

Робоча програма дисципліни «Тестування комп'ютерних засобів»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

120

Годин

Загальний обсяг дисципліни

4

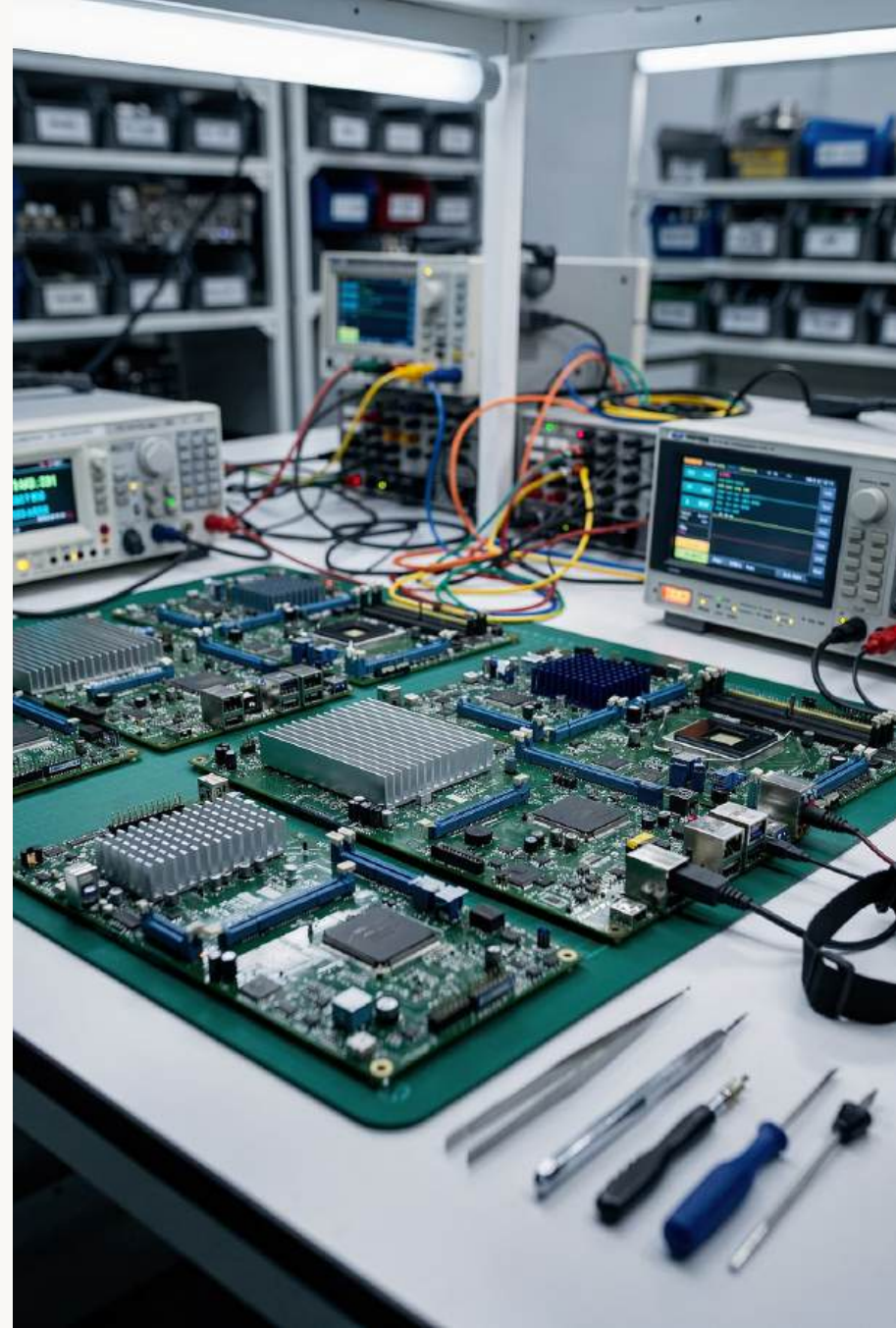
Кредити ЄКТС

Відповідно до стандарту

4

Модулі

Змістовних блоки курсу



Загальна інформація про дисципліну

Ідентифікація

Назва: Тестування комп'ютерних засобів

Спеціальність: 123 Комп'ютерна інженерія

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки

Лекції: 30 год. · **Лабораторні:** 30 год. · **СРС:** 60 год.

Призначення дисципліни

Дисципліна «Тестування комп'ютерних засобів» формує у студентів системне розуміння методів, засобів та технологій тестування апаратного і програмного забезпечення комп'ютерних систем. Курс охоплює теоретичні основи та практичні аспекти верифікації, валідації та діагностики комп'ютерних засобів — від окремих компонентів до інтегрованих систем.

Дисципліна є обов'язковою для підготовки бакалаврів зі спеціальності «Комп'ютерна інженерія» та забезпечує формування фахових компетентностей у сфері забезпечення якості та надійності комп'ютерних засобів.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання технічної інформації: виявлення причин відмов, порівняння методів тестування, формування обґрунтованих висновків щодо якості комп'ютерних засобів.

Комунікація

Здатність до усної та письмової комунікації: чітко описувати результати тестування, оформлювати технічні звіти та протоколи випробувань, аргументовано представляти висновки про стан комп'ютерних засобів.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання лабораторних і дослідницьких завдань у визначені строки, зокрема під час діагностики та тестування комп'ютерних компонентів.

Командна робота

Відповідальність, ініціативність та готовність працювати в команді під час проведення групових тестувань, розробки тест-планів та спільного аналізу результатів діагностики комп'ютерних засобів.

Студент повинен вміти: аналізувати технічну документацію та специфікації; застосовувати методи і засоби тестування апаратного та програмного забезпечення; планувати власну діяльність і дотримуватися термінів; коректно оформлювати звітну документацію; брати участь у командній роботі з діагностики та тестування комп'ютерних систем.

Фахові компетентності

Методи та засоби тестування

Розуміння сутності та методологічних основ тестування комп'ютерних засобів: знання видів тестування (функціональне, навантажувальне, стресове, регресійне), стандартів якості та підходів до верифікації і валідації апаратного і програмного забезпечення.

