Системные механизмы Windows

Системные механизмы

- диспетчеризация ловушек, в т.ч. прерываний, DPC (deferred procedure call), APC (asynchronous procedure call), исключений и системных сервисов
- диспетчер объектов исполнительной системы
- системные рабочие потоки
- LPC (local procedure call)
- Kernel Event Tracing
- Wow64

1. Диспетчеризация ловушек

Ловушки (trap)

- **Прерывания (interrupt)** – асинхронные события, которые могут произойти в любой момент, генерируемые, в основном, устройствами ввода-вывода и таймерами. Могут генерироваться программно.
- **Исключения (exception)** – синхронные события, возникновение которых связано с выполнением определенных инструкций.
- Механизм ловушек позволяет процессору перехватить управление над выполняемым потоком и передать управление специальной части ОС – **обработчику ловушек (trap handler)**

Типовые ситуации активизации обработчика ловушек

- Прерывания
- Вызов системного сервиса
- Аппаратные исключения
- Программные исключения
- Исключения, связанные с виртуальными адресами

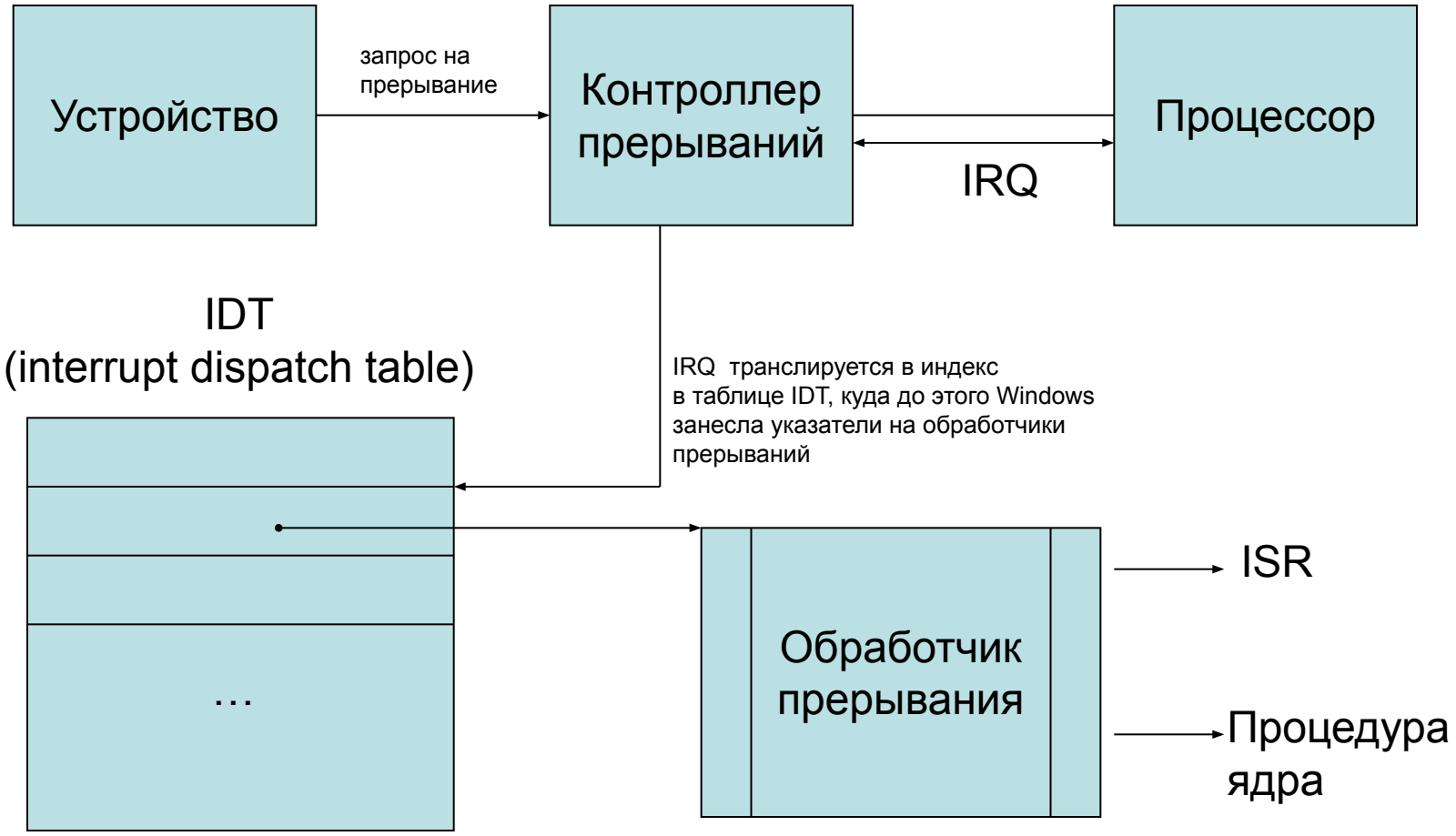
Общие принципы обработки ловушек

- Возникновение прерывания или исключения
- Переключение на стек режима ядра (если прерванный процесс выполняется в режиме пользователя)
- Запись статусной информации (контекста) процесса на стек ядра для последующего восстановления процесса
- Создание фрейма ловушки (trap frame) на стеке ядра
- Вызов соответствующего обработчика ловушки
- Выполнение обработчика
- Восстановление контекста прерванного процесса
- Возобновление прерванного процесса

Аппаратные прерывания

- Генерируется устройствами ввода-вывода с целью получить от процессора время на их обслуживание
- Могут генерироваться системным программным обеспечением
- Ядро может запретить прерывания
- Для обработки прерываний устанавливаются специальные обработчики ловушек прерываний, которые передают управления ISR (interrupt service routing, процедуре обслуживания прерывания) или внутренней процедуре ядра

