Операционные системы
Автор В.А.Серков

Подсистема управления процессами

Процесс (или по-другому, задача) - абстракция, описывающая выполняющуюся программу.

Для операционной системы процесс представляет собой единицу работы, заявку на потребление системных ресурсов.

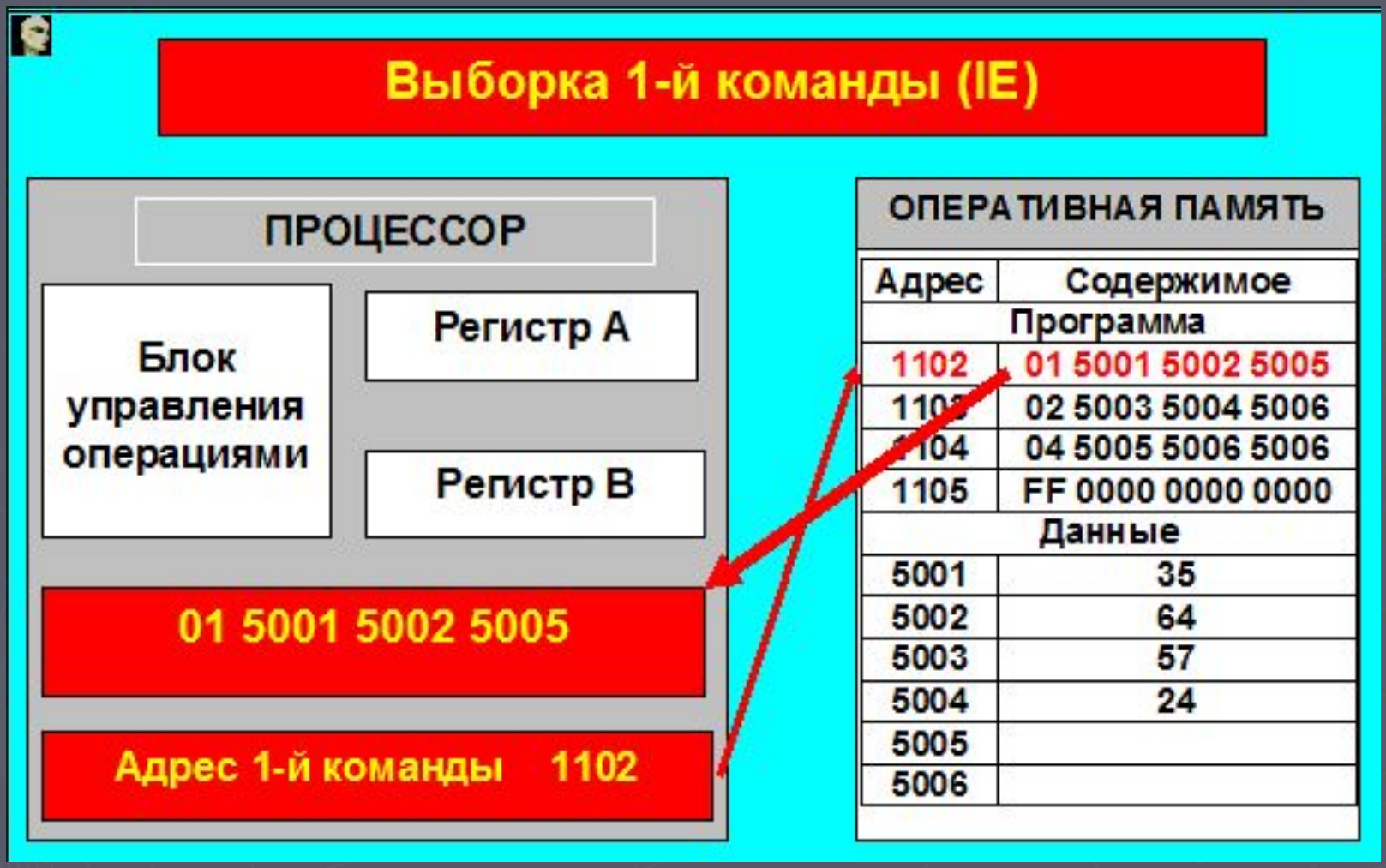
Программа это статический текст, который представляет собой последовательность машинных команд и хранится на одном из внешних носителей.

