**ЗАЩИТА ИНФОРМАЦИИ В МП**

**НАЗНАЧЕНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В МП**

* ОБЕСПЕЧЕНИЕ МУЛЬТИПРОГРАММНОГО РЕЖИМА РАБОТЫ ЗА СЧЕТ ПРЕДОТВРАЩЕНИЯ ВОЗМОЖНОСТИ ИЗМЕНЕНИЯ ОДНОЙ ПРОГРАММОЙ ОБЛАСТЕЙ ПАМЯТИ (КОДА, ДАННЫХ И СТЕКА), ИСПОЛЬЗУЕМЫХ ДРУГИМИ ПРОГРАММАМИ
* ЗАЩИТА СЕГМЕНТОВ И СТРАНИЦ (КОНТРОЛЬ ВЫПОЛНЕНИЯ РАЗРЕШЕННЫХ ОПЕРАЦИЙ ЧТЕНИЯ, ЗАПИСИ, ИСПОЛНЕНИЯ) КАК НЕЗАВИСИМЫХ И ОТДЕЛЬНО АДРЕСУЕМЫХ ОБЛАСТЕЙ ПАМЯТИ
* ФОРМИРОВАНИЕ ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ ПРИ ОБНАРУЖЕНИИ ОШИБОК ИСПОЛЬЗОВАНИЯ ПАМЯТИ ВО ВРЕМЯ ОТЛАДКИ ПРОГРАММ
* ОБНАРУЖЕНИЕ НЕВЫЯВЛЕННЫХ ПРИ РАЗРАБОТКЕ ОШИБОК В ПРИКЛАДНЫХ ПРОГРАММАХ, ПРИВОДЯЩИХ К НАРУШЕНИЯМ В ЛОКАЛИЗУЕМОМ АДРЕСНОМ ПРОСТРАНСТВЕ И ВЫДАЧА ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ СРЕДСТВАМИ ОПЕРАЦИОННОЙ СИСТЕМЫ

**СПОСОБЫ ЗАЩИТЫ ПРОГРАММ И ДАННЫХ**

ЗАЩИТА ПРИ УПРАВЛЕНИИ ПАМЯТЬЮ (СЕГМЕНТАЦИЯ И СТРАНИЧНАЯ АДРЕСАЦИЯ):

* ДОСТУПНОСТЬ СЕГМЕНТОВ, ДЕСКРИПТОРЫ КОТОРЫХ ЗАГРУЖЕНЫ В GDT ИЛИ LDT
* ВЫПОЛНЕНИЕ ТОЛЬКО РАЗРЕШЕННЫХ ОПЕРАЦИЙ С СЕГМЕНТАМИ

ЗАЩИТА ПО ПРИВИЛЕГИЯМ:

* КОНТРОЛЬ ВЫПОЛНЕНИЯ ПРИВИЛЕГИРОВАННЫХ КОМАНД (ЗАГРУЗКИ РЕГИСТРОВ ТАБЛИЦ ДЕСКРИПТОРОВ) И ДОСТУПА К ДЕСКРИПТОРАМ
* УРОВНИ ПРИВИЛЕГИЙ ОБЕСПЕЧИВАЮТ ИЗОЛЯЦИЮ ЗАДАЧ ПРИ ПОМОЩИ ЛОКАЛЬНЫХ ТАБЛИЦ ДЕСКРИПТОРОВ
* КАЖДАЯ ПРОГРАММА В СИСТЕМЕ РАБОТАЕТ НА СВОЕМ УРОВНЕ ПРИВИЛЕГИЙ

**ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРИ СЕГМЕНТАЦИИ ПАМЯТИ**

* ВСЕ КОНТРОЛЬНЫЕ ПРОВЕРКИ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СЕГМЕНТОВ И СТРАНИЦ ВЫПОЛНЯЮТСЯ В ЦИКЛЕ КОМАНДЫ ЗАГРУЗКИ СЕЛЕКТОРА В СЕГМЕНТНЫЙ РЕГИСТР
* ПРОВЕРКИ ВЫПОЛНЯЮТСЯ ПАРАЛЛЕЛЬНО С ТРАНСЛЯЦИЕЙ АДРЕСА (ПОЛУЧЕНИЕМ ФИЗИЧЕСКОГО АДРЕСА) БЕЗ СНИЖЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ
* ПРИ ОТСУТСТВИИ ОШИБОК ВЫПОЛНЯЕТСЯ КЭШИРОВАНИЕ ДЕСКРИПТОРА СЕГМЕНТА
* ПРИ ОБНАРУЖЕНИИ ОШИБОК КОНТРОЛЯ ВЫРАБАТЫВАЮТСЯ ПРОГРАММНЫЕ ПРЕРЫВАНИЯ

**ТИПЫ ПРОВЕРОК ПРИ СЕГМЕНТАЦИИ ПАМЯТИ**

1. ПРОВЕРКА ПОЛЯ TYPE ДЕСКРИПТОРОВ СЕГМЕНТОВ
2. ПРОВЕРКА ПРЕДЕЛОВ СЕГМЕНТОВ
3. ОГРАНИЧЕНИЯ НА ДОСТУПНОЕ АДРЕСНОЕ ПРОСТРАНСТВО ПРОГРАММЫ
4. ОГРАНИЧЕНИЯ НА ТОЧКИ ВХОДА В ПРОЦЕДУРЫ
5. ОГРАНИЧЕНИЯ СИСТЕМЫ КОМАНД

**КОНТРОЛЬ ПОЛЯ TYPE ДЕСКРИПТОРА СЕГМЕНТА**

* ИНФОРМАЦИЯ ДЛЯ КОНТРОЛЯ СЕГМЕНТНЫХ РЕГИСТРОВ БЕРЕТСЯ ИЗ ИХ ТЕНЕВЫХ РЕГИСТРОВ, В КОТОРЫХ КЭШИРУЕТСЯ ДЕСКРИПТОР СЕГМЕНТА (БАЗОВЫЙ АДРЕС, ПРЕДЕЛ, ТИП, УРОВЕНЬ ПРИВИЛЕГИЙ)

* Поле TYPE определяет не только сегмент кода или данных, а также порядок обращения к ним на чтение и запись:
* Бит «W» – разрешения записи определяет возможность при выполнении программ осуществлять запись данных в сегмент данных
* Бит «r» - разрешает программам чтение из сегмента кода (например, констант)

**ПРИМЕРЫ КОНТРОЛЯ ПОЛЯ TYPE**

ПРИ ЗАГРУЗКЕ СЕЛЕКТОРА ДЕСКРИПТОРА В СЕГМЕНТНЫЙ РЕГИСТР ПРОВЕРЯЕТСЯ СООТВЕТСТВИЕ ТИПА ДЕСКРИПТОРА:

* В РЕГИСТР CS МОЖЕТ БЫТЬ ЗАГРУЖЕН ТОЛЬКО СЕЛЕКТОР СЕГМЕНТА КОДА
* СЕЛЕКТОР СЕГМЕНТА ДАННЫХ УКАЗЫВАЕТ НА ДЕСКРИПТОР СЕГМЕНТА С РАЗРЕШЕНИЕМ ЧТЕНИЯ
* В РЕГИСТР SS МОЖЕТ БЫТЬ ЗАГРУЖЕН ТОЛЬКО СЕЛЕКТОР С РАЗРЕШЕНИЕМ ЧТЕНИЯ И ЗАПИСИ ДАННЫХ В СЕГМЕНТ

**ПРОВЕРКА СООТВЕТСТВИЯ НАЗНАЧЕНИЯ КОМАНД И ТИПА СЕГМЕНТА:**

* НИ КАКАЯ КОМАНДА НЕ МОЖЕТ ЗАПИСЫВАТЬ ДАННЫЕ В СЕГМЕНТ КОДА
* НИКАЯ КОМАНДА НЕ МОЖЕТ ЗАПИСЫВАТЬ В СЕГМЕНТ ДАННЫХ, ЕСЛИ НЕ УСТАНОВЛЕН БИТ РАЗРЕШЕНИЯ ЗАПИСИ (W)
* НИКАКАЯ КОМАНДА НЕ МОЖЕТ ЧИТАТЬ СЕГМЕНТ КОДА, ЕСЛИ НЕ УСТАНОВЛЕН БИТ РАЗРЕШЕНИЯ ЧТЕНИЯ (R)

