ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Управление памятью

Пакулов Артур

1

Управление памятью

Базовая модель памяти

Виртуальное адресное пространство 4Гб
делится на две равные части

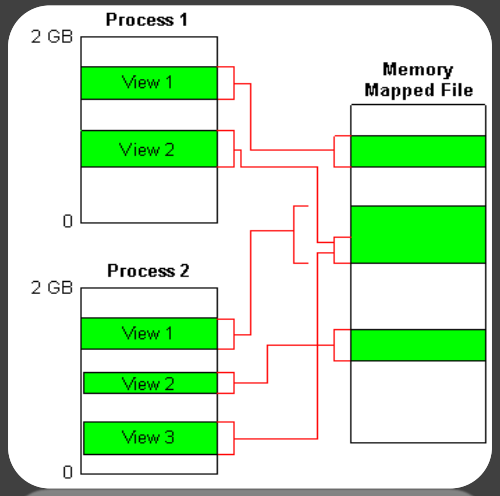
< 0x80000000 User Mode модули, подсистема Win32

> 0x80000000 Windows Kernel

Есть вариации, когда под User Mode отводится 3 Гб, а под ядро - 1 Гб

Три группы API функций

- ✓ Операции со страницами памяти
- ✓ Проецирование файлов в память
- ✓ Управление кучами



Перфиксы имён функций

Имена функций, предоставляемых:

- ✓ Диспетчером памяти - начинаются с префикса **Mm**
- ✓ Исполнительная подсистема (Executive) - начинаются с префикса **Ex**

```
MmMapIoSpace
MmAllocateMappingAddress
MmAllocatePagesForMdl
ExAllocatePoolWithTag
ExAllocatePool
```

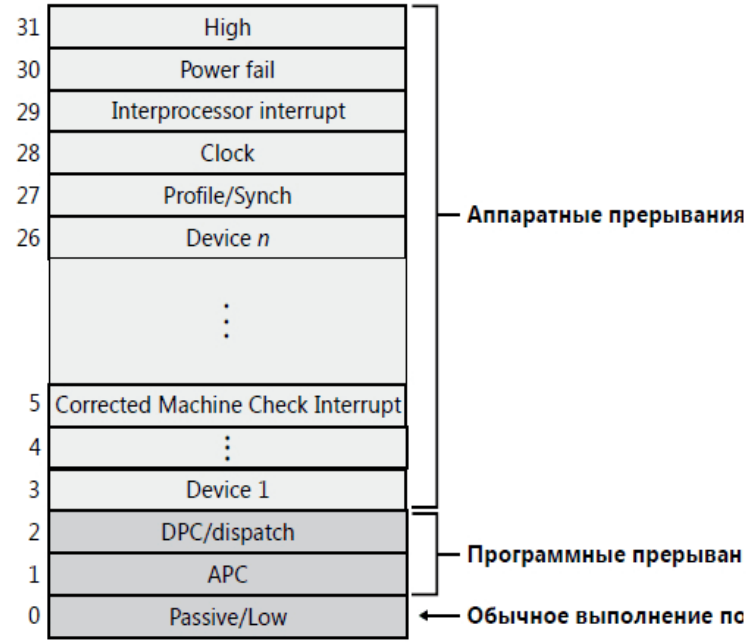
2

Уровни запросов прерываний

Уровни запросов прерываний

Windows устанавливает свою собственную схему приоритетности прерываний, известную как уровни запросов прерываний (IRQL)

