**21**

1. **Каким условиям должна удовлетворять проверочная матрица для образования кода Хэмминга? Пример формирования кода Хэмминга на основе построения проверочной матрицы. Примеры внесения и исправления одиночных и двойных ошибок.**

Для образования контрольного кода Хэмминга (КХ) используется проверочная матрица Н размерности r x n, где r - число контрольных бит, а n = k + r, где k - разрядность информационного слова, а n - длина кодового слова, записываемого в память.

1) векторы-столбцы матрицы Н не должны быть нулевыми и должны отличаться друг от друга;

2) сумма двух векторов-столбцов матрицы Н не должна равняться нулю или любому третьему вектору-столбцу матрицы Н.

Рассмотрим процесс формирования контрольного кода и синдрома ошибок на примере 5-разрядного информационного слова. Для контрольного кода потребуется 4 дополнительных разряда и один дополнительный бит для определения двойной ошибки:

d4 d3 d2 d1 d0 - информационное слово;

с4 d3 с2 с1 c0 - номер бита кода Хэмминга;

СТ С3 С2 С1 С0 - контрольный код Хэмминга, где бит СТ необходим для обнаружения двойной ошибки.

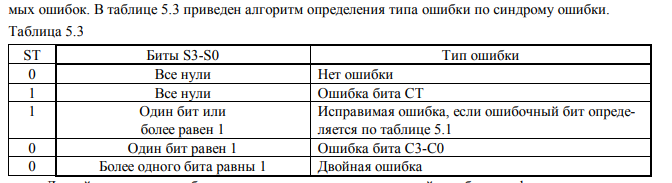
В соответствии со сформулированными требованиями разработаем проверочную матрицу для данного кода.

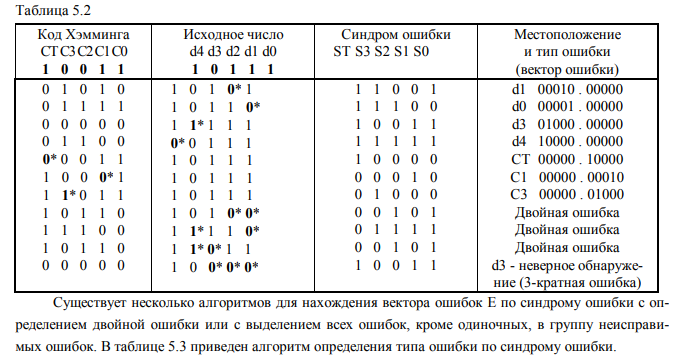


В таблице 5.2 приведены примеры внесения одиночных и двойных ошибок в разряды считанного

информационного слова или кода Хэмминга СT-С0. Синдром ошибки ST-S0 может быть получен сложением по модулю 2 считанного из ОЗУ контрольного кода и вновь полученного контрольного кода от

считанного информационного слова:

ST-S0 = (CT-C0)считанный ⊕ (СT-С0)полученный.



2. **Назначение бита достоверности строки кэш-памяти. Как используется значение этого бита при обращении к памяти, если произведен успешный поиск по тегу для полностью ассоциативного распределения кэш-памяти.?**

Бит достоверности данных d=1 указывает на принадлежность строки кэш-памяти, а нулевое значение означает, что данная ячейка свободна (в ней размещаются недостоверные данные, принадлежащие, например, другой программе).

А э Тег & RD & d | Y1 = выдача результата

**22**

**1. Что дает подход создания ЭВМ с единой архитектурой и переменным составом оборудования?**

Расширение сферы применения средств вычислительной техники (СВТ), особенно их применение для решения научно-технических задач, задач автоматизации производства, САПР, работы с базами данных, обработки статистической информации и управления производством привело к необходимости создания вычислительных систем (ВС), отличающихся составом технических средств (ТС) и техническими характеристиками: производительностью, емкостью оперативной памяти (ОП), внешних запоминающих устройств (ВЗУ)

Это привело к необходимости создания ЭВМ с единой архитектурой, но с переменным составом оборудования, который определяется выполняемыми ВС функциями. Такой подход означает выполнение отдельных функциональных устройств в виде модулей, которые могут объединяться в необходимом количестве в одной ЭВМ или говорят о ЭВМ проблемно-ориентированных на решение определенного класса задач. При этом существенное место для реализации такого подхода занимает сокращение числа типов (номенклатуры) выпускаемых семейств ЭВМ.