**КОНТРОЛЬ ПРЕДЕЛОВ СЕГМЕНТОВ**

* ПОЛЕ ПРЕДЕЛА (ОПРЕДЕЛЯЕТ ДОПУСТИМЫЕ ЗНАЧЕНИЯ СМЕЩЕНИЯ) В ДЕСКРИПТОРЕ СЕГМЕНТА ПОЗВОЛЯЕТ КОНТРОЛИРОВАТЬ ВЫХОД ПРОГРАММЫ ЗА ДОПУСТИМЫЕ ГРАНИЦЫ ОТВЕДЕННОГО ЕЙ АДРЕСНОГО ПРОСТРАНСТВА
* ОБНАРУЖИВАЮТСЯ ОШИБКИ В ПРОГРАММЕ – ВЫХОД ИНДЕКСА ЗА ГРАНИЦУ, НЕПРАВИЛЬНОЕ ВЫЧИСЛЕНИЕ УКАЗАТЕЛЯ
* ДЕЙСТВИТЕЛЬНАЯ ГРАНИЦА СЕГМЕНТА ОПРЕДЕЛЯЕТСЯ БИТОМ «G» (ГРАНУЛЯРНОСТЬ) – ДЛЯ СЕГМЕНТА КОДА И БИТАМИ «G» И «Е/ED» (НАПРАВЛЕНИЕ РАСШИРЕНИЯ) – ДЛЯ СЕГМЕНТА ДАННЫХ
* ДЛЯ ВСЕХ ТИПОВ СЕГМЕНТОВ КРОМЕ СЕГМЕНТА СТЕКА РЕАЛЬНЫЙ ОБЪЕМ ХРАНИМЫХ ДАННЫХ (В БАЙТАХ) НА ЕДИНИЦУ БОЛЬШЕ ЗНАЧЕНИЯ ПРЕДЕЛА

**ВЫХОД АДРЕСА ЗА ПРЕДЕЛ**

* ПРЕДЕЛ – АДРЕС ПОСЛЕДНЕГО БАЙТА В СЕГМЕНТЕ
* ВЫЗОВ ПРОГРАММНОГО ПРЕРЫВАНИЯ ПРИ НЕКОРРЕКТНОМ ОБРАЩЕНИИ К СЕГМЕНТУ ДАННЫХ ЗАВИСИТ ОТ ФОРМАТА ДАННЫХ И АДРЕСА ОБРАЩЕНИЯ:
* БАЙТ → АДРЕС > ПРЕДЕЛА
* СЛОВО → АДРЕС > (ПРЕДЕЛ-1)
* ДВОЙНОЕ СЛОВО → АДРЕС > (ПРЕДЕЛ-3)

**ДОПУСТИМЫЕ РАЗМЕРЫ СЕГМЕНТОВ**

* ПРИ G=0 ВЕЛИЧИНА ПРЕДЕЛА В БАЙТАХ ОПРЕДЕЛЯЕТСЯ 20-ТИ БИТНЫМ ПОЛЕМ ПРЕДЕЛА В ДЕСКРИПТОРЕ СЕГМЕНТА И НАХОДИТСЯ В ДИАПАЗОНЕ:

0 – 0FFFFFh (220-1 = 1 Мбайт) (ЕСЛИ ПРЕДЕЛ =0, В СЕГМЕНТЕ МОЖЕТ БЫТЬ ТОЛЬКО ОДИН БАЙТ)

* ПРИ G=1 ЗНАЧЕНИЕ ПОЛЯ ПРЕДЕЛА В ДЕСКРИПТОРЕ УМНОЖАЕТСЯ НА 212 (РАЗМЕР ОДНОЙ СТРАНИЦЫ). ВЕЛИЧИНА ПРЕДЕЛА В БАЙТАХ НАХОДИТСЯ В ДИАПАЗОНЕ:

0FFFh (212-1) – 0FFFFFFFFh (232-1) (4Кбайта – 4Гбайта) (220 СТРАНИЦ)

* ПРИ G=1 12 МЛАДШИХ РАЗРЯДОВ АДРЕСА НЕ УЧАСТВУЮТ В КОНТРОЛЕ НАРУШЕНИЙ ПРЕДЕЛА (КОНТРОЛИРУЮТСЯ ТОЛЬКО 20 СТАРШИХ РАЗРЯДОВ, ОПРЕДЕЛЯЮЩИХ НОМЕР СТРАНИЦЫ). ПРИ G=1 И НУЛЕВОМ ЗНАЧЕНИИ ПРЕДЕЛА СМЕЩЕНИЕ В СЕГМЕНТЕ ЛЕЖИТ В ДИАПАЗОНЕ:

0 – 4095 (АДРЕС БАЙТА В 0-ой СТРАНИЦЕ)

**КОНТРОЛЬ СЕГМЕНТА СТЕКА**

* ДЛЯ СЕГМЕНТА СТЕКА (EXPAND-DOWN ИЛИ НИЖНИЙ СТЕК) ДИПАЗОН ВОЗМОЖНЫХ ЗНАЧЕНИЙ СМЕЩЕНИЯ СОСТАВЛЯЕТ:

(ПРЕДЕЛ+1) – (232 -1)

* ПОСЛЕДНЯЯ ЗАПИСЬ В СТЕК МОЖЕТ БЫТЬ ВЫПОЛНЕНА, КОГДА УКАЗАТЕЛЬ СТЕКА = ПРЕДЕЛУ+1 (ПЕРЕД ЗАПИСЬЮ В СТЕК УКАЗАТЕЛЬ ДЕКРЕМЕНТИРУЕТСЯ)
* МАКСИМАЛЬНЫЙ РАЗМЕР СЕГМЕНТА СТЕКА ПРИ ФИКСИРОВАННОМ БАЗОВОМ АДРЕСЕ СООТВЕТСТВУЕТ ЗНАЧЕНИЮ ПРЕДЕЛА = «0»

**КОНТРОЛЬ ОБРАЩЕНИЙ К ТАБЛИЦАМ ДЕСКРИПТОРОВ**

* ДЛЯ КОНТРОЛЯ НАРУШЕНИЙ ПРИ ОБРАЩЕНИИ К ТАБЛИЦАМ ДЕСКРИПТОРОВ ИСПОЛЬЗУЮТСЯ РЕГИСТРЫ GDTR И IDTR, В КОТОРЫХ ХРАНЯТСЯ 16-ТИ РАЗРЯДНЫЕ ЗНАЧЕНИЯ ПРЕДЕЛОВ (РАЗМЕРОВ) ТАБЛИЦ
* ЗНАЧЕНИЕ ПРЕДЕЛА ОПРЕДЕЛЯЕТ АДРЕС ПОСЛЕДНЕГО БАЙТА, ОТНОСЯЩЕГОСЯ К ТАБЛИЦЕ
* ТАК КАК КАЖДЫЙ ДЕСКРИПТОР СОДЕРЖИТ 8 байт, РАЗМЕР ПРЕДЕЛА ТАБЛИЦЫ ДЛЯ ХРАНЕНИЯ N ДЕСКРИПТОРОВ ДОЛЖЕН СОСТАВЛЯТЬ 8N-1
* ДЕСКРИПТОР С НУЛЕВЫМ АДРЕСОМ В ТАБЛИЦЕ GDT ЯВЛЯЕТСЯ ПУСТЫМ. ТАКОЙ ДЕСКРИПТОР МОЖЕТ БЫТЬ ЗАГРУЖЕН В ТЕНЕВОЙ РЕГИСТР СЕГМЕНТНОГО РЕГИСТРА, НО ОБРАЩЕНИЕ К ПАМЯТИ С ИСПОЛЬЗОВАНИЕМ ПУСТОГО ДЕСКРИПТОРА ПРИВЕДЕТ К ПРОГРАММНОИМУ ПРЕРЫВАНИЮ