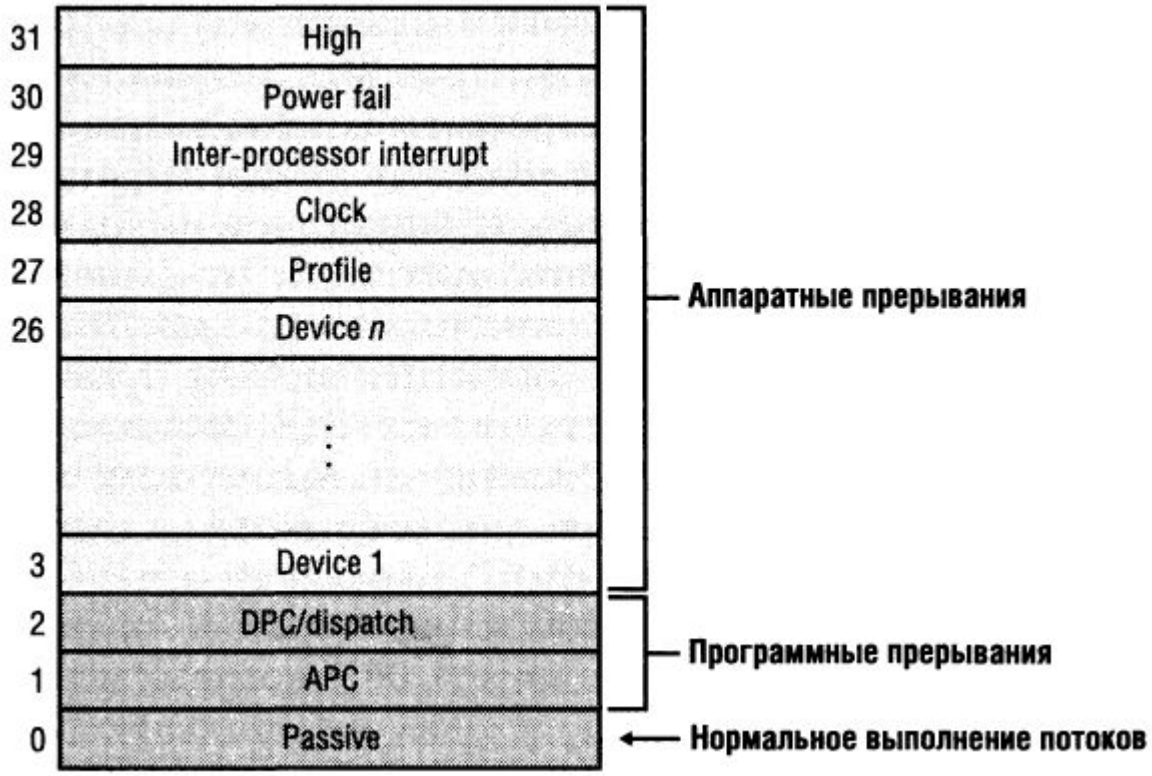
Обработка аппаратных прерываний



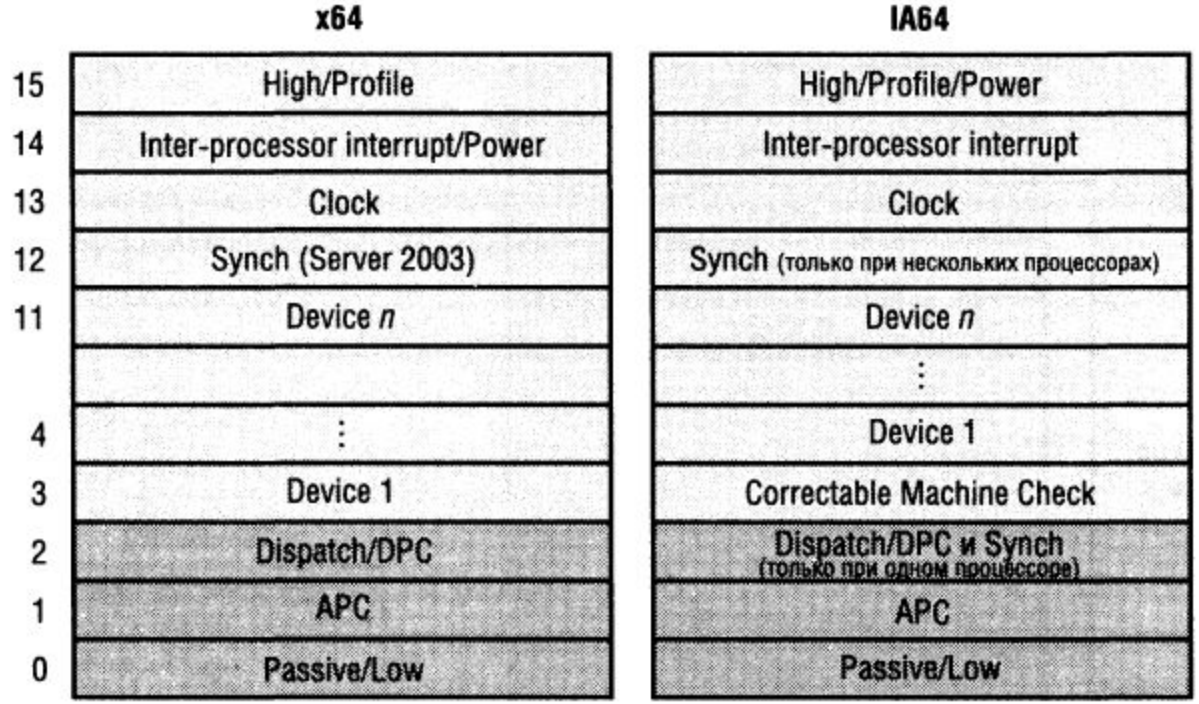
Уровень запросов прерываний (IRQL)

- IRQL – interrupt request level – показывает, какие прерывания могут быть получены указанным PIC (Programmable Interrupt Controller, программируемый контроллер прерываний)
- Процессы могут изменять IRQL на платформах с программируемыми контроллерами прерываний, используя специальные системные вызовы – *KeRaiseIrql* и *KaLowerIrql*
- Прерывания обрабатываются в соответствии с их уровнем – прерывания с более высоким IRQL могут прервать обработку прерываний с более низким IRQL

Уровни запросов прерываний (на платформе x86)



