В первых компьютерах память была маленькой по объему. Решением проблемы нехватки памяти явилось использование вспомогательной памяти, например, диска. Программист делил программу на несколько частей, так называемых оверлеев, каждый из которых помещался в память и сам ими управлял. Был предложен метод автоматического выполнения процесса наложения, при котором программист мог вообще не знать об этом процессе. В основе этого метода лежит использование виртуальной памяти.

Проблема усложняется при переходе к мультипрограммным системам, так как в них ОП одновременно используется для нескольких программ (задач). В таких системах необходимо исключить несанкционированное воздействие одних программ на другие. Это достигается за счет механизма *защиты памяти*.

Память должна распределяться динамически, что не должно приводить к фрагментации памяти.

Защита от записи - защита области памяти данной программы от попыток записи в нее со стороны других программ, а в некоторых случаях и своей программы. При этом чтение областей памяти допускается.

Защита от записи и чтения - запрет другим программам производить как запись, так и считывание в данной области памяти.

Для облегчения процесса отладки программ желательно выявлять и такие характерные ошибки в программах, как попытки использовать данные вместо команд и команд вместо данных в собственной программе.

Отметим следующие варианты защиты при различных операциях с памятью:

1. задается отношение к областям памяти чужой программы, определяющее, относится защита только к операции записи или к любому обращению к памяти;
2. задается одно из следующих отношений к области памяти собственной программы:
    a. разрешается полный доступ к данному блоку памяти;
    b. разрешается только считывание;
    c. разрешается обращение только через счетчик команд;
    d. разрешается обращение за исключением счетчика команд.

Если нарушается защита памяти, исполнение программы приостанавливается и вырабатывается запрос прерывания по нарушению защиты памяти.

Организация защиты не должна заметно снижать производительность системы и требовать слишком больших аппаратурных затрат.

Организация защиты памяти:

- *Защита отдельных ячеек памяти.* С каждой ячейкой памяти связывается дополнительная информация о защите, например, в простейшем случае это может быть один бит, указывающий можно ли в данную ячейку записывать информацию или нет.
- Метод граничных регистров. Граничные регистры указывают границы, куда программа имеет право доступа. Проверяется при каждом обращении.
- Память делится на блоки (сегменты). Каждому блоку ставится в соответствие *ключ защиты.* Каждой программе ставится в соответствие *ключ программы.* Доступ программы к данному блоку памяти определяется аппаратурой процессора на основе анализа ключа программы и ключа защиты памяти.