**НАЗНАЧЕНИЕ ЗАЩИТЫ ПО ПРИВИЛЕГИЯМ**

* ПРИВИЛЕГИИ – ЭТО ИЕРАРХИЧЕСКИ СВЯЗАННЫЕ АТРИБУТЫ ПРОГРАММНЫХ ОБЪЕКТОВ, КОТОРЫЕ РЕГЛАМЕНТИРУЮТ ПОРЯДОК ВЫПОЛНЕНИЯ КОМАНД И ДОСТУПА К СЕГМЕНТАМ И СТРАНИЦАМ В МНОГОЗАДАЧНОЙ СИСТЕМЕ С ЦЕЛЬЮ СОХРАНЕНИЯ ЦЕЛОСТНОСТИ СИСТЕМЫ
* ЗАЩИТА ПО ПРИВИЛЕГИЯМ – СПОСОБ ИСКЛЮЧИТЬ СЛУЧАЙНЫЙ ИЛИ УМЫШЛЕННЫЙ ДОСТУП ПРИКЛАДНЫХ ПРОГРАММ К КЛЮЧЕВЫМ КОМПОНЕНТАМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ (ЯДРО И УТИЛИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ, КРИТИЧЕСКИЕ ДАННЫЕ)
* МЕХАНИЗМ ЗАЩИТЫ ПО ПРИВИЛЕГИЯМ ДОЛЖЕН БЫТЬ ОСНОВАН НА АППАРАТНО ПОДДЕРЖИВАЕМЫХ ПРАВИЛАХ ВЗАИМОДЕЙСТВИЯ ПРОГРАММНЫХ ОБЪЕКТОВ, НАХОДЯЩИХСЯ НА РАЗНЫХ УРОВНЯХ ПРИВИЛЕГИЙ – ИСПОЛЬЗОВАНИЕ АТРИБУТОВ СЕГМЕНТОВ (ДЕСКРИПТОРЫ)
* СОХРАНЕНИЕ ЦЕЛОСТНОСТИ СИСТЕМЫ ПРИ ЗАЩИТЕ ПО ПРИВИЛЕГИЯМ НЕ ЗАВИСИТ ОТ НАДЕЖНОСТИ ПРИКЛАДНЫХ ПРОГРАММ И ЗАВИСИТ ТОЛЬКО ОТ НАЛИЧИЯ СКРЫТЫХ ОШИБОК В ОПЕРАЦИОННОЙ СИСТЕМЕ

**ЗАЩИТА ПО ПРИВИЛЕГИЯМ В IA-32**

* ПОЗВОЛЯЕТ ПРОКОНТРОЛИРОВАТЬ ИСПОЛЬЗОВАНИЕ ПРИВИЛЕГИРОВАННЫХ КОМАНД (ИЗМЕНЯЮЩИХ СИСТЕМНЫЕ РЕГИСТРЫ, ВВОДА/ВЫВОДА )И ДОСТУП К СЕГМЕНТАМ, СТРАНИЦАМ И СЕГМЕНТНЫМ ДЕСКРИПТОРАМ
* ДЛЯ КАЖДОЙ ВЫПОЛНЯЕМОЙ ПРОГРАММЫ ОПРЕДЕЛЯЕТСЯ УРОВЕНЬ ЕЕ ПРИВИЛЕГИЙ (КОДИРУЕТСЯ ДВУМЯ БИТАМИ CPL СЕГМЕНТНОГО РЕГИСТРА КОДА – ТЕКУЩИЙ УРОВЕНЬ ПРИВИЛЕГИЙ ПРОГРАММЫ)
* ЗНАЧЕНИЕ CPL ПРОВЕРЯЕТСЯ В MMU ПАРАЛЛЕЛЬНО С ФОРМИРОВАНИЕМ ФИЗИЧЕСКОГО АДРЕСА БЛОКАМИ СЕГМЕНТАЦИИ И СТРАНИЧНОГО ПРЕОБРАЗОВАНИЯ – ДОСТУПЕН ЛИ ЗАПРАШИВАЕМЫЙ СЕГМЕНТ ПРОГРАММЕ С УРОВНЕМ ПРИВИЛЕГИЙ CPL
* ОТКЛЮЧЕНИЕ МЕХАНИЗМА ЗАЩИТЫ ПО ПРИВИЛЕГИЯМ ВОЗМОЖНО ТОЛЬКО ПУТЕМ ПРИСВОЕНИЯ ВЫСШЕГО УРОВНЯ ПРИВИЛЕГИЙ ВСЕМ СЕЛЕКТОРАМ СЕГМЕНТОВ, ДЕСКРИПТОРАМ СЕГМЕНТОВ И ЭЛЕМЕНТАМ ТАБЛИЦ СТРАНИЦ (РТЕ)

**4-х УРОВНЕВАЯ СИСТЕМА ПРИВИЛЕГИЙ IA-32**

* 4-х УРОВНЕВАЯ СИСТЕМА ПРИВИЛЕГИЙ ЯВЛЯЕТСЯ РАСШИРЕНИЕМ 2-х УРОВНЕВОЙ СИСТЕМЫ USER/SUPERVISOR
* ЗАЩИТА ОС ОТ ВЛИЯНИЯ НА НЕЕ ДЕФЕКТОВ ПРИКЛАДНЫХ ПРОГРАММ ОБЕСПЕЧИВАЕТСЯ ПРИСВОЕНИЕМ ЯДРУ ОС НАИВЫСШЕГО УРОВНЯ ПРИВИЛЕГИЙ
* УТИЛИТЫ И СЛУЖЕБНЫЕ ПРОГРАММЫ ОПЕРАЦИОННОЙ СИСТЕМЫ ИМЕЮТ СЛЕДУЮЩИЕ ПО РАНГУ (ПРОМЕЖУТОЧНЫЕ) УРОВНИ ПРИВИЛЕГИЙ
* ПРИКЛАДНЫЕ ПРОГРАММЫ ИМЕЮТ НИЗШИЙ УРОВЕНЬ ПРИВИЛЕГИЙ
* УРОВНИ ПРИВИЛЕГИЙ (PL) ПРИСВАИВАЮТСЯ СЛЕДУЮЩИМ ПРОГРАММНЫМ ОБЪЕКТАМ:
* ЗАДАЧАМ (ПРОГРАММАМ) –CPL
* ДЕСКРИПТОРАМ – DPL
* СЕЛЕКТОРАМ – RPL

**УРОВЕНЬ ПРИВИЛЕГИЙ ТЕКУЩЕЙ ПРОГРАММЫ**

* 2 МЛАДШИХ БИТА СЕГМЕНТНОГО РЕГИСТРА КОДА CS ОПРЕДЕЛЯЮТ УРОВЕНЬ ПРИВИЛЕГИЙ ИСПОЛНЯЕМОЙ (ТЕКУЩЕЙ) ПРОГРАММЫ – БИТЫ CPL (CURRENT PRIVILEGE LEVEL)
* БИТЫ CPL СООТВЕТСТВУЮТ БИТАМ DPL В ДЕСКРИПТОРЕ СЕГМЕНТА КОДА
* 2 МЛАДШИХ БИТА РЕГИСТРА SS СОДЕРЖАТ КОПИЮ CPL
* БИТЫ CPL МОГУТ ИЗМЕНИТЬСЯ ПРИ ПЕРЕДАЧЕ УПРАВЛЕНИЯ ДРУГОМУ СЕГМЕНТУ КОДА ЧЕРЕЗ ШЛЮЗ ВЫЗОВА