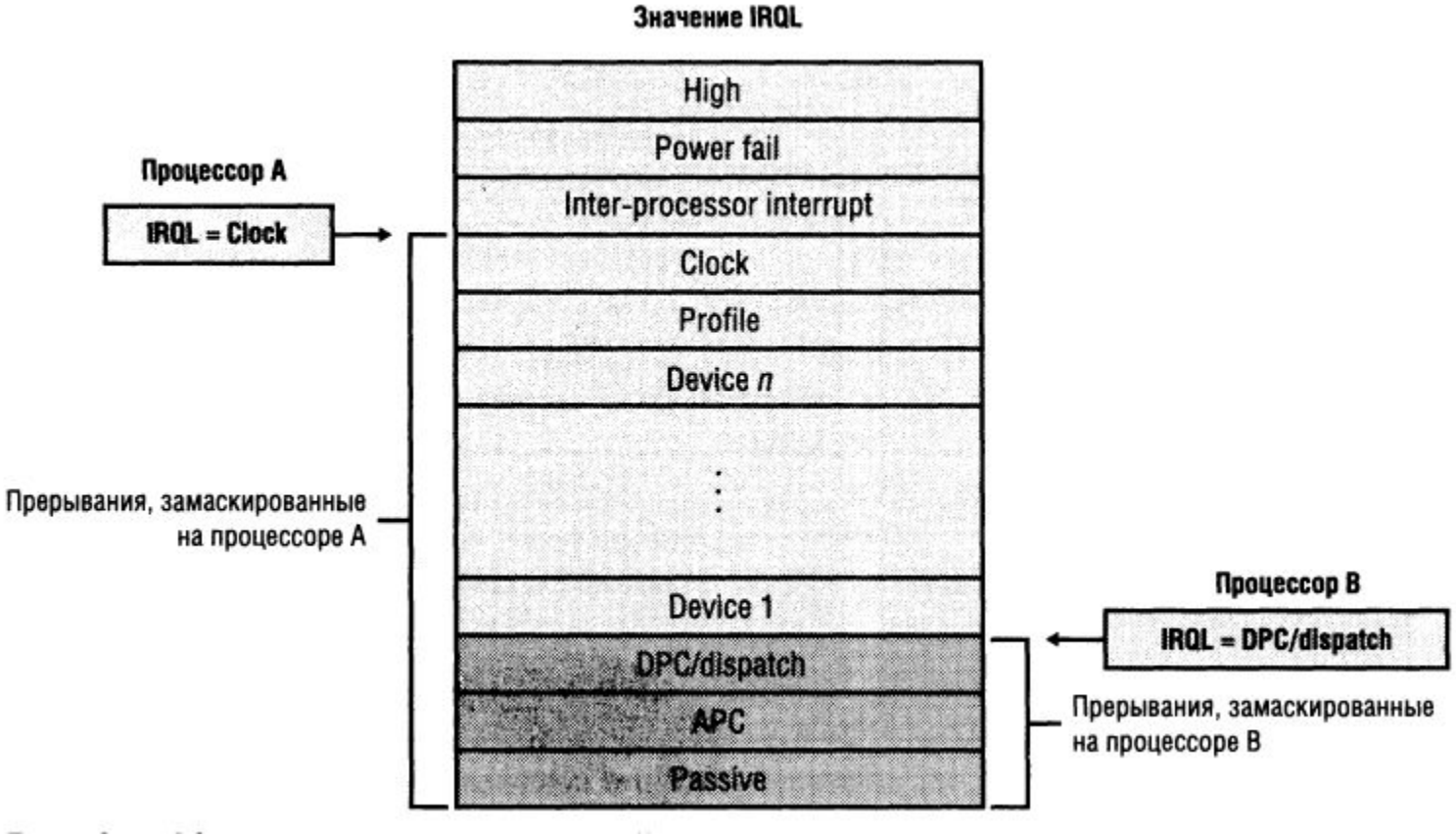
Уровни запросов прерываний (на платформе x64 и IA64)



Маскировка прерываний

- Прерывания могут быть замаскированы, т.е. их получение PIC не может быть выполнено, если для него установлен соответствующий IRQL
- Процессы могут изменять IRQL на платформах с программируемыми контроллерами прерываний, используя специальные системные вызовы – *KeRaiseIrql* и *KaLowerIrql*
- При изменении IRQL необрабатываемые прерывания могут «материализоваться»