Діагностика апаратних засобів

Здатність виконувати діагностику апаратних компонентів комп'ютерних систем: процесорів, модулів пам'яті, накопичувачів, материнських плат та периферійних пристроїв із використанням спеціалізованих діагностичних інструментів і методик.

Тестування програмного забезпечення

Знання основ тестування програмного забезпечення: розробки тест-кейсів, тест-планів та звітів про дефекти; використання автоматизованих засобів тестування; оцінювання якості ПЗ відповідно до стандартів ISO/IEC. Розуміння зв'язку між тестуванням ПЗ та апаратним середовищем.

Стандарти та нормативно-технічна база

Орієнтування в нормативно-технічній базі у сфері тестування та забезпечення якості комп'ютерних засобів; використання міжнародних стандартів (ISO/IEC 25010, IEEE 829, ISTQB) для формування технічних висновків та рекомендацій.

Результати навчання

01

Пояснення базових концепцій тестування

Пояснювати сутність ключових понять і явищ: верифікація, валідація, тест-кейс, тест-план, дефект, покриття коду, регресійне тестування, навантажувальне тестування, надійність, відмовостійкість.

03

Аналіз результатів та звітність

Аналізувати результати тестування та діагностики комп'ютерних засобів; виявляти дефекти та несправності; складати технічні звіти, протоколи випробувань та формувати рекомендації щодо усунення виявлених проблем.

02

Застосування методів тестування

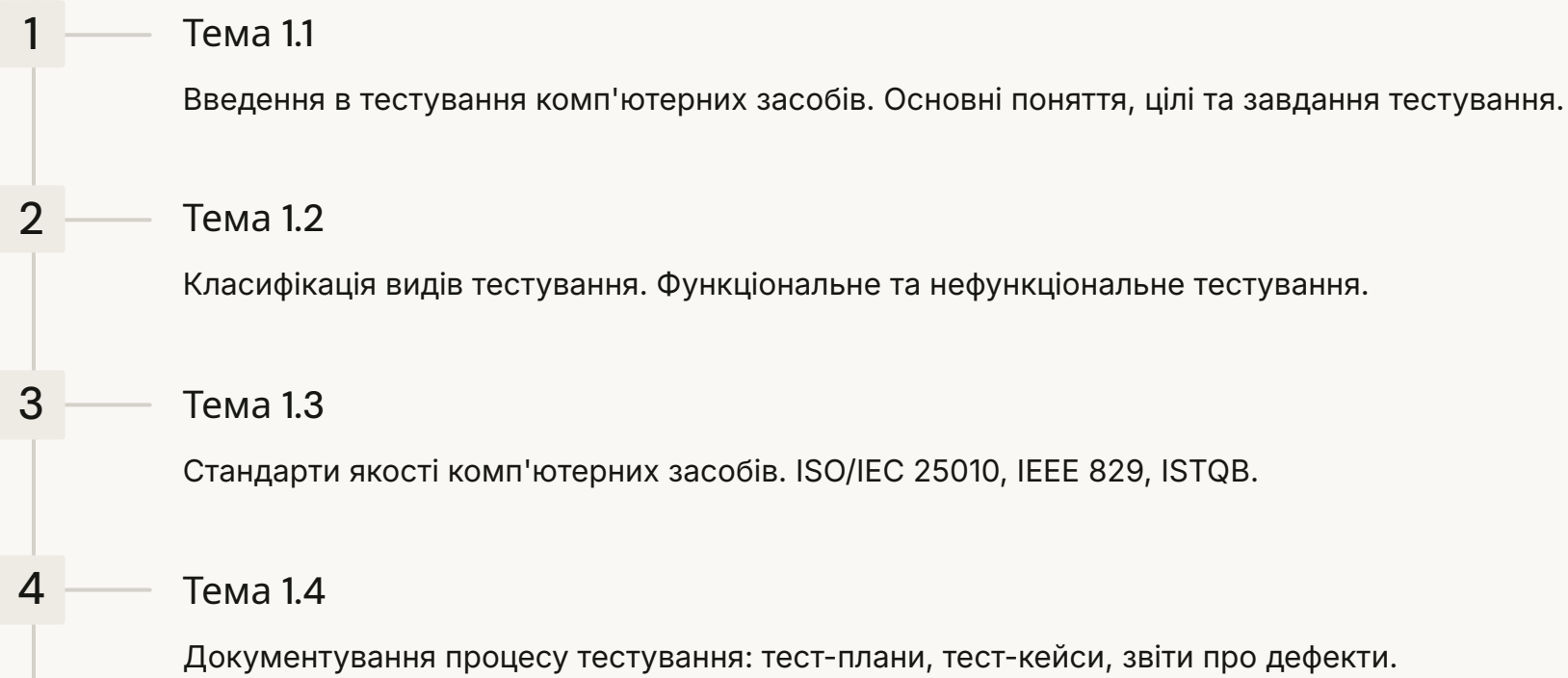
Застосовувати методи функціонального та нефункціонального тестування; розробляти тест-кейси та тест-плани; виконувати тестування апаратних компонентів і програмного забезпечення з використанням спеціалізованих інструментів.

04

Робота з інструментами та стандартами

Орієнтуватися в сучасних засобах автоматизованого тестування; використовувати міжнародні стандарти якості та нормативну документацію для обґрунтування технічних рішень у сфері тестування комп'ютерних засобів.

Основи тестування комп'ютерних засобів

- 
- 1 — Тема 1.1
Введення в тестування комп'ютерних засобів. Основні поняття, цілі та завдання тестування.
 - 2 — Тема 1.2
Класифікація видів тестування. Функціональне та нефункціональне тестування.
 - 3 — Тема 1.3
Стандарти якості комп'ютерних засобів. ISO/IEC 25010, IEEE 829, ISTQB.
 - 4 — Тема 1.4
Документування процесу тестування: тест-плани, тест-кейси, звіти про дефекти.

Введення в тестування комп'ютерних засобів

Лекційний матеріал (2 год.)

Лекція 1: Предмет та об'єкт дисципліни. Поняття «комп'ютерний засіб», «тестування», «якість». Цілі та завдання тестування: виявлення дефектів, верифікація, валідація. Місце тестування в життєвому циклі розробки ПЗ та апаратних систем. Принципи тестування (ISTQB). Психологія тестування.