**УРОВЕНЬ ПРИВИЛЕГИЙ ДЕСКРИПТОРА (СЕГМЕНТА)**

ДЕСКРИПТОРЫ СЕГМЕНТОВ СОДЕРЖАТ 2-х РАЗРЯДНОЕ ПОЛЕ DPL (DESCRIPTOR PRIVILEGE LEVEL) ДЛЯ ОПРЕДЕЛЕНИЯ УРОВНЯ ПРИВИЛЕГИЙ СЕГМЕНТА

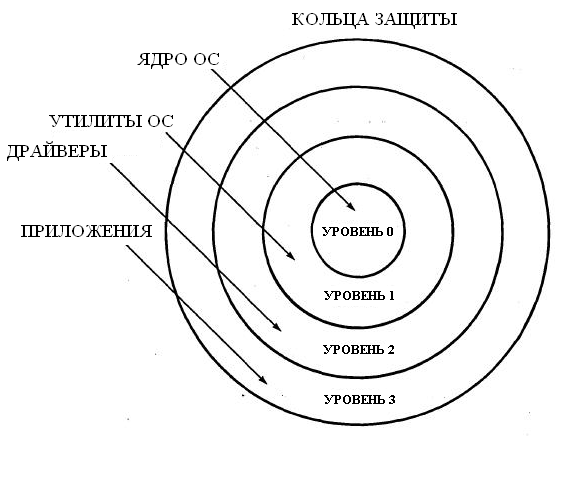
ПОЛЕ DPL ОПРЕДЕЛЯЕТ УРОВЕНЬ ПРИВИЛЕГИЙ ДАННЫХ В СЕГМЕНТЕ ДАННЫХ ИЛИ КОДА В СЕГМЕНТЕ КОДА

ПОЛЕ DPL ОПРЕДЕЛЯЕТ НАИМЕНЬШИЙ УРОВЕНЬ ПРИВИЛЕГИЙ, С КОТОРЫМ ВОЗМОЖЕН ДОСТУП К СЕГМЕНТУ

УРОВЕНЬ ПРИВИЛЕГИЙ СЕЛЕКТОРА

* 2 МЛАДШИХ БИТА СЕЛЕКТОРОВ СЕГМЕНТОВ DS,ES,FS,GS – БИТЫ RPL (REQUESTED PRIVILEGE LEVEL) ОПРЕДЕЛЯЮТ МАКСИМАЛЬНЫЙ ЗАПРАШИВАЕМЫЙ УРОВЕНЬ ПРИВИЛЕГИЙ СЕГМЕНТА, К КОТОРОМУ ПРОИСХОДИТ ОБРАЩЕНИЕ (НАПРИМЕР, ПРИ RPL=2, ЗНАЧЕНИЕ DPL=2,3. ЗДЕСЬ «2» – МАКСИМАЛЬНЫЙ УРОВЕНЬ ПРИВИЛЕГИЙ СЕГМЕНТА)
* ИСПОЛЬЗУЕТСЯ ДЛЯ СНИЖЕНИЯ ТЕКУЩЕГО УРОВНЯ ПРИВИЛЕГИЙ ПРОГРАММЫ ПРИ ОБРАЩЕНИИ К СЕГМЕНТУ.ПРИ RPL=0, УРОВЕНЬ ПРИВИЛЕГИЙ ПРОГРАММЫ ПРИ ОБРАЩЕНИИ К СЕГМЕНТУ ОПРЕДЕЛЯЕТСЯ CPL. ПРИ RPL=3, ВОЗМОЖНО ОБРАЩЕНИЕ К СЕГМЕНТУ ТОЛЬКО С DPL=3 НЕЗАВИСИМО ОТ ЗНАЧЕНИЯ CPL
* ИСПОЛЬЗУЕТСЯ ДЛЯ ПРОВЕРКИ ТОГО, ЧТО УКАЗАТЕЛЬ ДЛЯ ВЫЗОВА ПРОЦЕДУР ОС НЕ ПРЕДПОЛАГАЕТ ОБРАЩЕНИЯ К ДАННЫМ С УРОВНЕМ ПРИВИЛЕГИЙ ВЫШЕ, ЧЕМ ПРОГРАММА, КОТОРАЯ ФОРМИРУЕТ ЭТОТ УКАЗАТЕЛЬ

**УРОВНИ ПРИВИЛЕГИЙ КАК КОЛЬЦА ЗАЩИТЫ**

****

ВЫСШИЙ УРОВЕНЬ ПРИВИЛЕГИЙ = 0. НИЗШИЙ УРОВЕНЬ ПРИВИЛЕГИЙ = 3

ЯДРО ОС – ИНИЦИАЛИЗАЦИЯ, УПРАВЛЕНИЕ ПАМЯТЬЮ,

ЗАЩИТОЙ,ТЕСТИРОВАНИЕМ

УТИЛИТЫ – СУБД, БИБЛИОТЕКИ, СИСТЕМНЫЕ ФУНКЦИИ

ДРАЙВЕРЫ – УПРАВЛЕНИЕ ВВОДОМ/ВЫВОДОМ

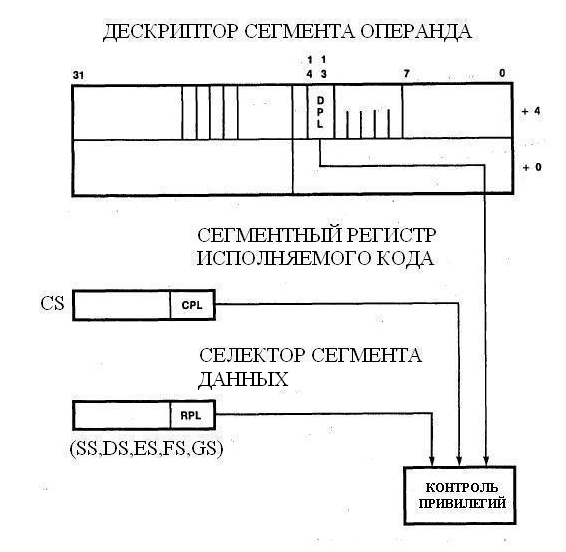
**БАЗОВЫЕ ПРАВИЛА КОНТРОЛЯ ПО ПРИВИЛЕГИЯМ В IA-32**

* ДОСТУП К ДАННЫМ, ХРАНИМЫМ В СЕГМЕНТЕ С УРОВНЕМ ПРИВИЛЕГИЙ «PR» , РАЗРЕШЕН ИСПОЛНЯМЫМ ПРОГРАММАМ С УРОВНЕМ ПРИВИЛЕГИЙ НЕ НИЖЕ «PR» (ИЗ ТЕКУЩЕГО ИЛИ ИЗ ВНУТРЕННЕГО КОЛЬЦА)
* ИСПОЛНЯЕМАЯ ПРОГРАММА ИЛИ ПРОЦЕДУРА С УРОВНЕМ ПРИВИЛЕГИЙ «PR» МОЖЕТ БЫТЬ ВЫЗВАНА ТОЛЬКО ПРОГРАММОЙ С УРОВНЕМ ПРИВИЛЕГИЙ НЕ ВЫШЕ «PR» (ПЕРЕДАЧА УПРАВЛЕНИЯ СНИЗУ-ВВЕРХ) (ИЗ ТЕКУЩЕГО ИЛИ ИЗ ВНЕШНЕГО КОЛЬЦА)

**ОСОБЕННОСТИ КОНТРОЛЯ УРОВНЕЙ ПРИВИЛЕГИЙ**

* УРОВНИ ПРИВИЛЕГИЙ КОНТРОЛИРУЮТСЯ В МОМЕНТ ЗАГРУЗКИ СЕЛЕКТОРА В СЕГМЕНТНЫЙ РЕГИСТР
* ПОРЯДОК КОНТРОЛЯ УРОВНЕЙ ПРИВИЛЕГИЙ ПРИ ОБРАЩЕНИИ К СЕГМЕНТУ ДАННЫХ ОТЛИЧАЕТСЯ ОТ ПОРЯДКА КОНТРОЛЯ УРОВНЕЙ ПРИВИЛЕГИЙ ПРИ ПЕРЕДАЧЕ УПРАВЛЕНИЯ В СЕГМЕНТЕ КОДА

