МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ ДЕРЖАВНИЙ ПОЛІТЕХНІЧНИЙ КОЛЕДЖ

Для спеціальності:

Спеціальність: 151 Автоматизація та

комп'ютерно-інтегровані технології

МЕТОДИЧНІ ВКАЗІВКИ

для самостійної роботи

з дисципліни: "Експлуатація технічних засобів ІС"

Харків 2019

Методичні вказівки для самостійної роботи з дисципліни “Експлуатація технічних засобів ІС” для студентів

Галузь знань: 15 Автоматизація та приладобудування

Спеціальність: 151 Автоматизація та комп’ютерно-інтегровані технології

Спеціалізація: 5.151.1 Обслуговування інтелектуальних інтегрованих систем

Укладач: викладач Дігтяр А.А. - Харків: ХДПК, 2019, 64 с.

Затверджено на засіданні циклової комісії інформаційних технологій

Протокол від _____2019 р. №____

Голова циклової комісії _____М.М. Бочарніков

“____” _____ _____ року

Схвалено методичною радою коледжу

Протокол від _____2019 р. №____

Голова методичної ради _____

“_____” _____ 2019 року

ПЕРЕДМОВА

Дисципліна “Експлуатація технічних засобів ІС” для студентів

Спеціальності: 151 Автоматизація та комп’ютерно-інтегровані технології

Програмою дисципліни передбачається вивчення сучасних способів та методів визначення надійності, діагностики комп’ютених систем і мереж.

Обчислювальні пристрої, персональні комп'ютери (ПК) і комп'ютерні системи є важливою складовою сучасного виробництва.

У методичних вказівках, розглянуто різноманітні аспекти забезпечення надійності обчислювальних пристроїв, персональних комп'ютерів, комп'ютерних систем та програмного забезпечення. Висвітлено питання модернізації та експлуатаціного обслуговування ПК.

Сутність і основні елементи теорії надійності

Тема : Сутність та основні елементи теорії надійності

План

1. Сутність теорії надійності
2. Елементи теорії надійності

Література [1] ст. 9-19

Обчислювальні пристрої, ПК і комп‘ютерні системи є важливою складовою сучасного виробництва. Нині ця галузь розвивається особливо інтенсивно. Однак розвиток засобів коп‘ютерної техніки неможливий без забезпечення їх надійності. Її , в свою чергу, характерізують багато показників і параметрів.

Однією з особливостей комп‘ютерних систем і мереж порівняно з іншими, наприклад, механічними, є те, що їх надійність визначає надійність елементів та надійність програмного забезпечення.

Надійність – властивість об‘єкта зберігати в часі у встановлених межах значення всіх параметрів, які характерізують здатність виконувати потрібні функції в заданих режимах та умовах застосуванн, технічного обслуговування, зберігання і транспортування.

Відмова – подія, яка полягає в утраті функційним модулем (системою) здатності виконувати потрібну функцію.

Ймовірність безвідмовної роботи P(t) - функція розподілу ймовірностей безвідмовної роботи об‘єкта, яка характеризує ймовірність того, що об‘єкт за час t не втратить працездатності.

Ймовірність безвідмовної роботи є одним із основних показників надійності технічних виробів. Значення P(t1, t2) за відносно короткі проміжки часу (година, доба) для сучасних електронних пристроїв близьке до 1. Наприклад, ймовірність безвідмовної роботи типової інтегральної схеми(ІС) за кілька годин роботи становить 0,999999. Проводити розрахунки з такими числами незручно тому доцільно перейти до відповідних ймовірностей відмови – 10-7...10-6.

Технічний ресурс виробу - прогнозована тривалімть його експлуатації від початку до моменту, коли інтесивність відмов збільшується до рівня, який робитьподальшу експлуатацію неможливою або недоцільною з економічних міркувань.

Контрольні запитання для самостійної роботи

1.Поміркуйте, як впливає складність об‘єкта на його надійність

2.Охарактеризуйте загальні властивості функції надійності

3.Які основні періоди життєвого циклу технічних об‘єктів? У чому полягає їх зміст?

4.Обгрунтуйте поняття „технічний ресурс виробу”.

5.Види розподілів: експоненціальний, нормальний, Вейбула.

6. Оцінка показників надійності мікросхем

7.Види відказів мікросхем (література доп. [1] ст.35-63)

Тема: „Методи забезпечення надійності”

План

1.Методи забезпечення надійності відновлюваних об‘єктів

2. Методи забезпечення надійності невідновлюваних об‘єктів

3.Особливості комп‘ютерних систем

Література [1]ст. 20-23

В теорії надійності всі об‘єкти поділяють на два великих класи: відновлювані і невідновлюван.

Підхід для забезпеченям надійості обох ласів зовсім різний.

Забезпечення надійності відновлюваних об‘єктів полягає в організації ефективного ремонту обладнання з мінімальними затратами часу.

Відновлювані об‘єкти – об‘єкти, які в період експлуатації в разі виникнення відмов можуть бути відремонтовані шляхом заміни несправних компонентов.

Для відновлюваних об‘єктів основним показником надійностіф вважають кофіцієнт готовності, що визначає частину корисного часу tk протягом якого об‘єкт нормально працює щодо загального часу експлуатації.

Тобто:

$$Kг = \frac{t_k}{t_k + t_в}, \quad (1)$$

де $t_в$ - час, що втрачено на відновлення працездатності. Він містить дві складові: t1 – час, що втрачено на пошук несправності; t2 – час власне відновлення.

Особливістю сучасного електронного обладнання є його модульна побудова, тому відновлення таких об‘єктів найчастіше може полягати у простій заміні несправного модуля (блока) справним. Вона не потребує великих затрат часу. Пошук несправності-навпаки, і впливає саме на кофіцієнт готовності.

До основних методів забезпечення надійності відновлюваної електронної апаратури належать:

- створення максимально сприятливих умов для прискорення ремонту;
- застосування автоматизованого пошуку несправностей на основі апаратного або програмного самоконтролю; тестового діагностування та використання спеціальноих автоматизованих систем контролю і діагностики.

Для невідновлюваних об‘єктів підхід до забезпечення надійності зовсім інший, оскільки вони не підлягають ремонту.

Невідновлювані об‘єкти - об‘єкти, для яких ремонт із конструктивних причин або умов експлуатації є неможливим.

Наприклад, інтегральні схеми, кінескопи, мікропроцесорні системи керування бортової апаратури тощо.

Показники надійності таких пристроїв залежать від складності невідновлюваних об‘єктів, при ймовірності безвідмовної роботи менше ніж 0,5 система стає непрацездатною. Однак цьому можна запобігти, якщо застосувати методи введення надлишковості.

Надлишковість поділяють на часову, інформаційну, структурну(апаратну).

Комп‘ютерні системи, які використовують для управління реальними об‘єктами, не можна беззастережно зарахувати до відновлюваних, ні до невідновлюваних об‘єктів.

До методів забезпечення надійності комп‘ютерних систем належать як методи , що застосовують для відновлюваних систем (прискорення пошуку неспрвностей), так і властиві невідновлюваним системам методи, наприклад, (структурна надлишковість). Принципова особливість таких систем полягає в багаторазових обчисленнях. Вони утворюються шляхом n-кратного повторення обчислювального процесу в таких розрізах:

- часовому (повторний рахунок);
- просторовому (на інших апаратних засобах);
- інформаційному (з використанням інших програм і даних).

Контрольні запитання для самостійної роботи

1. Охарактеризуйте поняття „Відновлювані об‘єкти”
2. Охарактеризуйте поняття „Невідновлювані об‘єкти”
3. У чому полягає суть поняття надлишковості?
4. Охарактеризуйте комп‘ютерні системи як синтез не відновлюваних об‘єктів.

Тема:” Резервування апаратури”
План

1.Основні види резервування
2.Мажорітарний метод резервування
3.Поняття відновлюючого органу
Література [1]ст. 25-33

Одним із методів підвищення надійності обчислювальних систем є резервування її складових.

Резервування – метод підвищення надійності шляхом включення резервних елементів при розроблені системи або в процесі її експлуатації.

Розрізняють поелементне і загальне резервування.

За включенням резерву виокремлюють постійне резервування і резервування заміщенням.

Постійне резрвування полягає у включенні резервної апаратури протягом усього часу функціонування основної.

Резервування заміщенням полягає у включенні резервного елемента структури замість елемента, який вийшов з ладу.

За такого резервування резерв може бути:

- ненавантаженим(апаратура не увімкнута у процесі функціонування);
- полегшеним (увімкнута частина резервної апаратури);
- навантаженим (увімкнута вся резервна апаратура).

До переваг цього способу резервування належать:

- один резервний елементвикористовують для кількох основних
- резервні елементи знаходяться у пасивному стані(наприклад, знеструмлені), що зберігає їх технічний ресурс.

Мажоритарний метод резервування вважається класичним. Він був запропонований Дж.фон Нейманом. Реалізують його як постійне резервування з логічним перемиканням на резервні елементи. Елементом цього методу є відновлюючий

орган (ВО), функція якого полягає в утворенні резуьтуючого сигналу за більшистю значень вхідних сигналів.

Контрольні запитання для самостійної роботи

1.У чому різниця між поелементним і загальним резервуванням?
2.Охарактеризуйте поняття „резервування заміщенням”
3.Який алгоритм відновлення сигналів при застосуванні мажорітарного методу?
4.Охарактеризуйте відновлюючий орган з пам‘яттю як метод резервування

Тема: „Надійність програмного забезпечення”

План

1.Порівняльний аналіз надійності апаратних засобів ПК і ПЗ
2.Оцінювання і прогнозування надйності програм
3.Помилки ПЗ
4.Шляхи забезпечення надійності ПЗ
Література [1]ст.241-264

Забезпечення надійності програмних засобів ПК і обчислювальних систем істотно відрізняється від забезпечення надійності апаратури. Щоб зрозуміти це потрібно ознайомитися із загальною методологією діагностування ПЗ.

Системний підхід – сумісний аналіз і розроблення всіх елементів системи.

Модуль – елемент програми, стандартизований за формою запису і зовнішніми зв’язками.

Надійність програмного забезпечення – властивість програми виконувати задані функції в заданих умовах роботи і на заданій ЕОМ.

Безвідмовність програмного забезпечення.

Оцінюють імовірністю роботи ПЗ без відмов протягом заданого часу в певних умовах зовнішнього середовища.

Відновлювальність ПЗ.

Її характеризують витрати часу і праці на усунення відмов через помилки в програмі та їхні наслідки. Високу надійність програми забезпечує швидке реагування на її спотворення, а також спотворення даних або обчислювального процесу, відновлення працездатності програм за час, менший ніж поріг між збоєм і відмовою.

Усталеніть функціювання. Це одна з характеристик ПЗ, яка полягає в здатності обмежувати наслідки власних помилок і несприятливих впливів зовнішнього середовища або протистояти їм.

Механізм виникнення відмов.

Порушення специфікації. Трапляється це насамперед у складних програмних системах, де окремі помилки програміста важко виявити.

Неточна або неповна специфікація. Виникає, коли при її складанні невідомі фактори, що впливають на роботу програми.

Коректність програми – це відповідніть її специфікації.

Прихованість помилок полягає у виявленні помилки в результаті великої кількості комбінацій вихідних даних.

Інтенсивність відмов – інтегральний критерій, що характеризує густину розподілу напрацювання до першої відмови, розраховану за умови, що до моменту часу, який розглядають система пропрацювала безвідмовно.

Оцінювання і прогнозування надійності програм.

Ці процедури здійснюються на основі математичних моделей Джелінські-Моранди, Шумана, Шика-Волвертона.

Експериментальне оцінювання кількості помилок у програмі. Визначають стосовно кількості виявлених природних і штучних помилок, якщо в програму була введена певна кількість однотипних з природними штучних помилок.

Надійність програмного комплексу. Визначають її як функцію надійності складових частин програмного комплексу.

Помилки програмного забезпечення.

Під поняттям „помилка” розуміють неправильність, похибку або ненавмисне спотворення об’єкта чи процесу. При цьому приймають, що правильний стан об’єкта або процесу відомий.

Залежно від складності первинні помилки ПЗ поділяють на такі типи:

- технологічні помилки підготовки машинних носіїв і документації, а також виведення і введення програм у комп’ютер та його засоби відображення
- алгоритмічні помилки, пов’язані з неповним формуванням необхідних умов розв’язання і некоректною постановкою завдання
- системні помилки, зумовлені відхиленням функціювання ПЗ у реальній системі від очікуваних під час проектування
- програмні помилки, пов’язані з некоректною постановкою завдання.

Шляхи забезпечення надійності ПЗ

Основні фактори, що визначають надійність функціювання ПЗ, об’єднують у 3 групи:

- фактори, які безпосередньо визначають надійність програм.
- методи проектування коректних програм.
- методи контролю і забезпечення надійності програм.

Визначальне значення для забезпечення надійності програм має третя група факторів. Для її підвищення і захисту інормації програмно-алгоритмічними методами використовують часову, інформаційну та програмну надлишковість.

Часова надлишковість. Це використання певної частини апаратних засобів і продуктитвності ЕОМ, зокрема ПК, для контролю виконання програм і відновлення обчислювального процесу. Передбачається певний резерв продуктивності, необхідний для контролю та підвиження надійності функціювання ПЗ.

Інформаційна надлишковість. Вона полягає у дублюванні накопичених почпткових і проміжних даних. Її використовіють для забезпечення достовірності даних, які потребують значного часу для відновлення чи найбільше впливають на нормальне функціювання ПЗ. Вони характеризують певні інтегральні відомості про зовнішній керований процес, і в разі їх руйнування можуть надовго припинити керування цим процесом та відповідне оброблення інформації.

Програмна надлишковість. Вона контролює і забезпечує достовірність найважливіших рішень з оброблення інформації та керуання. Її сутність полягає в

застосуванні кількох варіантів програм, що відрізняються методами розв'язання певного завдання або прогрпммною реалізацією одного й того самого методу.

Контрольні запитання для самостійної роботи

1.У чому полягають особливості системного підходу до забезпечення надійності ОТ?

2.Охарактерізуйте суть механізму відмов ПЗ?

3.Порівняйте залежності надійності апаратних і програмних засобів під час експлуатації.

4.Як визначають надійність програмних комплексів?

5.Які інують шляхи забезпечення ПЗ?

Тема: „Методологія діагностування програмного забезпечення (ПЗ)"

План

1.Загальні відомості діагностування ПЗ

2.Особливості процесу тестування ПЗ

Література [1]ст. 271-276

Методологія діагностування ПЗ пояснює суть методів і способів тестування програм, методики побудови тестів, процедур, які доводять програми до робочого стану. Вона визначає також послідовність видів тестування.

Діагностування як процес виявлення помилок у ПЗ є одним з основних методів підвищення його надійності. Здійснюють діагностування на всіх етапах життєвого циклу ПЗ, а саме на етапі планування, проектування і кодування.

Суть тестування полягає у перевірці роботи програм за результатами їх виконання зі спеціально підібраними наборами вихідних даних (тестами). Діагностування ПЗ здійснюють також і методом верифікації.

У процесі діагностування ПЗ крім тестування використовують процедури доведення, контролю, випробування, атестації, відлагодження.

З огляду на обсяг тестування може бути повним або вибірковим. За повного тестування програму тестують повністю, а за вибіркового – в окремих точках блоку вхідних даних.

Під час вибіркового тестування надійність програми повністю не забезпечують. Частина помилок може бути прихованою і не виявитися. Тому найчастіше використовують структурне вибіркове тестування. Воно полягає у розділенні блока вхідних даних на класи, кожен з яких дає змогу підтвердити певні властивості або працездатність окремих елементів структури. Вибір шляхів у структурі програми повинен здійснюватись так, щоб усі оператори програми були задіяні хоча б один раз. Для перевірки результатів роботи програми використовують числове і символьне тестування. Числове полягає у перевірці правильності числових резуоттатів роботи програм при певних тестових наборах.

Символьне передбачає виконання процедур, що ґрунтуються на символьних входах. Вхідні змінні позначають так, що вони дають змогу виразити вихідні змінні також у символьному вигляді. При цьому різним шляхам у програмі відповідають різні символьні входи і виходи.

Контроль складових ПЗ необхідно проводити у зазначеній послідовності й повному обсязі. Його визначають залежно від вимог надійності.

Контрольні запитання для самостійної роботи

1.Розкрийте суть первинних і вторинних помилок ПЗ

2.У чому суть технологічної помилки?

3.Загальна класифікація помилок ПЗ за видами робіт зі створеня і експлуатації ПЗ

4.У чому полягають особливості процесу тестування ПЗ?

Тема: „Тестування модулів та комплексне тестування програмної системи”

План

1.Суть процесу тестування модулів

2.Проектування тестів

Література [1]ст. 277-294

Процес тестування ПЗ починається з тестування модулів за наявності спроектованих тестів. Тому слід приділити цим процедурам особливу увагу.

Суть процесу тестування модулів

При тестуванні ПЗ увагу приділяють насамперед тестуванню автономних модулів. Суть цього процесу полягає в контролі окремого програмного модуля. Його метою є знаходження невідповідностей між логікою модулів та їх спряганням, з одного боку, і з зовнішніми специфікаціями, з іншої. Зовнішні специфікації охоплюють опис функцій, вхідних і вихідних даних та зовнішніх ефектів. Компіляцію модуля теж розглядають як тестування, оскільки компілятор виявляє більшість синтаксичних помилок, а також певні логічні і семантичні.