Тестування vs. налагодження: різниця між пошуком дефектів та їх усуненням. Вартість виправлення дефектів на різних етапах розробки. Підходи до тестування: статичне та динамічне, ручне та автоматизоване.

Ключові питання лекції

- Основні поняття: тестування, якість, дефект, відмова, помилка
- Сім принципів тестування за ISTQB
- Місце тестування в SDLC та моделях розробки (V-модель, Agile)
- Статичне та динамічне тестування: відмінності та застосування
- Вартість дефектів та економіка тестування

Лабораторна робота (2 год.)

Завдання 1. Ознайомлення з інструментами тестування: огляд середовища для проведення тестів, встановлення та налаштування тестового оточення (TestLink, JIRA або аналоги).

Завдання 2. Практика складання першого тест-кейсу: опис умов, кроків відтворення, очікуваного результату. Аналіз прикладів реальних звітів про дефекти.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Основи тестування»
- Підготовка реферату: «Роль тестування у забезпеченні якості комп'ютерних засобів»
- Вивчення сімох принципів тестування ISTQB з практичними прикладами



Очікуваний результат: студент розуміє предмет дисципліни, знає базові поняття та принципи тестування комп'ютерних засобів.

Класифікація видів тестування

1

Функціональне тестування

Перевірка відповідності функцій системи вимогам специфікації. Smoke, Sanity, Regression.

2

Нефункціональне тестування

Продуктивність, навантаження, стрес-тестування, тестування безпеки та зручності використання.

3

Структурне тестування

Тестування «білої скриньки»: перевірка внутрішньої структури, покриття коду та гілок.

4

Тестування змін

Регресійне та повторне тестування після внесення змін до компонентів або системи.

Лекційний матеріал (2 год.)

Класифікація тестування за рівнями: модульне, інтеграційне, системне, приймальне. Класифікація за цілями: функціональне та нефункціональне. Тестування «чорної», «білої» та «сірої» скриньок. Моделі тест-дизайну: еквівалентне розбиття, граничні значення, таблиці рішень, попарне тестування (Pairwise).

Лабораторна робота (2 год.) та СРС (7 год.)

Лабораторна: Розробка тест-кейсів для тестування апаратного компонента (наприклад, модуля оперативної пам'яті) методами еквівалентного розбиття та граничних значень. Аналіз покриття.

СРС: Опрацювання: Цибульник С.О., Барандич К.С. «Технології розроблення програмного забезпечення» (Київ: КПІ ім. Ігоря Сікорського, 2022) — розділи щодо тест-дизайну; складання порівняльної таблиці методів тестування.

Стандарти якості та документування тестування

Тема 1.3 — Стандарти якості (Лекція 3, 2 год.)

Міжнародні стандарти у сфері тестування та якості комп'ютерних засобів: ISO/IEC 25010 (SQuaRE) — модель якості ПЗ та системи; IEEE 829 — стандарт документування тестування; ISTQB — міжнародна кваліфікаційна схема тестувальників. Стандарти ISO/IEC 9126, DO-178C для вбудованих систем. Показники та метрики якості.

Лабораторна (2 год.): Аналіз вимог до якості реального апаратного засобу за ISO/IEC 25010; побудова матриці відповідності вимог та тест-кейсів; оцінка метрик покриття.

СРС (7 год.): Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Стандарти якості»; підготовка реферату «ISO/IEC 25010 як основа оцінювання якості комп'ютерних засобів».

Тема 1.4 — Документування тестування (Лекція 4, 2 год.)

Тестова документація: тест-стратегія, тест-план, тест-кейс, чек-ліст, звіт про дефект (баг-репорт), підсумковий звіт тестування. Атрибути якісного тест-кейсу. Системи управління тестуванням: TestLink, Zephyr, TestRail. Системи відстеження дефектів: JIRA, Bugzilla, Redmine. Метрики тестування: кількість дефектів, щільність дефектів, відсоток покриття.

Лабораторна (2 год.): Розробка повного комплексу тестової документації для заданого апаратного або програмного компонента; оформлення звіту про знайдений дефект у системі відстеження.

СРС (7 год.): Опрацювання: Баран С.В. «Розробка програмного забезпечення з використанням патернів проектування» (Кривий Ріг, 2023) — методи структурування коду для тестованості; підготовка порівняльної таблиці систем управління тестуванням.

Тестування апаратних компонентів комп'ютерних систем

Тема 2.1

Методи та засоби діагностики процесорів, системних плат та модулів оперативної пам'яті.

Тема 2.2

Тестування накопичувачів (HDD, SSD, NVMe) та підсистеми введення-виведення.

Тема 2.3

Тестування відеосистем, мережевих адаптерів та периферійних пристроїв.

Тема 2.4

Комплексне тестування комп'ютерних систем. Стрес-тестування та стабільність.

Діагностика процесорів, системних плат та оперативної пам'яті

Лекційний матеріал (2 год.)

Методи тестування центральних процесорів: перевірка стабільності, температурного режиму, продуктивності. Інструменти: CPU-Z, HWMonitor, Prime95, LinX, AIDA64. Тестування системних (материнських) плат: перевірка POST, BIOS/UEFI, роз'ємів та шин. Тестування оперативної пам'яті: методи виявлення бітових помилок, інструменти MemTest86+, HCI Memtest. Типові несправності та методи їх локалізації.

Ключові питання

- Методи стрес-тестування процесора та оцінка стабільності
- Діагностика термічних відмов та перегріву
- POST-коди та діагностика системних плат
- Алгоритми тестування пам'яті: March, Galloping
- Інтерпретація результатів MemTest86+

Лабораторна робота (2 год.)

Завдання 1. Проведення стрес-тестування процесора за допомогою Prime95 або LinX: моніторинг температур, частот та споживання енергії, інтерпретація результатів.

