4.1 ТИПОВІ ЗАСОБИ АПАРАТНОЇ ПІДТРИМКИ ОС

Операційна система тісно пов'язана з устаткуванням комп'ютера, на якому вона повинна працювати. ОС обслуговує користувачів, звертаючись при цьому до ресурсів апаратного забезпечення, до складу яких входить один або декілька процесорів. Окрім цього, вона управляє вторинною пам'яттю і пристроями введення-виведення. Апаратне забезпечення впливає на набір команд ОС і управління його ресурсами.

Значна частина операційних систем успішно працюють на різних апаратних платформах без істотних змін у своєму складі. Це пояснюється тим, що, незважаючи на відмінності в деталях, засоби апаратної підтримки ОС більшості комп'ютерів набули сьогодні багато типових рис. У результаті серед ОС можна виділити прошарок машинно-залежних компонентів ядра і зробити інші шари ОС загальними для різних апаратних платформ. Це повною мірою стосується і популярного сімейства 32-розрядних процесорів Intel: 80386, 80486, Pentium, Pentium Pro, Pentium II, Celeron і Pentium III-IV. Слід зазначити, що засоби підтримки операційної системи в усіх цих процесорах побудовані майже ідентично, тому далі у тексті для їх позначення ми будемо використовувати узагальнений термін «процесори Pentium».

Чіткої межі між програмною і апаратною реалізацією функцій ОС не існує – рішення про те, які функції ОС виконуватимуться програмно, а які апаратно, приймається розробниками апаратного і програмного забезпечення комп'ютера. Проте, практично усі сучасні апаратні платформи мають деякий типовий набір засобів апаратної підтримки ОС, в який входять такі компоненти:

- засоби підтримки привілейованого режиму;
- засоби трансляції адрес;
- засоби перемикання процесів;
- система переривань і системний таймер;
- засоби захисту областей пам'яті.

4.1.1 Засоби підтримки привілейованого режиму

Засоби підтримки привілейованого (захищеного) режиму ґрунтуються на системному регістрі процесора, що часто називається «словом стану» машини або

процесора. Цей регістр містить деякі ознаки, що визначають режими роботи процесора, у тому числі і ознаку поточного режиму привілеїв.

Зміна режиму привілеїв виконується за рахунок зміни слова стану машини в результаті переривання або виконання привілейованої команди. Число градацій привілейованості може бути різним у різних типів процесорів, найчастіше використовуються два рівні (ядро-користувач) або чотири (наприклад, ядро-супервізор-виконання-користувач у платформи VAX або 0-1- 2-3 у процесорів Intel x86/Pentium). В обов'язки засобів підтримки привілейованого режиму входить перевірка допустимості виконання активною програмою інструкцій процесора при поточному рівні привілейованості.

Основним режимом роботи процесора Pentium є захищений режим (protected mode). Для сумісності з програмним забезпеченням, розробленим для попередніх моделей процесорів Intel (головним чином, моделі 8086), в процесорах Pentium передбачений так званий реальний режим (real mode). У реальному режимі процесор Pentium виконує 16-розрядні інструкції і адресує один мегабайт пам'яті.

4.1.2 Засоби трансляції адрес

Засоби трансляції адрес виконують операції перетворення віртуальних адрес, які містяться в кодах процесу, в адреси фізичної пам'яті. Таблиці, призначені при трансляції адрес, мають великий об'єм, тому для їх зберігання використовуються області оперативної пам'яті, а апаратура процесора містить тільки покажчики на ці області. Засоби трансляції адрес використовують ці покажчики для доступу до елементів таблиць і апаратного виконання алгоритму перетворення адреси, що значно прискорює процедуру трансляції в порівнянні з її чисто програмною реалізацією.

4.1.3 Засоби перемикання процесів

Засоби перемикання процесів призначені для швидкого збереження контексту призупиненого процесу, і відновлення контексту процесу, який стає активним. Контекст процесу включає вміст усіх регістрів загального призначення процесора і регістр прапорів операцій. Контекст також містить системні регістри і покажчики, які пов'язані з цим процесом, а не з операційною системою, наприклад покажчик на таблицю трансляції адрес процесу. Для зберігання контекстів призупинених процесів

використовуються області оперативної пам'яті, які підтримуються покажчиками процесора.

Перемикання контексту виконується за певними командами процесора, наприклад, за командою переходу на нове завдання. Така команда викликає автоматичне завантаження даних зі збереженого контексту в регістри процесора,

4.1.4 Система переривань

Система переривань дозволяє комп'ютеру реагувати на зовнішні події, синхронізувати виконання процесів і роботу пристроїв введення-виведення, швидко переходити з однієї програми на іншу. Механізм переривань потрібний для того, щоб повідомити процесор про виникнення в обчислювальній системі деякої непередбачуваної події.