Процес тестування модуля здійснюється у кілька етапів:

Підготовка на основі зовнішніх специфікацій модуля тесту для кожної ситуації, для кожної з меж областей допустимих значень всіх недопустимих умов – усіх вхідних даних та областей зміни даних;

Перевірка тесту програми.

З’ясування того, чи охоплюють тести відповідно до тексту програми велику кількість можливих шляхів;

Перевірка чутливості програми, згідно з її текстом, стосовно окремих особливих значень вхідних даних.

Тестування автономних модулів здійснюють на основі кількох аксіом, що є фундаментальними принципами тестування:

- Високоякісним є той тест, який має високу ймовірність виявлення помилок, а не той, що демонструє правильну роботу програми;
- Однією з найважливіших проблем при тестуванні , виходячи з першої аксіоми, є з’ясування термінів закінчення тестування;
- Неможливо тестувати особисту програму;
- Необхідною частиною будь-якого тесту повинен бути опис очікуваних вихідних даних або результатів;
- Слід уникати невідтворюваних тестів;

- Необхідно розробляти тести як для правильних, так і для неправильних вхідних даних;
- Слід детально аналізувати результати проходження кожного тесту;
- Тестування проводять найкваліфікованіші програмісти;
- При розробленні ПЗ тестованість є ключовим завданням;
- Проект системи повинен передбачати , що кожний модуль, який підключається до системи , має бути в єдиному варіанті;
- Не можна змінювати програму з метою полегшення її тестування;
- Тестування слід починати з визначення цілей;

Усі розгалуження потрібно виконувати в кожному з можливих напрямів хоча б один раз.

Тестування модулів ПЗ здійснюють на основі відповідних методів – статичного і динамічного.

Статичне тестування полягає в тому, що одним з критеріїв обрання шляхів у структурі програми при тестуванні є задіяння всіма операторами хоча б один раз обраних шляхів. При цьому тестують команди за послідовністю їх розташування в тексті програми.

Статичний аналіз програми спеціалісти-тестувальники виконують неавтоматизовано.

Динамічне тестування (тестування гілок). Вимагає обрання таких шляхів, які перекривають усі гілки програми або всі розгалуження в усіх напрямах. Цей метод гарантує однократне тестування всіх гілок і операторів.

Головна вимога до програм або програмних систем – виконувати задані функції. Вони найповніше реалізуються при застосуванні функційного, структурного, символьного і регресивного тестування.

Інтеграція модулів, тестування зовнішніх функцій і комплексів програм.

Тестування модулів є дуже важливим етапом діагностування комплексу ПЗ. Наступними завданнями, які розв’язують під час розроблення і налагодження ПЗ, є інтеграція модулів у систему , її комплексне тестування і налагодження.

Суть і методи інтеграції програмних модулів.

Після проектування здійснюють інтеграцію модулів – злиття модулів у програму або програмну систему. Вибір послідовності злиття модулів у систему визначає форму, в якій записуються тести, послідовність програмування модулів, вибір засобів тестування і відповідно ефективність тестування.

Висхідне тестування. Суть його полягає в тому, що програму збирають і тестують знизу до гори. Тестують першими і автономно модулі найнижчого рівня. Потім – модулі , що безпосередньо викликають уже перевірені. Для тестування модулів вищого рівня повинні бути протестовані всі модулі нижчого рівня, які він викликає. За висхідного тестування для тестування кожного модуля потрібен драйвер – програма, що імітує надходження інформації з попередніх модулів.

Низхідне тестування. Полягає в тому, що програму збирають і тестують зверху вниз. Автономно тестують тільки головний модуль, що відповідає вершині графа. Потім до нього приєднують один за одним модулі, безпосередньо зв’язані з ним, і тестуютьо держану комбінацію. Процес повторюють, поки не будуть зібрані й перевірені всі модулі . низхідне тестування дає змогу чітко дотримуватися певної послідовності тестування.

Метод „великого стрибка” . Він є одним з найпоширеніших методів тестування. Використовують його лише для невеликих програм. Особливість цього методу полягає в автономному тестуванні спочатку кожного модуля. Потім усіх їх одночасно інтегрують у систему. Від низхідного тестування його відрізняє те, що всі модулі інтегрують у систему одночасно в останній момент. Це зумовлює ситуацію, коли у спряганнях між модулями тривалий час залишаються помилки, які можуть бути непоміченими. Для невеликих добре спроектованих програм, метод „великого стрибка” ефективний, для великих програм – неприйнятий.

Метод Сандвича . Це компромісний варіант між висхідним і низхідним тестуванням. Головна мета його полягає у використанні переваг цих методів й усуненні їх недоліків. Суть методу полягає в тому, що висхідне і нисхідне тестування починаються одночасно. Програміст збирає програму як знизу, так і зверху.

Використання цього методу має сенс при інтеграції і тестуванні великих програмних систем (операційних систем) та пакетів прикладних програм.

Важливу роль при діагностуванні ПЗ відіграють тестування спрягань і зовнішніх функцій.

Тестування спрягань . Під час цієї процедури перевіряють взаємозв’язок між модулями щодо використовуваної інформації і часу її надходження. Тести для контролю спрягань розробляють на основі аналізу архітектури програмної системи і структури програми. Цей аналіз грунтується на схемі інформаційних зв’язків у графі програмної системи і матриці взаємозв’язків модулів. Характер вихідних даних для кожного модуля визначають з таблиць вихідних змінних.

Тестування зовнішніх функцій. Його здійснюють з метою виявлення розходжень між програмою і її зовнішніми специфікаціями. Тому необхідною умовою такого тестування є наявність чітких і точних специфікацій.

Тести зовнішніх функцій розробляють так, щоб їх можна було використати багаторазово.

Збирання і комплексне тестування програмної системи

Після завершення автономного тестування модулів, тестування спрягань і тестування зовнішніх функцій приступають безпосередньо до інтеграції програмної системи. Цей процес починають з того, що складають план поступового збирання системи.

Кожний рівень або версію системи називають сіном. Збирання починають з нульового базового спіну і закінчують N-м спіном. За нульовий спін приймають операційну систему.

Збирання призначене виділити збірні вузли і скласти календарний план їх розроблення .

Ця робота повинна відповідати таким критеріям:

- У плані збирання слід враховувати обмеження, пов’язані з наявними ресурсами і графіком розроблення діагностичного забезпечення;
- Послідовність збирання необхідно базувати на каркасній (0-й спін) версії системи, що вже готова і працює;
- У плані має враховуватися залежність одних збірних вузлів від інших;
- Послідовність збирання має забезпечувати включення найважливіших функцій в перші спіни;
- У плані збирання слід мінімізувати застосування програм, що імітують відсутні у всіх спінах, крім останнього , певні фрагменти системи.

Після збирання системи здійснюють її комплексне тестування.

Комплексне тестування – пошук невідповідності системи своїй вихідній (початковій) меті.

Комплексні тести не зводять до перевірки окремих функцій системи. Їх розробляють у формі сценаріїв – послідовних дій користувача.

Загальні тенденції щодо розроблення комплексних тестів. Отже, тестування проводити:

- Стресових ситуацій реального середовища;
- Великих обсягів даних протягом тривалого часу;
- Конфігурації апаратури ПЗ;
- Сумісності з розробленими раніше версіями і програмними засобами;
- Захисту від несанкціонованого доступу;
- Вимог до пам’яті ПК;
- Продуктивності та ефективності системи;
- Налагодження системи;
- Надійності та готовності системи;
- Засобів відновлення після втрати даних або відмов;
- Зручності обслуговування системи;
- Документації для користувача;
- Психологічних факторів, зокрема невідповідності зовнішнім специфікаціям, неправильного формулювання відповідей і повідомлень;
- Зручності експлуатації системи.

Комплексне тестування проводять перед приймальними випробуваннями на завершальній стадії розроблення.

Контрольні запитання для самостійної роботи

1.Які особливості повного і вибіркового тестування?

2.Що розуміють під числовим тестуванням?

3.У чому суть символьного тестування?

4.Охарактеризуйте етапиз яких складається процес тестування модулів

5.Дайте загальну характеристику методу Сандвича

6.У чому полягає суть комплексного тестування системи і яку форму мають комплексні тести?

Тема: “Заходи до захисту електроживлення ЕОМ”.
План

1.Фактори зовнішнього впливу на якість електроживлення
2.Вимоги до системи електроживлення ЕОМ
3.Засоби захисту системи електроживлення ЕОМ
Література
http://ci.uz.gov.ua/ua/min_praci/nakaz_kom_nahliadu99_21.html
Правила охорони праці під час експлуатації електронно-обчислювальних машин.

Вимоги до системи електроживлення ЕОМ

Згідно з Наказом Міністерства України з питань надзвичайних ситуацій від 19 жовтня 2004 року N 126 Зареєстровано в Міністерстві юстиції України 4 листопада 2004 р. за N 1410/10009

1 Над та під залами електронно-обчислювальних машин (далі - ЕОМ), а також у суміжних з ними приміщеннях не дозволяється розташування приміщень категорій А і Б за вибухопожежною небезпекою. Приміщення категорії В повинні відділятися від залів ЕОМ протипожежними стінами.

2. Сховища інформації, приміщення для зберігання перфокарт, перфострічок, магнітних стрічок та пакетів магнітних дисків слід розміщати у відособлених приміщеннях, обладнаних негорючими стелажами й шафами. Зберігати перфокарти, перфострічки та магнітні стрічки на стелажах необхідно в металевих касетах.

3. Фальшпідлога у приміщеннях ЕОМ має бути з негорючих матеріалів або матеріалів груп горючості Г1, Г2 з межею вогнестійкості не менше 0,5 години. Простір під нею слід розділяти негорючими діафрагмами на відсіки площею не більше 250 м2. Діафрагми повинні мати межу вогнестійкості не менше 0,75 год. У місцях перетинання з діафрагмами комунікації слід прокладати у спеціальних обоймах, а зазори зашпаровувати негорючими матеріалами.

Звукопоглинаюче облицювання стін та стель цих приміщень слід виготовляти з негорючих матеріалів або матеріалів груп горючості Г1, Г2.

4. Персональні комп'ютери після закінчення роботи на них повинні відключатися від мережі.

5. Не рідше одного разу на квартал необхідно очищати від пилу агрегати та вузли, кабельні канали та простір між підлогами.

6. Не дозволяється:

розміщати машинні зали ЕОМ у підвалах;

проводити роботи з ремонту вузлів (блоків) ЕОМ безпосередньо в машинному залі;

зберігати постійно в залах ЕОМ перфокарти, перфострічки, магнітні стрічки, дискети, інші носії інформації, запасні блоки й деталі (зберігатися там можуть лише носії інформації, необхідні для поточної роботи);

залишати без нагляду ввімкнену в мережу електронну апаратуру, яка використовується для випробування та контролю ЕОМ.

Відповідно до Положення про Комітет по нагляду за охороною праці України, затвердженого Указом Президента України від 9 березня 1998 року N 182/98, та на підставі протокольного рішення редакційної комісії, створеної наказом Комітету від 3

листопада 1998 року N 214, про підсумки розгляду остаточної редакції проекту Правил охорони праці під час експлуатації електронно-обчислювальних машин затверджені

Нижче приведено Правила охорони праці під час експлуатації електронно-обчислювальних машин.

Згідно з ними:

1.Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

2.Використання нульового робочого провідника як нульового захисного провідника забороняється.

3. Нульовий захисний провід прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення.

4. Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників.

5. Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі повинна бути не менше площі перерізу фазового провідника. Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПВЕ.

6. У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

7. ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні підключатися до електромережі тільки з допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

8.Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників повинні мати спеціальні контакти для підключення нульового захисного провідника. Конструкція їх має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Необхідно унеможливити з'єднання контактів фазових провідників з контактами нульового захисного провідника.

9.Неприпустимим є підключення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ до звичайної двопровідної електромережі, в тому числі - з використанням перехідних пристроїв.

10. Електромережі штепсельних з'єднань та електророзеток для живлення персональних ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ слід виконувати за магістральною схемою, по 3 - 6 з'єднань або електророзеток в одному колі.

11.Штепсельні з'єднання та електророзетки для напруги 12 В та 36 В за своєю конструкцією повинні відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В.

Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 36 В, мають бути пофарбовані в колір, який візуально значно відрізняється віл кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

12. Індивідуальні та групові штепсельні з'єднання та електророзетки необхідно монтувати на негорючих або важкогорючих пластинах з урахуванням вимог ПВЕ та Правил пожежної безпеки в Україні.

13 Електромережу штепсельних розеток для живлення персональних ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ при розташуванні їх уздовж стін приміщення прокладають по підлозі поряд зі стінами приміщення, як правило, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

При розташуванні в приміщенні за його периметром до 5 персональних ЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

14. Електромережу штепсельних розеток для живлення персональних ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ при розташуванні їх у центрі приміщення, прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не дозволяється застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, що містять сірку.

Відкрита прокладка кабелів під підлогою забороняється.

15.Металеві труби та гнучкі металеві рукави повинні бути заземлені.

16 Заземлення повинно відповідати вимогам ДНАОП 0.00-1.21-98 "Правила безпечної експлуатації електроустановок споживачів".

Засоби захисту системи електроживлення

Сучасні інформаційні системи працюють на тактових частотах вище 2 ГГц. При таких тактових частотах вищі гармоніки центрального процесора сягають частот 10 ГГц і вище. Це означає, що інформація може витікати з системи на частотах від 1 до 10 ГГц як по ефіру, шляхом радіовипромінювання, так і по проводах мережі електроживлення.

Вітчизняні виробники мережевих фільтрів для захищеної техніки гарантують припинення витоку інформації по проводах мережі електроживлення на частотах до 1 ГГц, залишаючи діапазон 1-10 ГГц “неприкритим”. Фільтри ФЗП-103 ефективно протидіють витоку інформації в діапазоні 10 кГц..10 ГГц., зменшуючи витік в мережу сигналів до рівнів, на яких їх неможливо прочитати та розшифрувати

Захист від високовольтних імпульсів другого ступеня жорсткості

Сфери застосування:

Мережі живлення екранованих (серверних) кімнат та сейфів, окремо розташованих захищених компютерів, станцій мобільного та стаціонарного зв”язку тощо

Мережі живлення пожежних та охоронних сигналізацій, будь-якого устаткування з електронною схемою керування – електротранспорт, літальні апарати, ракети і т.д.

Основні загрози, від яких захищають фільтри ФЗП-103: виведення з ладу електронного устаткування (в тому числі і джерел безперервного живлення – UPS) внаслідок:

- грозової активності навесні та влітку, ударів блискавки поблизу підстанцій

- індустріальних завад: роботи потужних промислових установок, зварювального обладнання, проходження магістралей міського електротранспорту поблизу об”єктів захисту, аварійних замикань

- електромагнітного тероризму - розрядів штучного походження, що надходять на об”єкт захисту зовні

Довідка: наявність захисту від високовольтних імпульсів другого ступеня жорсткості, тобто від дії високовольтних імпульсних завад великої енергії тривалістю 10...50 мкс та від дії пачок високовольтних імпульсних завад наносекундного діапазону, напругою до 1 кВ, у вітчизняному ГОСТ 30334-95 є обов”язковою для ВСІХ технічних засобів цифрової обробки сигналів.

Електробезпека при монтажі, обриві або відсутності заземлення

Попри високі захисні властивості, проблемою вітчизняних та багатьох зарубіжних електромережних фільтрів є іхній струм витоку. Струм витоку є мірилом безпеки фільтра для людей,які працюють з комп’ютером або монтують на ньому захисне обладнання. Оскільки комп’ютери належать до класу радіоелектронних пристроїв з неконтрольованим заземленням, фільтр зі струмом витоку більше 20..30 мА, під’єднаний до комп’ютера, може перетворитися на замаскованого електричного стільця при обриві або відсутності заземлення

Рис.1. Фільтри протизавадні

Фільтри протизавадні ФЗП-103-1,2,3. ТУ У 31.1.-31731859-001-2003, узгоджені з ДСТСЗІ, сертифікат відповідності ДЦВ ТЗІ № UA1.105.118222-03 від 31.12.2003. (див.рис.1)

Номінальна робоча напруга 220 В змінного струму частотою 50 Гц, номінальний струм споживача 3 А, струм витоку 3.5 мА

Основні технічні характеристики фільтрів ФЗП103-1:

- номінальна робоча напруга: 220 В змінного струму частотою 50 Гц;
- номінальний струм споживача: 3 А;
- струм витоку, не більше: 3,5 мА;
- захищений діапазон частот: від 10 кГц...до 10 ГГц;
- робочий діапазон частот: 10 кГц...8 ГГц;
- вношуване загасання фільтра, не менше, при несиметричній схемі вимірювання: -
- амплітуда мікросекундної імпульсної завади великої енергії* на клемах МЕРЕЖА при ефективному поглинанні її фільтром: до 1000 В;
- амплітуда пачки наносекундних імпульсних завад** на клемах МЕРЕЖА при ефективному поглинанні її фільтром: до 1000 В;
- маса, не більше: 1,5 кг;
- габарити, не більше: 205 х 64 х 53 мм;
- гарантійний термін: 3 роки;
- повний установлений строк служби: не менше 15 років.

*Згідно стандарту ГОСТ 29280; **згідно стандарту ГОСТ 29156.

