систем та моделей якості програмного забезпечення. Внутрішня еволюція якості систем програмного забезпечення з відкритим кодом [13]. Моделі зрілості для практик забезпечення якості програмного забезпечення [14]. Оцінка змін якості системи під час еволюції програмного забезпечення: вплив шаблонів проектування, досліджених за допомогою аналізу залежностей [15].	
Тестова контрольна робота №4	**8**
Тема 5. Проблеми надійності програмного забезпечення 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. Комплексні показники надійності. Методи забезпечення надійності програмного забезпечення. Поняття структурної схеми надійності. Основні розрахункові співвідношення для показників безвідмовності. Наближені методи розрахунку показників безвідмовної роботи. 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. Фактори, що впливають на надійність програмного забезпечення. Приклади наукових досліджень з надійності програмного забезпечення. Надійність інформаційних систем в організаціях як фактор формування організаційної культури [16]. Підвищення безпеки та надійності інформаційних систем за допомогою технології блокчейн: тематичне дослідження щодо впливу та потенціалу [17]. Дослідження методу оцінки надійності системи високої надійності за трьома станами на основі попередньої інформації з багатьох джерел [18]. Моделі надійності систем моніторингу на основі БПЛА з декількома станами: проблеми зниження ефективності місії [19].	
Тестова контрольна робота №4	**8**
Тема 6. 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 програмного забезпечення з елементами надмірності та резервування. Використання надмірностей [20]. Стратегія гібридної відмовостійкості для мобільних розподілених систем [21]. Нова адаптивна відмовостійка структура в хмарі [22].	
Тестова контрольна робота №5	**8**
Тема 7. Методи захисту інформації при проектуванні інформаційних систем та цифрових сервісів, їх програмна реалізація в різних предметних областях. Проєктування інформаційних систем із засобами забезпечення стійкості до зловмисного програмного забезпечення. Проєктування розподілених систем виявлення комп'ютерних атак. Розроблення методів виявлення комп'ютерних атак. Інтеграція методів виявлення та розподілених систем в єдиний сенсор. 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 [23]. Методи побудови розподілених систем для виявлення комп'ютерних атак [24]. Методи безпеки аутентифікації та авторизації в інформаційних системах. Методи ідентифікації аномальних станів для систем виявлення вторгнень [25], [26].	
Тестова контрольна робота №7	**6**
ПРАКТИЧНІ ЗАНЯТТЯ	**48**
Практична робота 1 *(індивідуальне завдання)*	
Дослідження якості програмного забезпечення і реалізація методів	

оцінювання на основі відомих та удосконалених метрик.	
Захист практичної роботи №1	**8**
Практична робота 2 *(індивідуальне завдання)*	
Дослідження методів оптимізації автоматизованого тестування програмного забезпечення.	
Захист практичної роботи № 2	**8**
Практична робота 3 *(індивідуальне завдання)*	
Дослідження функційної безпеки та надійності інформаційних систем та програмного забезпечення як їх складової.	
Захист практичної роботи № 3	**8**
Практична робота 4 *(індивідуальне завдання)*	
Вразливості програмного забезпечення інформаційних систем та цифрових сервісів і методи їх виявлення.	
Захист практичної роботи № 4	**8**
Практична робота 5 *(індивідуальне завдання)*	
Розроблення інформаційних технологій з елементами надмірності та резервування.	
Захист практичної роботи № 5	**8**
Практична робота 6 *(індивідуальне завдання)*	
Застосовування сучасних програмно-технічних засобів, зокрема спеціалізованих, для реалізації методів захисту інформації при проектуванні програмного забезпечення та цифрових сервісів.	
Захист практичної роботи № 6	**8**
Загальна кількість	**100**

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп'ютерні пристрої.

Засоби дистанційної освіти: Moodle, MS Teams.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 – 89	добре
60 – 73	задовільно
0 – 59	незадовільно

Загальні критерії досягнення результатів навчання відповідають описам 8-го кваліфікаційного рівня НРК.