Прикладами таких подій можуть служити завершення операції введення-виведення зовнішнім пристроєм, некоректне завершення арифметичної операції. При виникненні умов переривання його джерело (контролер зовнішнього пристрою, таймер, арифметичний блок процесора і т.п.) виставляє певний електричний сигнал. Цей сигнал перериває виконання процесором послідовності команд і викликає автоматичний перехід на заздалегідь визначену процедуру, що називається процедурою обробки переривань.

У більшості моделей процесорів відпрацьовуваний апаратурою перехід на процедуру обробки переривань супроводжується заміною слова стану машини (або навіть усього контексту процесу), що дозволяє одночасно з переходом за потрібною адресою виконати перехід в привілейований режим. Після завершення обробки переривання відбувається повернення до виконання перерваного коду.

Переривання грають найважливішу роль в роботі будь-якої операційної системи, будучи її рушійною силою. Дійсно, велика частина дій ОС ініціюється перериваннями різного типу. Навіть системні виклики від додатків виконуються на багатьох апаратних платформах за допомогою спеціальної інструкції переривання, що викликає перехід до виконання відповідних процедур ядра (наприклад, інструкція int в процесорах Intel або SVC в мейнфреймах IBM).

Переривання бувають двох типів: **апаратні** і **програмні**.

Апаратні переривання – це спеціальний сигнал (запит переривання, IRQ), який передається процесору від апаратного пристрою. До апаратних переривань належать:

- переривання введення-виведення, які приходять від контролера периферійного пристрою (наприклад, такі переривання генерує контролер клавіатури при натисненні на клавішу);
- переривання, пов'язані з апаратними або програмними помилками (такі переривання виникають, наприклад, у разі збою контролера диска, доступу до захищених областей пам'яті, ділення на нуль).

Програмні переривання генерують програми, що виконують спеціальну інструкцію переривання. Така інструкція є в системі команд процесора. Обробка програмних переривань процесором не відрізняється від обробки апаратних переривань.

Якщо переривання сталося, то процесор передає управління спеціальній процедурі – обробнику переривань. Після виходу з обробника процесор продовжує виконання інструкцій перерваної програми. Відрізняють два типи програмних переривань залежно від того, яка інструкція буде виконана після виходу з обробника: для відмови (faults) повторюється інструкція, яка викликала переривання, для пасток (traps) – виконується наступна інструкція.

Усі переривання введення-виведення і програмні переривання належать до категорії пасток.

Для реалізації привілейованого режиму процесора в одному з його регістрів передбачений спеціальний біт (біт режиму), який вказує, в якому режимі працює процесор. У разі апаратного або програмного переривання процесор автоматично перемикається в привілейований режим.

Альтернативою перериванням є періодичне опитування стану кожного пристрою з боку процесора. Подібний підхід, що називається послідовним опитуванням (pooling), підвищує накладні витрати і збільшує складність комп'ютерної системи. Переривання позбавляють процесор від необхідності постійно опитувати системні пристрої.

4.1.5 Системний таймер

Системний таймер, що часто реалізовується у вигляді швидкодіючого регістра-лічильника, потрібний операційній системі для витримки інтервалів часу. Для цього в регістр таймера програмно завантажується значення необхідного інтервалу в умовних одиницях, з якого потім автоматично з певною частотою (при кожному імпульсі кварцевого генератора) починає відніматися по одиниці. Частота «тиків» таймера, як правило, тісно пов'язана з частотою тактового генератора процесора.

Не слід плутати таймер ні з тактовим генератором, який виробляє сигнали, синхронізуючі усі операції в комп'ютері, ні з системним годинником, якій працює на батареях і веде незалежний відлік часу. Досягши нульового значення лічильника таймер ініціює переривання, яке обробляється процедурою операційної системи. Переривання від системного таймера використовуються ОС в першу чергу для стеження за тим, як окремі процеси витрачають час процесора. Наприклад, в системі розподілу часу при обробці чергового переривання від таймера планувальник процесів може примусово передати управління іншому процесу, якщо цей процес вичерпав виділений йому квант часу.

4.1.6 Засоби захисту областей пам'яті

Засоби захисту областей пам'яті забезпечують на апаратному рівні перевірку можливості програмного коду здійснювати з даними певної області пам'яті такі операції, як читання, запис або виконання (при передачах управління). Якщо апаратура комп'ютера підтримує механізм трансляції адрес, то засоби захисту областей пам'яті вбудовуються в цей механізм. Функції апаратури з захисту пам'яті полягають в порівнянні рівнів привілеїв поточного коду процесора і сегменту пам'яті, до якого робиться звернення.