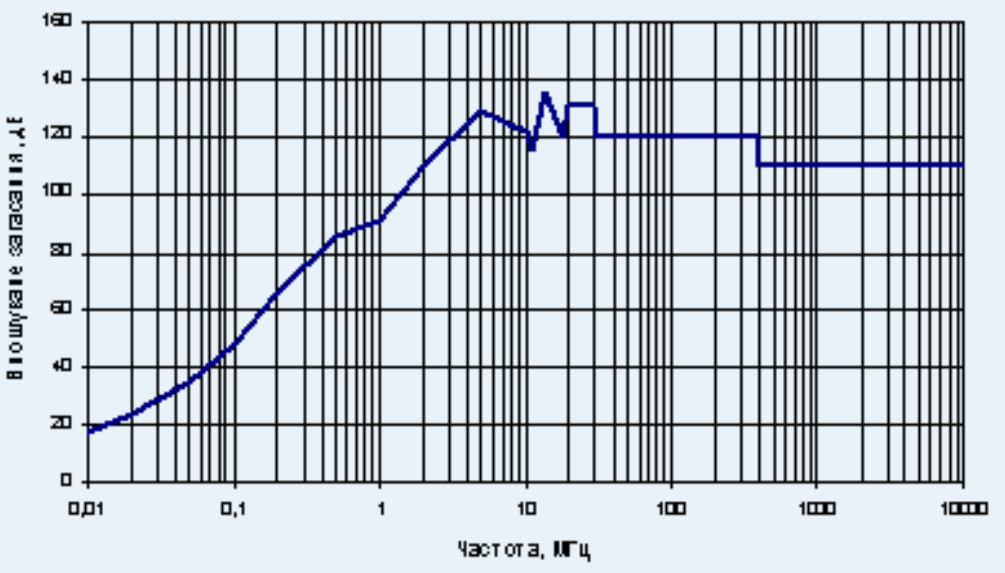

Рис. 2 Графік роботи протизавадного фільтру

Контрольні запитання для самостійної роботи

1. Для чого призначені діагностичні програми фірм- виробників комп'ютерів та комп'ютерного обладнання?
2. Наведіть кілька найбільш використовуваних діагностичних програм у складі операційних систем
3. Які відмінності мають діагностичні програми загального призначення від раніше згаданих діагностичних програм?
4. Дайте загальну характеристику найбільш використовуваних діагностичних програм загального призначення.

Тема:"Основні поняття і завдання технічної діагностики обчислювальних пристроїв і систем".

План

1. Основні поняття і завдання технічної діагностики
2. Поняття – технічне діагностування
3. Особливості технічного контролю як елемента діагностування
4. Види технічного контролю

Література [1] ст. 78-95

Застосування методів і засобів контролю обчислювальних пристроїв і систем дає змогу визначити, чи придатний об'єкт контролю для подальшого використання за основним призначенням. У разі непридатності використання за основним призначенням його вважають несправним. Для переведення об'єкта з несправного стану у справний необхідно знайти місце і причину прояву несправності, а також усунути її. Вивчення процесів виявлення несправностей, знаходження місця і причини їх прояву належать до галузі технічної діагностики.

Основні поняття і завдання технічної діагностики

Суть технічної діагностики обчислювальних пристроїв і систем

Технічна діагностика – галузь знань, що досліджує стани ОД і розробляє методи їх розпізнавання, визначає принципи проектування та організації пристроїв і систем технічного діагностування.

Предметом технічної діагностики є стан будь-яких технічних об'єктів, їх називають об'єктами діагностування (ОД).

Процес визначення стану ОД і є технічною діагностикою. Вона розв'язує такі основні завдання:

1) перевірка працездатності ОД. Якщо показники задовільні, переходять до використання пристрою або системи за призначенням, якщо ні – до аналізу їх стану;

2) пошук несправних компонентів і елементів ОД, у результаті якого необхідно їх знайти, а також вказати їхні дефекти (несправності) або причини відмови;

3) прогнозування стану об'єкта на чітко визначений час, коли відомий закон поступової зміни параметрів ОД., їх зміна призведе до того, що пристрій або система не зможе виконувати своїх функцій у майбутньому.

Технічний стан об'єкта – стан, який характеризують у певний момент часу за певних умов зовнішнього середовища значення параметрів, установлених технічною документацією на об'єкт.

Обчислювальні пристрої і системи можуть перебувати у справному або несправному стані. Якщо система перебуває в несправному стані, то в цій ситуації постають такі завдання:

1) пошук несправних елементів і компонентів. При цьому пошук несправних елементів є нижчим рівнем, ніж пошук несправних компонентів;

2) визначення вихідних параметрів компонентів і елементів. Якщо вони відхилилися від номінальних або не виконують своїх логічних функцій, то їх вважають несправними. Надалі компоненти і елементи підлягають відновленню чи заміні. В такому разі виконуються такі операції:

- виділяють компоненти і елементи, параметри яких відхилились від номінальних, але ще не перейшли граничні допуски;
- визначають швидкість виходу параметрів за граничні і на основі цього прогнозують стан об'єкта на майбутнє;

Залежно від типу елементів і компонентів об'єкта застосовують такі підходи: регульовані компоненти і елементи у разі оборотних змін параметрів підстроюють до номіналу, у протилежному випадку – замінюють справними, як і несправні нерегульовані

Поняття – Технічне діагностування

Технічне діагностування – процес визначення технічного стану об'єкта з означеною точністю.

Під ним розуміють процедуру локалізації несправностей об'єкта , тобто виявлення несправної частини ОД. Об'єктом технічного діагностування є виріб або його складові частини, технічний стан яких потрібно визначити.

Крім того, об'єктами технічного діагностування, особливо на етапах виробництва і експлуатації комп'ютерної техніки, є:

Пристрої з компонентами підвищеного ступеня інтеграції – змонтовані на друкованих платах цифрові пристрої, що є функцій ними вузлами модулів і блоків комп'ютерів та комп'ютерних систем, з наявними в них компонентами підвищеного ступеня інтеграції – цифровими ВІС та інтегральними схемами надвисокого ступеня інтеграції;

програмні засоби – засоби, що складаються з програм і документації, яка стосується їх функціювання;

системи програмування – програмні засоби, які функціюють у програмному середовищі та призначені для розроблення й використання програм.

Діагностування програмного забезпечення (ПЗ) здійснюють за допомогою:

програм контролю – діагностичних програм для перевірки вхідних програм або даних на наявність синтаксичних, семантичних та інших помилок;

програм трасування – діагностичних програм, що можуть простежити виконання кількох або всіх команд програми і записати результати кожного етапу.

Діагностування ПЗ спрямоване на пошук помилок – діяльність, внаслідок якої у програмі виявляють помилки, її здійснюють в основному на етапі налагоджування – виявлення, локалізації та усунення помилок у програмі.

Особливості технічного контролю як елемента діагностування

Технічний контроль – процес, забезпечує виявлення несправностей у роботі цифрових пристроїв , комп'ютерів, комп'ютерних систем і мереж, викликаних відмовою або збоями апаратурних засобів, помилками в програмах, помилкою оператора тощо.

Об'єктами технічного контролю є будь-яка продукція, процеси її створення використання, транспортування, зберігання, технічного обслуговування і ремонту, а також відповідна документація, процеси її створення, використання, транспортування, зберігання, технічного обслуговування і ремонту, а також відповідна документація.

Контроль ПКПСІ. Процес, який забезпечує встановлення їх відповідності заданим технічним нормам. Результат фіксують у формі"придатний-непридатний".

Контроль здійснюють у два етапи: 1) отримання первинної інформації про фактичний стан об'єкта контролю (ОК) та про ознаки і показники його властивостей; 2) співставлення первинної інформації із заздалегідь відомими вимогами, нормами, критеріями і отримання вторинної інформації про розбіжність фактичних і необхідних даних або виявлення відповідності (невідповідності) фактичних даних очікуваним.

Види технічного контролю

Залежно від завдань, що вирішують, виокремлюють контроль працездатності, прогнозуючий і діагностичний.

Контроль працездатності. Встановлює відповідність параметрів ОК певним, наперед заданим граничним значенням. При цьому констатують тільки правильність функціювання ОК без зазначення причини відмови.

Прогнозуючий контроль. На основі проведених контрольно-вимірювальних операцій з певною ймовірністю передбачають поведінку ОК протягом певного часу після цієї процедури.

Діагностичний контроль. Визначають не тільки відповідність ОК його технічним характеристикам, а й встановлюють причини відмови. Таке визначення співзвучне технічному діагностуванню, але треба мати на увазі, що при діагностуванні встановлення несправності ОК проводять на нижчому ієрархічному рівні.

Контроль здійснюють за допомогою апаратури або засобів контролю технічного стану, що включають апаратуру і програми. Щодо засобів, які використовуються для реалізації контролю, його поділяють на апаратний, програмний і змішаний.

Апаратний контроль. Здійснюють за допомогою апаратури контролю, його характеризує висока швидкість.

Програмний контроль. Проводять засобами контролю, але при цьому відпрацьовують діагностичні програми. Він пов'язаний з додатковими витратами процесорного часу і необхідністю збільшувати об'єм пам'яті для розміщення програм контролю.

Змішаний контроль. Поєднує апаратний і програмний контролі з метою їх спрощення та підвищення ефективності. Як засвідчує досвіт, така практика є найдоцільнішою.

За характером взаємодії засобів контролю з ОК розрізняють активний і пасивний контроль.

Активний контроль. Об'єкт контролю вивчають шляхом подачі тестових впливів на його входи, а також генерації певних режимів з відповідними параметрами;

Пасивний контроль. Стан об'єкта визначають на основі вивчення вихідних параметрів, наявних в ОК за фізичною природою його функціювання (амплітуда, частота та інші параметри вихідних сигналів).

Залежно від часу проведення контроль поділяють на оперативний і тестових.

Оперативний контроль. Здійснюють у процесі вирішення основних експлуатаційних завдань. Він дає змогу виявляти несправності безпосередньо під час відпрацювання завдань. Такий контроль є неповним, оскільки його виконують на невідповідних для нього завданнях.

Тестовий контроль. Проводять у спеціально відведені проміжки часу з метою розв'язання тестових завдань. Це забезпечує контроль об'єкта в цілому або його компонентів і елементів, а також контроль виконання команд програми.

Для з'ясування оцінюючих характеристик стану ОК використовують допусковий, кількісний та інформаційний контроль.

Допусковий контроль. Встановлює дійсне значення параметра відносно його гранично допустимих значень без вимірювання значення параметра

Кількісний контроль. Дає кількісну оцінку відхилення параметрів ОК від їх номінальних і граничних значень, а також вимірює і оцінює абсолютні значення параметрів, що контролюються.

Інформаційний контроль(доповнення до кількісного контролю). Забезпечує локалізацію місця виникнення передбачуваної несправності й надає інструкції для її усунення.

Крім цих видів контролю, використовують:

Параметричний контроль – контроль, що здійснюють шляхом вимірювання електричних параметрів пристроїв і сигналів, які вони обробляють.

Функцій ний контроль – перевіряє здатність ОК правильно виконувати функції, покладені на нього.

Функційно-статичний контроль – перевірку правильності функціювання ОК здійснюють у діапазоні мінімальних і максимальних робочих частот.

Внутрішньо схемний контроль – за якого тестові впливи подають на внутрішні контрольні точки друкованих плат, а з інших внутрішніх контактів контрольних точок цієї плати знімають відповідні реакції.

Контрольні запитання для самостійної роботи

1. У чому суть технічної діагностики? Які основні завдання вона вирішує?
2. Поясніть, у чому суть технічного діагностування.

3. Обґрунтуйте поняття “технічний контроль в обчислювальній техніці “
4. Назвіть і охарактеризуйте види контролю
5. Особливості контролю як елемента діагностування.
6. Оцінювання ефективності діагностування обчислювальних пристроїв.

Методи діагностування цифрових, мікропроцесорна пристроїв і ПК

Тема:”Цифрові і мікропроцесорні пристрої як об‘єкти діагностування”.
План

1.Види тестового діагностування
2.Комбінації і стратегії систем тестування
3.Алгоритм пошуку несправностей за тестовим діагностуванням
Література [1]ст. 96-131

Види тестового діагностування

Під діагностуванням у радіоелектроніці та в обчислювальній техніці розуміють процедуру локалізації несправностей ОД. Виокремлюють декілька видів діагностування (контролю).

1. Робоче технічне діагностування (робоче діагностування). Його суть полягає в подачі на об’єкт робочих впливів.

2. Тестове технічне діагностування (тестове діагностування). На об’єкт подають тестові впливи.

3. Експрес-діагностування. Проводять за обмеженої кількості параметрів протягом заздалегідь установленого часу.

4. Оперативне тестове діагностування (оперативне діагностування). Надходження інформації про технічний стан об’єкта за заздалегідь спланованою стратегією в процесі функціювання об’єкта.

5. Безперервне технічне діагностування (безперервне діагностування). Надходження інформації про технічний стан об’єкта відбувається безперервно.

6. Періодичне технічне діагностування (періодичне діагностування) надходження інформації про технічний стан об’єкта відбувається через встановлені інтервали часу.

7. Самодіагностування. Здійснюється за допомогою вмонтованих засобів діагностування.

Часто використовують також функційне, тестове і змішане діагностування.

1. Функційне діагностування. Вхідними впливами, що надходять на ОД, є робочі впливи, передбачені робочим алгоритмом функціювання об’єкта. Не слід плутати функційне діагностування з діагностуванням об’єкта в процесі його функціювання (це більш загальне поняття). Функцій не діагностування, наприклад ТЕЗа чи окремого модуля, може проводитись не під час функціювання системи, складовою частиною якої вони є, а здійснюватися за допомогою зовнішніх засобів шляхом емуляції роботи цієї системи. Це, по суті, робоче діагностування. Функційне діагностування поділяють на апаратне, програмне і змішане.

2. Тестове діагностування. На ОД подають тестові дії, що відрізняються від робочих. Вихідні реакції ОД і вхідні впливи набувають специфічного характеру, невластивого

робочим режимам об’єкта. У тестовому діагностуванні виокремлюють: загальне (структурне), по компонентне і комбіноване.

—Тестове загальне (структурне) діагностування. Його здійснюють у цілому, тобто контролюють цілісність і правильність монтажу, вихідних параметрів ОД та правильність виконання відповідних функцій всією структурою об’єкта. Тестові дії подають на входи ОД через крайові з’єднувачі, а відповідні реакції знімають з вихідної частини з’єднувачів, інколи – із внутрішніх контрольних точок структури об’єкта.

Загальне діагностування поділяють на функцій не тестування, параметричний контроль, функційно-параметричний контроль (йому відповідає термін “контроль технічного стану” або визначення продуктивності комп’ютерної системи).

— Тестове по компонентне діагностування. Це послідовність окремих перевірок кожного компонента структури, за умови, що на нього не впливають зв’язані з ним компоненти. У таких випадках діагностуванням вважають ідентифікацію несправностей (процес виявлення несправності із заданою точністю) елементів контрольованих компонентів. ЇЇ поділяють на етапи: констатація факту наявності несправності; встановлення типу і класу несправності; встановлення місця прояву несправності.

У покомпонентному діагностуванні виокремлюють по елементне, пофрагментене і змішане.

—Поелементне діагностування. Передбачає проведення допускового контролю під час оцінювання параметрів кожного електрорадіоелемента пристрою. Тому такий вид діагностування інколи називають внутрішньо схемним параметричним контролем, внутрішньо схемним діагностуванням або внутрішньо схемним контролем.

—Пофрагментне і змішане діагностування. Ці види діагностування характеризують об’єкт, до якого належать.

—Тестове комбіноване діагностування. Проведення певних послідовних структурних і по компонентних перевірок як об’єкта в цілому, так і його фрагментів, компонентів і елементів спільними апаратурними засобами. Це спрощує процес тестування за рахунок його максимального наближення до робочих режимів функціювання пристрою, який діагностують, пошуку несправностей різних класів. Досягнення заданої глибини пошуку дефектів.

Змішане діагностування. Охоплює комбінації різноманітних видів діагностування.

Засоби діагностування поділяють на такі види:

– автоматичний засіб технічного діагностування. Функціює без участі оператора;

– Автоматизований засіб технічного діагностування. Функціює з частковою участю оператора;

– Вмонтований засіб технічного діагностування. є складовою частиною об’єкта;

– Зовнішній засіб технічного діагностування. Конструктивно відокремлений від об’єкта ;

– Бортовий засіб технічного діагностування. як самостійний виріб входить до складу бортового літального чи іншого рухомого апарата;

– Наземний засіб технічного діагностування. входить до складу наземного устаткування;

– Спеціалізований засіб технічного діагностування. призначений для діагностування одного об’єкта або групи однотипних об’єктів.

Види тестового діагностування.

Функційне діагностування. При реалізації цього методу вхідними впливами , що надходять на об’єкт діагностування, є робочі впливи, які передбачені робочим алгоритмом функціювання об’єкта.

Тестове структурне (загальне) діагностування. Його суть полягає у цілому. На входи МПП подають тестові впливи, а на виходах реєструють відповідні реакції, за якими аналізують правильність виконання функцій, що реалізуються цифровою структурою пристрою.

Необхідними умовами здійснення структурного методу діагностування є вимірювання і аналіз різноманітних діагностичних параметрів ОД, а також виконання складних процедур і програм перевірок, що, в свою чергу, ускладнює процедуру діагностування.

Тестове покомпонентне діагностування. Його суть полягає у проведенні послідовних перевірок кожного компонента структури окремо при виконанні умови виключення взаємного впливу зв’язаних з ним компонентів. Компонентами в даному випадку є вмонтовані в друковану плату інтегральні схеми та ін.