**КОНТРОЛЬ ПРИВИЛЕГИЙ ПРИ ДОСТУПЕ К ДАННЫМ В СЕГМЕНТАХ ДАННЫХ**

****

ЗАГРУЗКА СЕЛЕКТОРА В СЕГМЕНТЫ ДАННЫХ ТОЛЬКО ПРИ DPL≥CPL. ДЛЯ SS И CS DPL=CPL

ЗАГРУЗКА ОПЕРАНДА ВОЗМОЖНА, ЕСЛИ ТОЛЬКО DPL≥MAX(CPL,RPL)

Т.Е. УРОВЕНЬ ПРИВИЛЕГИЙ СЕГМЕНТА ДАННЫХ (DPL) НИЖЕ УРОВНЕЙ ПРИВИЛЕГИЙ КАК ТЕКУЩЕЙ ПРОГРАММЫ (CPL), ТАК И ЗАПРАШИВАЕМОГО УРОВНЯ ПРИВИЛЕГИЙ СЕГМЕНТА (RPL)

MAX(CPL,RPL)=EPL – ЭФФЕКТИВНЫЙ УРОВЕНЬ ПРИВИЛЕГИЙ

**КОНТРОЛЬ ДОСТУПА К ДАННЫМ В СЕГМЕНТЕ КОДА**

* ПРАКТИКА ИСПОЛЬЗВАНИЯ ПЗУ ДЛЯ ХРАНЕНИЯ ИСПОЛНЯЕМОГО КОДА И КОНСТАНТ, ИСПОЛЬЗУЕМЫХ ПРИ ВЫПОЛНЕНИИ ПРОГРАММ

* ИНОГДА ПРИ РАЗРАБОТКЕ ПРОГРАММ ВОЗНИКАЕТ НЕОБХОДИМОСТЬ ОРГАНИЗАЦИИ ХРАНЕНИЯ ДАННЫХ В СЕГМЕНТЕ КОДА (НАПРИМЕР, КОНСТАНТ)

* ДОСТУП К ДАННЫМ В СЕГМЕНТЕ КОДА ВОЗМОЖЕН ПРИ УСЛОВИИ, ЧТО НЕКОТОРЫЙ СЕГМЕНТ ДАННЫХ ОТОБРАЖАЕТСЯ НА ТУ ЖЕ ОБЛАСТЬ ПАМЯТИ, ЧТО И СЕГМЕНТ КОДА (ИДЕНТИЧНЫЙ БАЗОВЫЙ АДРЕС И ПРЕДЕЛ)
* ДЛЯ ДОСТУПА К ДАННЫМ В СЕГМЕНТЕ КОДА НЕОБХОДИМО ЗАГРУЗИТЬ В НЕКОТОРЫЙ СЕГМЕНТНЫЙ РЕГИСТР ДАННЫХ СЕЛЕКТОР ЧИТАЕМОГО СЕГМЕНТА КОДА

**ЗАЩИТА СЕГМЕНТОВ КОДА ПО ПРИВИЛЕГИЯМ**

* ПРОБЛЕМА ВОЗНИКАЕТ ПРИ ВЫПОЛНЕНИИ КОМАНД ПЕРЕХОДА, ВЫЗОВА ПРОЦЕДУР И ПРЕРЫВАНИЙ, ВОЗВРАТА ИЗ ПРОЦЕДУР И ОБРАБОТЧИКОВ ПРЕРЫВАНИЙ
* ПРЯМАЯ ПЕРЕДАЧА УПРАВЛЕНИЯ (МЕЖСЕГМЕНТНЫЕ ПЕРЕХОДЫ) БЕЗ ИЗМЕНЕНИЯ СТАТУСА ЗАЩИТЫ СЕГМЕНТА НЕВОЗМОЖНА
* ВАРИАНТЫ РЕШЕНИЯ ПРОБЛЕМЫ:
* ПОДЧИНЕННЫЕ СЕГМЕНТЫ КОДА (ПРЯМАЯ ПЕРЕДАЧА)
* ШЛЮЗЫ ВЫЗОВА (КОСВЕННАЯ ПЕРЕДАЧА)

**КОНТРОЛЬ ПРИ ПЕРЕДАЧЕ УПРАВЛЕНИЯ В ТЕКУЩЕМ СЕГМЕНТЕ   
(КОРОТКИЕ ПЕРЕХОДЫ)**

* ПРИ ПЕРЕДАЧЕ УПРАВЛЕНИЯ И ВОЗВРАТЕ В ТОЧКУ ВЫЗОВА В ПРЕДЕЛАХ ТЕКУЩЕГО СЕГМЕНТА КОДА («КОРОТКИЕ» ПЕРЕХОДЫ И ВЫЗОВЫ) КОНТРОЛИРУЕТСЯ ТОЛЬКО ВОЗМОЖНЫЙ ВЫХОД ЗА ПРЕДЕЛ СЕГМЕНТА БЕЗ КОНТРОЛЯ УРОВНЕЙ ПРИВИЛЕГИЙ
* ЗНАЧЕНИЕ ПРЕДЕЛА ХРАНИТСЯ В ТЕНЕВОМ РЕГИСТРЕ СЕГМЕНТНОГО РЕГИСТРА CS (ПОЛЕ ПРЕДЕЛА В ДЕСКРИПТОРЕ СЕГМЕНТА), ПОЭТОМУ КОНТРОЛЬ ВЫХОДА ЗА ПРЕДЕЛ СЕГМЕНТА НЕ ТРЕБУЕТ ОБРАЩЕНИЯ К ПАМЯТИ И ПРАКТИЧЕСКИ НЕ УХУДШАЕТ ПРОИЗВОДИТЕЛЬНОСТЬ ПРОЦЕССОРА

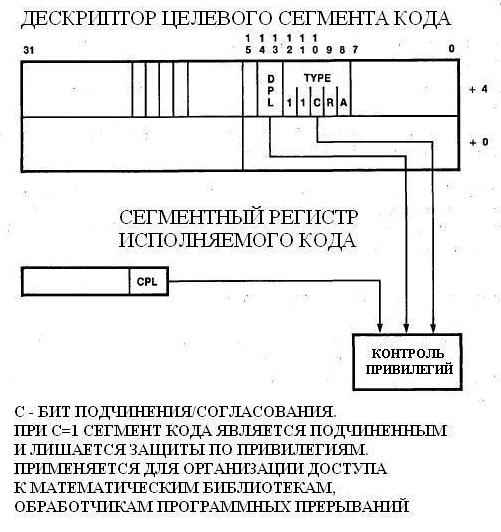
**ПРОБЛЕМА «ДЛИННЫХ» ПЕРЕХОДОВ И ВЫЗОВОВ**

* ПРИ ВЫПОЛНЕНИИ ДЛИННЫХ ПЕРЕХОДОВ И ВЫЗОВОВ ПРОЦЕДУРЫ НАХОДЯТСЯ В ДРУГИХ (ЦЕЛЕВЫХ) СЕГМЕНТАХ С УНИКАЛЬНЫМИ УРОВНЯМИ ПРИВИЛЕГИЙ, ПОЭТОМУ КОНТРОЛЬ УРОВНЕЙ ПРИВИЛЕГИЙ НЕОБХОДИМ
* ДВА СПОСОБА ОБРАЩЕНИЯ К ЦЕЛЕВЫМ СЕГМЕНТАМ ПРИ ВЫПОЛНЕНИИ КОМАНД ПЕРЕХОДА И ВЫЗОВА ПРОЦЕДУРЫ:
* АДРЕСНАЯ ЧАСТЬ КОМАНДЫ УКАЗЫВАЕТ НА ДЕСКРИПТОР ЦЕЛЕВОГО СЕГМЕНТА КОДА
* АДРЕСНАЯ ЧАСТЬ КОМАНДЫ УКАЗЫВАЕТ НА ДЕСКРИПТОР ШЛЮЗА ВЫЗОВА