Маскировка прерываний



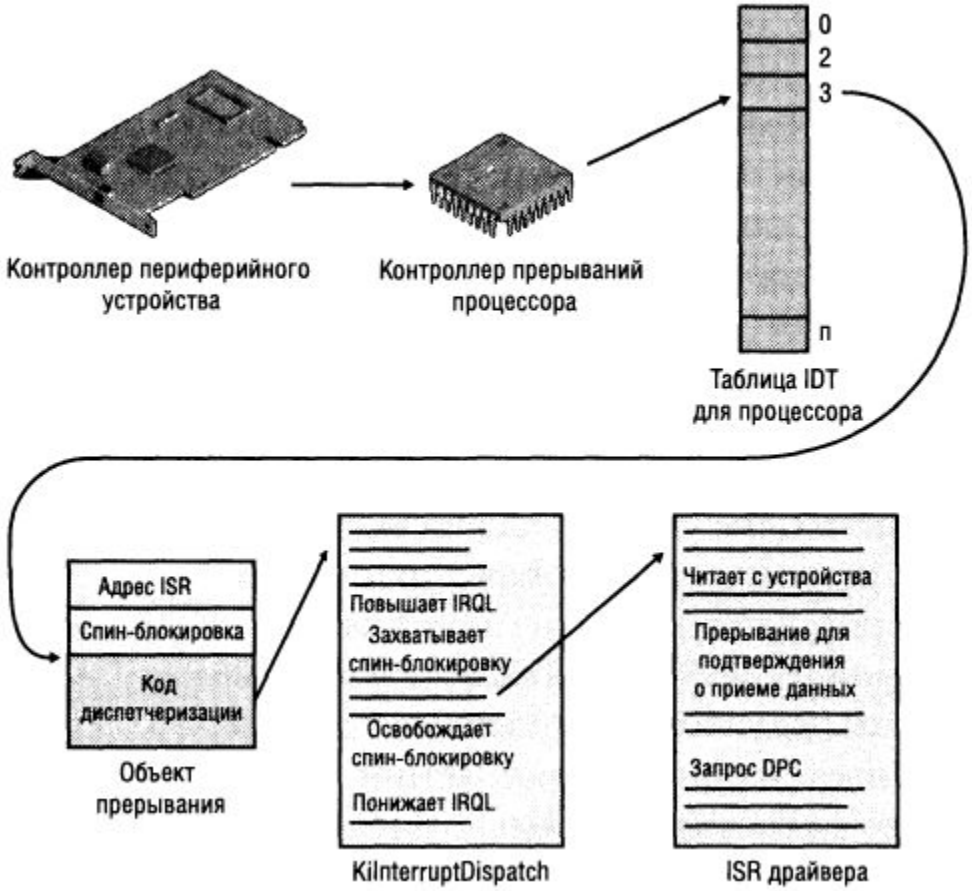
Маскировка прерываний на уровне HAL

- Обращение к PIC – медленная операция, поэтому реально она фактически не выполняется
- На уровне HAL реализуется механизм *отложенный IRQL (lazy IRQL)*
- Маска прерывания при этом не меняется – HAL фиксирует новый уровень прерывания
- При возникновении прерывания с более низким IRQL HAL откладывает его выполнение до момента понижения уровня запроса прерывания

Связь прерываний и IRQL

- Механизм IRQL, реализованный в Windows, не поддерживается аппаратно
- Конкретные устройства определяются в системе драйвером шины, который в т.ч. выполняет назначение номеров прерываний (IRQ)
- Драйвер шины обращается к уровню HAL, который и увязывает IRQ с уровнями IRQL
- Трансляция IRQ-IRQL на разных платформах выполняется по-разному
  - Однопроцессорная x86: IRQL = 27-IRQ
  - Многопроцессорная x86: прямым перебором
  - x64 и IA64: путем деления вектора прерываний на 16

Уровень ядра: объект прерывания



Программные прерывания

- Диспетчеризация или DPC
- Обработка прерываний, не критичных во времени
- Обработка событий таймеров
- APC
- Асинхронный ввод-вывод

Прерывания DPC или диспетчеризация

- Для выполнения отложенных операций диспетчеризации процессов, например, при перераспределении процессорного времени на глубоко вложенных частях программного кода
- Процессор откладывает выполнение прерываний диспетчеризации в том случае, когда IRQL находится на уровне DPC/dispatch или выше
- После того, как уровень IRQL понижается прерывания DPC могут быть выполнены

Обработка DPC