Діалектично методи структурного і по компонентного тестування взаємодоповнюють один одного з точки зору повноти діагностування і глибини пошуку несправностей. Тому комбінація цих методів є виправданою. Під час її здійснення структурні і по компонентні перевірки поєднують за певними стратегіями.

Найбільш повною комбінацією цих методів реалізують у методі тестового комбінованого діагностування обчислювальних пристроїв. При цьому комбіноване тестування не ототожнюють з простим поєднанням структурних і по компонентних перевірок. Тестове комбіноване діагностування описує власна теорія, стратегії і алгоритми.

Тестове комбіноване діагностування. Під ним розуміють тестування, що полягає у проведенні послідовних структурних і по компонентних перевірок як ОД у цілому, так і його фрагментів і компонентів спільними апаратурно-програмними засобами. Це здійснюють з метою спрощення процесу тестування за рахунок його максимального наближення до робочих режимів роботи обчислювального пристрою чи системи, які діагностують. Пошуку несправностей різних класів. Досягнення необхідної глибини пошуку несправностей.

Комбінації і стратегії систем тестування

Для підвищення ефективності процесу діагностування на виробництві використовують різні комбінації систем тестування в одній технологічній лінії та різні стратегії. Серед них — послідовна (тандемна), паралельна і паралельно-послідовна (паралельно-тандемна).

За послідовної стратегії за допомогою систем по компонентного діагностування (СПД) виявляють насамперед статичні несправності. Якщо такі є, то їх усувають у процесі усунення несправностей (УН). Після цього ОД подають на систему структурного діагностування (ССД) для контролю за принципом “придатний-непридатний”.

При паралельній стратегії за допомогою ССД проводять передусім відбракування за принципом “придатний-непридатний”. Потім несправні ПКПСІ надходять для ідентифікації несправностей статичного типу на СПД, після їх усунення вони повертаються для повторного контролю за принципом “придатний-непридатний”.

При паралельно-послідовній стратегії за допомогою першої ССД здійснюють спочатку контроль за принципом “придатний2-непридатний”. Потім вироби, що не пройшли контроль, надходять на СПД для ідентифікації несправностей статичного типу. Після їх усунення їх передають на іншу ССД для контролю за принципом “придатний-непридатний” та ідентифікації окремих класів динамічних несправностей.

При реалізації тестування ПКПСІ за допомогою системи комбінованого діагностування (СКД) воно істотно спрощується. Конфігурація технологічної лінії для всіх стратегії буде одна й та сама. До її складу входять СКД і дільниця (технологічне місце) усунення несправностей.

При послідовній стратегії тестування, що реалізується на СКД, контроль за принципом “придатний-непридатний” не проводять. Спочатку ідентифікують і усувають несправності статичного типу. Якщо їх немає, то ті самі операції здійснюють з несправностями динамічного типу і на цій основі роблять висновок про придатність виробу. Така стратегія найефективніша, коли кількість несправностей статичного і динамічного типів досить велика і вироби випускають порівняно невеликими серіями.

У паралельній стратегії тестування ПКПСІ, що реалізується на СКД, виокремлюють два типи.

1. Здійснюють контроль за принципом ”придатний-непридатний”. У відбракованих виробах ідентифікують і усувають несправності статичного типу. Після цього вони повторно проходять контроль за принципом ”придатний-непридатний”. Ця стратегія найефективніша, якщо несправності динамічного типу мають незначну питому вагу і вироби випускають великими серіями.

2. Здійснюють контроль за принципом ”придатний-непридатний”. У відбракованих виробах ідентифікують і усувають несправності статичного типу. На цій основі роблять висновок про придатність виробу. Така стратегія найефективніша, коли ігнорують ідентифікацію несправностей динамічного типу, і це призводить до необґрунтованих втрат при різній серійності виробництва ПКПСІ.

Стратегії тестового комбінованого діагностування порівняно зі стратегіями поетапного застосування систем структурного і по компонентного діагностування простіші і ефективніші. Цього досягають, використовуючи насамперед тільки одну систему діагностування — СКД у процесі діагностування ПКПСІ. Це дає змогу уникнути необхідності передавати вироби для тестування від однієї системи до іншої, внаслідок чого зменшується кількість операторів і обслуговуючого персоналу.

Крім того. Комбінації ССД і СПД орієнтовані в основному на ідентифікацію несправностей статичного типу. А використовуючи стратегії СКД та ідентифікуючи водночас несправності статичного і динамічного типів, можна підвищити достовірність контролю та діагностування ПКПСІ.

Алгоритм пошуку несправностей за тестовим діагностуванням

Для розроблення алгоритмів пошуку несправностей за тестового комбінованого діагностування ПКПСІ використовують такий ієрархічний підхід:

1) визначення несправних ПКПСІ шляхом відбракування виробів за принципом “придатний-непридатний”;

2) визначення несправних фрагментів ПКПСІ певних функцій них вузлів;

3) визначення несправних компонентів і елементів у фрагменті структури ПКПСІ.

Етап 1.

Проводять структурне тестування ОД шляхом подавання тестових впливів, що найбільш наближені до робочих. Тестові послідовності складають на основі інформації про алгоритм роботи пристрою. Це спрощує їх складання.

Етап 2.

Здійснюють тестування фрагментів структури пристроїв (фрагментів ТЕЗів) шляхом подавання сигналів тестових впливів. Що генерують відповідно до часової діаграми роботи цих фрагментів, і зчитування відповідних реакцій в запрограмований момент. Модель фрагмента складають на алгоритмічному або функційному рівні, що робить простішим складання тестових послідовностей.

Етап 3.

Проводять по компонентно-структурне тестування, передусім компонентів підвищеного ступеня інтеграції — ВІС і НВІС фрагмента структури. Тестову програму для діагностування розробляють на основі їх моделей.

Контрольні запитання для самостійної роботи

1. Дефекти і несправності цифрових і мікропроцесорних пристроїв
2. Які основні відмінності кількісного контролю від інформаційного?
3. Що розуміють під діагностуванням в обчислювальній техніці? Назвіть його види.
4. Охарактеризуйте процедуру ідентифікації несправностей.
5. У чому суть функційного діагностування і чим воно відрізняється від тестового?
6. Дайте характеристику поняттю “ефективність системи діагностування “. Яким чином її визначають?
7. Особливості МПП як об‘єктів діагностування.
8. Принципи діагностування МПП.

Тема „Контроль і діагностування багатопроцесорних систем”
План

1. Суть процесу діагностування багатопроцесорних систем: Види ядер
2. Класифікація моніторів

Література [1]ст.132-140

Суть процесу діагностування багатопроцесорних систем

Тестове діагностування багатопроцесорних систем (БПС) здійснюють різними способами. Найпоширенішим з них є спосіб організації діагностування БПС за допомогою ядра.

Ядро – сукупність апаратних і програмних засобів, що забезпечують реалізацію тестового діагностування системами.

Ядро завжди вважають справним. Є кілька типів ядер. Серед них виокремлюють плаваюче, жорстке, централізоване і розподілене ядро.

Плаваючим ядром називають ядро, склад якого непостійний.

Жорстке ядро – ядро, склад якого постійний.

Централізованим вважають ядро, що організують на одному заздалегідь візначеному справному комп”ютері.

Розподілене ядро – ядро, що може бути організоване на будь-якому комп”ютері комп”ютернох системи (КС), навіть на неперевірений. Істинний стан системи при цьому візначають у процесі взаємних перевірок.

Одні з найпоширених – БПС із централізованим ядром, для побудови яких використовують спеціальний обслуговуючий сервісний процесор, призначений для контролю чи діагностування системи, а також підтримання працездатності основної системи, зокрема центрального процесора. Як обслуговуючий процесор, використовують автономний комп”ютер, що має свою конструкцію. Щоб зменшити ймовірність спільних відмов обслуговуючого і основного процесора, їх часто функційно і конструктивно відділяють один від одного. Обслуговуючий процесор має своє окреме програмне забезпечення, яке сумісне з програмним забезпеченням основного процесора, але не перебуває під його контролем.

Аппаратура обслуговуючого процесора складається з контролера (пристрою керування) із засобами порівняння кодови комбінацій, набору адаптерів, призначених для спрягання обслуговуючого процесора з пристроями основної системи, одного або кількох пультів керування з дисплеями. До системи можуть входити і дистанційні пульти керування, зв”язані з обслуговуючим персоналом через модеми, що служать для передавання сигналів через канази зв”язку. Вони знаходяться в центрі обслуговування різних обчислювальних систем.

Класифікація моніторів

Монітори будують на основі різноманітних методів вимірювань і засобів їх реалізації. Серед них виокремлюють трасуючий і вибірковий методи.

Трасуючий метод. Полягає у реєстрації подій, що відповідність моментам зміни стану обчислювальної системи. До них належать початок і кінець завдання, крок завдання, етап процесорної обробки, звертання до зовнішньої пам”яті та ін. Монітори, що вимірюють процес функціювання системи цим методом, називають трасуючими.

Монітор реєструє події у вигляді подвійного набору даних Т, що складається з послідовності записів Si, S2, S3 …, які відповідають послідовності подій. Тут реєструють момент виникнення події, імена процесу (I^^Ja*-“) і ресурсу, з якими вона пов”язана, і параметри події, наприклад число байтів даних, що передаються. Використання пристрою системи можуть відображати діаграми.

Вібірковий метод. Його функцією є реєстрація стану обчислювальної системи в задані моменти часу через проміжки d. У моменти t = ni, n = 1,2,3…, вибірковий монітор реєструє стан системи, фіксуючи у відповідних записах дані з керуючих таблиць. Можна фіксувати електричні сигнали, що характеризують стан пристроїв системи в задані моменти. Отримані дані дають змогу оцінити тривалість процесів і розміри ресурсів, а також ймовірність станів.

Тривалість станів визначають як Pt =ni/n , де ni – кількість вибірок, при яких зареєстровано даний стан i, n - тривалість процесу вимірювань, що визначають кількістю вибірок. Головна перевага вибіркового монітору – вимірювання безлічі швидких процесів за обмеженої швидкості.

Залежно від виконуваних функцій монітори поділяють на універсальні і спеціалізовані.

Універсальний монітор. Реєструє всі події чи більшість із них. Тому подійного набору достатньо, щоб побудувати трасу процесів і використання ресурсів. Обсяг даних, що вимірюються, досить великий і становить 10^7 і більше байт на один процес. Універсальні монітори використовують в окремих випадках, наприклад для оцінювання конкретних системних або прикладних процесів.

Спеціалізований монітор. Реєструє певну частину подій чи станів. Це спрощує процес вимірювань. Такі монітори широко використовують для обліку виконаних робіт та оцінювання завантаженності ресурсів, а також як постійно діючи вимірювальні засоби для діагностування систем протягом усього часу їх функціонування.

Для діагностування комп”ютерних систем використовують програмні монітори. Вони реалізовані у вигляді програми, яку виконує ця сама комп”ютерна система. Залежно від їх місцезнаходження в комп”ютерній системі програмні монітори поділяють на вбудовані й автономні.

Вдубований програмний монітор. Це сукупність програм, що входять до складу операційної системи. Він має статус керуючої програми операційної системи і призначений для видачі мінімальних відомостей про систему.

Автономний програмний монітор. Це сукупність прикладних програм операційної системи. Вони дають змогу фіксувати широкий спектр подій при трасуючому і вібірковому методах вимірювань. Призначені для видавання розширених відомостей про систему.

Крім того, існують апаратурні монітори. Комплекс технічних і програмних засобів, призначених для діагностування процесів функціонування комп”ютерних систем. Монітор, аналізуючи електричні сигнали, що характеризують стан окремих блоків і пристроїв системи, отримує інформацію про її стан . вимірювання проводять у визначених точках блоків і пристроїв за допомогою зондів. Дані вимірювань записують на певні носії та аналізують, їх оперативні оцінювання використовують для контролю за правильністю функціювання.

Контрольні запитання для самостійної роботи

1. Охарактеризуйте етапи пошуку несправностей пристроїв з компонентами підвищеного ступеня інтеграції, згідно з ієрархічним підходом при тестовому комбінованому діагностуванні.
2. Назвіть особливості мікропроцесорних пристроїв як об'єктів діагностування. Чим вони зумовлені?
3. Які основні принципи сучасної методології тестування МПП?
4. У чому суть способу організації діагностування багатопроцесорних систем за допомогою централізованого жорсткого і плаваючого ядра, розподіленого жорсткого і плаваючого ядра?
5. Охарактеризуйте функції , які виконує обслуговуючий сервісний процесор.
6. Які події реєструють універсальний і спеціалізований монітори?
7. Ідентифікація несправностей локальних обчислювальних мереж.

Тема „Методологія поетапного діагностування цифрових і мікропроцесорних пристроїв"

План

1. Сутність технологічного процесу діагностування
2. Реалізація технологічного процесу діагностування
3. Особливості моделювання процесу діагностування на різних етапах життєвого циклу пристрою

Література [1] ст.140-173

Сутність технологічного процесу діагностування

Кожен пристрій проходить процеси проектування, виробництва і експлуатації. Виробничий процес можна поділити на сукупність часткових процесів – основних, допоміжних і обслуговуючих. Слід розглянути основні процеси, тобто технологічні процеси виробництва, а також процеси проектування і експлуатації. Зокрема, звернути увагу на поетапний процес діагностування Ц і МПП.

Технологічний процес діагностування Ц і МПП складається з послідовних технологічних діагностичних операцій. Може бути представлений лінійно, циклічно або комбіновано.

Лінійний технологічний процесс діагностування – це послідовний ланцюжок операційний.

Циклічний технологічний процес діагностування – замкнута послідовність операцій ланцюжка.

Комбінований технологічний процесс діагностування – послідовний ланцюжок технологічних операцій з паралельними розгалуженнями і (або) замкнутими ланцюжками операцій.

Основні принципи технологічного процесу діагностування Ц і МПП: можливість реалізації; розумна достатність і раціональність (економічна ефективність); поетапна наступність та ієрархічність реалізації.

Структурною одиницею технологічного процесу діагностування Ц і МПП є технологічна діагностична операція – частина технологічного процесу діагностування,

яку здійснюють над одним чи кількома ОД, на одному робочому місці, одним чи кількома спеціалістами-експертами або спеціалістами-розробниками.

Технологічні процеси діагностування Ц и МПП базуються на відповідних методах діагностування. наЙпоширеніши з них: функційний, тестовий і змішаний.

Методи тестового діагностування реалізують в основному за допомогою зовнішніх щодо МПП засобів. Внутрішні засоби діагностування використовують для контролю діагностування функцій, які має виконувати МПП.

Вибір методу діагностування залежить від обраного рівня моделі мікропроцесорного пристрою як ОД.

Основними принципами моделювання Ц і МПП як об"єктів діагностування є: багаторівневе моделювання МПП; синтез математичної моделі МПП або цифрових пристроїв за їх фрагментами, які можна подавати на різних ієрархічних рівнях; опис компонентів підвищеного ступеня інтеграції (ВІС і НВІС) покомпонентно-структурними моделями на етапах виробництва і експлуатації.

Головні цілі моделюванная:

- розроблення детального формалізованого опису технологічного процесу діагностування Ц и МПП;
- задання послідовності й взаємозв"язку технологічних діагностичних операцій процесу діагностування;
- одержання необхідних значень діагностичних параметрів ОД;
- вибір критеріїв оптимізації моделей діагностування з метою подальшої оцінки ефективності технологичного процесу.

Особливості моделювання на різних етапах життєвого циклу пристрою

Моделювання процесу діагностування Ц МПП здійснюють на етапах проектування, виробництва та експлуатації пристрою.

Моделювання на етапі проектування. Особливості моделювання процесу діагностування Ц і МПП на етапі проектування пов"язані з особливостями діагностичних операцій. Щодо пристроїв, змонтованих на друкованих платах (картриджах), такими діагностичними операціями є:

- вибір тестопридатних мікропроцесорних комплектів (набірів мікросхем системної логіки) інтегральних схем (ІС);
- розроблення фрагментів тестових структур пристрою на базі спеціальних ІС;
- розроблення методик компонування елементів і компонентів пристроїв, враховуючи вимоги контролю і діагностування (необхідна кількість контрольних точок, транспортування несправностей на вихід структури пристрою або на контрольні точки для спостереження їх прояву);
- вибір додаткових контрольних точок для діагностування пристрою;
- декомпозиція структури (цифрової, аналого-цифрової) пристрою з метою реалізації обраного методу діагностування;
- аналіз і вибір міжкомпонентних та міжфрагментних зв"язків (ліній, шин, магистралей) для діагностування пристрою.

Діагностичні операції класифікують на три групи:

1. Діагностичні операції при розробленні узагальненої моделі процесу діагностування. Цю групу описує множина загальних діагностичних операцій Е, які спільні для всіх етапів життєвого циклу пристрою або системи.

2. Діагностичні операції, пов”язані з особливостями моделюваня процесу діагностування на етапі проектування. Вони становлять множину Еосп..

3. Усі діагностичні операції, задіяні в процесі діагностування пристроїв на етапі проектування, становлять множину Епр.. Моделювання процесу діагностування полягає у вибірковому поєднанні загальних діагностичних операцій множини Евиб. а Е з діагностичними операціями множини Еосп.-. У результаті утворюється ланцюжок діагностичних операцій, який описує множина Епр., що є об”єднанням діагностичних операцій процесу діагностування пристроїв на етапі проектування.

