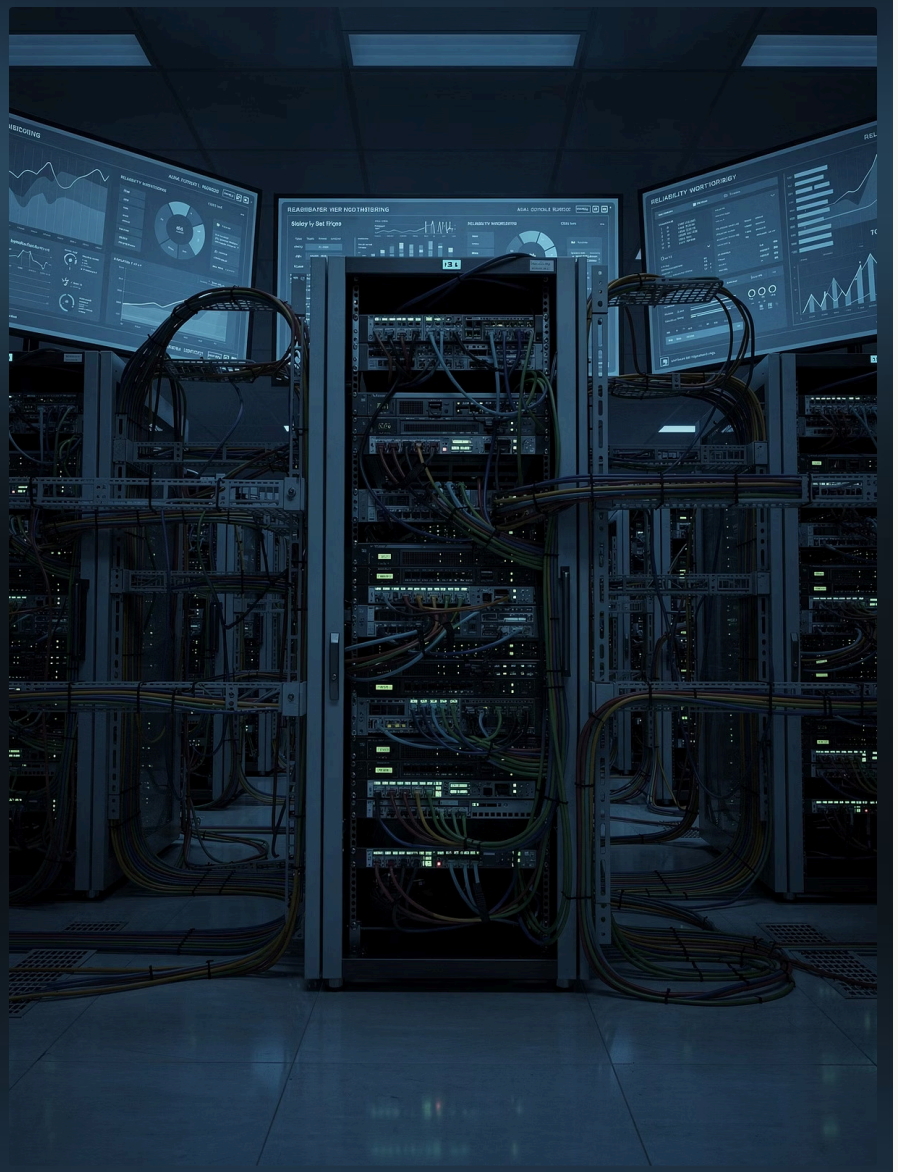


Силабус дисципліни «Надійність комп'ютерних систем та мереж»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ · БАКАЛАВР · ОП ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС

120

Годин загальний обсяг дисципліни

4

Кредити ЄКТС відповідно до стандарту

4

Змістовних модулі курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Надійність комп'ютерних систем та мереж

Спеціальність: 123 Комп'ютерна інженерія

ОП: Організація захисту інформації в ІКС

Ступінь: Бакалавр

Обсяг: 120 годин / 4 кредити ЄКТС

Модулів: 4 змістовних блоки курсу

Мета дисципліни

Дисципліна «Надійність комп'ютерних систем та мереж» формує у студентів спеціальності «Комп'ютерна інженерія» (ОП «Організація захисту інформації в інформаційно-комунікаційних системах») систематизовані знання про теорію надійності, методи оцінювання та забезпечення відмовостійкості комп'ютерних систем і мереж. Курс спрямований на розвиток здатності аналізувати показники надійності, проектувати надійні мережеві інфраструктури та застосовувати методи резервування, діагностики й відновлення систем у контексті захисту інформації.