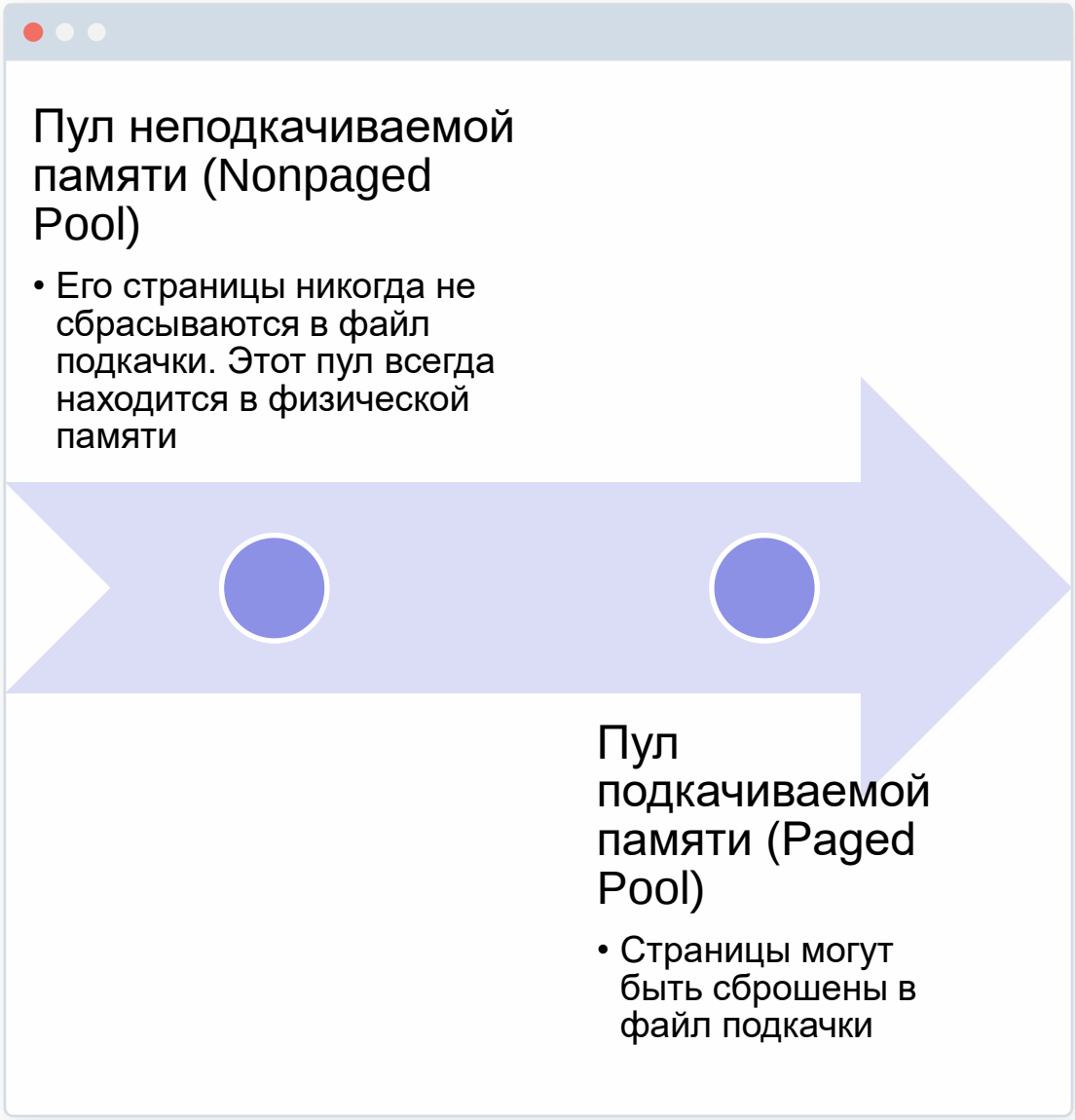
Всего 32 приоритета прерываний [0..31]. Самое приоритетное - 31