Моделювання на етапі виробництва. Діагностичними операціями процесу діагностування Ц і МПП на етапі виробництва, що пов”язані з особливостями моделювання, є:

- вхідний контроль компонентів пристрою з метою виявлення несправностей компонентів (невиконання заданих згідно з технічними умовами функції, незадовільні робочі характеристики та ін.);
- візуальний контроль пристроїв з метою виявлення механічних пошкоджень плати або компонентів, неправильної орієнтації мікросхем на платі видносно шин живлення, незмонтованих компонентів, компонентів з іншими реалізуючими функціями та ін.;
-програмний контроль за принципом “придатний-непридатний” для встановлення правильності функціювання ОД і відбракування несправних пристроїв;
- виявлення детермінованих несправностей;
- ідентифікація статичних несправностей (коротке замикання провідників, обриви, константні (“=0” чи “=1”) і логічні несправності та ін.);
- ідентифікація динамічних несправностей (логічні і не логічні несправності), зокрема, тих, причини яких “змагання” сигналів, несправностей, що проявляються в результаті дії завад, які виникають у лініях під час перемикання груп елементів компонента чи компонентів пристрою та ін.);
- ідентифікація несправностей, пов”язаних із шинною структурою пристрою;
- виявлення випадкових несправностей;
- повторний програмний контроль за принципом “придатний-непридатний” після усунення виявлених несправностей.

Ці операції теж поділяють на три групи:

1. Діагностичні операції, перераховані при розробленні узагальненої моделі процесу діагностування. Вони складають елементи множини Е. Їхня основна властивість та, що частина їх або всі вони можуть входити до складу діагностичних операцій будь-якого життєвого циклу пристрою.

2. Діагностичні операції, властиві процесу діагностування тільки на етапі виробництва. Вони – елементи множини Еже..

3. Усі діагностичні операції задіяні в процесі діагностування пристроїв на етапі виробництва. Це елементи множини Евир.

Моделювання процесу діагностування пристроїв на етапі виробництва – вибіркове поєднання загальних діагностичних операцій множини Е з діагностичними операціями множини Еосв. Утворюеться ланцюжок діагностичних операцій, що є елементами множини Евир. Він і складає послідовність діагностичних операцій процесу діагностування Ц і МПП на етапі виробництва.

Послідовність проведення № діагностичних операцій – це стратегія діагностування Ц і МПП. Її вибір грунтується на застосованому методі діагностування і відповідних апаратних і програмних засобах.

Моделювання на етапі експлуатації. Головне завдання процесу діагностування Ц і МПП на етапі експлуатації полягає в контролі працездатності пристрою та визначенні дефектних компонентів і елементів у разі його несправності. Особливість цього процесу в тому, що контроль працездатності здійснюють на місці використання об"єктів за основним призначенням. За наявності резервний справний пристрій замінює несправний. Діагностування пристрою з глибиною пошуку несправності до компонента чи елемента проводять здебільшого в діагностичних лабораторіях. При здійсненні контролю працездатності переважають програмні засоби, а при ідентифікації несправних компонентів і елементів пристрою використовують як програмні, так і апаратні. Це слід враховувати, моделюючи процесс діагностування пристроїв на етапі експлуатації.

Особливості моделювання процесу діагностування пристроїв на етапі експлуатації пов"язані з такими діагностичними операціями:

- періодичний візуальний контроль пристроїв щодо механічних та інших пошкоджень;
- програмний контроль пристрою під час вмикання в мережу живлення або проведення профілактичних робіт;
- контроль і діагностування за допомогою діагностичних програм операційних систем на місці використання пристрою за основним призначенням;
- контроль і діагностування за допомогою програм фірм-виробників пристроїв, який проводять на місце їх використання за основним призначенням;
- контроль і діагностування за допомогою програм фірм-виробників пристроїв, що здійснюють у спеціолізованих діагностичних лабораторіях;
- контроль і діагностування пристроїв за допомогою програм фірм, які спеціалізуються на їх розробленні, здійснюють у спеціалізованих діагностичних лабораторіях.

Ці діагностичні операції можуть поділятися на підоперації нижчого ієрархісного рівня залежно від типу контрольованого або діагностованого пристрою і типів несправностей, що ідентифікують у ньому.

На єтапі експлуатації віявлять недоліки і помилки моделювання попередніх етапів. З метою їх усунення інформацію про них передають у підрозділи, що проектують і виробляють Ц і МПП.

Контрольні запитання для самостійної роботи

1. Обґрунтуйте поняття "несправність Ц і МПП ".
2. У чому суть збою Ц або МПП?
3. Що, на вашу думку , є причинами виникнення дефектів на етапі виробництва обчислювальних пристроїв?
4. Назвіть типи несправностей обчислювальних пристроїв. Дайте їм загальну характеристику.
5. Поясніть взаємозв'язок класів і підкласів несправностей обчислювальних пристроїв.
6. Розкрийте суть технологічного процесу діагностування Ц або МПП.

7. Особливості моделювання на різних етапах життєвого циклу пристрою. Процес поетапного діагностування.

Засоби діагностування цифрових і мікропроцесорних пристроїв

Тема:"Апаратні засоби діагностування цифрових МПП і ПК".

План

1. Види апаратних засобів
2. Види контролю і діагностування
3. Вимоги до систем діагностування
4. Структура систем діагностування

Література [1] ст. 182-195

Апаратні засоби діагностування цифрових і мікропроцесорних пристроїв

Сьогодні важко перевагу апаратним або програмним засобам діагностування Ц і МПП. Найкращий результат дає їх комбінація, оскільки програмні засоби діагностування мають відпрацьовуватись за допомогою апаратних засобів.

Класифікація апаратних засобів контролю діагностування

Апаратні засоби діагностування Ц і МПП поділяють на зовнішні і вбудовані. Зовнішні засоби конструктивно від'єднані від ОД, а вбудовані входять до його складу.

До зовнішніх апаратних засобів контролю і діагностики Ц і МПП належать: контрольно-вимірювальні прилади, пульти, стенди; аналізатори і тестери; контрольно-діагностичні комплекси і системи.

Контроль-вимірювальні прилади, пульти і стенди. Їх використовують для ремонтів, сервісного обслуговування, вхідного і вихідного контролю при ручному способі та слабко вираженій автоматизації цих процесів.

Аналізатори і тестери. Застосовують для параметричного, функційного, тестового або комбінованого контролю і діагностування ІС, у тому числі ВІС і НВІС, а також змонтованих на їх базі вузлів, пристроїв, що розміщують на друкованих платах . за допомогою більшості цих засобів процес контролю автоматизують, а самі вони можуть бути як універсальні, так і спеціалізовані. Керування їхньою роботою здійснює вмонтована в них мікроЕОМ.

Контрольно-діагностичні комплекси і системи. Їх використовують для здійснення всіх чи окремих видів контролю і діагностування ІС різного ступеня інтеграції, змонтованих друкованих плат, цифрових пристроїв і систем. Процес контролю і діагностування за допомогою цих засобів частково або повністю автоматизований. У структурі комплексу чи системи є одна або кілька ЕОМ.

Види контролю і діагностування

Критерії класифікації апаратури контролю і діагностування: функційне призначення, види контролю і діагностування, ступінь автоматизації процесу контролю і діагностування, етапи контролю і діагностування, конструктивне виконання засобів контролю і діагностування.

Функційне призначення. Характеризує засоби контролю і діагностування за спеціалізацією. Засоби контролю та діагностування обчислювальних пристроїв і систем за функційним призначенням можна поділити на апаратуру для контролю і діагностування інтегральних схем малого і середнього ступенів інтеграції, друкованих плат та мікропроцесорів, мікропроцесорних пристроїв, комп'ютерних систем.

Види контролю і діагностування. За цим критерієм засоби поділяють на апаратуру параметричного, функційного, тестового контролю і діагностування.

Ступінь автоматизації процесу контролю і діагностування. визначає продуктивність і технічні можливості засобів. Ступінь автоматизації має градацію.

Апаратура з ручним керуванням. Їх використовують як контрольно-вимірювальні прилади та прості стенди на різних етапах життєвого циклу обчислювальних пристроїв. Це зумовлено простотою користування і порівняно низькими вартісними витратами. Але вона мало продуктивна.

Автоматизовані засоби (системи) контролю і діагностування. вони мають значно більша продуктивність. Використовуючи такі системи вручну, можна проводити контактування ОД із системою, початкове завантаження системи і деякі інші операції. Контролю або діагностування проводять у діалоговому режимі.

Засоби автоматичного контролю і діагностування. Вони найефективніші. Увесь процес контролю чи діагностування проходить автоматично після задання початкових умов.

Етапи контролю і діагностування. тісно пов'язані з етапами життєвого циклу обчислювальних пристроїв і систем, зокрема етапами проектування, виробництва і експлуатації.

Етап проектування. За допомогою лабораторних досліджень перевіряють правильність синтезованих цифрових структур, а також налагодження і коригування технологічного процесу виготовлення пристроїв.

Етап виробництва. Його починають з відбракування непридатних комірок кристала. До складу такої апаратури входить зондова установка для перевірки фрагментів структури кристала. За допомогою апаратури вхідного контролю проводять відбір ІС різних ступенів інтеграції за критеріями надійності, електричної і функційної сталості параметрів.

Етап експлуатації. Під час діагностування, сервісного обслуговування і ремонтів обчислювальних пристроїв і систем за допомогою апаратних засобів проводять контроль ІС, змонтованих друкованих плат і вузлів, а також пристроїв у цілому з метою пошуку дефективних компонентів і заміни їх справними. Також при цьому широко використовують програмні засоби.

Конструктивне використання засобів контролю і діагностування. Залежить воно від експлуатаційного призначення засобів.

Прилади з ручним керуванням. Інколи для пошуку дефектних компонентів обчислювальних пристроїв достатньо простих приладів з ручним керуванням. Найчастіше під час ручного пошуку несправностей використовують логічний пробник, логічний пульсатор, струмів зонд.

Логічний пробник. Призначений для реєстрації логічних станів та імпульсів у логічних схемах. Він потребує інтерпретації напруг. При підключенні до схеми світло діоди цього приладу показують наявність Н-рівня, L-рівня або імпульсів. Деякі логічні

пробники можуть працювати як з ТТЛ-, так і з МОН-схемами і виявляти імпульси різних типів. Щоб почати роботу з приладом, його підключають до відповідного джерела живлення. У процесі реєстрації логічних рівнів чи імпульсів видаються відповідні звукові сигнали.

Логічний пульсатор. Генерує прямокутні сигнали. Натиском кнопки на корпусі приладу в контролю точку схеми подають один цикл прямокутного сигналу(Н- чи L-рівень). Він може змінити один рівень контрольної точки на інший. Головна складність цього способу в тому, що треба досконально знати схему, яку діагностують.

Струмовий зонд. Прилад належить до безконтактних методів вимірювання імпульсних струмів. Чутливий елемент зонда – трансформаторний перетворювач. Прилад дає змогу простежити шлях струму від генератора імпульсів до дефектного елемента. Сприймаюча катушка струмового зонду завдяки електромагнітній індукції виявляє змінний струм імпульсного сигналу, коли він переключається з одного рівня в інший, однак зовсім не реагує на постійний струм.

Автоматизовані засоби контролю і діагностування. Вони забезпечують якісно новий рівень контролю і діагностування обчислювальних пристроїв. Серед них найчастіше використовують логічний і сигнатурний аналізатори.

Логічний аналізатор. За його допомогою проводять логічний аналіз стану ОД(ОК) у часових проміжках. Він автоматизує етапи реєстрації та відображення інформації про реальні процеси в ОД. Цей прилад скорочує час налагодження МПП у 10-20 разів. Його застосовують на різних етапах життєвого циклу пристроїв, у тому числі на етапах проектування, виробництва і експлуатації. Він може реєструвати послідовності логічних сигналів одночасно і синхронно в багатьох контрольних точках протягом тривалих інтервалів часу в однократному і періодичних режимах. Також реєструє послідовності станів у зв’язку з однократними подіями, стани в контрольних точках в інтервалі часу, що перемежовується з обраним або до, або після обраного, асинхронні події. Крім того оперативно відображає зареєстровану інформацію в різних режимах і форматах. Режими відображення діагностичної інформації в часі не залежать від режимів реєстрації. Індикація зареєстрованої інформації може тривати як завгодно довго. Робочі операції, що виконує користувач логічного аналізатора під час контролю чи діагностування, переважно автоматизовані. Суть операцій в тому, щоб відображати відповідні реакції, перетворювати, вимірювати, порівнювати, шукати і приймати рішення.

Під час діагностування МПП прилади підключають насамперед до шин адреси, даних, керування. Для виявлення місця прояву несправності підбирають контрольні точки синхронізації та запуску. Логічний аналізатор складається з декількох елементів.

Запам’ятовуючий пристрій (ЗП). Призначений для приймання і зберігання діагностичної інформації з ОД. Його ємність залежить від кількості вхідних каналів аналізатора.

Пристрій перетворення діагностичної інформації (ППІ). Побудований на базі мікропроцесорного контролера (мікроЕОМ) або в більш ранніх розробках у вигляді автомата з жорсткою логікою.

Пристрій введення (ПВив).Це — дисплей для відображення діагностичної інформації після її оброблення пристроєм керування.

Пульт керування (ПК). Призначений для задання оператори режимів роботи аналізатора.

Пристрій аналізатора інформації (ПАІ). Генерує сигнали керування логічного аналізатора при збіганні кодів на виході пристрою введення з кодами, що встановлює оператор.

Основними характеристиками логічних аналізаторів є кількість вхідних каналів, глибина ЗП (біт/канал) та максимальна частота реєстрації сигналів діагностичної інформації.

За функційним призначенням логічні аналізатори поділяють на: 1) аналізатори логічних часових послідовностей (АЛЧП), що використовують синхронну реєстрацію сигналів; 2) аналізатори логічних станів (АЛС) із синхронною реєстрацією.

Сигнатурний аналізатор. Принцип його роботи багато в чому збігається з методами контролю за допомогою логічного аналізатора. Це, зокрема, вибір контрольних точок ОД, складання тестових впливів, аналіз відповідних реакцій та ін. Проте він має і певні відмінності. Сигнатурний аналізатор використовують тоді, коли істотно зростає довжина тестових послідовностей, особливо для пристроїв з компонентами підвищеного ступеня інтеграції. Це вимагає враховувати надійність обладнання для генерації тестів. Тому щоб знизити надлишковість цієї апаратури, використовують компактну форму представлення послідовностей для її аналізу після проходження через пристрій, що контролюють чи діагностують.

Стискання відповідних реакцій реалізують на регістрах зсуву зі зворотними зв’язками. Принцип роботи сигнатурного аналізатора полягає в тому, що відповідні реакції з ОД перекодовуються в ньому на короткі коди (сигнатури). Їх порівнюють з еталонами, які отримують або шляхом розрахунків. Або з тими, що знімають із заздалегідь справного ОД. Подавання тестів здійснюють зі спеціального генератора або програмними методами. Необхідно дотримуватись. Щоб інтервал часу подавання на ОД сигналів тестових впливів дорівнював часу аналізу.

Контрольні запитання

1. Які існують апаратні засоби діагностування Ц і МПП?
2. Види приладів з ручним керуванням.
3. У чому полягає сутність сигнатурного аналізу Ц і МПП
4. Які існують засоби тестування мікропроцесорів?
5. Ефективність систем діагностування.

Тема: «Програмні засоби діагностування ПК»

План :

1. Класифікація діагностичних програм
2. Суть і особливості діагностичних програм
3. Особливості процедури програми POST

Література [2] ст..265-305;
Література [1] ст.214-227.

1. Класифікація діагностичних програм:

1) POST (Power-On Self Test – само тестування комп'ютера при вмиканні живлення). Програма виконується під час кожного вмикання комп'ютера.

2) Діагностичні програми фірм-виробників. „IBM", „ Compag", „ Hewlett-Pachard", „ Dell", „ Genrad" та інші випускають для своїх систем спеціалізоване діагностичне програмне забезпечення, яке складається з наборів тестів для контролю працездатності компонентів комп'ютера.

3) Діагностичні програми обладнання комп'ютерів і комп'ютерних систем фірм-виробників. Такі фірми розробляють діагностичні програми для контролю і діагностування певного пристрою.

4) Діагностичні програми операційних систем (ОС). Операційні системи Windows 9x і Windows NT розробляють з кількома діагностичними програмами для перевірки різних компонентів комп'ютера.

5) Діагностичні програми загального призначення. Забезпечують належне тестування будь-яких IBM- сумісних комп'ютерів.

2. Суть і особливості діагностичних програм

Самоперевірка при вмиканні комп'ютера (POST). Ця процедура є послідовністю підпрограм, яка зберігається на материнській платі в ROM BIOS. Вони призначені для діагностування основних компонентів системи відразу після її включення. Під час цієї процедури завантаження операційної системи затримується.

При включенні комп'ютера автоматично тестується Центральний процесор, ПЗП (програмований запам'ятовуючий пристрій), допоміжні елементи материнської плати, оперативної пам'яті і периферійних пристроїв. Ці тести виконуються дуже швидко і не так високоякісно, як діагностичні програми виробників. Виявивши несправність компонента, видається попередження або повідомлення про помилку чи несправність.

3. Особливості процедури програми POST

Процедура POST передбачає такі способи ідентифікації несправностей, як звукові сигнали; повідомлення, що виводяться на екран монітора; шістнадцяткові коди помилок, які подаються в порт введення-виведення.

За серйозної несправності завантаження системи зупиняється і з'являється повідомлення про несправність, за яким визначають її причину. Такі несправності називають фатальними помилками.