Форми навчання

- Лекції — 30 годин
- Лабораторні заняття — 30 годин
- Самостійна робота — 60 годин

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання технічної інформації у сфері надійності та безпеки комп'ютерних систем: виявлення ключових показників, порівняння методів забезпечення надійності, формування обґрунтованих висновків і прийняття інженерних рішень. Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки звітів з лабораторних робіт і аналітичних записок.

Здатність до усної та письмової технічної комунікації: чітко пояснювати поняття надійності, аргументовано обґрунтовувати вибір методів резервування та захисту. Відповідальність, ініціативність та готовність працювати в команді під час виконання лабораторних і практичних завдань.

- Аналізувати навчальну та наукову інформацію у сфері надійності систем
- Виділяти головне та узагальнювати результати досліджень
- Планувати власну діяльність і дотримуватися дедлайнів
- Коректно спілкуватися з викладачами та одногрупниками
- Брати участь у командній роботі при розробці інженерних рішень

Фахові компетентності

Розуміння основних понять теорії надійності, показників безвідмовності, ремонтопридатності, збереженості та довговічності комп'ютерних систем і мереж. Знання методів математичного моделювання надійності, структурних схем надійності, методів резервування та відновлення систем.

Здатність застосовувати методи аналізу надійності для проектування захищених і відмовостійких мережевих інфраструктур, оцінювати ризики відмов в інформаційно-комунікаційних системах та обирати ефективні засоби забезпечення їх безперервної роботи.

- Розраховувати показники надійності комп'ютерних систем і мереж
- Аналізувати структурні схеми надійності складних систем
- Застосовувати методи резервування для підвищення надійності
- Проводити діагностику та відновлення працездатності систем
- Оцінювати надійність мережевих протоколів і телекомунікаційних засобів

Результати навчання

Після успішного завершення курсу студент повинен демонструвати такі результати навчання:

1

Знання та розуміння

Пояснювати сутність ключових понять теорії надійності: безвідмовність, ремонтопридатність, збереженість, довговічність, інтенсивність відмов, середній час напрацювання до відмови. Характеризувати моделі відмов, закони розподілу часу безвідмовної роботи та методи їх застосування.

2

Аналіз та оцінювання

Аналізувати структурні схеми надійності послідовних, паралельних і змішаних систем. Оцінювати вплив параметрів надійності окремих елементів на надійність системи в цілому, виявляти «вузькі місця» та критичні компоненти мережевої інфраструктури.

3

Застосування знань

Застосовувати методи резервування (постійне, навантажене, ненавантажене) для підвищення надійності комп'ютерних систем і мереж. Використовувати програмні засоби моделювання надійності для обґрунтування інженерних рішень у сфері захисту інформаційно-комунікаційних систем.

4

Комунікація та рефлексія

Аргументовано представляти результати аналізу надійності комп'ютерних систем. Формувати інженерну культуру відповідального проектування та свідоме ставлення до забезпечення надійності й безпеки інформаційних ресурсів.

Модуль 1. Основи теорії надійності комп'ютерних систем

ЗМІСТОВНИЙ МОДУЛЬ 1

Тема 1.1

Вступ до теорії надійності. Предмет, завдання та місце дисципліни в підготовці фахівців з захисту інформації. Основні поняття: надійність, безвідмовність, ремонтопридатність, збереженість, довговічність. Стандарти і нормативна база у сфері надійності. Класифікація відмов.

Тема 1.2

Показники надійності невідновлюваних систем. Ймовірність безвідмовної роботи. Інтенсивність відмов. Середнє напрацювання до відмови. Закони розподілу часу безвідмовної роботи: експоненціальний, Вейбулла, нормальний. Методи статистичної оцінки показників.

Тема 1.3

Показники надійності відновлюваних систем. Коефіцієнт готовності та коефіцієнт оперативної готовності. Середнє напрацювання на відмову. Інтенсивність відновлення. Потік відмов. Стаціонарні та нестаціонарні характеристики надійності.

Тема 1.4

Математичні моделі надійності елементів. Марківські моделі надійності. Графи стани-переходи для дво- та багатостанових елементів. Рівняння Колмогорова. Метод мінімальних перерізів і мінімальних шляхів. Застосування до аналізу відмов компонентів ІКС.