**ПОДЧИНЕННЫЕ СЕГМЕНТЫ КОДА**

* В ПОДЧИНЕННОМ СЕГМЕНТЕ ОТКЛЮЧЕНА ЕГО ЗАЩИТА И ОТМЕНЕН ИНДИВИДУАЛЬНЫЙ УРОВЕНЬ ПРИВИЛЕГИЙ (БИТЫ DPL В ДЕСКРИПТОРЕ ИГНОРИРУЮТСЯ)
* УРОВЕНЬ ПРИВИЛЕГИЙ ПОДЧИНЕННОГО СЕГМЕНТА ОПРЕДЕЛЯЕТСЯ УРОВНЕМ ПРИВИЛЕГИЙ ТОЙ ПРОГРАММЫ, ИЗ КОТОРОЙ ЕМУ ПЕРЕДАНО УПРАВЛЕНИЕ
* ПОСЛЕ ПЕРЕДАЧИ УПРАВЛЕНИЯ В ПОДЧИНЕННЫЙ СЕГМЕНТ БИТЫ CPL СООТВЕТСТВУЮТ БИТАМ DPL СЕГМЕНТА КОДА, ИЗ КОТОРОГО БЫЛО ПЕРЕДАНО УПРАВЛЕНИЕ (КОРРЕКЦИЯ БИТОВ CPL В СООТВЕТСТВИИ СО ЗНАЧЕНИЕМ БИТОВ DPL ПОДЧИНЕННОГО СЕГМЕНТА НЕ ВЫПОЛНЯЕТСЯ)
* СЕГМЕНТ СТАНОВИТСЯ ПОДЧИНЕННЫМ ПРИ УСТАНОВКЕ БИТА «С»=1 В ЕГО ДЕСКРИПТОРЕ

**КОНТРОЛЬ УРОВНЕЙ ПРИВИЛЕГИЙ ПРИ ИСПОЛЬЗОВАНИИ ДЕСКРИПТОРА СЕГМЕНТА**

**** ВЫПОЛНЕНИЕ «ДЛИННЫХ» ПЕРЕХОДОВ И ВЫЗОВОВ С ПЕРЕДАЧЕЙ УПРАВЛЕНИЯ

В ДРУГОЙ (ЦЕЛЕВОЙ СЕГМЕНТ) ЧЕРЕЗ ДЕСКРИПТОР СЕГМЕНТА ВОЗМОЖНО, ЕСЛИ:

1. DPL ЦЕЛЕВОГО СЕГМЕНТА РАВЕН

CPL СЕГМЕНТНОГО РЕГИСТРА

ИСПОЛНЯЕМОГО КОДА.

1. ЦЕЛЕВОЙ СЕГМЕНТ ЯВЛЯЕТСЯ

ПОДЧИНЕННЫМ (С=1) И ЕГО

DPL<CPL ИСПОЛНЯЕМОГО КОДА

(ЦЕЛЕВОЙ СЕГМЕНТ ИМЕЕТ БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ ПРИВИЛЕГИЙ).

**КОНТРОЛЬ УРОВНЕЙ ПРИВИЛЕГИЙ ПРИ ПОМОЩИ ДЕСКРИПТОРОВ ШЛЮЗОВ**

* ДЛЯ КОНТРОЛЯ ПЕРЕДАЧИ УПРАВЛЕНИЯ МЕЖДУ СЕГМЕНТАМИ КОДА С РАЗЛИЧНЫМИ УРОВНЯМИ ПРИВИЛЕГИЙ ИСПОЛЬЗУЮТСЯ ДЕСКРИПТОРЫ ШЛЮЗОВ (ИЛИ ПРОСТО ШЛЮЗЫ)
* ШЛЮЗЫ - СПЕЦИАЛЬНЫЕ СИСТЕМНЫЕ ОБЪЕКТЫ (СОЗДАЮТСЯ И УПРАВЛЯЮТСЯ ОПЕРАЦИОННОЙ СИСТЕМОЙ)
* ВСЕГО ОПЕРАЦИОННОЙ СИСТЕМОЙ ПОДДЕРЖИВАЮТСЯ 4 ТИПА ТАКИХ ДЕСКРИПТОРОВ:

1. ШЛЮЗ ВЫЗОВА

2. ШЛЮЗ «ЛОВУШКИ»

3. ШЛЮЗ ПРЕРЫВАНИЯ

4. ШЛЮЗ ЗАДАЧИ

**НАЗНАЧЕНИЕ ДЕСКРИПТОРА ШЛЮЗА ВЫЗОВА**

* ШЛЮЗ ВЫЗОВА – ПОМЕЩАЕТСЯ В GDT ИЛИ LDT И ОБЕСПЕЧИВАЕТ КОСВЕННУЮ ЗАЩИЩЕННУЮ ПЕРЕДАЧУ УПРАВЛЕНИЯ МЕЖДУ СЕГМЕНТАМИ КОДА С РАЗЛИЧНЫМИ УРОВНЯМИ ПРИВИЛЕГИЙ
* ВЫПОЛНЯЕТ ДВЕ ФУНКЦИИ:

1. ОПРЕДЕЛЕНИЕ ТОЧКИ ВХОДА В ПРОЦЕДУРУ
2. ОПРЕДЕЛЕНИЕ УРОВНЯ ПРИВИЛЕГИЙ, ТРЕБУЕМОГО ДЛЯ КОРРЕКТНОГО ВЫЗОВА ПРОЦЕДУРЫ

* КОМАНДЫ «ДЛИННОГО» ПЕРЕХОДА АДРЕСУЮТ НЕ ЦЕЛЕВОЙ СЕГМЕНТ (СЕГМЕНТ НАЗНАЧЕНИЯ), А ИМЕННО ШЛЮЗ ВЫЗОВА
* ШЛЮЗ ВЫЗОВА ОПРЕДЕЛЯЕТ БАЗОВЫЙ АДРЕС ЦЕЛЕВОГО СЕГМЕНТА КОДА И СМЕЩЕНИЕ В ЭТОМ СЕГМЕНТЕ – ТОЧКУ ВХОДА В ПРОЦЕДУРУ (ФАКТИЧЕСКИ ЕЕ ФИЗИЧЕСКИЙ АДРЕС)

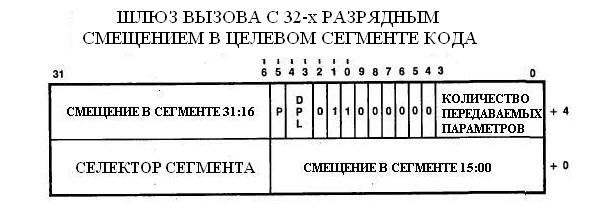
**ИДЕЯ ИСПОЛЬЗОВАНИЯ ШЛЮЗА**

* В ДЕСКРИПТОР ШЛЮЗА ЗАПИСЫВАЕТСЯ СЕЛЕКТОР ЦЕЛЕВОГО СЕГМЕНТА ДЛЯ НАХОЖДЕНИЯ ЕГО БАЗОВОГО АДРЕСА (В ДЕСКРИПТОРЕ СЕГМЕНТА)
* В ДЕСКРИПТОР ШЛЮЗА ЗАПИСЫВАЕТСЯ СМЕЩЕНИЕ В ЦЕЛЕВОМ СЕГМЕНТЕ, КОТОРОЕ ОПРЕДЕЛЯЕТ АДРЕС ВЫЗЫВАЕМОЙ ПРОЦЕДУРЫ
* СМЕЩЕНИЕ В ШЛЮЗЕ – ОБЕСПЕЧИВАЕТ ЗАЩИТУ ОТ ВХОДА В СЕРЕДИНУ ПРОЦЕДУРЫ ИЛИ В СЕРЕДИНУ КОМАНДЫ ПРИ ПРЯМОМ ВЫЗОВЕ (ЕСЛИ ИСПОЛЬЗОВАТЬ СМЕЩЕНИЕ ИЗ УКАЗАТЕЛЯ)