**2. Что означает термин защита по привилегиям? Уровни привилегий ЦП Intel 486 и их характеристика.**

Механизм защиты процессора опирается на описание различных системных объектов (сегментов) с помощью дескрипторов. В каждом дескрипторе имеется двухбитное поле уровня привилегий дескриптора – DPL, которое определяет, каким программам разрешается доступ к дескриптору и, следовательно, описываемому им объекту (сегменту).

Термин привилегия подразумевает права или возможности, которые обычно не разрешаются.

Процессор Intel (кроме 8086) поддерживает 4 уровня привилегий 0, 1, 2, 3: чем меньше номер, тем выше уровень привилегии. Число программ, выполняемых на каждом уровне, уменьшается с увеличением уровня привилегии (уменьшением номера привилегии).

При выполнении почти каждой команды осуществляется проверка защиты по привилегиям для следующих ситуаций:

* возможности выполнения текущей команды (для привилегированных команд);
* возможности обращения к данным других программ;
* возможности передачи управления (переходу) в другой сегмент кода (программ), имеющему другой уровень привилегии по отношению к текущему кодовому сегменту

**23**

**1. Методы обратной записи при обновлении ОП. Сущность и отличия методов. Простая обратная запись. Достоинства и недостатки. Численные оценки метода.**

**Простая обратная запись SWB**

Если А∉Teg (кэш-памяти), то по одной из выбранных стратегий замещения определяется строка, подлежащая удалению из кэш-памяти в ОП, и выполняется процедура удаления (перезаписи) выбранной строки в ОП как при чтении, так и при записи, а затем реализуется процедура замещения кэш-памяти, т.е. из ОП считывается запрашиваемая строка и записывается в СОЗУ данных на место удаленной строки, а в память тегов - новый тег считанной строки. Затем требуемое слово записывается или считывается из кэш-памяти по ранее рассмотренному алгоритму, т.к. теперь А ∈Teg. Данный метод проигрывает в быстродействии, если при замещении строк (А∉Teg) удаляется строка, которая не модифицировалась (не изменялась за время пребывания в кэш-памяти (особенно для программ)).

**Флаговая обратная запись FWB**

Является развитием предыдущего метода. Каждой строке ставится в соответствие бит флага записи слова в строку w, т.е. в структуру кэш-памяти вводится дополнительная одноразрядная память флагов емкостью, равной числу строк. Параллельно с чтением памяти тегов выполняется чтение памяти флагов. Если А∈Teg и выполняется запись в СОЗУ данных, то параллельно в одноименной ячейке памяти флагов устанавливается бит w=1. Если А∉Teg, то анализируется значение бита флага и процедура удаления строки из кэш-памяти в ОП выполняется только в том случае, если бит w был установлен в "1", иначе данная процедура не выполняется, а сразу производится замещение строки из ОП в кэш-память со сбросом бита w замещаемой строки. Существенный выигрыш данный метод дает, если в кэш-памяти хранится программа, т.к. в область программ запись не производится и не требуется процедура удаления строк из кэш-памяти в ОП.

**Регистровая обратная запись PWB**

Является модификацией метода SWB, при котором к магистрали данных между кэш-памятью и ОП подключается регистровый буфер (типа FIFO), который позволяет сократить время простоя кэш-памяти на выполнение процедур обновления ОП и замещения кэш-памяти. В регистр помещается строка, подлежащая удалению из кэш-памяти, а ее запись в ОП выполняется после обновления кэш-памяти из ОП. Таким образом, обращение к кэш-памяти со стороны процессора возможно сразу после обновления строки в кэш-памяти, а запись удаленной из кэш-памяти строки в ОП будет отложена и выполнена параллельно с работой кэш-памяти. При этом выигрыш во времени составляет от одного обращения к ОП при использовании расслоения обращений к ОП до k х Тзу при использовании ОП без расслоения обращений.

**Флаговая регистровая обратная запись FPWB**

Является комбинацией методов PWB и FWB и не требует дополнительных комментариев.

**2. Какие проверки выполняются в устройстве сегментного преобразования адресов при выполнении команд формата только со смещением в сегменте в ЦП Intel 486????????**

При доступе к сегментам выполняется дополнительный контроль по размеру при обращении к таблице сегментов (размер таблицы сегментов значительно меньше таблицы страниц, определяется при инициализации системы, может быть переменным и задается в поле L регистра базового адреса таблицы сегментов CR), а при обращении в дескрипторе сегмента в поле М задается его размер

**24**

**1. Приведите определения: что такое стратегия замещения кэш-памяти и стратегия обновления ОП?**

Так как емкость кэш-памяти невелика, то при очередном обращении за информацией к кэш-памяти возможна ситуация, когда эта информация отсутствует в кэш-памяти. В подобных случаях необходимо выбрать одну из строк, хранящихся в кэш-памяти, и заменить ее на новую строку. Способ определения строки, удаляемой из кэш-памяти, называется стратегией замещения кэш-памяти (или назначение кандидата на удаление).