Модуль 2. Структурна надійність комп'ютерних систем і мереж

ЗМІСТОВНИЙ МОДУЛЬ 2

Тема 2.1

Структурні схеми надійності. Послідовне з'єднання елементів. Паралельне з'єднання. Змішані структури. Метод розкладання. Метод булевої алгебри. Побудова та аналіз структурних схем надійності для типових конфігурацій комп'ютерних мереж.

Тема 2.2

Резервування як метод підвищення надійності. Загальне та роздільне резервування. Постійне резервування. Резервування із заміщенням (навантажене та ненавантажене). Ковзне резервування. Часове резервування. Порівняльна ефективність методів резервування для мережевих вузлів.

Тема 2.3

Надійність мережевих топологій та протоколів. Надійність з'єднань шина, зірка, кільце, mesh. Протоколи забезпечення відмовостійкості: STP/RSTP, LACP, OSPF, BGP. Аналіз надійності каналів передачі даних. Показники якості мережевих сервісів (SLA).

Модуль 3. Надійність та безпека інформаційно-комунікаційних систем

ЗМІСТОВНИЙ МОДУЛЬ 3

Тема 3.1

Відмовостійкість серверних та хмарних інфраструктур. Кластеризація та балансування навантаження. High Availability (HA) рішення. Технології RAID для забезпечення надійності зберігання даних. Резервне копіювання та відновлення. Концепція RTO і RPO. Хмарні моделі надійності.

Тема 3.2

Надійність засобів захисту інформації. Надійність криптографічних модулів та засобів автентифікації. Відмовостійкість систем виявлення вторгнень (IDS/IPS). Надійність міжмережевих екранів і VPN-шлюзів. Моделювання загроз доступності як аспекту інформаційної безпеки.

Тема 3.3

Людський фактор та організаційні аспекти надійності. Вплив помилок персоналу на надійність систем. Класифікація людських помилок. Регламенти технічного обслуговування та планового відновлення. Управління інцидентами (ITIL/ISO 20000). Нормативно-правова база забезпечення надійності ІКС в Україні.

Модуль 4. Діагностика, випробування та забезпечення надійності

ЗМІСТОВНИЙ МОДУЛЬ 4

Тема 4.1

Технічна діагностика комп'ютерних систем. Поняття технічного стану та діагностики. Методи контролю: тестовий та функціональний. Діагностичні моделі. Засоби апаратної та програмної діагностики. Побудова діагностичних тестів. Локалізація несправностей у мережевому обладнанні.

Тема 4.2

Випробування на надійність та збір статистики відмов. Методи прискорених випробувань. Планування та проведення випробувань на надійність. Методи обробки результатів. Статистичні критерії перевірки гіпотез щодо законів розподілу. Накопичення та аналіз статистики відмов в ІКС.

Тема 4.3

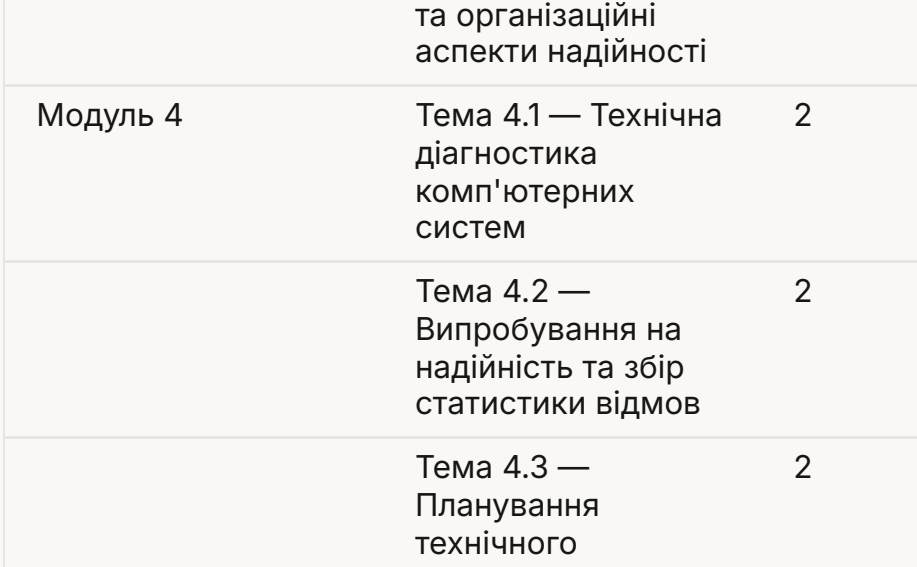
Планування технічного обслуговування та управління ресурсом. Стратегії технічного обслуговування: планово-попереджувальне, за станом, коригувальне. Оптимізація міжремонтних інтервалів. Управління життєвим циклом обладнання. Оцінка залишкового ресурсу компонентів.