**ДОСТОИНСТВА ШЛЮЗА ВЫЗОВА**

* КОСВЕННАЯ ПЕРЕДАЧА УПРАВЛЕНИЯ НЕ ПОЗВОЛЯЕТ ВЫЗЫВАЮЩЕЙ ПРОГРАММЕ ИСКАЗИТЬ ВЫЗЫВАЕМУЮ ПРОГРАММУ
* ВЫЗЫВАЕМЫЕ ПРОГРАММЫ НЕВИДИМЫ ДЛЯ ВЫЗЫВАЮЩИХ ПРОГРАММ
* ПРИ МОДИФИКАЦИИ ОС ДОСТУП К ПРОЦЕДУРАМ ОС ИЗ ПРИКЛАДНЫХ ПРОГРАММ СОХРАНЯЕТСЯ МОДИФИКАЦИЕЙ АДРЕСНОЙ ИНФОРМАЦИИ В ШЛЮЗЕ ВЫЗОВА

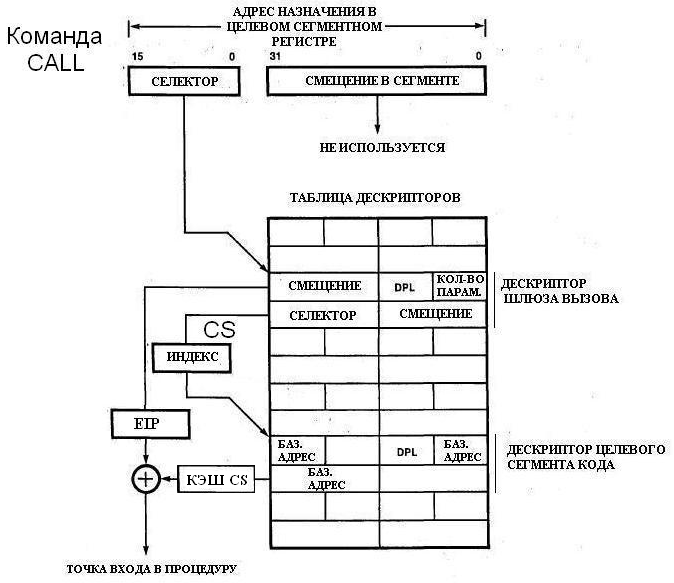
**ФОРМАТ ШЛЮЗА ВЫЗОВА**

****

ШЛЮЗ ВЫЗОВА СОДЕРЖИТ ПОЛЯ:

1. СЕЛЕКТОРА ЦЕЛЕВОГО СЕГМЕНТА (АДРЕС ЕГО ДЕСКРИПТОРА)
2. 32-Х РАЗРЯДНОГО СМЕЩЕНИЯ В ЦЕЛЕВОМ СЕГМЕНТЕ
3. «Р» – БИТ ПРИСУТСТВИЯ,
4. ПОЛЕ ДЛЯ УКАЗАНИЯ КОЛИЧЕСТВА ПАРАМЕТРОВ, ПЕРЕДАВАЕМЫХ ИЗ СТЕКА ТЕКУЩЕЙ ПРОГРАММЫ В СТЕК ВЫЗЫВАЕМОЙ ПРОГРАММЫ

**ОПРЕДЕЛЕНИЕ ТОЧКИ ВХОДА В ПРОЦЕДУРУ**

****

**КАК РАБОТАЕТ ШЛЮЗ ВЫЗОВА?**

1. КОМАНДА «ДЛИННОГО» ПЕРЕХОДА - ПЕРЕДАЧИ УПРАВЛЕНИЯ В БОЛЕЕ ПРИВИЛЕГИРОВАННЫЙ ЦЕЛЕВОЙ СЕГМЕНТ СОДЕРЖИТ СЕЛЕКТОР ЦЕЛЕВОГО СЕГМЕНТА И СМЕЩЕНИЕ В НЕМ.
2. ПРИ ИСПОЛЬЗОВАНИИ ШЛЮЗА СМЕЩЕНИЕ В КОМАНДЕ ИГНОРИРУЕТСЯ - ОНО БУДЕТ ИЗВЛЕКАТЬСЯ ИЗ ШЛЮЗА ВЫЗОВА.
3. ПО СЕЛЕКТОРУ В КОМАНДЕ ПЕРЕХОДА ВЫПОЛНЯЕТСЯ ОБРАЩЕНИЕ К ТАБЛИЦЕ ДЕСКРИПТОРОВ И НАХОЖДЕНИЕ ШЛЮЗА ВЫЗОВА КАК СИСТЕМНОГО ОБЪЕКТА (ПО БИТУ «S» В ДЕСКРИПТОРЕ ШЛЮЗА).
4. ПОЛЕ «СЕЛЕКТОР СЕГМЕНТА» ШЛЮЗА ОПРЕДЕЛЯЕТ АДРЕС ДЕСКРИПТОРА ЦЕЛЕВОГО СЕГМЕНТА КОДА, В КОТОРОМ НАХОДИТСЯ ВЫЗЫВАЕМАЯ ПРОЦЕДУРА. ПОЭТОМУ ЭТОТ СЕЛЕКТОР ИЗ ШЛЮЗА ЗАПИСЫВАЕТСЯ В СЕГМЕНТНЫЙ РЕГИСТР КОДА CS.
5. СМЕЩЕНИЕ, СОДЕРЖАЩЕЕСЯ В ШЛЮЗЕ ВЫЗОВА ЗАПИСЫВАЕТСЯ В РЕГИСТР УКАЗАТЕЛЯ КОМАНД EIP.
6. ПО СЕЛЕКТОРУ, ЗАПИСАННОМУ В СЕГМЕНТНЫЙ РЕГИСТР КОДА CS ВЫПОЛНЯЕТСЯ ОБРАЩЕНИЕ К ДЕСКРИПТОРНОЙ ТАБЛИЦЕ И ИЗВЛЕЧЕНИЕ ДЕСКРИПТОРА «ЦЕЛЕВОГО» СЕГМЕНТА (ДЕСКРИПТОР КЭШИРУЕТСЯ В ТЕНЕВОЙ РЕГИСТР СЕГМЕНТНОГО РЕГИСТРА КОДА CS).
7. ИЗ ДЕСКРИПТОРА «ЦЕЛЕВОГО» СЕГМЕНТА ИЗВЛЕКАЕТСЯ ЕГО БАЗОВЫЙ АДРЕС.
8. СУММИРОВАНИЕ ПОЛУЧЕННОГО БАЗОВОГО АДРЕСА С СОДЕРЖИМЫМ РЕГИСТРА EIP ПОЗВОЛЯЕТ ПОЛУЧИТЬ ТРЕБУЕМЫЙ ФИЗИЧЕСКИЙ АДРЕС ПРОЦЕДУРЫ (ТОЧКА ВХОДА), КОТОРОЙ ПЕРЕДАЕТСЯ УПРАВЛЕНИЕ.