После загрузки программы в оперативную память и последующего запуска начинается процесс выполнения программы (процесс).

Среда выполнения программы

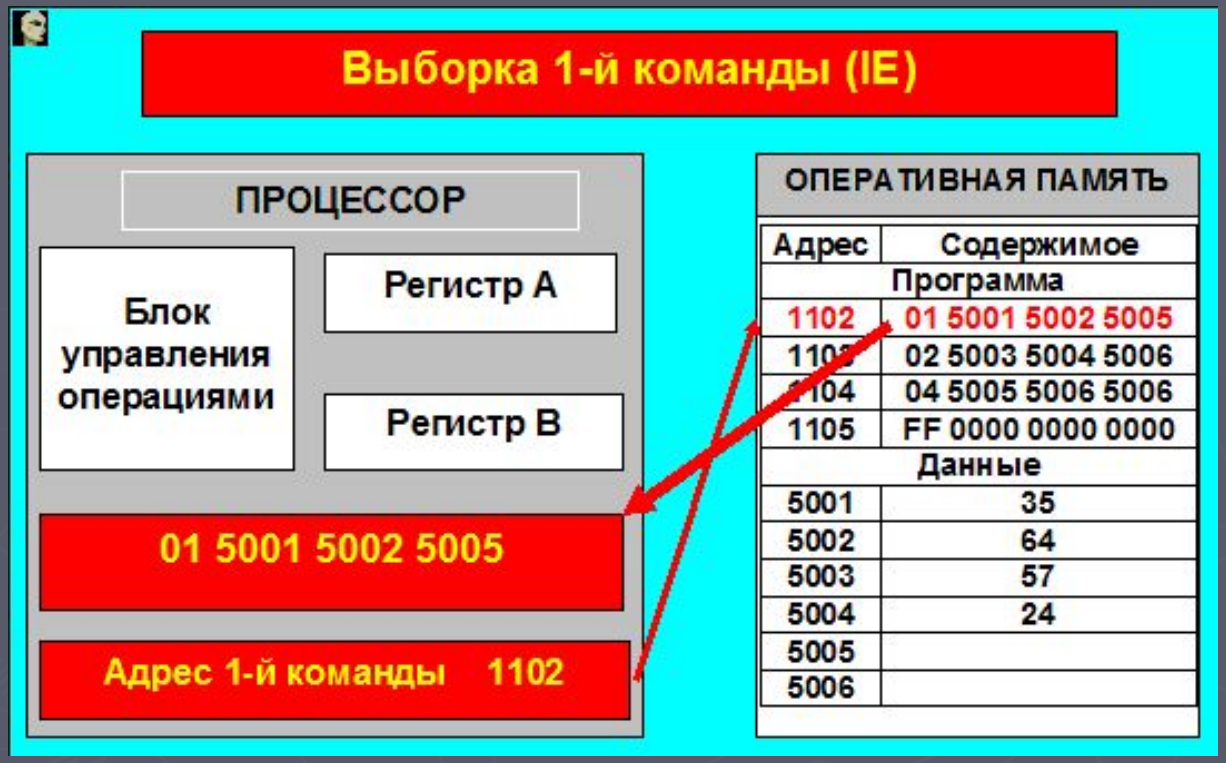
Адрес	Содержимое
Программа	
1102	01 5001 5002 5005
1103	02 5003 5004 5006
1104	04 5005 5006 5006
1105	FF 0000 0000 0000
1106	
Данные	
5001	35
5002	64
5003	57
5004	24
5005	
5006	