Тема 4.4

Комплексне забезпечення надійності та безперервності бізнесу. Плани забезпечення безперервності роботи (BCP) та відновлення після катастроф (DRP). Аналіз впливу на бізнес (BIA). Стандарти ISO 22301 та ISO/IEC 27031. Інтеграція надійності та інформаційної безпеки в ІКС.

Розподіл навчального часу — 120 годин

Модуль	Тема	Лекції (год.)	Лабораторні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 — Вступ до теорії надійності	2	2	4
	Тема 1.2 — Показники надійності невідновлюваних систем	2	2	4
	Тема 1.3 — Показники надійності відновлюваних систем	2	2	4
	Тема 1.4 — Математичні моделі надійності елементів	2	2	4
Модуль 2	Тема 2.1 — Структурні схеми надійності	2	2	4
	Тема 2.2 — Резервування як метод підвищення надійності	2	2	4
	Тема 2.3 — Надійність мережевих топологій та протоколів	4	4	8
Модуль 3	Тема 3.1 — Відмовостійкість серверних та хмарних інфраструктур	4	4	8
	Тема 3.2 — Надійність засобів захисту інформації	4	4	8
	Тема 3.3 — Людський фактор та організаційні аспекти надійності	2	2	4
Модуль 4	Тема 4.1 — Технічна діагностика комп'ютерних систем	2	2	4
	Тема 4.2 — Випробування на надійність та збір статистики відмов	2	2	4
	Тема 4.3 — Планування технічного обслуговування	2	2	4
	Тема 4.4 — Комплексне забезпечення надійності та BCP/DRP	2	2	4
Разом		**30**	**30**	**60**



Структура навчального часу

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

- **Лекції (30 год. — 25%):** подача ключового теоретичного матеріалу з теорії надійності
- **Лабораторні (30 год. — 25%):** практичне розрахунки, моделювання, аналіз систем
- **Самостійна робота (60 год. — 50%):** поглиблене вивчення, підготовка завдань

Самостійна робота становить **50% обсягу дисципліни** — студенти набувають навичок самостійного аналізу надійності реальних систем.

Самостійна робота студентів та методи викладання

Форми самостійної роботи

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками з теорії надійності, нормативними документами (ДСТУ, ISO/IEC), науковими статтями у фахових виданнях. Конспектування ключових положень, порівняння підходів різних авторів до оцінювання надійності комп'ютерних систем.

Індивідуальні завдання

Виконання розрахункових завдань із визначення показників надійності систем, побудови структурних схем надійності, оцінки ефективності резервування. Підготовка аналітичних записок щодо надійності реальних мережевих інфраструктур та засобів захисту інформації.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: Держспецзв'язку (**cip.gov.ua**), ДСТСЗІ СБУ, Державна служба якості освіти (**sqe.gov.ua**). Аналіз чинних стандартів ДСТУ, міжнародних стандартів ISO/IEC 27001, 22301, пошук актуальної наукової інформації.

Підготовка до занять

Підготовка до лабораторних занять шляхом опрацювання теоретичного матеріалу та методичних вказівок; підготовка до тестувань через вивчення ключових термінів і формул; систематизація знань перед контрольними роботами та модульними тестами.

Методи викладання

Лекції

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

Лабораторні роботи

Практичне моделювання показників надійності, побудова структурних схем, розрахунок коефіцієнтів готовності; студенти оформлюють звіти з аналізом отриманих результатів.

Кейс-аналіз

Аналіз реальних відмов та інцидентів в ІКС; студенти виявляють причини, моделюють структурні схеми надійності та пропонують заходи підвищення відмовостійкості.

Робота з нормативними документами

Опрацювання стандартів ДСТУ, ISO/IEC та галузевих норм у сфері надійності та інформаційної безпеки; формування навичок роботи з технічною документацією.