Для записи данных в кэш-память и ОП при выполнении команд в ЦП также существует несколько методов замещения старой информации. Эти методы называются стратегией обновления оперативной памяти.

**2. В каких направлениях ведутся работы по совершенствованию технических средств ЭВМ? Их характеристика на примерах.**

* совершенствования элементной базы, т.е. применения новых более быстродействующих БИС и СБИС;
* повышения производительности ВС за счет применения новых технологий и структурных решений как для ЦП, так и для периферийных БИС;
* увеличения объема ОП и ВЗУ, совершенствования организации хранения данных, реализации виртуальной памяти, использования как внутренней на кристалле, так и внешней кэш-памяти;
* дальнейшего развития системы ПО как в области прикладных программ, так и ОС;
* создания мультипрограммных и многомашинных вычислительных систем, работающих в реальном времени, локальных и глобальных ВС;
* развития системы ввода-вывода и расширения номенклатуры ПУ;
* повышения надежности ВС, развития эффективных систем контроля и диагностики;
* за счет совершенствования технологии.

**25**

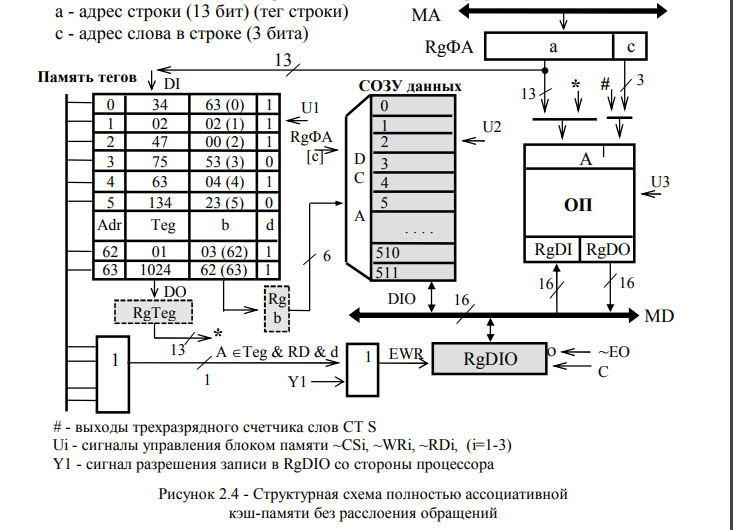
1. **Какие процедуры выполняются в общем случае при обращении к кэш-памяти, если произошел успешный поиск по тегу для секторного распределения**

Выполняется обращение к памяти бит достоверности строк.

**2. Каким условиям должна удовлетворять проверочная матрица для образования кода Хэмминга? Пример формирования кода Хэмминга на основе построения проверочной матрицы. Примеры внесения и исправления одиночных и двойных ошибок.**

21(1 вопрос)

**26**

**1. Приведите схему включения кэш-памяти и ОП без расслоения обращений и оценку быстродействия для процедур обновления ОП и замещения кэш-памяти одной строки.**

При отсутствии запрашиваемой строки в кэш-памяти необходимо выполнить процедуры обновления ОП и замещения кэш-памяти. Время выполнения этих процедур в существенной степени зависит от принятых стратегий обновления ОП и замещения кэш-памяти, которые будут рассмотрены ниже, а также от принципов организации доступа к ОП и СОЗУ данных и структуры магистрали данных системного интерфейса.

ОП и СОЗУ данных без расслоения обращений; Процедура обновления ОП требует 8 обращений к СОЗУ данных и 8 обращений для записи строки в ОП, т.е. потребуется 8 х Tозу+ 8х tсозу дан. и столько же обращений для замещения строки кэш-памяти

ОП с расслоением обращений на ширину выборки строки, СОЗУ данных без расслоения обращений; Тогда процедура обновления ОП потребует 8 x tсозу для чтения строки из СОЗУ данных и записи в RgDI через DMS и одного обращения Tозу к ОП для записи строки и столько же обращений для замещения строки кэш-памяти.