Завдання 2. Тестування модуля оперативної пам'яті за допомогою MemTest86+: запуск повного циклу тестів, аналіз знайдених помилок, складання протоколу.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

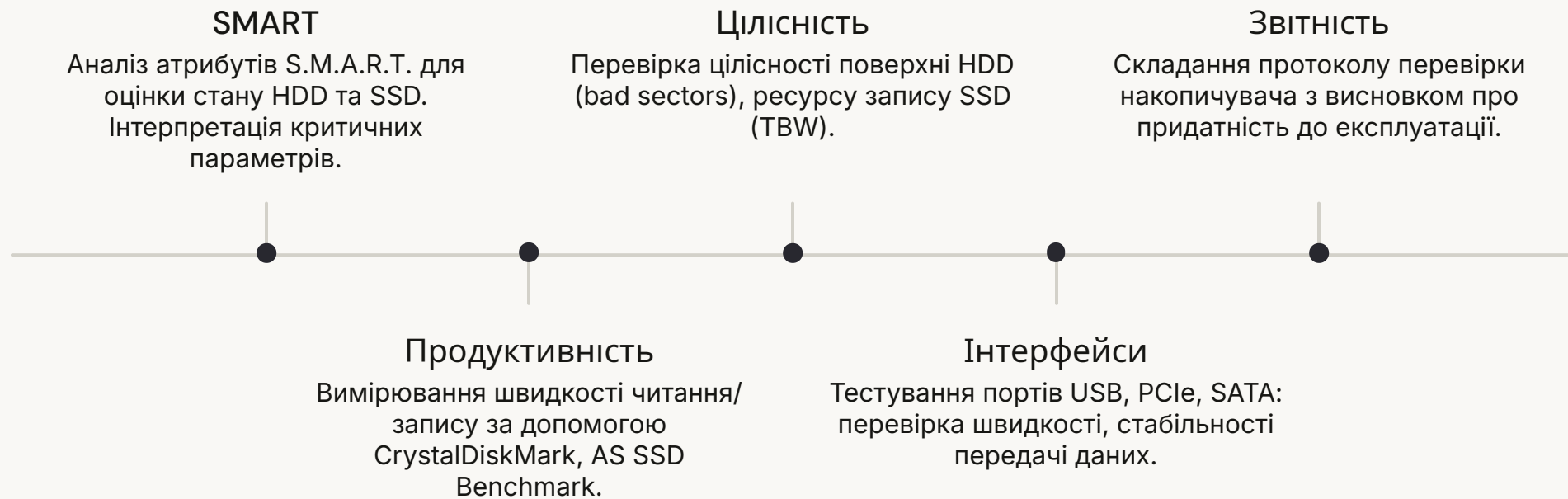
Самостійна робота (7 год.)

- Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Апаратне тестування»
- Підготовка реферату: «Методи виявлення та локалізації несправностей процесора та пам'яті»
- Складання хронологічної схеми алгоритму комплексної діагностики ПК



Очікуваний результат: студент вміє виконувати тестування процесорів та пам'яті, інтерпретувати результати і складати протоколи діагностики.

Тестування накопичувачів та підсистеми введення-виведення



Лекційний матеріал (2 год.)

Технології накопичувачів: HDD, SSD (NAND: SLC, MLC, TLC, QLC), NVMe, eMMC. Параметри SMART та їх значення для оцінки стану накопичувача. Методи тестування: перевірка швидкості, цілісності даних, поверхневого сканування. Інструменти: CrystalDiskInfo, CrystalDiskMark, HDDScan, Victoria HDD. Тестування інтерфейсів введення-виведення: USB, PCIe, SATA, Thunderbolt.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Комплексне тестування накопичувача: аналіз SMART-атрибутів, виміри швидкості читання/запису, поверхневе сканування; складання протоколу з висновком про технічний стан.

СРС: Опрацювання: Цибульник С.О., Барандич К.С. «Технології розроблення програмного забезпечення» (Київ: КПІ, 2022) — розділ «Тестування систем зберігання»; підготовка аналітичної записки «Порівняння методів тестування HDD та SSD накопичувачів».

Тестування відеосистем, мережевих адаптерів та комплексне тестування

Тема 2.3 — Відеосистеми та периферія (Лекція 7, 2 год.)

Тестування відеокарт: бенчмаркінг (3DMark, Unigine Superposition), перевірка стабільності під навантаженням, моніторинг температур GPU. Тестування моніторів: Dead Pixel Test, перевірка рівномірності підсвічування.

Тестування мережевих адаптерів: пропускна здатність, затримки, втрата пакетів (iperf3, ping, traceroute).

Тестування периферійних пристроїв: принтери, сканери, маніпулятори.

Лабораторна (2 год.): Проведення бенчмаркінгу відеокарти за допомогою 3DMark або Furmark; тестування мережевого адаптера за допомогою iperf3; інтерпретація результатів та складання звіту.

СРС (7 год.): Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024); підготовка реферату «Методи тестування відеопідсистеми та мережевих компонентів».

Тема 2.4 — Комплексне тестування системи (Лекція 8, 2 год.)

Комплексне тестування комп'ютерної системи як цілісного об'єкта. Стрес-тестування системи: AIDA64 Stability Test, комбіноване навантаження на CPU+GPU+RAM+Storage. Оцінка теплового режиму та стабільності під тривалим навантаженням. Метод «виключення компонентів» для локалізації несправностей. Складання комплексного протоколу технічного стану ПК.

Лабораторна (2 год.): Проведення комплексного стрес-тесту системи за допомогою AIDA64; моніторинг всіх ключових параметрів; складання зведеного протоколу технічного обстеження комп'ютера з висновками та рекомендаціями.

СРС (7 год.): Підготовка аналітичної записки «Методологія комплексного тестування персонального комп'ютера: послідовність, інструменти, критерії оцінки».

Тестування програмного забезпечення комп'ютерних засобів

Тема 3.1

Функціональне тестування ПЗ. Методи «чорної скриньки». Розробка тест-кейсів за специфікацією вимог.

Тема 3.2

Структурне тестування ПЗ. Методи «білої скриньки». Покриття коду та аналіз гілок виконання.

Тема 3.3

Нефункціональне тестування: продуктивність, навантаження, безпека, зручність використання.

Тема 3.4

Верифікація та валідація вбудованого ПЗ (firmware, BIOS/UEFI, драйвери) комп'ютерних засобів.