3

Системные кучи

Системные кучи

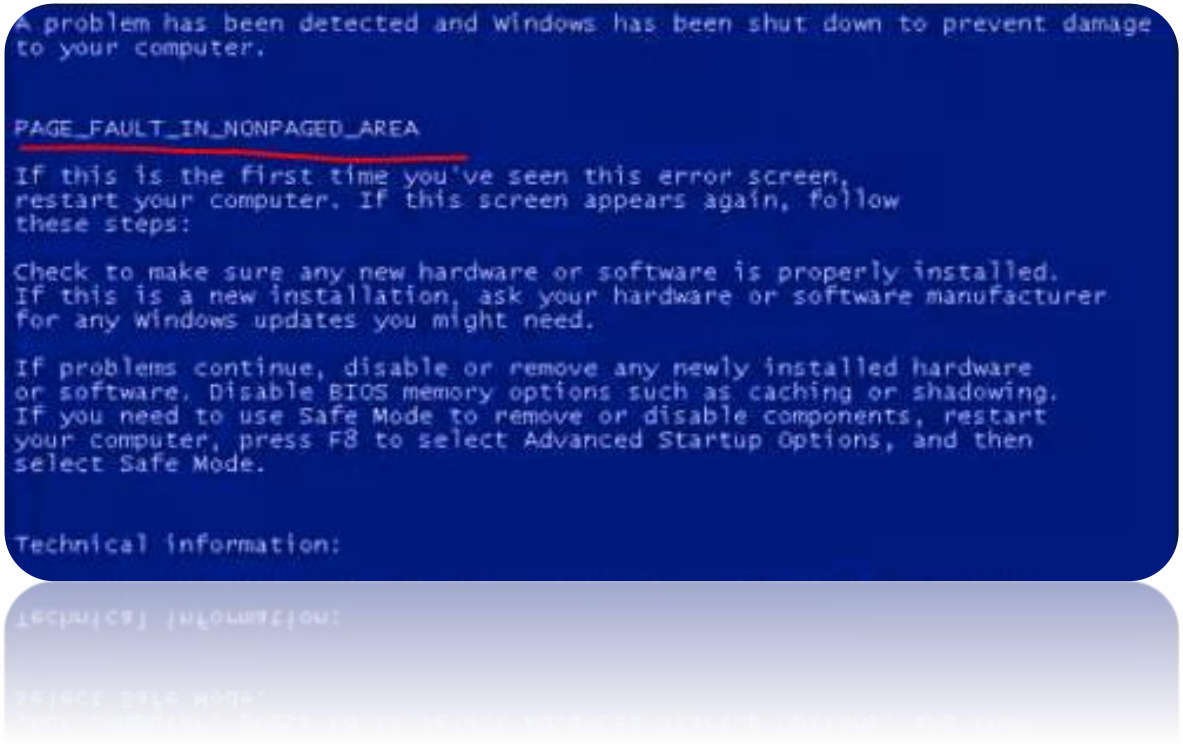


Оба пула находятся в системном адресном пространстве ➔ *доступны из контекста любого процесса*

Примечание

Обращение к памяти сброшенной в файл подкачки при IRQL >= DISPATCH_LEVEL

Ведёт к BSOD

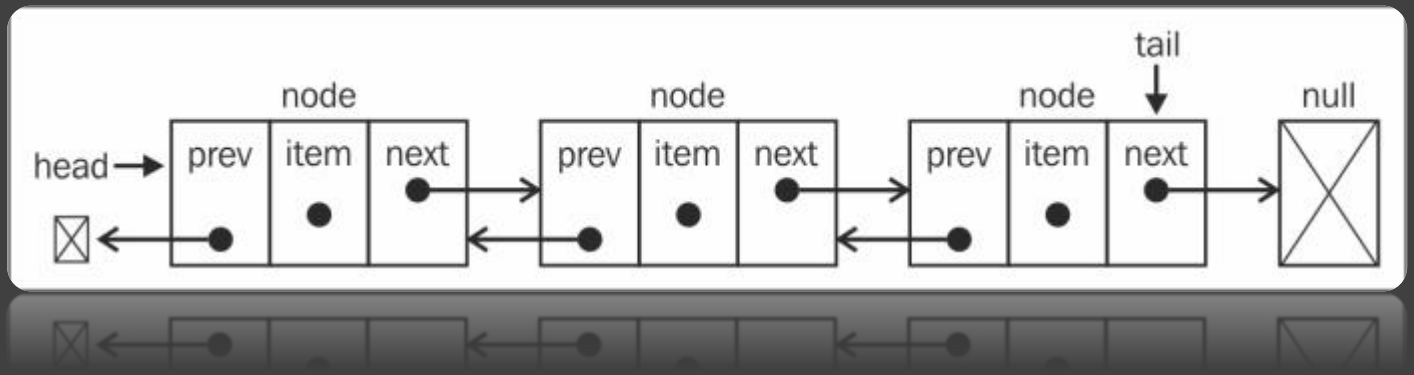


3

Ассоциативные списки

Ассоциативные списки

Если приходит запрос на выделение блока памяти из кучи, то диспетчер куч пытается подобрать свободный блок подходящего размера