Реализация процесса



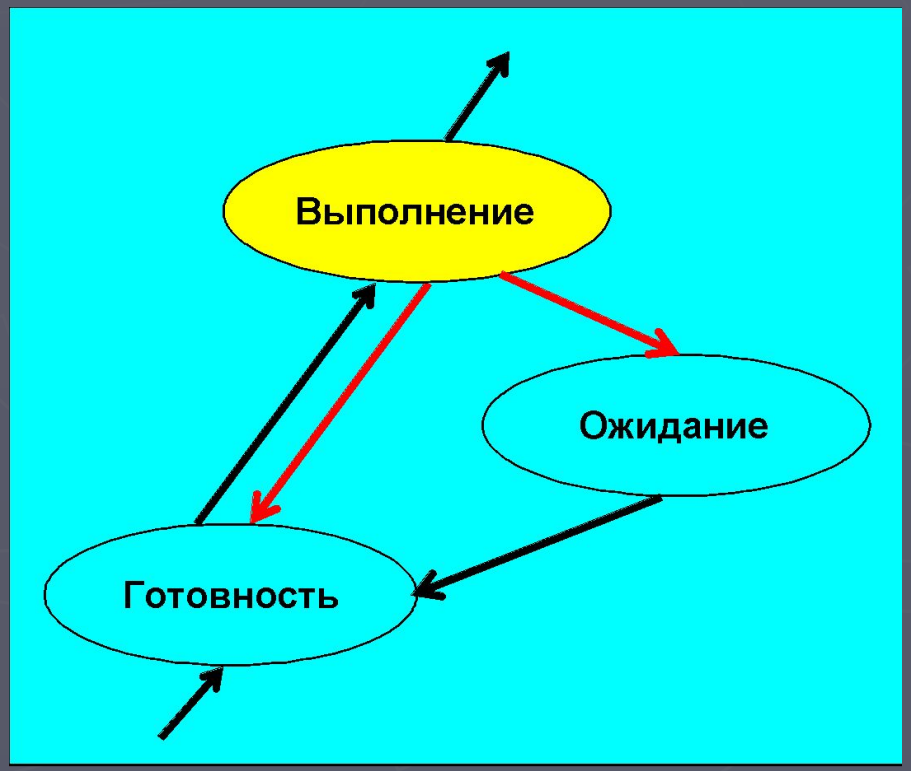
Прикладная программа выполняет систематическую последовательность действий с данными. Данные представляются и хранятся на т.н. **носителях данных**. Совокупность носителей данных, используемых при какой-либо обработке данных, будем называть **информационной средой**.

Набор данных, содержащихся в какой-либо момент в информационной среде, будем называть **состоянием** этой информационной среды.

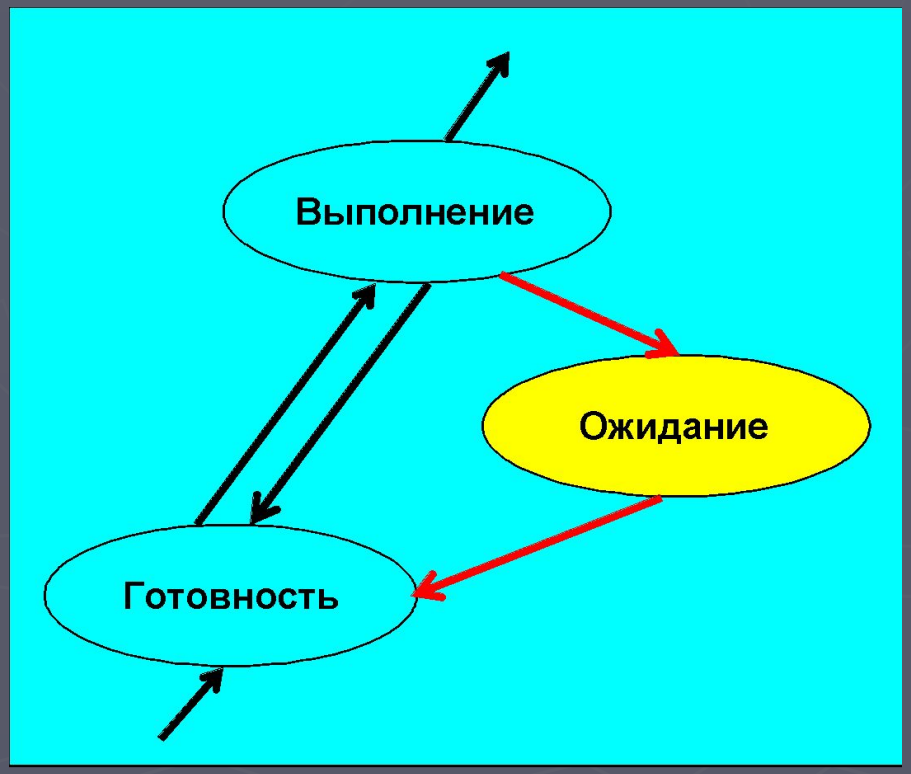


Процесс можно определить как последовательность сменяющих друг друга состояний некоторой информационной среды.