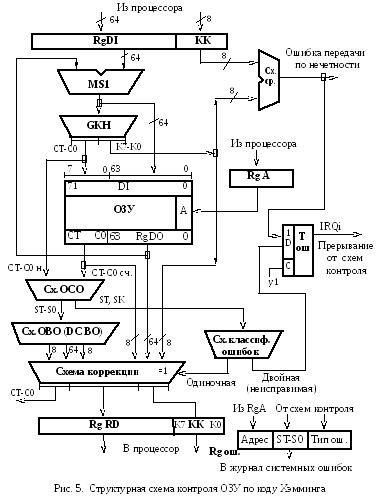
ОП с расслоением обращений на ширину выборки строки, СОЗУ данных с расслоением обращений и двусторонним доступом; Однако этот метод необходимо рассматривать только для перспективных разработок, когда ОП конструктивно будет размещаться на одной плате (ТЭЗе) с ЦП или между ОП и внутренней кэш-памятью подключается внешняя быстродействующая кэш-память большой емкости. Иначе надежность работы системы резко снижается, а реализация внешней дополнительной 128-разрядной шины данных не дает существенного выигрыша в быстродействии, так как при вероятности попадания в кэш-память 90% выигрыш составит 0,1 х 7 тактов = 0.7 такта на команду для рассматриваемого примера.

**2. Техническая реализация и алгоритм работы схемы КО-ОД. Достоинства и недостатки.**

КО-ОД - коррекция одиночных ошибок и обнаружение двойных (код Хэмминга, коды с нечетными весами столбцов проверочной матрицы) в основном используются для однобитовых БИС памяти, КО-ОД - коррекция одиночных ошибок и обнаружение двойных (код Хэмминга, коды с нечетными весами столбцов проверочной матрицы) в основном используются для однобитовых БИС памяти, т.к. выход из строя даже всей БИС не нарушает работу ОЗУ ;т.к. выход из строя даже всей БИС не нарушает работу ОЗУ;

Код Хэмминга обеспечивает исправление всех одиночных ошибок и обнаружение двойных. Рассмотрим пример организации системы контроля ОП для 64-разрядного информационного слова, поступающего из процессора вместе с битами контрольного кода по нечетности для каждого байта слова (8 бит контрольного кода нечетности КК для контроля правильности передачи информационного слова из процессор для записи в ОП). Это позволяет в дальнейшем получать контрольные биты нечетности байт непосредственно из схемы генерации кода Хэмминга для минимизации аппаратурных затрат и позволяет легко переходить от кода Хэмминга СТ-С0 к контрольному коду по нечетности К7-К0.

Рассмотрим алгоритм работы системы контроля КО-ОД.



**При записи:**

информация из процессора поступает в RgDI в виде 64-разрядного слова и 8 бит нечетности для каждого байта слова (рис. 5), а адрес для записи - в RgA;

с выходов RgDI через MS1 слово поступает на генератор кода Хэмминга и бит нечетности GKH для формирования кода Хэмминга СТ-С0 и контрольных бит нечетности байт К7-К0. На схеме сравнения (Сх.ср.) определяется правильность приема информации из процессора в RgDI путем сравнения бит контрольного кода нечетности, принятых из процессора, и бит нечетности, сформированных схемой GKH;

если сигнал ошибки передачи по нечетности не выработан, то сформированный код Хэмминга СТ-С0 с выходов GKH вместе с информационными разрядами слова записывается в ОП;

если выработан сигнал ошибки передачи по нечетности, то выполняется попытка повторной передачи информации из процессора с контрольными битами КК для классификации типа отказа: постоянный или случайный (сбой) (иногда до восьми раз);

если попытка восстановления информации классифицируется как постоянный отказ, то устанавливается триггер ошибки и вырабатывается сигнал прерывания от схем контроля и блокируется запись в ОП, иначе выполняется запись слова и бит кода Хэмминга СТ-С0 в ОП.

**Чтение из ОП**

Из ОП считываются 64 бита слова и 8 бит кода Хэмминга СТ-С0 сч. Считанное 64-разрядное слово через MS1 поступает на схемы генератора формирования кода Хэмминга и бит нечетности байт слова.

2. Полученные в GKH биты СТ-С0н сравниваются со считанными из ОП битами СТ-С0 сч. и при их несовпадении схема определения синдрома ошибки (Сх.ОСО) формирует код синдрома ошибки ST-S0, определяющего номер позиции ошибочного бита в слове (матрица Н), а также тип ошибки на схеме классификации ошибок (одиночная или двойная).