Функціональне тестування програмного забезпечення

Лекційний матеріал (2 год.)

Функціональне тестування: визначення, цілі, місце в SDLC. Методи тестування «чорної скриньки»: еквівалентне розбиття, аналіз граничних значень, таблиці рішень, тестування переходів між станами, use case-тестування. Розробка тест-кейсів на основі специфікації вимог. Smoke-тестування та Sanity-тестування. Критерії завершення тестування.

Ключові питання

- Методи тест-дизайну для функціонального тестування
- Розробка тест-кейсів на основі вимог
- Smoke та Sanity тестування: відмінності та застосування
- Критерії входу та виходу з тестування
- Пріоритизація тест-кейсів

Лабораторна робота (2 год.)

Завдання 1. Розробка тест-кейсів для функціонального тестування заданого програмного компонента (наприклад, утиліти діагностики) методами еквівалентного розбиття та граничних значень.

Завдання 2. Виконання тестування за розробленими тест-кейсами, фіксація результатів, оформлення звіту про дефекти у системі відстеження.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Функціональне тестування»
- Підготовка реферату: «Методи тест-дизайну: порівняльний аналіз ефективності»
- Складання повного набору тест-кейсів для визначеного програмного модуля



Очікуваний результат: студент вміє розробляти тест-кейси методами «чорної скриньки» та виконувати функціональне тестування ПЗ.

Структурне тестування програмного забезпечення

Лекційний матеріал (2 год.)

Структурне тестування («біла скринька»): визначення, принципи.
Критерії покриття: покриття операторів, гілок, шляхів, умов. Юніт-тестування: фреймворки (JUnit, NUnit, PyTest, Google Test).
Мутаційне тестування як метод оцінки якості тестового набору.
Інструменти аналізу покриття коду: gcov, Istanbul, JaCoCo.
Інтеграційне тестування: стратегії (знизу-вгору, зверху-вниз, «великий вибух»).

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Розробка юніт-тестів для заданого програмного модуля з використанням обраного фреймворку; вимірювання покриття коду; аналіз непокритих гілок та розробка додаткових тест-кейсів.

СРС: Опрацювання: Цибульник С.О., Барандич К.С. «Технології розроблення програмного забезпечення» (Київ: КПІ, 2022) — розділи з юніт-тестування; підготовка аналітичної записки «Інструменти вимірювання покриття коду: порівняльна характеристика».

- ❑ **Очікуваний результат:** студент вміє розробляти юніт-тести, вимірювати покриття коду та інтерпретувати результати структурного тестування.

Нефункціональне тестування та верифікація вбудованого ПЗ

Тема 3.3 — Нефункціональне тестування (Лекція 11, 2 год.)

Навантажувальне та стрес-тестування ПЗ: інструменти Apache JMeter, Locust, k6. Тестування продуктивності: метрики (час відповіді, пропускна здатність, використання ресурсів). Тестування безпеки: OWASP Top 10, інструменти SAST/DAST. Тестування зручності використання (Usability Testing). Тестування сумісності та портабельності. Тестування надійності та відмовостійкості.

Лабораторна (2 год.): Проведення навантажувального тестування веб-сервісу за допомогою Apache JMeter або Locust; побудова графіків часу відповіді та пропускну здатності; визначення точки деградації системи.

СРС (7 год.): Опрацювання: Трофименко О.Г., Дика А.І. (Одеса: Фенікс, 2024) — розділ «Нефункціональне тестування»; підготовка есе «Тестування безпеки ПЗ: методи та інструменти».

Тема 3.4 — Верифікація вбудованого ПЗ (Лекція 12, 2 год.)

Вбудоване програмне забезпечення (firmware): BIOS/UEFI, мікропрограми периферії, драйвери. Особливості тестування вбудованого ПЗ. Верифікація оновлень BIOS/UEFI: процедура, ризики, відкат. Тестування драйверів пристроїв: функціональне, стабільності, сумісності. Стандарти для вбудованих систем: DO-178C, IEC 61508. Тестування UEFI за допомогою SCT (UEFI Self Certification Tests).

Лабораторна (2 год.): Верифікація версії BIOS/UEFI, тестування стабільності після оновлення мікропрограми; перевірка драйверів пристрою на сумісність та стабільність.

СРС (7 год.): Підготовка аналітичної записки «Ризики оновлення firmware та методи їх мінімізації при тестуванні комп'ютерних засобів».

Автоматизація тестування та сучасні підходи до забезпечення якості

Тема 4.1

Автоматизоване тестування: принципи, інструменти, фреймворки. Selenium, Playwright, Cypress.

Тема 4.2

CI/CD та тестування в умовах безперервної інтеграції. DevOps підходи до забезпечення якості.

Тема 4.3

Тестування комп'ютерних мереж та телекомунікаційних засобів. Протоколи та інструменти.

Тема 4.4

Сучасні тенденції: AI-assisted testing, тестування IoT-пристроїв, хмарних та вбудованих систем.

Автоматизоване тестування: принципи та інструменти

Лекційний матеріал (2 год.)

Поняття автоматизованого тестування. Переваги та обмеження автоматизації. Критерії вибору тест-кейсів для автоматизації. Піраміда тестування (Unit → Integration → E2E). Фреймворки автоматизації UI-тестування: Selenium WebDriver, Playwright, Cypress. Фреймворки API-тестування: Postman, RestAssured. Page Object Model як патерн проектування тестів. Основи написання автотестів на Python/Java.

Ключові питання

- Критерії доцільності автоматизації тест-кейсів
- Піраміда тестування та її практичне застосування
- Архітектура Selenium WebDriver
- Page Object Model: реалізація та переваги
- Підтримка та розвиток автотестів

Лабораторна робота (2 год.)

Завдання 1. Розробка автоматизованого тесту для веб-застосунку або утиліти діагностики за допомогою Selenium або Playwright: написання сценарію, запуск, аналіз результатів.

Завдання 2. Реалізація патерну Page Object Model для організації автотестів. Рефакторинг наявних тест-кейсів.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (7 год.)

- Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Автоматизація»
- Підготовка реферату «Порівняння фреймворків автоматизованого тестування: Selenium, Playwright, Cypress»
- Розробка автоматизованого тест-сюиту для заданого компонента



Очікуваний результат: студент вміє розробляти автоматизовані тести та застосовувати патерни організації тестового коду.

CI/CD та DevOps–підходи до забезпечення ЯКОСТІ



Commit & Build

Розробник вносить зміни → автоматичний збір проекту (Jenkins, GitLab CI, GitHub Actions).



Automated Testing

Автоматичний запуск юніт-тестів, інтеграційних та E2E тестів у конвеєрі CI/CD.



Report & Feedback

Формування звітів про результати тестування, сповіщення команди про дефекти та регресії.

Лекційний матеріал (2 год.)

Концепції DevOps та Agile QA. Безперервна інтеграція (CI) та безперервне постачання (CD). Інтеграція тестів у конвеєри: Jenkins, GitLab CI/CD, GitHub Actions. Shift-left testing — рання інтеграція тестування. TDD (Test-Driven Development) та BDD (Behaviour-Driven Development). Docker та контейнеризація для ізольованого тестового середовища. Моніторинг якості в продакшн-середовищі.

Лабораторна (2 год.) та СРС (7 год.)

Лабораторна: Налаштування простого CI-конвеєра (GitHub Actions або GitLab CI) з автоматичним запуском тест-сьюту при кожному коміті; аналіз звітів та налаштування сповіщень.

СРС: Опрацювання: Баран С.В. «Розробка програмного забезпечення з використанням патернів проектування» (Кривий Ріг, 2023) — розділи DevOps і CI; підготовка аналітичної записки «DevOps та зсув тестування вліво: переваги для якості комп'ютерних засобів».

Тестування комп'ютерних мереж та телекомунікаційних засобів

Лекційний матеріал (2 год.)

Методи тестування комп'ютерних мереж: перевірка пропускної здатності, затримки, втрати пакетів. Інструменти: iperf3, Wireshark, Nmap, ping, traceroute, MTR. Тестування мережевого обладнання: комутатори, маршрутизатори, точки доступу Wi-Fi. Тестування мережевих протоколів: TCP/IP, HTTP/HTTPS, DNS. Аналіз мережевого трафіку. Тестування VPN та безпеки мережі. Тестування QoS (Quality of Service).

Ключові питання

- Метрики якості мережі: пропускна здатність, затримка, джитер
- Аналіз мережевих пакетів за допомогою Wireshark
- Тестування Wi-Fi: рівень сигналу, перешкоди, пропускна здатність
- Сканування мережі та виявлення вразливостей (Nmap)
- Тестування мережевого обладнання на відмовостійкість

Лабораторна робота (2 год.)

Завдання 1. Аналіз мережевого трафіку за допомогою Wireshark: захоплення пакетів, фільтрація, виявлення аномалій та проблем продуктивності.

Завдання 2. Вимірювання параметрів мережі за допомогою iperf3: пропускна здатність, затримка, джитер; складання протоколу тестування мережевого сегменту.

Завдання 3. Тестування мережевої сумісності та безпеки за допомогою Nmap: сканування відкритих портів, виявлення служб.

Самостійна робота (7 год.)

- Опрацювання: Кулаков Ю.О. «Комп'ютерні мережі» (Київ: КПІ ім. Ігоря Сікорського, 2022) — розділи щодо тестування та діагностики мереж
- Підготовка реферату «Методи тестування бездротових мереж Wi-Fi 6/6E»
- Аналіз захопленого трафіку: виявлення та опис аномалій



Очікуваний результат: студент вміє тестувати комп'ютерні мережі, аналізувати трафік та складати протоколи тестування мережевого обладнання.

Сучасні тенденції: AI-assisted testing, IoT та хмарні системи

Лекційний матеріал (2 год.)

Використання штучного інтелекту та машинного навчання в тестуванні (AI-assisted testing): генерація тест-кейсів, самолікування тестів, аналіз результатів. Тестування IoT-пристроїв: особливості, протоколи (MQTT, CoAP), інструменти. Тестування хмарних систем (Cloud Testing): AWS, Azure, Google Cloud. Тестування мобільних застосунків. Тестування вбудованих систем та мікроконтролерів (Arduino, STM32). Перспективи розвитку тестування комп'ютерних засобів.

Ключові питання

- AI у тестуванні: можливості та обмеження
- Особливості тестування IoT-пристроїв
- Тестування хмарних рішень: масштабованість та відмовостійкість
- Тестування мікроконтролерних систем
- Тренди та перспективи QA-індустрії

Лабораторна робота (2 год.)

Завдання 1. Тестування IoT-сценарію: перевірка взаємодії пристрою з протоколом MQTT, тестування стабільності з'єднання та цілісності даних.

Завдання 2. Підготовка та захист міні-проекту: «Сучасні підходи до автоматизованого тестування комп'ютерних засобів — огляд інструментів та практичні рекомендації».

Завдання 3. Дискусія: «Як AI змінює роль тестувальника в IT-індустрії?»

Самостійна робота (7 год.)

- Опрацювання: Трофименко О.Г., Дика А.І. «Тестування та забезпечення якості програмних систем» (Одеса: Фенікс, 2024) — розділ «Сучасні тенденції»
- Підготовка аналітичної записки «Тестування IoT-пристроїв: методологія та інструменти»
- Аналіз AI-інструментів для автоматизованого тестування: Testim, Mabl, Applitools