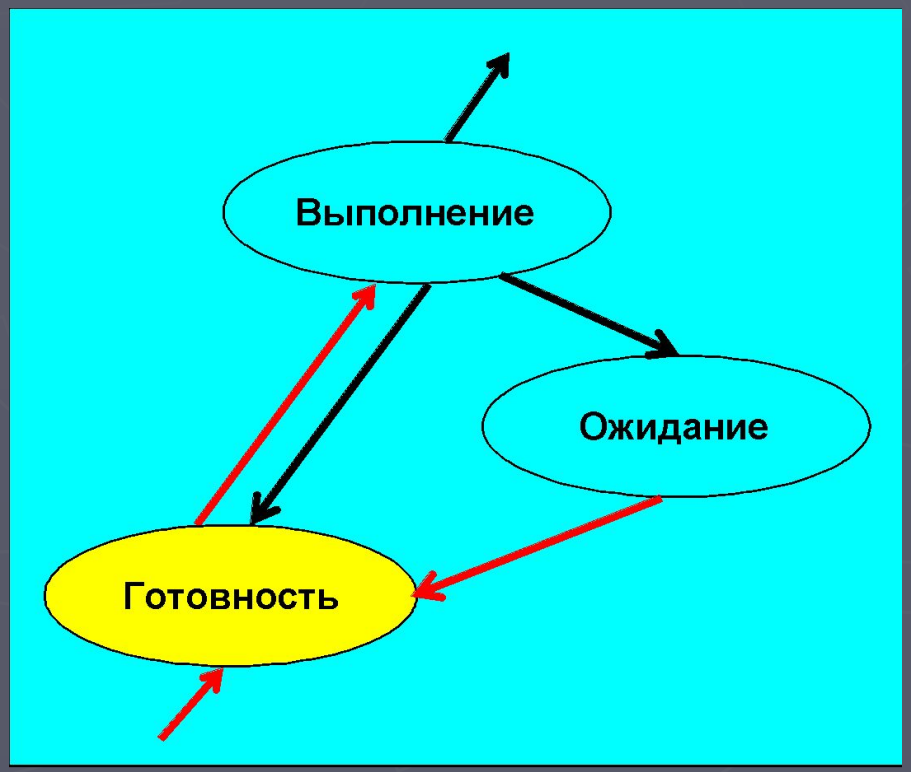
Выполнение - активное состояние процесса, во время которого процесс обладает всеми необходимыми ресурсами и непосредственно выполняется процессором.