При одиночной ошибке по коду синдрома ошибки ST-S0 схема определения вектора ошибки (Сх.ОВО) формирует код вектора ошибки Е, а в схеме коррекции ошибок выполняется ее исправление путем инверсии ошибочного бита, а также выполняется изменение бита нечетности того байта, в котором выполнена коррекция. Скорректированная информация поступает в RgRD, а из него в процессор.

Неисправимая (двойная) ошибка ОП вызывает установку бита ошибки в Тош и прерывание от схем контроля. Все случаи ошибок, обнаруженные при обращении к памяти, фиксируются в пункте 5.

Адрес слова ОП, синдром ошибки и тип ошибки сначала запоминаются в специальном регистре ошибок для последующей перезаписи его значения в системный журнал ошибок ОС (область в ОП и на резидентном диске).

**27**

**1. Какие виды корректирующих кодов Вы знаете? Как зависит обнаруживающая способность корректирующих кодов от типа БИС памяти?**

Все корректирующие коды можно классифицировать по обнаруживающей способности:

- КО-ОД - коррекция одиночных ошибок и обнаружение двойных (код Хэмминга, коды с нечетными весами столбцов проверочной матрицы) в основном используются для однобитовых БИС памяти, т.к. выход из строя даже всей БИС не нарушает работу ОЗУ;

- КО-ОД-ООГ - код КО-ОД с дополнительной способностью обнаружения кратной ошибки в одной группе (под группой подразумеваются БИС ОЗУ с организацией k-бит слова (4 бита, 8 бит));

- КОГ-ОДГ - коды с коррекцией ошибок в одной группе и обнаружением в двух группах, т.к.

ошибка в одной группе может вызвать ошибку в соседней группе (ошибка в байте вызывает ошибку в соседнем байте (БИС памяти));

- КД-ОТ - с коррекцией двойных и обнаружением тройных ошибок.

Благодаря корректирующему коду ОЗУ может нормально работать при наличии как случайных отказов (сбоев), так и постоянных отказов

**2. Назначение бита достоверности строки кэш-памяти. Как используется значение этого бита при обращении к памяти, если А П Тег для прямого распределения кэш-памяти?**

d = выдача результата

**28**

**1. Как осуществляется определение принадлежности запрашиваемых данных кэш-памяти для частично-ассоциативного распределения?**

Если хотя бы один тег совпал, то вырабатывается сигнал A ∈Teg и на выходе шифратора CD формируется двоичный номер модуля СОЗУ данных, в котором находится запрашиваемая строка.

**2. Организация защиты памяти на уровне страниц. Какие методы контроля при защите на уровне страниц используются в ЦП Intel 486?**

Защита на уровне страниц в основном предназначена для предотвращения взаимодействия программ друг с другом. Контроль достоверности обращения к памяти осуществляется параллельно со страничным преобразованием адреса (т.е. не ухудшает характеристики производительности процессора) и является более простым, чем при сегментации памяти, так как не использует полей типа страницы (кода или данных) и предела (размер всех страниц одинаков и определяется разрядностью смещения).

Различают две разновидности контроля на уровне страниц: ограничение адресуемой области памяти и контроль типа обращений. Доступом к страницам управляют биты элемента таблицы страниц: PCD, PWT, U/S, R/W. Защита применяется к таблицам страниц первого и второго уровня (элементу каталога и страницы).

**Ограничение адресуемой области памяти**. Для страниц используется не четыре, а только два уровня привилегий: Уровень супервизора (U/S=0) для операционной системы, других системных программ (драйверов устройств и т.д.) и защищенных системных данных (таблиц страниц и т.д.). Уровень пользователя (U/S=1) для прикладных программ и данных. При CPL= 0, 1 или 2 процессор работает на уровне супервизора и ему доступны все страницы, а при CPL=3 процессор работает на уровне пользователя и ему доступны только страницы уровня пользователя. Механизм защиты состоит в сравнения бита U/S с полем CPL.