- Звукові коди помилок, що видає процедура POST.

Якщо процедура POST виявляє несправності, то комп'ютер подає характерні звукові сигнали, за якими визначають несправний пристрій або компонент (під час вмикання справного комп'ютера чути один короткий звуковий сигнал). Видається серія довгих чи коротких звукових сигналів або їх комбінація. Це залежить від фірми-розробника BIOS та її версії. Звукові коди несправностей IBM- сумісних комп'ютерів наведені в таблицях 1 – 4.

Таблиця 1

IBM POST

№ п/п	Звуковий сигнал	Місце виконання несправності
1	1 короткий	Система справна. Процедура POST завершена
2	2 коротких	Є несправність, код помилки виведений на екран
3	Немає сигналу	Несправний блок живлення або системна плата
4	Неперервний сигнал	
5	Короткі сигнали, що повторюються	
6	1 довгий, 1 короткий	Системна плата
7	1 довгий, 2 коротких	Адаптер дисплея (MDA, CGA)
8	1 довгий, 3 коротких	Розширений графічний адаптер (EGA)
9	3 довгих	Плата клавіатури 3270

Таблиця 2

Звукові сигнали процедури POST AMI BIOS

№ п/п	Звуковий сигнал	Фатальна помилка
1	1 короткий	Помилка регенерації динамічного ОЗП
2	2 коротких	Помилка схеми контролю парності
3	3 коротких	Несправність у перших 64 Кбайт ОЗП
4	4 коротких	Несправність системного таймера
5	5 коротких	Помилка процесора
6	6 коротких	Помилка у схемі керування лінією A20 у контролері клавіатури
7	7 коротких	Помилка переключення у віртуальний режим
8	8 коротких	Помилка зчитування-запису відеопам'яті
9	9 коротких	Помилка контрольної суми ROM BIOS
10	10 коротких	Помилка зчитування-запису CMOS (Complimentary Metal Oxide Semiconductor – комплементарна структура метал-оксид-напівпровідник (КМОН))-пам'яті
11	11 коротких	Помилка кеш-пам'яті
12	Звуковий сигнал	Не фатальна помилка
13	1 довгий, 3 коротких	Помилка в основній або розширеній пам'яті
14	1 довгий, 8 коротких	Не виконується тест на відповідний сигнал дисплея

Таблиця 3

Критичні помилки, які визначають під час виконання процедури POST Phoenix BIOS

№ п/п	Звуковий код	Код порту 80h	Пояснення
1	Немає	01h	Виконується тестування регістрів CPU (Central Processor Unit – центральний процесор)
2	1 – 1 – 3	02h	Помилка зчитування або запису в CMOS-пам'ять
3	1 – 1 – 4	03h	Неправильна контрольна сума системної BIOS
4	1 – 2 – 1	04h	Несправність програмованого таймера інтервалів

Таблиця 4

Некритичні помилки, які визначають під час виконання процедури POST Phoenix BIOS

№ п/п	Звуковий код	Код порту 80h	Пояснення
1	4 – 2 – 1	34h	Перевіряється переривання синхроімпульсів таймера або виявлена несправність
2	4 – 2 – 2	35h	Перевіряється відключення або виявлена несправність
3	4 – 2 – 3	36h	Несправність схеми керування лінією A20
4	4 – 2 – 4	37h	Непередбачене переривання в захищеному режимі
5	4 – 3 – 1	38h	Виконується перевірка ОЗП або виявлена несправність за адресою, що перевищує FFFFh
6	4 – 3 – 3	3Ah	Перевіряється канал 2 таймера або виявлена несправність
7	4 – 3 – 4	3Bh	Перевіряються години поточного часу або виявлена несправність
8	4 – 4 – 1	3Ch	Перевіряються послідовні порти або виявлена несправність
9	4 – 4 – 2	3Dh	Перевіряються паралельні порти або виявлена несправність
10	4 – 4 – 3	3Eh	Перевіряється співпроцесор або виявлена несправність
11	Low*1 – 1 – 2	41h	Помилка вибору системної плати
12	Low*1 – 1 – 2	42h	Несправність розширеної CMOS-пам'яті

За появи критичних помилок система зупиняє роботу і подальше виконання операцій стає неможливим. Наслідки некритичних помилок менш серйозні.

- Повідомлення про помилки, що видає на екран процедура POST. Процедура POST у комп'ютерах XT, PS/2 і IBM- сумісних комп'ютерах відображає на екрані хід тестування оперативної пам'яті. Останнє виведене число вказує на кількість пам'яті, що успішно пройшла перевірку. Наприклад, у сучасних комп'ютерах з'являється повідомлення: 32768 КВ ОК. У справному комп'ютері це число повинно збігатися з кількістю встановленої в ньому пам'яті.

Якщо під час тестування процедура POST виявила несправність, то на екран дисплея виводиться відповідне повідомлення, наприклад 1790-Disk 0 Error. Далі, скориставшись керівництвом з експлуатації, з'ясовують, яка несправність відповідає цьому кодові.

- Коди помилок, що видає процедура POST у порти введення-виведення. На початку виконання кожного тесту за адресою спеціального порту введення-виведення POST видає коди, що прочитуються тільки за допомогою спеціальної плати адаптера, яку встановлюють у роз'єм розширення. Раніше (90-ті роки) такі плати розробляли для тестування материнських плат. Тепер окремі фірми випускають їх для сервісного обслуговування.

Під час виконання процедури POST на вбудованому індикаторі POST-плати, встановленої в роз'єм розширення, швидко змінюються двозначні шістнадцяткові числа. Якщо числа не змінюються, то на індикаторі відображається код тесту, під час якого відбувся збій. Це дещо локалізує місце прояву несправності.

Контрольні запитання для самостійної роботи

1. Які функції виконує програма POST?
2. Види сигналів програми POST.
3. У чому полягають особливості процедури програми POST?
4. Характеризуйте діагностичні програми фірм-виробників ПК.
5. Вбудовані засоби тестування МП старших поколінь фірми Intel
6. Зовнішні апаратні засоби тестування компонентів ПК.
7. Інтерфейс та підтримка JTAG.

Тема: „Засоби діагностування інтерфейсів, портів, адаптерів і периферійного обладнання”

План:

1.Загальна характеристика інтерфейсів введення-виведення
2.Способи тестування послідовних портів
3.Тестування периферійного обладнання
Література [1]ст. 227-240

Загальна характеристика інтерфейсів введення-виведення

У сучасних комп’ютерах як засоби комунікації використовують послідовні і паралельні порти. Це – інтерфейси введення-виведення.

Послідовні порти. До них підключають двонапрямлені пристрої, що передають інформацію в комп’ютер і приймають її з нього. Серед них – модеми, миша, сканери та інше.

Паралельні порти. Їх використовують для підключення принтерів, які працюють в однонапрямленому режимі, мережних адаптерів, дисководів для жорстких та гнучких дисків та CD-ROM.

Послідовні та паралельні порти тестують програмним і апаратно-програмним способом. Програмне тестування проводять за допомогою спеціальних програм, апаратно-програмне – за допомогою роз’ємів-заглушок, що підключають до портів.

Тестування послідовних портів. Цю процедуру здійснюють за допомогою MICKROSOFT DIAGNOSTICS (MSD) і тесту із замиканням петлі. Крім того, проконтролювати роботу послідовних портів можна у Windows 95/98.

MICKROSOFT DIAGNOSTICS. Ця діагностична програма належить до програмних засобів тестування і входить до складу MS DOS 6.x, Microsoft Windows і Windows 9x. На компакт-диску з Windows 95 вона міститься в каталозі \ other\ msd, а на ком пакт-диску Windows 98 – у каталозі \ tools\ oldmsdos. При інсталяції операційної системи програма автоматично не встановлюється. Її треба запустити безпосередньо з компакт-диску або скопіювати з нього заздалегідь на жорсткий диск.

Щоб запустити MSD, переходять у каталог (він може вказуватись у змінній PATH), в якому розташований файл MSD.EXE. В командному рядку DOS вводять MSD і натискають ENTER. На екрані з’являється меню. Для послідовних портів обирають опцію COM PORTS. У цьому випадку з’являється інформація про мікросхему UART, що встановлена в послідовному порту комп’ютера, та про доступні порти. Якщо один з портів не реагує на тест, то він не потрапляє у звіт програми. Також MSD видає інформацію щодо портів, які в цей момент використовують. Багато програм типу MSD працюють краще в середовищі DOS, тому їх рекомендують запускати повторно в цьому самому режимі.

Windows 95/98. У цій операційній системі також відображається інформація про те, чи працюють порти. Щоб перевірити і проконтролювати їх роботу, треба клацнути правою кнопкою миші на піктограмі „ Мій комп’ютер ” („My Computer”) і в меню, що з’явилося, обрати пункт „Властивості” („Properties”). Далі у діалоговому вікні обирають вкладку „Пристрої” („Device Manager”). На екрані відобразиться список підключених до комп’ютера пристроїв. Якщо пристрій функціює неправильно, то поряд з назвою

з’явиться знак оклику в жовтому колі. Далі розкривають список портів і двічі клацають на потрібному. Windows 95/98 вкаже, чи працює цей порт або назве пристрій, з яким він конфліктує.

Засоби діагностування периферійних пристроїв ПК

Під периферійними пристроями часто розуміють сукупність периферійної апаратури (пристрої введення і виведення інформації – клавіатура, монітор, принтер) та їх блоків керування, оскільки в деяких випадках вони є одним цілим з логічної і конструктивної точки зору. Блок керування периферійним апаратом виконує функцію перетворення інформації і керування конкретними його механізмами. Сукупність уніфікованих технічних і програмних засобів та правил спрягання процесорного блока з периферійною апаратурою називають інтерфейсом введення – виведення.

Контрольні запитання для самостійної роботи

1.Які існують види діагностичних програм для контролю апаратних засобів IBM-сумісних комп’ютерів?

2. Назвіть способи тестування послідовних і паралельних портів.

3.Характерізуйте несправностім адаптерів та моніторів, звукових плат.

4.Способи розв‘язання конфліктів ресурсів.

5. Пошук несправностей клавіатури, комп‘ютерної миши.

Тема:”Основні характеристики продуктивності мережі”.

План:

1. Вимоги до комп'ютерних мереж.
2. Основні характеристики продуктивності мережі.
3. Надійність і безпека
4. Література [4] https://752679216.netacad.com/courses/900845/assignments/syllabus/

Вимоги до комп'ютерних мереж

Відповідність до стандартів є лише однією з багатьох вимог, що пред'являються до сучасних мереж. Важливішим є виконання мережею певного набору послуг, наприклад, надання доступу до файлових архівів або веб-сторінок публічних Internet-сайтів, обмін електронною поштою в межах підприємства або в глобальних масштабах, інтерактивний обмін голосовими повідомленнями IP-телефонії тощо.

Решта вимог — продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість — пов'язані з якістю виконання цього основного завдання.

І хоча всі перераховані вище вимоги є важливими, часто поняття «**Якість обслуговування**» (*Quality of Service, QOS*) комп'ютерної мережі трактується вужче: воно містить лише дві важливі характеристики мережі — продуктивність і надійність.

Продуктивність

Потенційно висока продуктивність — це одна з основних переваг розподілених систем, до яких відносяться комп'ютерні мережі. Ця властивість забезпечується принциповою можливістю розподілу робіт.

Основні характеристики продуктивності мережі:

Час реакції мережі.

Швидкість передачі трафіку.

Пропускна здатність.

Затримка передачі і варіанти затримки передачі.

Час реакції мережі

В загальному випадку час реакції визначається як інтервал між відправленням запиту користувача до мережної служби і отриманням відповіді на нього.

Час реакції мережі є інтегральною характеристикою продуктивності мережі з погляду користувача. Саме цю характеристику має на увазі користувач, коли говорить: «Сьогодні мережа працює поволі».

Значення цього показника залежить від типу служби, до якої звертається користувач, від того, який користувач і до якого сервера звертається, а також від поточного стану елементів мережі — завантаженості сервера та сегментів, комутаторів і маршрутизаторів, через які проходить запит.

Тому, варто усереднювати цей показник по користувачах, серверах і годинах доби (від чого в значній мірі залежить завантаження мережі).

Час реакції мережі зазвичай складається з кількох складових.

Час підготовки запитів на клієнтському комп'ютері.

Час передачі запитів між клієнтом і сервером через сегменти мережі і проміжне комунікаційне устаткування.

Час обробки запитів на сервері.

Час передачі відповідей від сервера до клієнта.

Час обробки отриманих від сервера відповідей на клієнтському комп'ютері.

Очевидно, що розкладання часу реакції на складові користувачу не є цікавим, головним є кінцевий результат. Проте, для мережного фахівця дуже важливим є виділення з загального часу реакції складових, що відповідають етапам власне мережної обробки даних, — передачі даних від клієнта до сервера через сегменти мережі і комунікаційне обладнання.

Знання мережних складових часу реакції дозволяє оцінити продуктивність окремих елементів мережі, виявити вузькі місця і за необхідності виконати модернізацію мережі для підвищення її загальної продуктивності.

Швидкість передачі трафіку.

Середня швидкістьобчислюється шляхом ділення загального об'єму переданих даних на час їх передачі, зазвичай обирається достатньо тривалий проміжок часу — година, день або тиждень.

Миттєва швидкістьвідрізняється від середньої тим, що для усереднення вибирається дуже маленький проміжок часу — наприклад, 10 мс або 1 с.

Максимальна швидкість— це найбільша швидкість передачі, що зафіксована протягом періоду спостереження.

Зазвичай, при проектуванні, налаштуванні і оптимізації мережі використовуються такі показники, як середня і максимальна швидкість.

Середня швидкість, з якою обробляє трафік окремий елемент мережі або мережа в цілому, дозволяє оцінити роботу мережі впродовж тривалого часу, протягом якого піки і спади інтенсивності трафіку компенсують один одного.

*Максимальна швидкість*дозволяє оцінити, як мережа буде долати пікові навантаження, які є характерними для особливих періодів роботи, наприклад в ранкові години, коли співробітники підприємства майже одночасно реєструються в мережі і звертаються до розподілених файлів чи баз даних.

Зазвичай, при визначенні швидкісних характеристик певного сегменту чи пристрою в переданих даних не виділяється трафік певного користувача, застосування або комп'ютера — обчислюється загальний об'єм переданої інформації. Проте, для точної оцінки якості обслуговування така деталізація є бажаною, і системи керування мережами дозволяють її виконувати.

Пропускна здатність

Пропускна здатність - це максимально можлива швидкість обробки трафіку, що визначена стандартом технології, на якій побудована мережа. Пропускна здатність відображає максимально можливий об'єм даних, що передається по мережі або її частині в одиницю часу.

Пропускна здатність не є характеристикою, призначеною для користувача, оскільки вона свідчить про швидкість виконання внутрішніх операцій мережі — передачі пакетів даних між вузлами мережі через різні комунікаційні пристрої. Вона безпосередньо характеризує якість виконання основної функції мережі — транспортування повідомлень, тому її частіше використовують при аналізі продуктивності мережі, ніж час реакції або швидкість.

Пропускна здатність вимірюється або в бітах в секунду, або в пакетах в секунду.

Пропускна здатність мережі залежить як від характеристик фізичного середовища передачі (мідний кабель, оптичне волокно, скручена пара) так і від наявного способу

передачі даних (технологія Ethernet, FastEthernet, ATM). Пропускна здатність часто використовується як характеристика не стільки мережі, скільки власне технології, на якій побудована мережа.

На відміну від часу реакції або швидкості передачі трафіку пропускна здатність не залежить від завантаженості мережі і має постійне значення, що визначається використаними в мережі технологіями.

На різних ділянках гетерогенної мережі, де використовується кілька різних технологій, пропускна здатність може бути різною. Для аналізу і налаштування мережі корисно знати дані про пропускну здатність окремих її елементів.

Важливо відзначити, що із-за послідовного характеру передачі даних різними елементами мережі загальна пропускна здатність будь-якого складеного шляху в мережі буде мінімальною з пропускних здатностей елементів маршруту. Для підвищення пропускної здатності складеного шляху необхідно в першу чергу звернути увагу на найповільніші елементи.

Іноді корисно оперувати загальною пропускною здатністю мережі, яка визначається як середня кількість інформації, що передається між всіма вузлами мережі за одиницю часу. Цей показник характеризує якість мережі в цілому, не розкладаючи його по окремих сегментах або пристроях.

Затримка передачі

Затримка передачі визначається як час між моментом надходження даних на вхід мережного пристрою або частини мережі та моментом появи їх на виході цього пристрою.

Цей параметр продуктивності за сенсом є близьким до часу реакції мережі, але відрізняється тим, що завжди характеризує лише мережні етапи обробки даних, без затримок обробки кінцевими вузлами мережі.

Звичайну якість мережі характеризують величинами максимальної затримки передачі і варіантом затримки. Не всі типи трафіку є чутливими до затримок передачі, оскільки, зазвичай затримки не перевищують сотень мілісекунд, рідше — кількох секунд.

Затримки пакетів, що зумовлені файловою службою, службою електронної пошти або службою друку, мало впливають на якість цих служб з погляду користувача мережі.

З іншого боку, затримки пакетів, що містять голосові або відеодані, можуть призводити до значного зниження якості наданої користувачу інформації — виникає ефект «відлуння», неможливість розібрати деякі слова, вібрації зображення тощо.

Всі вказані характеристики продуктивності мережі є достатньо незалежними. Тоді як пропускна здатність мережі є постійною величиною, швидкість передачі трафіку може коливатися в залежності від завантаження мережі, не перевищуючи встановлених меж пропускної здатності.