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни **на підставі поточного оцінювання знань** за умови, якщо набрана кількість балів з поточного тестування та виконання і захисту практичних робіт складатиме не менше 60 балів.

Теоретична частина оцінюється за результатами здачі 7 контрольних тестових робіт, кожна з яких містить тестові закриті запитання з однією вірною відповіддю (розподіл % за окремими контрольними роботами див. в таблиці розділу 4). Загалом за 7 контрольних тестових робіт отримується **максимум 52 бали**, тобто 52 % від оцінки за дисципліну.

Лабораторні роботи (6 робіт – у вигляді індивідуального завдання з кожної, розподіл % див. в таблиці розділу 4) виконуються у письмовому вигляді, загалом 6 лабораторних враховуються як 48% (максимум 48 балів). У сумі за лабораторну частину курсу при поточному оцінюванні отримується **максимум 48 балів**.

Отримані бали за теоретичну частину та лабораторні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

Максимальне оцінювання поточного контролю в балах:

Теоретична частина	Лабораторна частина	**Разом**
52	48	**100**

6.3. Критерії оцінювання підсумкової роботи. У випадку якщо здобувач вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку проводиться **підсумкове оцінювання (іспит)** під час сесії.

Іспит проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з **60 тестових завдань** з чотирма варіантами відповідей, одна правильна відповідь оцінюється в 1 бал **(разом 60 балів)** та **10 тестових завдань** з практичної частини, кожне з запитань оцінюється максимум у 4 бали **(разом 40 балів**), причому:

4 бали – відповідність еталону;

3 бали – відповідність еталону з незначними помилками;

2 бали – часткова відповідність еталону, питання повністю не розкрите;

1 бал – невідповідність еталону, але відповідність темі запитання;

0 балів – відповідь не наведена або не відноситься до теми запитання.

Отримані бали за запитання з теоретичної та практичної частини курсу додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 балів.

7. Політика курсу

7.1. Політика щодо академічної доброчесності. Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення

плагіату у Національному технічному університеті "Дніпровська політехніка" https://cutt.ly/IBesJEc

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2. Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану корпоративну університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання. Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання підсумкового оцінювання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять. З 24.02.2022 реалізація освітньої діяльності відбувається в умовах правового режиму воєнного стану. Наявна низка небезпек: повітряні тривоги, ризики припинення енергозабезпечення, мобільного та Інтернет-зв'язку. Згідно з наказами по університету у 2024-2025 навчальному році освітня діяльність здобувачів всіх форм навчання здійснюється з використанням дистанційних технологій через синхронні та асинхронні комунікації.

Відвідування онлайн лекцій та практичних занять реалізується через приєднання до «команди» Microsoft Teams. Під час повітряної тривоги заняття перериваються і продовжуються лише за умов перебування учасників освітнього процесу у захищених приміщеннях. Викладачем (за технічної та безпекової можливості) здійснюється запис заняття для підтримки асинхронного формату навчання.

У випадках відсутності енергозабезпечення, мобільного та Інтернет-зв'язку викладачем забезпечується асинхронний формат навчання та комунікація зі здобувачами за допомогою каналів зв’язку, що функціонують.

Про причини неможливості взяти участь в онлайн заняттях, ускладненні доступу до матеріалів на дистанційних платформах НТУ «ДП» тощо здобувач вищої освіти має повідомити викладача в особистих повідомленнях чатів Microsoft Teams, або листом на корпоративну е-пошту НТУ «ДП», або через старосту чи представника адміністрації факультету.

8. Рекомендовані джерела інформації

Базова:

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 (SQuaRE). 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., & 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. 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

14. Al MohamadSaleh, A.; Alzahrani, S. Development of a Maturity Model for Software Quality Assurance Practices. *Systems* 2023, *11*, 464. https://doi.org/10.3390/systems11090464

15. Alenezi, M. Internal Quality Evolution of Open-Source Software Systems. *Appl. Sci.* 2021, *11*, 5690. https://doi.org/10.3390/app11125690

16. 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.

17. 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

18. 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

19. 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.

20. 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

21. 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

22. 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

23. 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

24. 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

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

26. 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

27. 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.