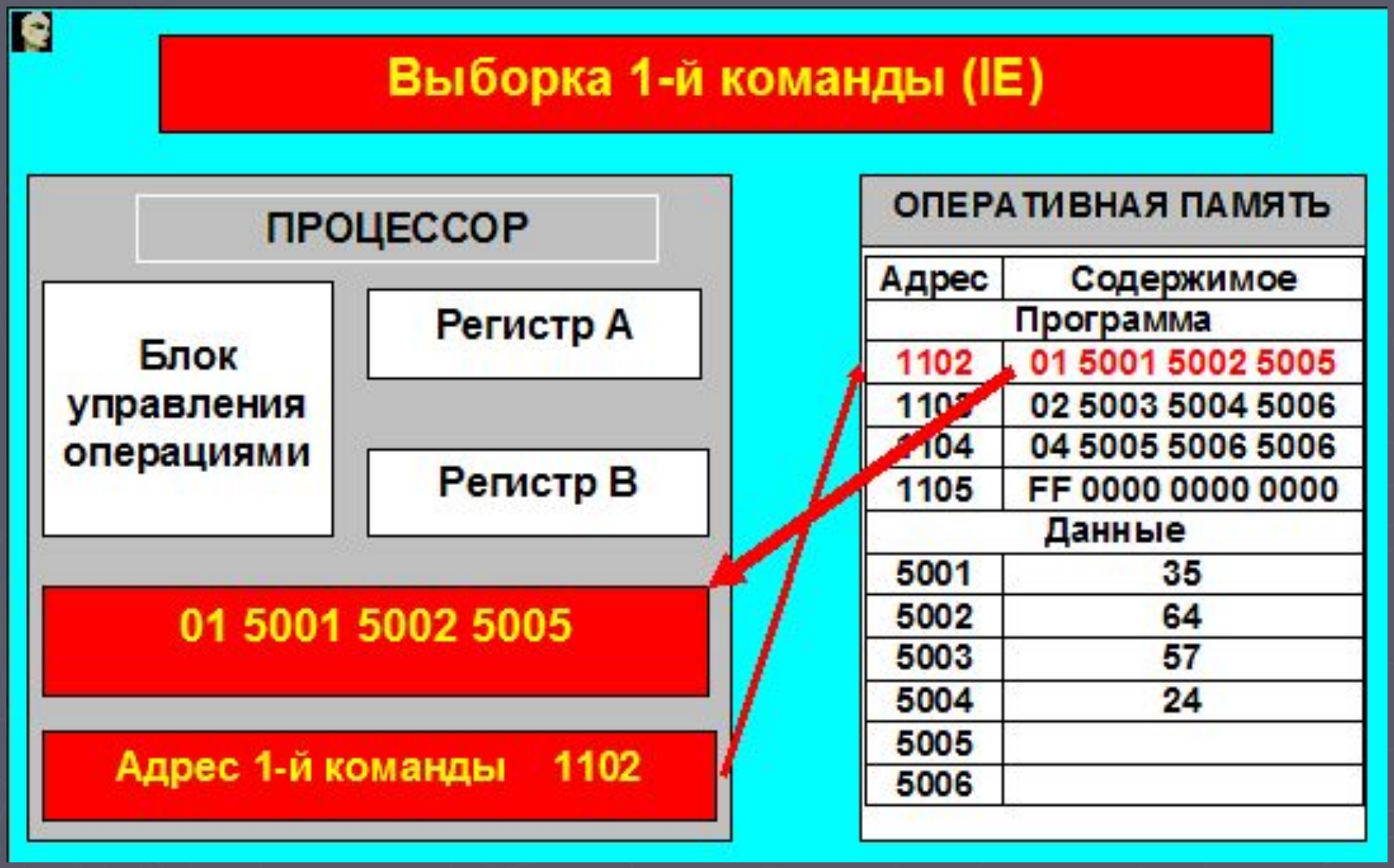
Ожидание - пассивное состояние процесса, процесс заблокирован, он не может выполняться по своим внутренним причинам.



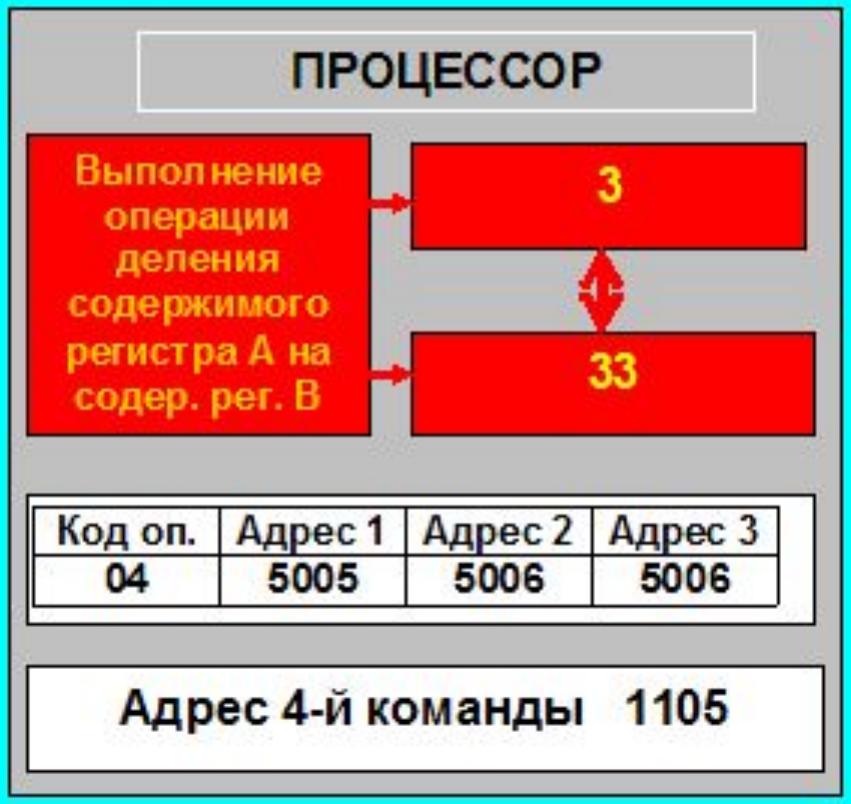
Готовность - также пассивное состояние процесса, но в этом случае процесс заблокирован в связи с внешними обстоятельствами.