Надійність і безпека

Однією з первинних цілей створення розподілених систем, до яких відносяться і комп’ютерні мережі, було досягнення більшої надійності у порівнянні з окремими обчислювальними машинами. Важливо розрізняти кілька аспектів надійності.

Для простих технічних пристроїв використовуються наступні показники надійності:

Середній час напрацювання на відмову.

Вірогідність відмови.

Інтенсивність відмов.

Проте, ці показники є придатними лише для оцінки надійності простих елементів і пристроїв, які можуть знаходитися лише в двох станах, — працездатному або непрацездатному. Складні системи, що складаються з багатьох елементів, окрім станів працездатності і непрацездатності, можуть мати інші проміжні стани, які ці характеристики не враховують.

Для оцінки надійності складних систем застосовується інший набір характеристик:

Готовність або коефіцієнт готовності.

Збереження даних.

Узгодженість (несуперечність) даних.

Вірогідність доставки даних.

Безпека.

Відмовостійкість.

Готовність або коефіцієнт готовності (*availability*) означає період часу, протягом якого система є готовою до використання. Готовність може бути підвищена шляхом введення надлишковості до структури системи: ключові елементи системи повинні існувати в кількох екземплярах, щоб при відмові одного з них функціонування системи забезпечували інші елементи.

Високонадійна комп'ютерна система повинна як мінімум мати високу готовність, але цього недостатньо. Необхідно забезпечити **збереження даних**і захист їх від спотворень. Крім того, повинна підтримуватися**узгодженість** (несуперечність) даних, наприклад якщо для підвищення надійності на кількох файлових серверах зберігається кілька копій даних, то потрібно постійно забезпечувати їх ідентичність.

Оскільки мережа працює на основі механізму передачі пакетів між кінцевими вузлами, однією з характеристик надійності є **вірогідність доставки пакету**до вузла призначення без спотворень. Разом з цією характеристикою можуть використовуватися і інші показники: вірогідність втрати пакету (із-за переповнення буфера маршрутизатора, не збіганні контрольної суми, відсутності працездатного шляху до вузла призначення тощо), вірогідність спотворення окремого біта переданих даних, співвідношення кількості втрачених і доставлених пакетів.

Іншим аспектом загальної надійності є **безпека**(*security*), тобто здатність системи захистити дані від несанкціонованого доступу. В розподіленій системі це зробити набагато складніше, ніж в централізованій. В мережах повідомлення передаються по лініях зв'язку, що часто проходять через загальнодоступні приміщення, в яких можуть бути встановлені засоби прослуховування ліній. Іншим вразливим місцем можуть стати залишені без нагляду персональні комп'ютери. Крім того, завжди є потенційна загроза злому захисту мережі від неавторизованих користувачів, якщо мережа має виходи в глобальні загальнодоступні мережі.

Ще однією характеристикою надійності є **відмовостійкість**(*fault tolerance*). В мережах під відмовостійкістю розуміють здатність системи приховати від користувача відмову окремих її елементів. Наприклад, якщо копії таблиці бази даних зберігаються одночасно на кількох файлових серверах, користувачі можуть просто не помітити відмови однієї з них. У відмовостійкій системі вихід з ладу одного з її елементів призводить до певного зниження якості її роботи (деградації), а не до повного останову. Так, при відмові одного з файлових серверів збільшується лише час доступу до бази

даних із-за зменшення ступеня розпаралелювання запитів, але в цілому система буде продовжувати виконувати свої функції.

Контрольні запитання для самостійної роботи

1. Які вимоги є визначальними для підвищення продуктивності мережі?
2. Що вкладається у поняття «прозорість мережі»?
3. Які складові визначають час реакції мережі?
4. За якими часовими критеріями визначають швидкість передачі трафіку?
5. Які вимоги висуваються до хорошої системи керування?

Тема: “Параметри оцінювання якості обслуговування”.

План:

1. Пропускна здатність.
2. Затримки передачі пакетів.
3. Рівень втрат і спотворень пакетів.
   Література [4] https://752679216.netacad.com/courses/900845/assignments/syllabus/

Важливі параметри для оцінювання якості обслуговування:

Пропускна здатність.

Затримки передачі пакетів.

Рівень втрат і спотворень пакетів.

Якість обслуговування гарантується для любого потоку даних, тобто для послідовності пакетів, що мають певні загальні ознаки, наприклад адресу вузла-джерела, інформацію, що ідентифікує тип застосування тощо.

До потоків застосовують поняття агрегації та диференціювання. Так, потік даних від одного комп'ютера може бути представлений як сукупність потоків від різних застосувань, а потоки від комп'ютерів одного підприємства агреговані до одного потоку даних абонента певного провайдера послуг.

Механізми підтримки якості обслуговування самі по собі не створюють пропускної здатності. Фактична пропускна здатність каналів зв'язку і транзитного комунікаційного устаткування — це ресурси мережі, що є відправною точкою для роботи механізмів QOS. Механізми QOS лише керують розподілом наявної пропускної здатності відповідно до вимог застосувань і налаштувань мережі. Найочевиднішим способом перерозподілу пропускної здатності мережі є керування чергами пакетів.

Оскільки дані, якими обмінюються два кінцеві вузли, проходять через певну кількість проміжних мережних пристроїв, таких як концентратори, комутатори і маршрутизатори, то підтримка QOS вимагає взаємодії всіх мережних елементів на шляху трафіку, тобто «з-кінця-в-кінець» («*end-to-end*», «e2e»). Будь-які гарантії QOS настільки відповідають дійсності, наскільки їх забезпечує найбільш «слабкий» елемент в ланцюжку між відправником і одержувачем. Тому, слід чітко розуміти, що підтримка QOS лише в одному мережному пристрої, нехай навіть і магістральному, може лише дещо покращити якість обслуговування або ж зовсім не мати впливу на параметри QOS.

Контрольні запитання для самостійної роботи

1. Який показник якості мережі залежить від фізичного середовища передачі?
2. Які вимоги висуваються до мережі, що передає мультимедійний трафік?
3. Про що свідчить хороша розширюваність мережі?
4. Що може забезпечити добра масштабованість мережі?
5. Які параметри є важливими для оцінювання якості обслуговування?

Тема: "Захист даних і конфіденційність".

План:

1. Захист інформації.
2. Види захисту інформації.

Література [4] https://752679216.netacad.com/courses/900845/assignments/syllabus/

За́хист інформа́ції (англ. *Data protection*) — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Термін вживається в Україні для опису комплексу заходів по забезпеченню інформаційної безпеки.

Захист інформації ведеться для підтримки таких властивостей інформації як:

Цілісність

— неможливість модифікації інформації неавторизованим користувачем.

Конфіденційність

— інформація не може бути отримана неавторизованим користувачем.

Доступність

— полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

Загрози інформації

Відповідно до властивостей І., виділяють такі загрози її безпеці:

загрози цілісності:

знищення;

модифікація;

загрози доступності:

блокування;

знищення;

загрози конфіденційності:

несанкціонований доступ (НСД);

витік;

розголошення.

Аспекти захисту інформації

Конфіденційність — захист від несанкціонованого ознайомлення з інформацією.

Цілісність — захист інформації від несанкціонованої модифікації.

Доступність — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Види захисту інформації

Кожен вид ЗІ забезпечує окремі аспекти ІБ:

Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

попередження витоку по технічним каналам;

попередження блокування ;

Інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Криптографічний — попереджує доступ за допомогою математичних перетворень повідомлення (ІП):

попередження несанкціонованої модифікації ;

попередження НС розголошення.

Організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Тема: “Захист конфіденційності в Інтернеті”.

План:

1. Чи в безпеці ваша інформація в Інтернеті?
2. Шляхи потрапляння інформації в Інтернеті.

Література [4] https://752679216.netacad.com/courses/900845/assignments/syllabus/

Інформація — це валюта Інтернету. Конфіденційність в Інтернеті залежить від можливості контролювати як обсяг особистої інформації, яку ви надаєте, так і осіб, які мають доступ до такої інформації.

Чи в безпеці ваша інформація в Інтернеті?

Під час виконання повсякденних дій в Інтернеті ви можете розкривати особисту інформацію, якою можуть скористатися інші люди, щоб втрутитися у ваше особисте життя. До такої інформації можуть відноситися конфіденційні відомості, як-от IP-адреса, адреса електронної пошти, ваше поточне фізичне розташування або ж домашня чи робоча адреси. Наприклад, під час здійснення покупок в Інтернеті часто вимагається введення даних кредитної картки і домашньої адреси.

Шляхи потрапляння інформації в Інтернеті

Компанії, державні органи та інші організації збирають дані під час:

- настроювання онлайнового облікового запису;
- здійснення покупки в інтернет-магазині;
- реєстрації для участі в конкурсі;

- участі в опитуванні;
- завантаження безкоштовного програмного забезпечення;
- перегляду веб-сторінок;
- використання програм на комп’ютері чи мобільному пристрої;
- публікації фотографій або статусу в соціальних мережах.

Що відбувається з вашою інформацією?

Корпорація Майкрософт та інші відповідальні компанії використовують особисті відомості для покращення роботи з їх продуктами та послугами (наприклад, допомагаючи здійснювати операції, запам’ятовуючи параметри або надаючи персоналізований вміст і спеціальні пропозиції).

Операції в Інтернеті (наприклад, реєстрація в службі або здійснення покупки) пов’язуються з вами за допомогою такої інформації, як адреса доставки чи номер кредитної картки. Однак у більшості випадків компанії збирають дані, у яких не визначається ваше ім’я. Веб-сайти відстежують відвідані вами сторінки і клацання мишею, але не вас особисто.

Також ваші особисті відомості можуть поширитися в Інтернеті, бо ви вказали власні дані в резюме, чатах, на сторінках соціальних мереж, наприклад Facebook, чи коментарях в групах обговорень або в Twitter.

До того ж інформацію про вас можуть публікувати інші люди. Друзі можуть писати про вас або публікувати фотографії з вами і вашою родиною. Крім того, для пошуку доступні документи державних установ, наприклад фотографії вашого будинку та його вартість, ваше свідоцтво про народження та копії вашого підпису. Парафіяльні групи, клуби та професійні асоціації також можуть розкрити ваше повне ім’я, інформацію про місце роботи і пожертвування.

Важливість вашої інформації, оприлюдненої в Інтернеті

Інформація про вас, яка доступна в Інтернеті, важлива з двох причин.

- По-перше, компанії та рекрутери можуть використовувати таку інформацію, яка представляє собою вашу репутацію в Інтернеті, задля оцінки вашої відповідності посаді.
- По-друге, злочинці можуть використовувати дані про вас в Інтернеті, щоб націлити на вас фішингові атаки, викрасти ваші особисті дані та здійснити інші злочини. Ризик можна знизити, якщо дотримуватися наведених у цій статті порад щодо захисту конфіденційності в Інтернеті.

Інформація в Інтернеті допускає можливість пошуку і часто є постійною. На відміну від даних, збережених на папері, потужні засоби пошуку в Інтернеті та засоби групування даних можуть полегшити збір даних для створення вашого повного профілю.

Після публікації даних в Інтернеті вони фактично залишаться там назавжди і їх (залежно від політики конфіденційності компанії, яка зберігає дані), у кінцевому підсумку, зможе побачити будь-хто в Інтернеті. Веб-сайти, окрім даних, які вони отримали від вас, можуть архівувати все, що ви публікуєте. Друзі (або колишні друзі) можуть розголошувати вашу інформацію або ж це може статися через хакерів і недоліки в системі безпеки.

Тема: “Захист домену кібербезпеки. Зловмисники та експеременти з кібербезпеки”.

План:

1. Система кібербезпеки України.
2. Хакерські атаки.
3. Уразливі сфери діяльності.

Література ttps://uk.wikipedia.org/wiki

Комп'ютерна безпека — це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «**Кібербезпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Створення безпечних комп'ютерних систем і додатків є метою діяльності мережевих інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики, так і економіки. У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів.

Кібербезпека — це безпека IT систем (обладнання та програм). Кібербезпека є частиною інформаційної безпеки будь-якої організації.

Згідно із загальноприйнятим визначенням, безпечна комп'ютерна інформаційна система — це ідеальна система, яка коректно і у повному обсязі реалізує *ті і лише ті* цілі, що відповідають намірам її власника[3].

На практиці побудувати складну систему, що задовольняє цьому принципові, неможливо, і не лише з огляду на ймовірність виникнення несправностей і помилок, але й через складність визначення і формулювання часто-густо суперечливих очікувань проектувальника системи, програміста, законного власника системи, власника даних, що обробляються, та кінцевого користувача. Навіть після їхнього визначення у багатьох випадках важко або й неможливо з'ясувати, чи функціонує програма у відповідності із сформульованими вимогами. У зв'язку з цим забезпечення безпеки зводиться найчастіше до управління ризиком: визначення потенційних загроз, оцінка ймовірності їхнього настання та оцінка потенційної шкоди, із наступним ужиттям запобіжних заходів в обсязі, що враховує технічні можливості й економічні обставини.

Система кібербезпеки України

Систему кібербезпеки України формують:

- Академічна кібербезпека (ВНЗ, дослідницькі інститути і т. д.);
- Державна кібербезпека (законодавча база, Держспецзв'язку(CERT-UA), кіберполіція, СБУ, Міністерство оборони, Розвідувальні органи, НБУ.);
- Комерційна кібербезпека (вендори, програмні та апаратні рішення, методики та методи, досвід, технології і т. д.).

- Некомерційні волонтерські та громадські організації (ІнформНапалм, Український кіберальянс)

Попри все, рівень захищеності кіберпростору України залишається незадовільним. На думку експертів, українські системи залишаються вразливими до хакерських атак. Цьому сприяє недостатня компетентність спеціалістів, що працюють на державній службі. Зі сторони бізнесу причина вразливості полягає в необізнаності та неусвідомленості загрози[7]. В Україні наразі не існує централзованого управління реагування кіберзлочини[8].

Ця спеціальність є новою в Україні і на даний момент її викладають всього в декількох передових ВНЗ нашої країни[9].

Хакерські атаки

За рік від 2017 до 2018 року в світі збільшилася кількість DDoS-атак та атак рівня інфраструктури (Layer 3 і 4) на 16 %, кількість reflection-based атак збільшилася на 4 % та на 38 % збільшилася кількість атак рівня додатків. Серед найвідоміших жертв атак стали такі компанії: Coincheck, 5th Avenue, Lord & Taylor, Exactis та інші[18]. Серед жертв також були всі міські системи міста Атланта.

Найпоширеніші атаки

Загалом можна виділити перелік таких найбільш поширених хакерських атак:

DoS, DDoS, 4DoS — атаки на відмову в обслуговуванні

Атаки на CPU (центральний процесор)

Атаки на RAM (оперативна пам'ять)

Атаки на дисковий простір (комп'ютерна пам'ять)

Проникнення всередину периметра (SQL ін'єкція, метод «грубої сили» та інше)

Фішинг (email, formjacking, XSS, etc.)

Вимагання (ransomware — програма-шантажист)

Уразливості

Для кращого розуміння методів захисту комп'ютерної системи слід спочатку ознайомитися з типами атак, які можуть бути здійснені проти неї. Такі небезпеки зазвичай можна віднести до однієї з наступних категорій.

Чорний хід (бекдор)

Чорний хід, або бекдор у комп'ютерній системі, криптосистемі чи алгоритмі — це метод обходу звичайного процесу аутентифікації, забезпечення віддаленого доступу до комп'ютера, одержання доступу до незашифрованої інформації тощо.

Бекдори можуть відбуватися у формі встановлення програми (наприклад, Back Orifice) або змін у роботі існуючої програми чи фізичного пристрою.

DoS-атака

На відміну від інших атак, DoS-атаки застосовуються не для одержання несанкціонованого доступу чи керування системою, а для того, щоб унеможливити роботу останньої. В результаті атаки акаунт окремої жертви може виявитися заблокованим унаслідок умисного багаторазового введення невірного пароля, або ж унаслідок перевантаження мережі буде заблоковано усіх її користувачів. На практиці цьому виду атак дуже складно перешкодити, оскільки для цього необхідно проаналізувати поведінку цілих мереж, а не лише поведінку невеличкої частини коду.

Атаки безпосереднього доступу

Користувач, який одержав несанкціонований доступ до комп'ютера (чи його частини), може встановлювати на ньому різні типи програмного (у тому числі модифікації операційних систем, віруси, програмні кілоґґери) та апаратного (апаратні кілоґґери, пристрої для прослуховування) забезпечення, внаслідок чого безпека системи опиниться під загрозою. Такий порушник може також легко скачати великі об'єми даних на зовнішні носії. Ще одним видом атак безпосереднього доступу є завантаження операційної системи з зовнішнього носія із наступним зчитуванням даних з жорсткого диску (дисків). Цей різновид атак є зазвичай єдиним методом атакування комп'ютерів, що не підключені до інтернету.

Уразливі сфери діяльності

Комп'ютерна безпека є вкрай важливою практично для всіх технологічних галузей, що функціонують за участю комп'ютерних систем.

АвіаціяАвіаційна галузь є особливо важливою з точки зору комп'ютерної безпеки, оскільки пов'язані із нею ризики стосуються життя людей, цінного обладнання й вантажів, а також авіатранспортної інфраструктури. Безпека системи може опинитися під загрозою через неправильне функціонування апаратного і програмного забезпечення, помилкові дії оператора чи неполадки, пов'язані із середовищем, в якому працює комп'ютерна система. Причиною таких загроз, що реалізуються через уразливість комп'ютерних систем, може бути саботаж, шпіонаж, промислова конкуренція, тероризм, технічні неполадки та людський фактор.