**РАЗРЕШЕНИЕ ПЕРЕХОДОВ И ВЫЗОВОВ**

* ДЛЯ КОМАНДЫ JMP ПРИ ПЕРЕДАЧЕ УПРАВЛЕНИЯ В ОБЫЧНЫЙ СЕГМЕНТ КОДА («С»=0) ОДНОВРЕМЕННО ДОЛЖНЫ ВЫПОЛНЯТЬСЯ ДВА УСЛОВИЯ:

MAX (CPL,RPL) ≤ DPL (ШЛЮЗА)

DPL (ДЕСКРИПТОР ЦЕЛЕВОГО СЕГМЕНТА КОДА) = CPL

* ДЛЯ КОМАНД JMP (БИТ «С»=1) И CALL ОДНОВРЕМЕННО ДОЛЖНЫ ВЫПОЛНЯТЬСЯ ДВА УСЛОВИЯ:

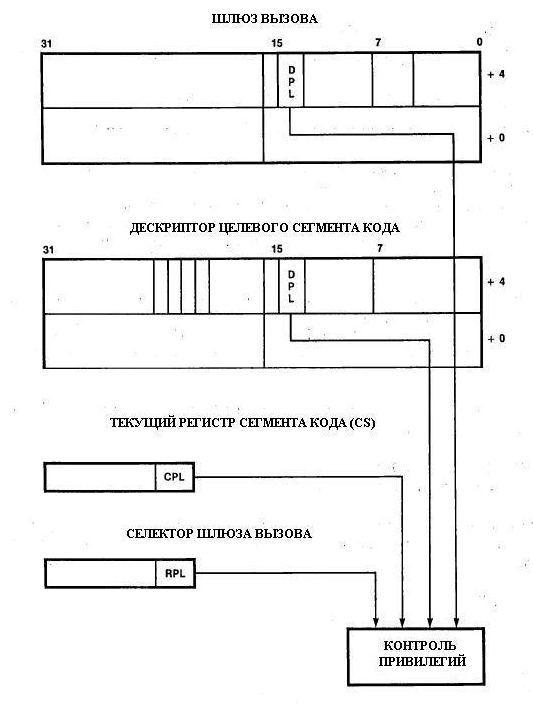
MAX (CPL,RPL)≤DPL (ШЛЮЗА)

DPL (ДЕСКРИПТОР ЦЕЛЕВОГО СЕГМЕНТА КОДА) ≤ CPL

(ЦЕЛЕВОЙ СЕГМЕНТ ИМЕЕТ БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ ПРИВИЛЕГИЙ)

* ЕСЛИ ЭТИ УСЛОВИЯ ВЫПОЛНЯЮТСЯ, ТО В ПОЛЕ CPL СЕЛЕКТОРА, ЗАГРУЖЕННОГО ИЗ ДЕСКРИПТОРА ШЛЮЗА, УСТАНАВЛИВАЕТСЯ ЗНАЧЕНИЕ DPL ИЗ ДЕСКРИПТОРА ВЫЗЫВАЕМОГО СЕГМЕНТА
* ЕСЛИ ЭТИ УСЛОВИЯ НЕ ВЫПОЛНЯЮТСЯ, ТО ВЫРАБАТЫВАЕТСЯ ПРОГРАММНОЕ ПРЕРЫВАНИЕ

**КОНТРОЛЬ УРОВНЕЙ ПРИВИЛЕГИЙ ПРИ ВХОДЕ В ПРОЦЕДУРУ ЧЕРЕЗ ШЛЮЗ ВЫЗОВА**

****

ПЕРЕДАЧА УПРАВЛЕНИЯ ЧЕРЕЗ ШЛЮЗЫ ТОЛЬКО В БОЛЕЕ ПРИВИЛЕГИРОВАННЫЕ СЕГМЕНТЫ. УРОВЕНЬ ПРИВИЛЕГИЙ ШЛЮЗА ВЫЗОВА НЕ ДОЛЖЕН ПРЕВЫШАТЬ УРОВЕНЬ ПРИВИЛЕГИЙ ВЫЗЫВАЮЩЕЙ ПРОГРАММЫ.

**КОНТРОЛЬ ДОСТУПА К СТРАНИЦЕ**

* ПРИ КОНТРОЛЕ ДОСТУПА К СТРАНИЦАМ РАССМАТРИВАЮТСЯ ТОЛЬКО ДВА УРОВНЯ ПРИВИЛЕГИЙ : ПОЛЬЗОВАТЕЛЬ (USER) C DPL=3 И СУПЕРВИЗОР (SUPERVISOR) C DPL=0,1,2.
* ПОРЯДОК ДОСТУПА К СТРАНИЦЕ ОПРЕДЕЛЯЕТСЯ СЛЕДУЮЩИМИ БИТАМИ:
* U/S – В ЭЛЕМЕНТЕ ТАБЛИЦЫ СТРАНИЦ (РТЕ) (U/S=0 – СУПЕРВИЗОР)
* R/W – В ЭЛЕМЕНТЕ ТАБЛИЦЫ СТРАНИЦ (РТЕ) (R/W=0 – ТОЛЬКО ЧТЕНИЕ)
* WP – В РЕГИСТРЕ ФЛАГОВ (EFLAGS) (WP=1 ЗАПРЕЩАЕТ СУПЕРВИЗОРУ ЗАПИСЬ НА СТРАНИЦУ ПОЛЬЗОВАТЕЛЯ С R/W=0 )
* БИТ «WP» ПРЕДНАЗНАЧЕН ДЛЯ ЗАЩИТЫ ТОЛЬКО ЧИТАЕМЫХ СТРАНИЦ (СПЕЦИФИЦИРОВАННЫХ ПОЛЬЗОВАТЕЛЕМ) ОТ ПОПЫТОК ПРИВИЛЕГИРОВАННЫХ ПРОГРАММ (УРОВЕНЬ СУПЕРВИЗОРА)(СPL=0,1,2) ОБРАТИТЬСЯ К НИМ ДЛЯ ЗАПИСИ ДАННЫХ

**ПОРЯДОК ДОСТУПА К ЗАЩИЩЕННОЙ СТРАНИЦЕ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **U/S** | **R/W** | **WP** | **ПОЛЬЗОВАТЕЛЬ** | **СУПЕРВИЗОР** | **ПРОГРАММНОЕ**  **ПРЕРЫВАНИЕ ПРИ ПОПЫТКЕ ЗАПИСИ** |
| 0 | 0 | 0 | НЕТ ДОСТУПА | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ++ |
| 0 | 1 | 0 | НЕТ ДОСТУПА | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ++ |
| 1 | 0 | 0 | ЧТЕНИЕ/ИСПОЛНЕНИЕ | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ++ |
| 1 | 1 | 0 | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ |  |
| 0 | 0/0 | 1 | НЕТ ДОСТУПА | ЧТЕНИЕ/ИСПОЛНЕНИЕ | + (++) |
| 0 | 1 | 1 | НЕТ ДОСТУПА | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ++ |
| 1 | 0/0 | 1 | ЧТЕНИЕ/ИСПОЛНЕНИЕ | ЧТЕНИЕ/ИСПОЛНЕНИЕ | + (++) |
| 1 | 1 | 1 | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ | ЧТЕНИЕ/ЗАПИСЬ/  ИСПОЛНЕНИЕ |  |

**(++) - ПОПЫТКА ПОЛЬЗОВАТЕЛЯ, (+) - ПОПЫТКА СУПЕРВИЗОРА**

**КОММЕНТАРИЙ К ТАБЛИЦЕ**

* ПРИ WP=1 ПОПЫТКА СУПЕРВИЗОРА ОБРАТИТЬСЯ К СТРАНИЦЕ С РАЗРЕШЕНИЕМ ТОЛЬКО ЧТЕНИЯ (R/W=0) ВЫЗЫВАЕТ ПРОГРАММНОЕ ПРЕРЫВАНИЕ
* ПРИ WP=0 СУПЕРВИЗОР МОЖЕТ ОБРАЩАТЬСЯ К СТРАНИЦЕ НА ЗАПИСЬ НЕЗАВИСИМО ОТ ЗНАЧЕНИЯ БИТА «R/W»
* ПОПЫТКА ОБРАЩЕНИЯ ПОЛЬЗОВАТЕЛЯ К СТРАНИЦЕ С УРОВНЕМ ПРИВИЛЕГИЙ СУПЕРВИЗОРА (U/S=0) )ВЫЗЫВАЕТ ПРОГРАММНОЕ ПРЕРЫВАНИЕ
* ПОПЫТКА ОБРАЩЕНИЯ ПОЛЬЗОВАТЕЛЯ К СТРАНИЦЕ С РАЗРЕШЕНИЕМ ТОЛЬКО ЧТЕНИЯ (R/W=0) ВЫЗЫВАЕТ ПРОГРАММНОЕ ПРЕРЫВАНИЕ