Типы ассоциативных списков

Односвязный список

- singly linked list

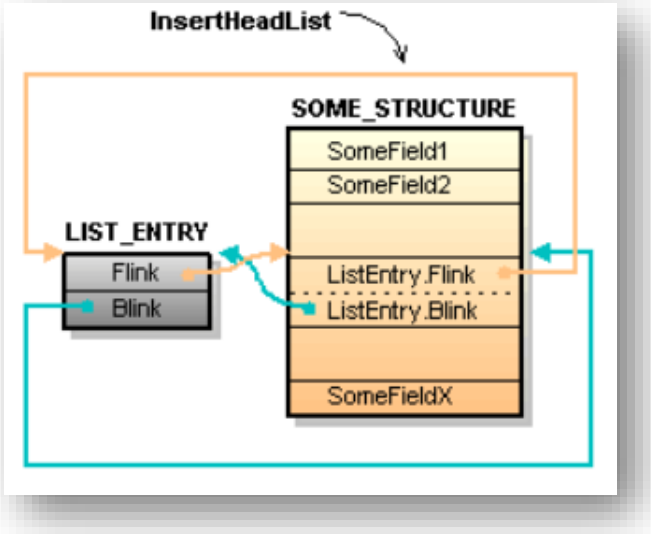
S-список

- S-list, sequenced singly-linked list

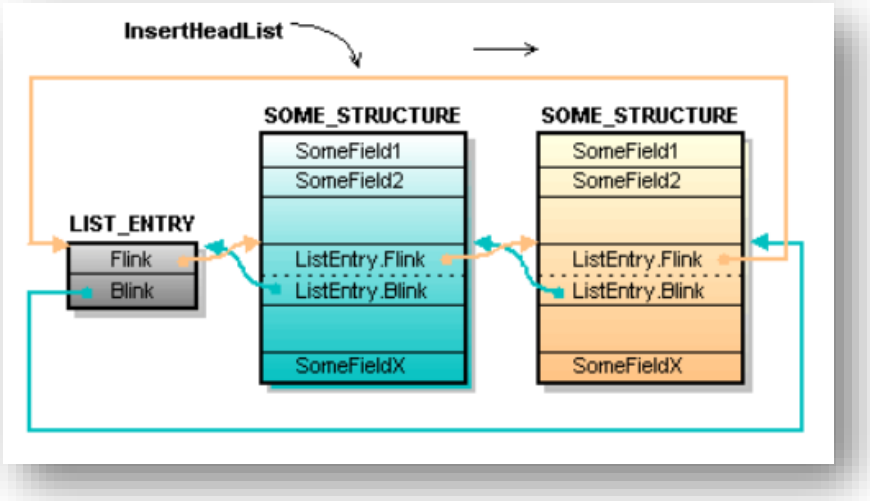
Двусвязный список

- doubly linked list

- ✓ ExInitializePagedLookasideList
- ✓ InitializeListHead
- ✓ AddEntry
- ✓ RemoveEntry
- ✓ ExDeletePagedLookasideList



- ✓ ExInitializePagedLookasideList
- ✓ InitializeListHead
- ✓ AddEntry
- ✓ RemoveEntry
- ✓ ExDeletePagedLookasideList



Проецирование файлов в память

На объекте “проекция файла” работают:

- буфер обмена
- оконные сообщения
- сокеты

Функции

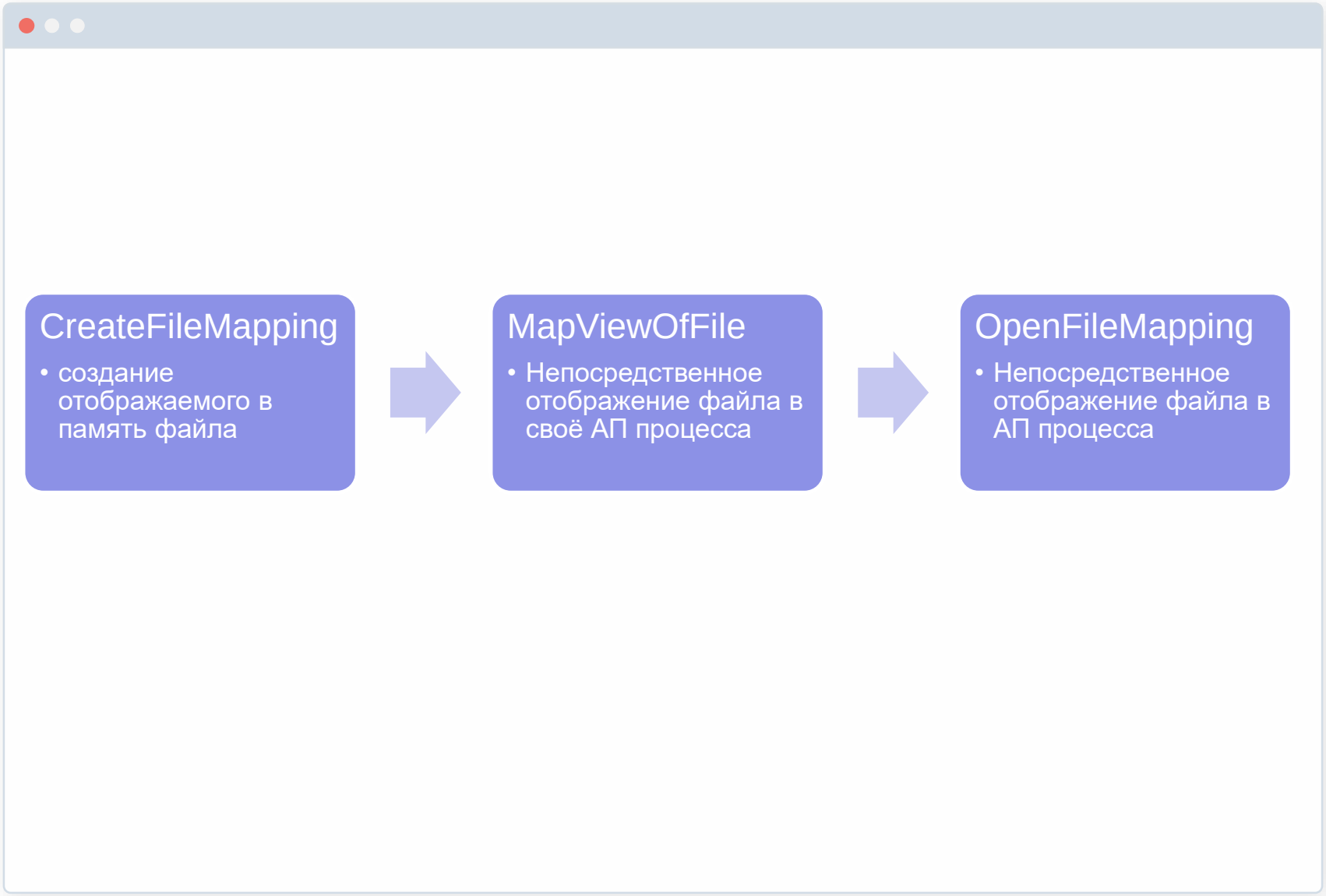

CreateFileMapping
• создание отображаемого в память файла
MapViewOfFile
• Непосредственное отображение файла в своё АП процесса
OpenFileMapping
• Непосредственное отображение файла в АП процесса

Таблица описания памяти (Memory Descriptor List, MDL)