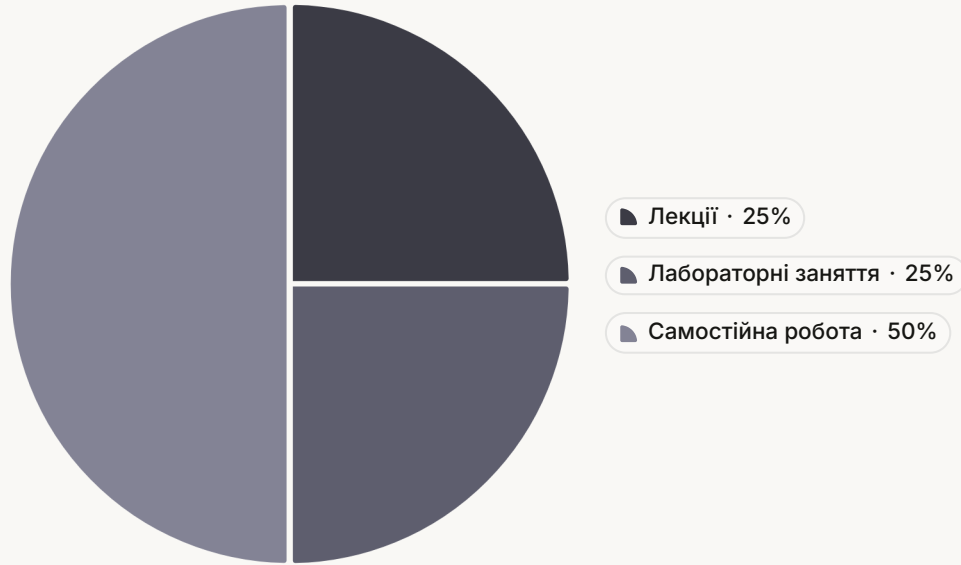
Очікуваний результат: студент орієнтується в сучасних тенденціях тестування, може обрати відповідні інструменти для тестування IoT та хмарних систем.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Введення в тестування	2	2	7
	Тема 1.2 — Класифікація видів тестування	2	2	7
	Тема 1.3 — Стандарти якості	2	2	7
	Тема 1.4 — Документування тестування	2	2	7
Модуль 2	Тема 2.1 — Процесори, плати та пам'ять	2	2	7
	Тема 2.2 — Накопичувачі та введення-виведення	2	2	7
	Тема 2.3 — Відеосистеми та мережеві адаптери	2	2	7
	Тема 2.4 — Комплексне тестування системи	2	2	7
Модуль 3	Тема 3.1 — Функціональне тестування ПЗ	2	2	7
	Тема 3.2 — Структурне тестування ПЗ	2	2	7
	Тема 3.3 — Нефункціональне тестування	2	2	7
	Тема 3.4 — Верифікація вбудованого ПЗ	2	2	7
Модуль 4	Тема 4.1 — Автоматизоване тестування	2	4	7
	Тема 4.2 — CI/CD та DevOps QA	2	2	7
	Тема 4.3 — Тестування мереж	2	2	7
	Тема 4.4 — AI-testing, IoT, хмарні системи	2	2	7
Разом	16 тем	30	30	60

 **Загальний обсяг: 120 годин = 4 кредити ЄКТС.** Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **120 годин (4 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

Лекції — 30 год. (25%)

Системне подання теоретичного матеріалу: методи та засоби тестування, стандарти якості, інструментальна база — з використанням схем, таблиць та прикладів із реальної практики.

Лабораторні — 30 год. (25%)

Практичне відпрацювання навичок діагностики апаратних засобів, розробки тест-кейсів, автоматизованого тестування та аналізу результатів. Рівна частка з лекціями підкреслює практичну спрямованість курсу.

Самостійна робота — 60 год. (50%)

Поглиблене вивчення, підготовка звітів та рефератів, робота з інструментами та науковою літературою. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис



Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками (Трофименко, Цибульник, Баран, Кулаков та ін.), стандартами ISO/IEC та ISTQB, науковими статтями у фахових виданнях. Студент конспектує ключові положення, виділяє головні поняття та порівнює підходи різних авторів.



Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: ISTQB (istqb.org), IEEE Standards (standards.ieee.org), Національної бібліотеки України (nbuv.gov.ua), репозиторіїв КПІ (ela.kpi.ua). Аналіз наукових статей та пошук актуальної інформації про методи та інструменти тестування.



Індивідуальні завдання

Виконання аналітичних завдань (порівняльний аналіз інструментів, розробка тест-планів, аналіз результатів діагностики); творчих завдань — реферати, аналітичні записки, міні-дослідження з тестування комп'ютерних засобів та актуальних методів QA.



Підготовка до занять

Підготовка до лабораторних робіт (попереднє опрацювання теорії та методів); підготовка до тестувань (ключові терміни та концепції); підготовка до контрольних робіт за кожним модулем (систематизація знань, вирішення типових задач діагностики).

Форми контролю знань

1

Поточний контроль

Завдання: тестові та практичні вправи за темами змістовного модуля.

Оцінюються якість виконання лабораторних робіт, звіти про тестування, рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань) або захисту лабораторної роботи.

2

Проміжний контроль

Комплексне завдання або реферат, що охоплює теми змістовного модуля (теоретичні питання, розробка тест-плану, аналіз результатів тестування).

Оцінюються повнота відповіді, обґрунтованість та практична застосованість висновків. Проводиться після завершення кожного змістовного модуля.

3

Підсумковий контроль

Іспит відповідно до навчального плану. Форма проведення — тестування та письмові відповіді на питання.

Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Тестування комп'ютерних засобів» поєднує класичні академічні та інтерактивні методи, що забезпечує формування як теоретичної бази, так і практичних навичок тестування, необхідних для майбутньої професійної діяльності в сфері комп'ютерної інженерії та ІТ.



Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць та реальних прикладів; студенти ведуть конспекти та задають уточнювальні запитання.



Лабораторні роботи

Практичне відпрацювання навичок тестування апаратних та програмних компонентів у спеціалізованих лабораторіях; застосування реальних інструментів та методик.



Кейс-стаді

Аналіз реальних ситуацій виявлення дефектів та несправностей; студенти виявляють проблему, пропонують методи тестування та обґрунтовують висновки.



Дискусії

Обговорення дискусійних питань у сфері забезпечення якості та тестування; розвиток критичного мислення та аргументації щодо вибору інструментів і методів.



Самостійне дослідження

Підготовка аналітичних записок, рефератів і звітів; розвиток навичок самостійного пошуку та систематизації інформації у сфері тестування та QA.



Проектна робота

Розробка міні-проектів з автоматизації тестування; формування навичок командної роботи, планування та реалізації тестових стратегій.



Усі методи спрямовані на формування компетентностей, передбачених освітньо-професійною програмою спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література — Підручники та посібники (2022–2024 рр.)

1. Трофименко О.Г., Дика А.І.