Наслідки успішних навмисних чи ненавмисних злочинних дій із комп'ютерною системою в авіації можуть бути різноманітними, від розголошення конфіденційної інформації до порушення цілісності системи, що може призвести до таких серйозних проблем, як витік інформації (крадіжка чи втрата даних), простій у роботі мережі чи системи управління повітряним рухом, а це, у свою чергу, може призвести до призупинення роботи аеропорту, втрати повітряного судна, загибелі пасажирів. Ще більшому ризикові піддаються військові системи, що керують майном та обладнанням військового призначення.

Захист комп'ютера

Існує багато шляхів захисту комп'ютерів, серед них методи, що ґрунтуються на використанні безпечних операційних систем та апаратного забезпечення, здатного захистити комп'ютерну систему.

Превентивні методи захисту

Згідно зі слів експертів з кібербезпеки можна виділити такі методи захисту[20]:

безпечна побудова серверної частини

здійснювати регулярне оновлення всіх елементів інфраструктури

робити тестування навантаження

проводити аналіз коду використовуваних бібліотек

проводити аналіз коду програми

ідентифікувати вразливості шляхом сканування

проводити регулярний аудит інформаційної безпеки

Безпека і проектування систем

Хоча під час проектування комп'ютерної системи необхідно взяти до уваги чимало характеристик, безпека є серед них однією з найважливіших. За даними опитування, проведеного корпорацією Symantec у 2010 році, 94 % організацій, що взяли участь в опитуванні, планували вжити заходів з підвищення безпечності їхніх комп'ютерних систем, а 42 % зазначили, що вважають неналежний рівень кібербезпеки за основний ризик.

Незважаючи на те, що більшість організацій вдосконалюють системи інформаційного захисту, чимало кіберзлочинців знаходять шляхи їхнього обходу і продовжують свою діяльність. Нині спостерігається зростання числа майже усіх типів кібератак. В опитуванні 2009 року щодо комп'ютерних злочинів і кібербезпеки, проведеному Інститутом комп'ютерної безпеки, респонденти відзначили суттєве зростання числа атак шляхом застосування зловмисних програмних засобів, DoS-атак, викрадання паролів та дефейсу сайтів.

Безпека користувача

У зв'язку з тим, що інтернет-технології проникають у всіх сфери життя людини, а подекуди й інтегруються в тіло людини, питання кібербезпеки користувача набуває

особливої ваги. При сучасному рівні розвитку технологій та їхній інтегрованості в життя людини це не лише питання доступу до інформації. Технології стають все ближче до тіла, до мозку і очей, до м'язів людини. Наприклад, у 2016 в Одесі на конференції Black Sea Summit вперше в Україні людині вживили чіп в руку, якою він міг оплачувати рахунки, як банківською картою[23]. Також в останні роки набуває популярності імплантація чипів, які б замінювали ключі, карти, ідентифікаційні дані. Так, наприклад, в 2019 році проект «xNT» почав розсилку покупцям чіпів для імплантації в руку[24]. Відповідно, все більше зростає загроза, що кібератаки можуть торкнутися фізичного стану людини. Тому кібербезпека — це також і безпека життя людини[25]. За даними фахівців компанії InDevLab – більш ніж 90% взломів відбувається саме завдяки соціальній інженерії. Це відбувається через те що хакери намагаються залякати людину чи створити такі обставини за яких у людини є обмежений час на роздуми і потрібно здійснити якусь дію, наприклад перерахувати кошти на зазначений рахунок.

Базові правила кібербезпеки користувача:

Створення складного пароля, що складатиметься із довільного набору символів, букв та цифр.

Регулярне оновлення паролів (раз у півроку).

Не переходити за шкідливими або підозрілими посиланнями. Причина полягає в тому, що багато інтернет ресурсів містять комп'ютерні черв'яки або інші віруси. Особливу увагу варто звертати на Торрент-файли.

Найбезпечніше використовувати ліцензоване програмне забезпечення.

Не публікувати інформацію, що може мати компрометуючий характер.

Підтримка «чистоти переписок».

Контрольні запитання для самостійної роботи

1. Кібервійна.
2. Перелік кібератак.
3. Полювання на кіберзагрози.
4. Інформаційна безпека.
5. Кіберпростір.
6. Кіберзлочин.
7. Асоціація аудиту і контролю інформаційних систем.

КОРОТКИЙ ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

Автономний програмний монітор — сукупність прикладних програм операційної системи. Вони дають змогу фіксувати широкий спектр подій при трасуючому і вибірковому методах вимірювань. Призначені для видавання розширених відомостей про систему.

Активні профілактичні заходи — операції, які мають на меті продовжити час безвідмовної роботи ПК.

Безвідмовність — властивість функційного модуля (системи) виконувати належні функції в певних умовах протягом заданого інтервалу часу або напрацювання.

Вбудований програмний монітор — сукупність програм, що входять до складу операційної системи. Він має статус керуючої програми операційної системи і призначений для видавання мінімальних відомостей про систему.

Вектор помилки E = (ei7 e2) — двійкова комбінація, яка містить одиниці в розрядах слова, що спотворені.

Відмова — подія, яка полягає в утраті функційним модулем (системою) здатності виконувати потрібну функцію.

Відновлювані об'єкти — об'єкти, які в період експлуатації в разі виникнення відмов можуть бути відремонтовані шляхом заміни несправних компонентів.

Відновлювальне обслуговування — обслуговування, яке проводять для відновлення працездатного стану і ресурсів функційного модуля (системи).

Відповідна реакція (вихідна реакція) — сукупність логічних контрольованих сигналів на вихідних контактах у заданому такті контролю чи діагностування, які є реакцією об'єкта на подані на його входи тестові впливи.

Внутрішній модем — модем, що знаходиться всередині конструкції системного блока.

Вторинна помилка — спотворення вихідних результатів при виконанні програми.

Глибина пошуку місця відмови (несправності) — характеристика, де вказують складову частину об'єкта, з точністю до якої визначають місце відмови.

Готовність — властивість об'єкта бути здатним виконувати потрібні функції в заданих умовах у будь-який час або протягом заданого інтервалу часу за умови забезпечення необхідними зовнішніми ресурсами.

Достовірність діагностування — ступінь об'єктивної відповідності результату контролю дійсному технічному стану об'єкта.

Достовірність помилкового функціювання — властивість обчислювального пристрою, що характеризує здатність засобів контролю визнати помилковим результат роботи пристрою за наявності хибних сигналів помилок, що видаються засобами контролю.

Достовірність правильного функціювання — властивість обчислювального пристрою, що характеризує здатність засобів контролю визнати правильним результат роботи пристрою за наявності пропуску помилок засобами контролю.

Достовірність функціювання — властивість обчислювального пристрою, що характеризує здатність засобів контролю визнати результат роботи пристрою правильним або помилковим за наявності пропуску помилок чи видачі хибних сигналів помилок засобами контролю.

Драйвер — програма, що імітує надходження інформації з попередніх модулів.

Експертні системи технічної діагностики — пакет програм, що класифікує ОД і несправності, які виникають у них, проводить їх аналіз, видає консультації і ставить діагноз.

Експлуатаційна ситуація — обставини, що зумовлюють вплив зовнішнього середовища, мету і режими функційного використання системи, запит на систему і результати її функціювання.

Еталонні реакції (реакції, що вимагаються) — сукупність логічних контрольованих сигналів на вихідних контактах, які відповідають розрахованим для справного ОК (ОД) відповідним реакціям у заданих тактах контролю (діагностування).

Ефективність (лат. effectivus — дійовий) системи діагностування — ступінь її пристосованості до процесу визначення технічного стану ОД і пошуку в ньому дефектів.

Жорстке ядро — ядро, склад якого постійний.

Збій — короткочасне порушення правильної роботи цифрового чи мікропроцесорного пристрою, після якого його працездатність відновлюється або її відновлює оператор без проведення ремонту.

Зовнішній модем — модем, що знаходиться за межами системного блока. Інтеграція (лат. integratio - поповнення) модулів — злиття модулів у програму або програмну систему.

Інтенсивність відмов — інтегральний критерій l(t), що характеризує густину розподілу напрацювання до першої відмови, розраховану за умови, що до моменту часу, який розглядають, система пропрацювала безвідмовно.

Ймовірність безвідмовної роботи — ймовірність того, що при заданих умовах експлуатації протягом інтервалу часу t не виникне відмова.

Ймовірність безвідмовної роботи P(t) — функція розподілу ймовірностей безвідмовної роботи об'єкта, яка характеризує ймовірність того.що об'єкт за час t не втратить працездатності.

Ймовірність невиявленої відмови (несправності) в даному елементі (групі) — ймовірність того, що за наявності відмови в результаті діагностування приймається рішення про її відсутність у даному елементі (групі).

Ймовірність невиявленої відмови (несправності) при діагностуванні — умовна ймовірність того, що непрацездатний об'єкту результаті діагностування визнають працездатним.

Ймовірність хибної відмови (несправності) в даному елементі (групі) — ймовірність того, що за відсутності відмови в результаті діагностування приймається рішення про її наявність у даному елементі (групі).

Ймовірність хибної відмови (несправності) під час діагностування — ймовірність того, що працездатний об'єкт у результаті діагностування виявиться непрацездатним.

Кодова відстань між двома словами d — кількість розрядів, за якими одне слово відрізняється від іншого.

Комбінований технологічний процес діагностування — послідовний ланцюжок технологічних операцій з паралельними розгалуженнями і (або) замкнутими ланцюжками операцій.

Комплексне тестування — пошук невідповідності системи своїй вихідній (початковій) меті.

Коректність програми — відповідність її специфікації. Оскільки специфікація може не відповідати фактичним вимогам до програми, то трапляються випадки, коли некоректна програма працює надійно або, навпаки, коректна — ненадійно.

Кратність помилок t — кількість розрядів, спотворених помилкою.

Лінійний технологічний процес діагностування — послідовний ланцюжок операцій.

Логічна динамічна несправність — стан, який призводить до спотворення логічних функцій, що реалізують елементи структури в динамічних режимах роботи.

Міра довіри С — ймовірність того, що модель правильно відхилятиме хибне припущення.

Модернізація (франц. modernisation — оновлення) — заміна в комп'ютері застарілих компонентів на нові з вищими параметрами, якщо це дає змогу зробити конструкція комп'ютера.

Модуль (лат. modulus — міра) — елемент (компонент) програми, стандартизований за формою запису і зовнішніми зв'язками.

Надійність — властивість об'єкта зберігати в часі у встановлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання і транспортування.

Надійність програмного забезпечення — властивість програми виконувати задані функції в заданих умовах роботи і на заданій ЕОМ.

Невідновлювані об'єкти — об'єкти, для яких ремонт із конструктивних причин або умов експлуатації є неможливим.

Неготовність — стан об'єкта, в якому він нездатний виконувати потрібну функцію з будь-якої причини.

Нелогічна динамічна несправність — стан, який призводить до появи неправильних значень сигналів на виходах структури в динамічних режимах роботи і не пов'язаний зі спотворенням елементами структури логічних функцій, що ними реалізуються.

Несправність ВІС або НВІС — стан, зумовлений дефектами одного чи кількох елементів внутрішньої структури кристала або провідників, що з'єднують його з виводами цієї ВІС (НВІС). Враховуючи це, несправністю цифрового чи мікропроцесорного пристрою вважають стан, зумовлений дефектами одного чи кількох компонентів (елементів) їх структури або провідників, що з'єднують компоненти в цю структуру.

Несправність Ц або МПП — формалізоване представлення факту прояву дефекту цих пристроїв у вигляді неправильних значень сигналів на входах і виходах.

Пасивні профілактичні заходи — роботи, спрямовані на захист комп'ютера від зовнішніх шкідливих дій.

Первинна помилка — спотворення в тексті програми.

Періодичне обслуговування — обслуговування, яке виконують через задані інтервали часу щодо встановленого часового графіка.

Питомі витрати — відношення об'єму буферної пам'яті до швидкості передавання тест-векторів.

Плаваюче ядро — ядро, склад якого непостійний.

Повнота діагностування — характеристика, яка визначає можливість виявлення відмов (несправностей) в об'єкті з використанням обраного методу його діагностування (контролю).

Показник ефективності використання діагностичних засобів — кількісна характеристика ступеня досягнення корисних результатів при використанні системи в конкретній експлуатаційній ситуації з урахуванням експлуатаційних витрат.

Показник якості — кількісна характеристика однієї або кількох властивостей системи, які складають її якість, що розглядається стосовно певних умов створення і споживання.

Породжуюча матриця Q кода — матриця, рядки якої в сукупності утворюють базис групи, що відповідає множині всіх кодових слів.

Правильний результат роботи обчислювального пристрою — результат, коли пристрій справді працює правильно, відсутні сигнали помилок, або результат, коли пристрій справді працює неправильно, про що свідчить сигнал помилки.

Пропуск помилки засобами контролю — результат неправильної роботи пристрою і відсутності сигналу помилки. Якщо пристрій працює правильно, а засоби контролю сигналізують про помилку, то це свідчить, що їх контролюють не повністю або зовсім не контролюють.

Профілактичне обслуговування — обслуговування, яке здійснюють для попередження відмов функційного модуля (системи).

Резервування (франц. reserve — запас) — метод підвищення надійності шляхом включення резервних елементів при розробленні системи або в процесі її експлуатації.

Ремонтопридатність — властивість об'єкта бути пристосованим до підтримання і відновлення стану, в якому він здатний виконувати належні йому функції за допомогою технічного обслуговування і ремонту.

Розподілене ядро — ядро, що може бути організоване на будь-якому комп'ютері комп'ютерної системи (КС), навіть на непе-ревіреній.

Середній час відновлення — середній час, потрібний для відновлення працездатності для відомого інтервалу часу використання функційного модуля (системи).

Середнє напрацювання між відмовами — відношення сумарного напрацювання відновлювального об'єкта до математичного сподівання кількості його відмов протягом цього напрацювання.

Середній час напрацювання на відмову — відношення сумарного часу напрацювання відновлювального об'єкта (пристрою) до математичного сподівання кількості його відмов протягом цього часу.

Система технічного діагностування — сукупність засобів об'єкта і виконавців, необхідна для проведення діагностування (контролю) за правилами, встановленими технічною документацією. Як правило, вона охоплює зовнішні засоби технічного діагностування.

Системний підхід — сумісний аналіз і розроблення всіх елементів системи.

Тестовий (англ. test — випробування) контроль — контроль, під час якого на об'єкт контролю подають тестові впливи.

Технічна діагностика — галузь знань, що досліджує стани ОД і розробляє методи їх розпізнавання, визначає принципи проектування та організації пристроїв і систем технічного діагностування.

Технічне діагностування — процес визначення технічного стану об'єкта з означеною (заданою) точністю.

Технічне обслуговування системи — будь-яка діяльність, призначена для збереження або відновлення працездатності функційного модуля (системи).

Технічний контроль — процес, що забезпечує виявлення несправностей у роботі цифрових пристроїв, комп'ютерів, комп'ютерних систем і мереж, викликаних відмовою або збоями апаратурних засобів, помилками в програмах, помилкою оператора тощо.

Технічний ресурс виробу — прогнозована тривалість його експлуатації від початку до моменту, коли інтенсивність відмов збільшується до рівня, який робить подальшу експлуатацію неможливою або недоцільною з економічних міркувань.

Технічний стан об'єкта — стан, який характеризують у певний момент часу за певних умов зовнішнього середовища значення параметрів, установлених технічною документацією на об'єкт.

Технологічна діагностична операція — частина технологічного процесу діагностування, яку здійснюють над одним чи кількома ОД, на одному робочому місці, одним чи кількома спеціалістами-експертами або спеціалістами-розробниками.

Тривалість діагностування — інтервал часу, необхідний для проведення діагностування об'єкта.

Функції ненадійності — криві, отримані в результаті експерименту або на основі оброблення статистичних даних про кількість відмов.

Функційний (лат. functio — виконання) (робочий) контроль — контроль, під час якого на об'єкт контролю подають робочі впливи.

Централізоване ядро — ядро, що організують на одному заздалегідь визначеному справному комп'ютері.

Циклічний код — кільце, тобто замкнута сукупність елементів, для яких задані дві операції та зворотні до них.

Циклічний технологічний процес діагностування — замкнута послідовність операцій ланцюжка.

Ядро — сукупність апаратних і програмних засобів, що забезпечують реалізацію тестового діагностування системи.

Якість експлуатації — сукупність властивостей процесу експлуатації системи, від яких залежить відповідність цього процесу і його результатів встановленим вимогам.

Якість системи — сукупність властивостей системи, що дає змогу задовольняти певні потреби відповідно до її призначення.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Локазюк В.М. , Савченко Ю.Г. "Надійність, контроль, діагностика Ii модернізація ПК"
2. Иыду К. А. Надежность, контроль и диагностика вычислительных машин и систем: Учебн. пособие для вузов. – М.: Высш. шк., 1989. – 216 с.
3. Канер Сэм и др. Тестирование программного обеспечения: Пер. с англ. / Сэм Канер, Джек Фолк, Енг Кек Нгуен. – К.: Издательство «Диа Софт»,2000. – 544 с.
4. Липаев В. В. Качество программного обеспечения. – М.: Финансы и статистика, 1983. – 263 с.

ЗМІСТ