28. Hsu, K.-H.; Szu-Tu, H.-C.; Tsai, C.-H. Assessing System Quality Changes during Software Evolution: The Impact of Design Patterns Explored via Dependency Analysis. *Electronics* 2024, *13*, 1444. https://doi.org/10.3390/electronics13081444

29.Робоча програма навчальної дисципліни "Технології та методи забезпечення надійності та безпеки інформаційних систем та технологій". Доступ до ресурсу: http://kiis.khmnu.edu.ua/wp-content/uploads/sites/31/rob_progr_tekhnolog_metody_istas_onp2024_v_scan_ppp.pdf

30. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

Додаткова:

1. Основи теорії надійності програмних систем. Навчальний посібник. / Яковина В. С., Сенів М. М. – Львів: Видавництво Львівської політехніки, 2020. 248 с.

2. Marvin Rausand, Anne Barros, Arnljot Hoyland. System reliability theory: models, statistical methods and applications. Wiley, 3rd edition, 2020. 864 p.

3. Ramesh Gulati. Maintenance and Reliability Best Practices. Industrial Press, 3rd edition, 2020. 768 p.

4. Aman Ullah. Software Reliability in Safety Critical Systems. OmniScriptum Publishing KS. 2016. – 60 p.

5. Hoang Pham. Statistical reliability engineering: methods, models and applications. Springer, 1st. edition, 2021. 517 p.

Shvachych G., Pobochii I., Khokhlova T., Kholod A., Moroz D. Multiprocessor Computing based Parallel Structures of Mathematical Models of Tridiagonal Systems. 5th International Conference on Inventive Computation Technologies. 2020. P. 1031–1035.

6. Shvachych G., Moroz B., Martynenko A., Hulina I., Busygin V., Moroz D. Model of Speed Spheroidization of Metals and Alloys Based on Multiprocessor Computing Complexes. Machine Learning for Predictive Analysis. Networks and Systems. Springer. 2020. P. 33–41.

7. Moroz. D. Research of the influence of a network interface on the efficiency of modular multiprocessor systems. Fundamental and applied research in the modern world : Abstracts of VIII International Scientific and Practical Conference. Boston, USA. 2021. P. 162–171.

8. Shvachych G., Pobochij I., Sazonova M., Bilyi O., Moroz D. Intelligent decision support system. International Academy Journal Web of Scholar. 2021. № 2 (52). P. 1–9. 5.

9. Shvachych G., Vozna N., Ivashchenko O., Bilyi O., Moroz D. Method of lines in distributed problems of experimental data processing. International Academy Journal Web of Scholar. 2021. № 2(52). P. 1–7. Режим доступу: https://rsglobal.pl/index.php/wos/article/view/1951/1759

10. Shvachych G., Vozna N., Ivashchenko O., Bilyi O., Moroz D. Efficient algorithms for parallelizing tridiagonal systems of equations. System technologies. Dnipro. 2021. № 5 (136). P. 110–119 .

11. Моделі, методи та засоби аналізу надійності програмних систем: монографія / В.С. Яковина, Д.В. Федасюк, М.М. Сенів, О.О. Нитребич. – Львів: Видавництво Львівської політехніки, 2015.-220с.

12. Ilia Vonta, Mangey Ram. Reliability Engineering: theory and applications (Advanced research in reliability and system assurance engineering). CRC Press, 1st edition, 2018, 228 p.

13. Nikolay Pavlov, Anton Iliev, Asen Rahnev and Nikolay Kyurkchiev. Some Software Reliability Models. OmniScriptum Publishing KS. 2018. – 124 p.

14. B.S. Dhillon. Enginnering Systems Reliability, Safety and Maintence An Integrated Approach. CRC Press, 1st edition. 2019. 298 p.

15. ДСТУ ISO/IEC TR 24774:2016 Інженерія систем і програмних засобів.

Керування життєвим циклом. Настанови щодо опису процесу (ISO/IEC TR 24774:2010, IDT).

16. 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)

17. 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)

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

19. 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)

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

21. 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)

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

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