Самостійне дослідження

Підготовка розрахункових звітів і аналітичних записок за обраною темою; розвиток навичок самостійного аналізу надійності та систематизації інженерних рішень.

Форми контролю знань

1

Поточний контроль

Завдання: розрахункові та тестові вправи за темами змістовного модуля. Оцінюються регулярність виконання лабораторних робіт, якість звітів і рівень засвоєння теоретичного матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Включає усні опитування, захист лабораторних робіт та розв'язання типових задач з теорії надійності.

2

Проміжний контроль

Самостійна робота — комплексне розрахункове завдання або аналітична записка, яка охоплює теми змістовних модулів (теоретичні питання, розрахунок показників надійності, аналіз структурних схем, обґрунтування методу резервування). Оцінюються повнота відповіді, правильність розрахунків та обґрунтованість висновків. Проводиться після кожного змістовного модуля.

3

Підсумковий контроль

Залік/іспит відповідно до навчального плану. Форма проведення — тестування та розв'язання розрахункових задач. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали оцінювання: 100-бальна система з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Усі методи контролю спрямовані на формування компетентностей, передбачених освітньо-професійною програмою «Організація захисту інформації в інформаційно-комунікаційних системах» спеціальності 123 «Комп'ютерна інженерія».

Рекомендована література та ресурси

Навчальна та наукова література (2022–2024)

1. Вишняков В. М. Захист інформації в комп'ютерних системах: навч. посіб. — Київ : КНУБА, 2022. — 248 с.
2. Бурячок В. Л., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. — Вид. 2-ге, доповн. — Львів : Магнолія 2006, 2024. — 310 с.
3. Корченко О. Г., Казмірчук С. В., Ткач Ю. М. Менеджмент інформаційної безпеки: підручник. — Київ : НАУ, 2022. — 352 с.
4. Складанний П. М., Семко В. В. Технології захисту мережевої інфраструктури: навч. посіб. — Київ : КУБГ, 2023. — 228 с.
5. Толюпа С. В., Лазаренко С. В., Наконечний В. С. Надійність та безпека телекомунікаційних систем: навч. посіб. — Київ : НАУ, 2023. — 280 с.
6. Хорошко В. О., Браіловський М. М., Зибін С. В. Технології захисту інформації: підручник. — Київ : ЦК «Компринт», 2022. — 312 с.
7. Дудикевич В. Б., Хорошко В. О., Лук'яненко Л. В. Надійність та відмовостійкість комп'ютерних мереж: монографія. — Львів : Львівська політехніка, 2023. — 256 с.
8. Гулак Г. М., Юдін О. К., Бучик С. С. Аналіз вразливостей інформаційних систем: навч. посіб. — Київ : НАУ, 2022. — 200 с.
9. Кравченко Ю. В., Пилипенко А. М. Комп'ютерні мережі та безпека: підручник. — Київ : Ліра-К, 2023. — 336 с.
10. Задорожня Т. М., Соколов В. Ю. Управління інцидентами та безперервністю ІКС: навч. посіб. — Київ : КУБГ, 2024. — 188 с.

Офіційні інтернет-ресурси та нормативна база

1. Державна служба спеціального зв'язку та захисту інформації України. — URL: **https://cip.gov.ua/**
2. ДСТСЗІ СБУ — нормативні документи у сфері технічного захисту інформації. — URL: **https://www.sbu.gov.ua/**
3. Національний банк України — стандарти інформаційної безпеки. — URL: **https://bank.gov.ua/**
4. Верховна Рада України — законодавство у сфері захисту інформації. — URL: **https://zakon.rada.gov.ua/**
5. Національна бібліотека України ім. В. І. Вернадського. — URL: **https://nbuv.gov.ua/**
6. Журнал «Безпека інформації» (електронне видання). — URL: **https://jrnl.nau.edu.ua/**
7. Науковий журнал «Кібербезпека: освіта, наука, техніка». — URL: **https://csecurity.kubg.edu.ua/**
8. ISO/IEC стандарти онлайн (ISO 22301, ISO/IEC 27001, ISO/IEC 27031). — URL: **https://www.iso.org/**

Рекомендована література охоплює видання **2022–2024 років** українських авторів відповідно до вимог актуальності навчально-методичного забезпечення ОП «Організація захисту інформації в ІКС».