Используется для для описания набора страниц физической памяти, представляющей ВАП конкретного процесса

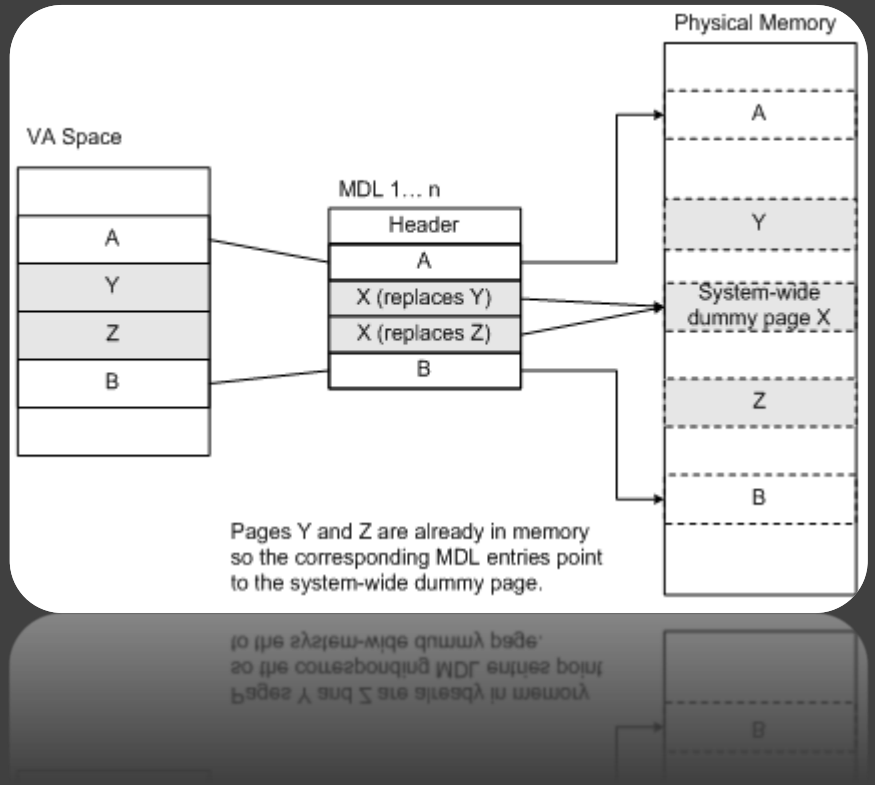


Таблица описания памяти (Memory Descriptor List, MDL)

OTUS

Структура MDL – заголовок, сразу за которым идёт массив из элементов DWORD – номеров физических страниц (Page Frame Number)

```
MDL STRUCT
    Next                PVOID       ?
    _Size               SWORD       ?
    MdlFlags            SWORD       ?
    Process             PVOID       ?
    MappedSystemVa      PVOID       ?
    StartVa             PVOID       ?
    ByteCount           DWORD       ?
    ByteOffset          DWORD       ?
MDL ENDS
PMDL typedef PTR MDL
```

Заполнение массива

MmBuildMdlForNonPagedPool - заполняет массив номеров физических страниц и обновляет некоторые поля заголовка MDL

```C++
void MmBuildMdlForNonPagedPool(
  PMDL MemoryDescriptorList
);
```

Отображение страницы в АП процесса

MmMapLockedPagesSpecifyCache

```C++
PVOID MmMapLockedPagesSpecifyCache(
  PMDL                                                                  MemoryDescriptorList,
  __drv_strictType(KPROCESSOR_MODE / enum _MODE,__drv_typeConst)KPROCESSOR_MODE AccessMode,
  __drv_strictTypeMatch(__drv_typeCond)MEMORY_CACHING_TYPE              CacheType,
  PVOID                                                                 RequestedAddress,
  ULONG                                                                 BugCheckOnFailure,
  ULONG                                                                 Priority
);
```

- MemoryDescriptorList – регион физической памяти, который нужно отобразить
- AccessMode – User/Kernel mode
- RequestedAddress – запрос VA

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!