Тестування та забезпечення якості програмних систем : навч. посібник / Нац. ун-т «Одеська юридична академія». — Одеса : Фенікс, 2024. — 195 с. DOI: 10.32837/11300.27717

2. Цибульник С.О., Барандич К.С.

Технології розроблення програмного забезпечення : Підручник. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 270 с. URL: ela.kpi.ua

3. Баран С.В.

Розробка програмного забезпечення з використанням патернів проектування : Навчальний посібник. — Кривий Ріг : Державний університет економіки і технологій, 2023. — 203 с.

4. Кулаков Ю.О.

Комп'ютерні мережі : навчальний посібник. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 247 с. URL: ela.kpi.ua

5. Трофименко О.Г., Дика А.І., Лобода Ю.Г.

Аналіз інструментів тестування вебзастосунків. // Кібербезпека: освіта, наука, техніка. — 2023. — № 4(20). — С. 62–71. DOI: 10.28925/2663-4023.2023.20.6271

6. Трофименко О.Г., Пастернак Ю.Ю., Манаков С.Ю., Лобода Ю.Г.

Автоматизація тестування вебсайтів електронної комерції. // Сучасна спеціальна техніка. — 2022. — № 2(65). — С. 46–59. DOI: 10.36486/mst2411-3816

7. Кузьмніх В.О., Коваль О.В., Тараненко Р.А.

Управління версіями програмних засобів проекту : навчальний посібник. — Київ : КПІ ім. Ігоря Сікорського, 2022. — 141 с. URL: ela.kpi.ua

8. Доценко С.І.

Організація та системи керування базами даних : навчальний посібник. — Харків : УкрДУЗТ, 2023. — 117 с. (Рекомендується для тем 3.1–3.2)

Нормативно-правова база та офіційні ресурси

→ Закон України «Про стандартизацію» від 05.06.2014 № 1315-VII

Визначає правові та організаційні засади стандартизації в Україні, у т.ч. у сфері ІТ та комп'ютерних засобів. zakon.rada.gov.ua

→ Закон України «Про технічні регламенти та оцінку відповідності» від 15.01.2015 № 124-VIII

Регулює порядок технічного регулювання та підтвердження відповідності комп'ютерних засобів. zakon.rada.gov.ua

→ ДСТУ ISO/IEC 25010:2023

Системна та програмна інженерія. Вимоги до якості та оцінювання систем та програмного забезпечення (SQuaRE). Модель якості систем та програмного забезпечення.

→ IEEE Std 829 — Standard for Test Documentation

Міжнародний стандарт документування тестування програмного забезпечення. Визначає структуру тест-плану, тест-кейсу та звіту про тестування.

→ Закон України «Про освіту» від 05.09.2017 № 2145-VIII

Визначає засади освітньої діяльності в Україні, у т. ч. підготовку бакалаврів за спеціальністю 123. zakon.rada.gov.ua

Офіційні ресурси та фахові видання

ISTQB — International Software Testing Qualifications Board

istqb.org — міжнародна кваліфікаційна схема тестувальників, офіційні силабуси, глосарії, стандарти та методичні матеріали.

Репозиторій КПІ ім. Ігоря Сікорського

ela.kpi.ua — відкритий доступ до навчальних посібників, конспектів лекцій та методичних матеріалів з інформаційних технологій.

Національна бібліотека України ім. В. І. Вернадського

nbuv.gov.ua — електронні ресурси, наукові статті, монографії з комп'ютерних наук та інформаційних технологій.

Міністерство освіти і науки України

mon.gov.ua — освітні стандарти, навчальні програми, методичні матеріали для спеціальності 123 «Комп'ютерна інженерія».

Журнал «Кібербезпека: освіта, наука, техніка»

csecurity.kubg.edu.ua — фахове видання з актуальних питань кібербезпеки та тестування програмних систем.

IEEE Xplore Digital Library

ieeexplore.ieee.org — стандарти IEEE, наукові статті та матеріали конференцій з комп'ютерної інженерії та тестування.

ResearchGate — Українські публікації

researchgate.net — наукові публікації українських дослідників у сфері тестування програмного забезпечення та комп'ютерних засобів.

Держстандарт України (ДП «УкрНДНЦ»)

uas.org.ua — державні стандарти України (ДСТУ) у сфері інформаційних технологій та комп'ютерної техніки.

Зв'язок дисципліни зі спеціальністю 123 «Комп'ютерна інженерія»

Чому «Тестування комп'ютерних засобів» для інженерів?

Дисципліна є невід'ємною складовою підготовки бакалаврів зі спеціальністю 123 «Комп'ютерна інженерія». Уміння якісно тестувати та діагностувати комп'ютерні засоби — ключова навичка для інженера, що відповідає за надійність, продуктивність та безпеку апаратно-програмних комплексів.

Сучасний фахівець у сфері комп'ютерної інженерії повинен вміти не лише розробляти, але й верифікувати та валідувати рішення, що є критично важливим для забезпечення якості кінцевого продукту та задоволення вимог замовника.

Практичне значення для майбутньої кар'єри

- Діагностика та технічне обслуговування комп'ютерних систем і мереж
- Робота QA-інженером або тест-менеджером у IT-компаніях
- Забезпечення якості вбудованих систем та IoT-пристроїв
- Розробка та впровадження автоматизованих систем тестування
- Відповідність продуктів міжнародним стандартам якості ISO/IEC
- Навички роботи з інструментами CI/CD та DevOps-культура

Ключові компетентності курсу — Підсумок



Курс охоплює всі ключові аспекти тестування комп'ютерних засобів — від теоретичних основ до сучасних методів автоматизації — і формує у студентів цілісне розуміння забезпечення якості в комп'ютерній інженерії.

Бажаємо успіхів у вивченні Тестування комп'ютерних засобів!

120

Годин

Загальний обсяг дисципліни

4

Кредити ЄКТС

Відповідно до стандарту

16

Тем

У 4 змістовних модулях

8

Джерел

Рекомендованої літератури 2022–2024 рр.

«Якість — це не акт, а звичка.» — Арістотель

Спеціальність 123 · Комп'ютерна інженерія · Бакалавр · 4 кредити ЄКТС