**Контроль типа обращений**. В механизме защиты предусмотрены только два типа доступа к памяти:

♦ разрешение доступа только для считывания из страницы (R/W=0);

♦ разрешение доступа для считывания/записи из/в страницу (R/W=1). Таким образом, используется двухуровневая защита страниц:

♦ если процессор работает на уровне пользователя, то записать информацию можно только в страницы, которые

а) принадлежат уровню пользователя (U/S=1, CPL=3):

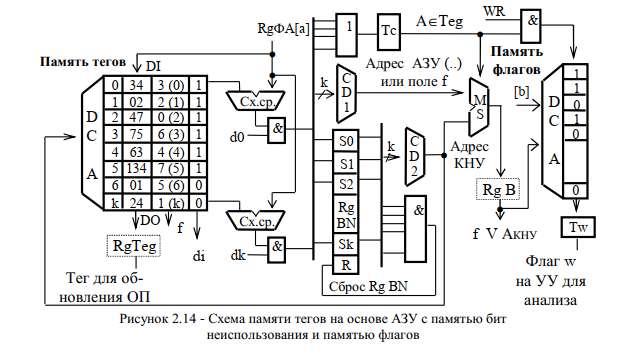
б) отмечены как допускающие считывание и запись (R/W=1);

в) страницы уровня супервизора недоступны с уровня пользователя ни для считывания, ни для записи (U/S=1, CPL=0, 1, 2).

При попытке нарушения этих правил генерируется прерывание особого случая общей защиты

**29**

**1. Техническая реализация стратегии замещения кэш-памяти по биту неиспользования для частично-ассоциативного распределения кэш-памяти Алгоритм замещения.??????**



1. **Приведите алгоритм преобразования ЛА в ФА при сегментной организации памяти на примере, если формат команды включает поле селектора сегмента и смещения в сегменте для ЦП Intel. Поле индикатора таблицы TI=0. ????????**

При сегментной адресации все пространство адресов делится на множество сегментов различной длины, определяемой необходимым размером данного сегмента. Начальный адрес сегмента называется базовым, а за каждым сегментом закреплен соответствующий номер. Порядок разбиения на сегменты может быть произвольным, а исполнительный адрес определяется номером сегмента (базовым адресом) и смещением внутри сегмента.

Отсюда ЛА можно представить в виде двух целочисленных величин (полей): номера сегмента и смещения. При этом разрядность смещения определяет максимальный размер сегмента в байтах. В ряде 16-разрядных процессоров для удобства преобразования ЛА в ФА сегмент разбивается на блоки, кратные 2k-1 байт, т.е. смещение разбивается еще на два поля: номера блока в сегменте и адреса байта в блоке.

**30**

**1. Как или чем определяется кандидат на удаление из кэш-памяти при замещении строки для всех видов распределения?**

Полностью ассоциативное:

При замещении строк кандидатами на удаление могут выступать любые строки в кэш-памяти, в зависимости от принятой стратегии.

Частично-ассоциативное:

Кандидатом на удаление из кэш-памяти однозначно назначается группа из четырех строк полем [b] RgФА, а конкретная строка определяется ассоциативно по одному из методов замещения строк.

Секторное:

Если адрес (сектор) не принадлежит АЗУ (памяти тегов), то определяется кандидат на удаление сектора из кэш-памяти.

**2. Что означает термин защита по привилегиям? Уровни привилегий ЦП Intel 486 и их характеристика.**

Механизм защиты процессора опирается на описание различных системных объектов (сегментов) с помощью дескрипторов. В каждом дескрипторе имеется двухбитное поле уровня привилегий дескриптора – DPL, которое определяет, каким программам разрешается доступ к дескриптору и, следовательно, описываемому им объекту (сегменту).

Термин привилегия подразумевает права или возможности, которые обычно не разрешаются.

Процессор Intel (кроме 8086) поддерживает 4 уровня привилегий 0, 1, 2, 3: чем меньше номер, тем выше уровень привилегии. Число программ, выполняемых на каждом уровне, уменьшается с увеличением уровня привилегии (уменьшением номера привилегии).

При выполнении почти каждой команды осуществляется проверка защиты по привилегиям для следующих ситуаций:

* возможности выполнения текущей команды (для привилегированных команд);
* возможности обращения к данным других программ;
* возможности передачи управления (переходу) в другой сегмент кода (программ), имеющему другой уровень привилегии по отношению к текущему кодовому сегменту.

Защита доступа к данным. Большинство программ в мультизадачной среде разделяют сегменты данных, т.е. несколько программ могут использовать одни сегменты данных. Программам не разрешается считывание/запись данных из сегментов, которые имеют более высокий уровень привилегий, т.е. «движение» к данным внутрь колец защиты запрещается и любая такая попытка приводит к формированию нарушения общей защиты.

Передача управления. Ограничения защиты для вызова (перехода) на выполнение других кодовых сегментов (программ), находящихся на других уровнях привилегий, еще более жесткие, так как передача управления (с помощью команд FAR CALL и JMP) разрешается только программам, уровни привилегий которых совпадают, т.е. находятся на одном уровне кольца защиты.