Контекст и дескриптор процесса


Выборка 1-й команды (IE)
ПРОЦЕССОР
Блок управления операциями
Регистр A
Регистр B
01 5001 5002 5005
Адрес 1-й команды 1102
ОПЕРАТИВНАЯ ПАМЯТЬ
Адрес
Содержимое
Программа
1102
01 5001 5002 5005
1103
02 5003 5004 5006
1104
04 5005 5006 5006
1105
FF 0000 0000 0000
Данные
5001
35
5002
64
5003
57
5004
24
5005
5006

Выполнение операции (EX)



ОПЕРАТИВНАЯ ПАМЯТЬ

Адрес	Содержимое
Программа	
1102	01 5001 5002 5005
1103	02 5003 5004 5006
1104	04 5005 5006 5006
1105	FF 0000 0000 0000
Данные	
5001	35
5002	64
5003	57
5004	24
5005	99
5006	33

Состояние операционной среды отображается состоянием регистров и программного счетчика, режимом работы процессора, указателями на открытые файлы, информацией о незавершенных операциях ввода-вывода, кодами ошибок выполняемых данным процессом системных вызовов и т.д. Эта информация называется **контекстом процесса**.

Кроме этого, операционной системе для реализации планирования процессов требуется дополнительная информация: идентификатор процесса, состояние процесса, данные о степени привилегированности процесса, место нахождения кодового сегмента и другая информация. Эта информация называют **дескриптором процесса.**

Очереди процессов представляют собой дескрипторы отдельных процессов, объединенные в списки. Таким образом, каждый дескриптор, кроме всего прочего, содержит, по крайней мере, один указатель на другой дескриптор, соседствующий с ним в очереди.

Такая организация очередей позволяет легко их переупорядочивать, включать и исключать процессы, переводить процессы из одного состояния в другое.

Создать процесс - это значит:

- создать информационные структуры, описывающие данный процесс, то есть его дескриптор и контекст;
- включить дескриптор нового процесса в очередь готовых процессов;
- загрузить кодовый сегмент процесса в оперативную память или в область свопинга.

Алгоритмы планирования процессов

Планирование процессов включает в себя решение следующих задач:

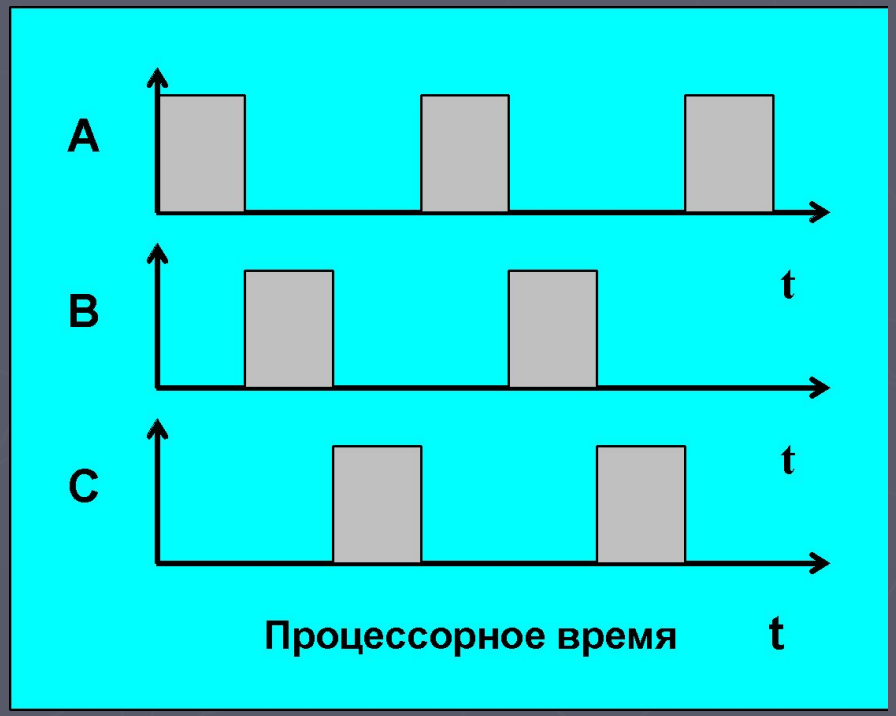
- определение момента времени для смены выполняемого процесса;
- выбор процесса на выполнение из очереди готовых процессов;
- переключение контекстов "старого" и "нового" процессов.

Первые две задачи решаются программными средствами, а последняя в значительной степени аппаратно.

Режим квантования

Каждому процессу определяется фиксированный квант (промежуток) времени и операционная система поочередно выделяет им ресурсы процессора, смена активного процесса происходит, если:

- процесс завершился и покинул систему;
- произошла ошибка;
- процесс перешел в состояние ОЖИДАНИЕ;
- исчерпан квант процессорного времени, отведенный данному процессу.



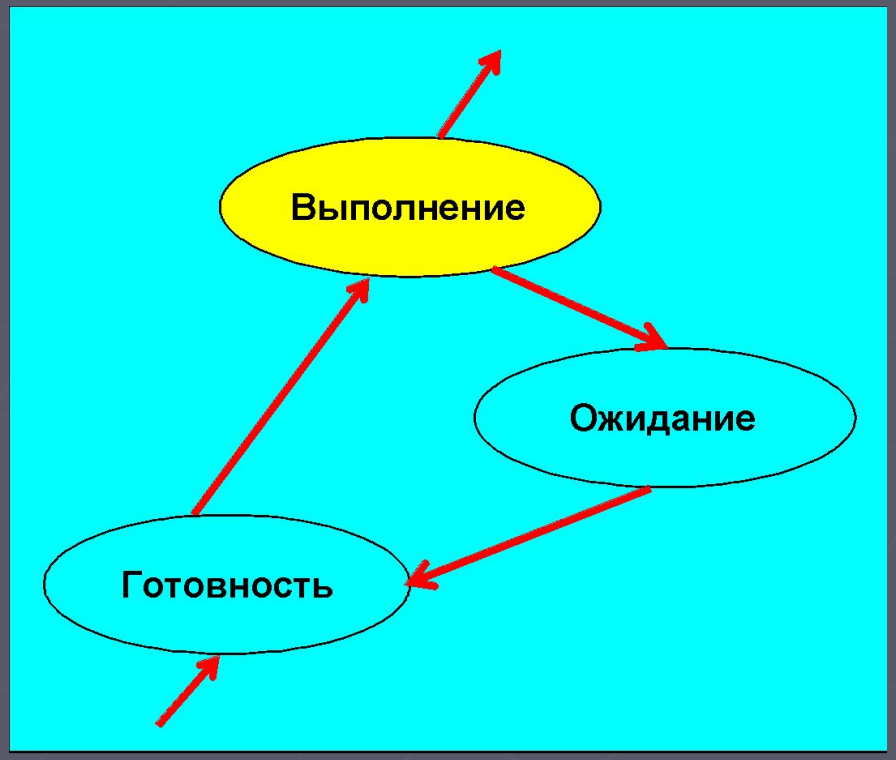
Приоритетное планирование

Приоритет - это число, характеризующее степень привилегированности процесса при использовании ресурсов вычислительной машины, в частности, процессорного времени: чем выше приоритет, тем выше привилегии.

Всегда из очереди готовых процессов выбирается для выполнения тот, который обладает наивысшим приоритетом.

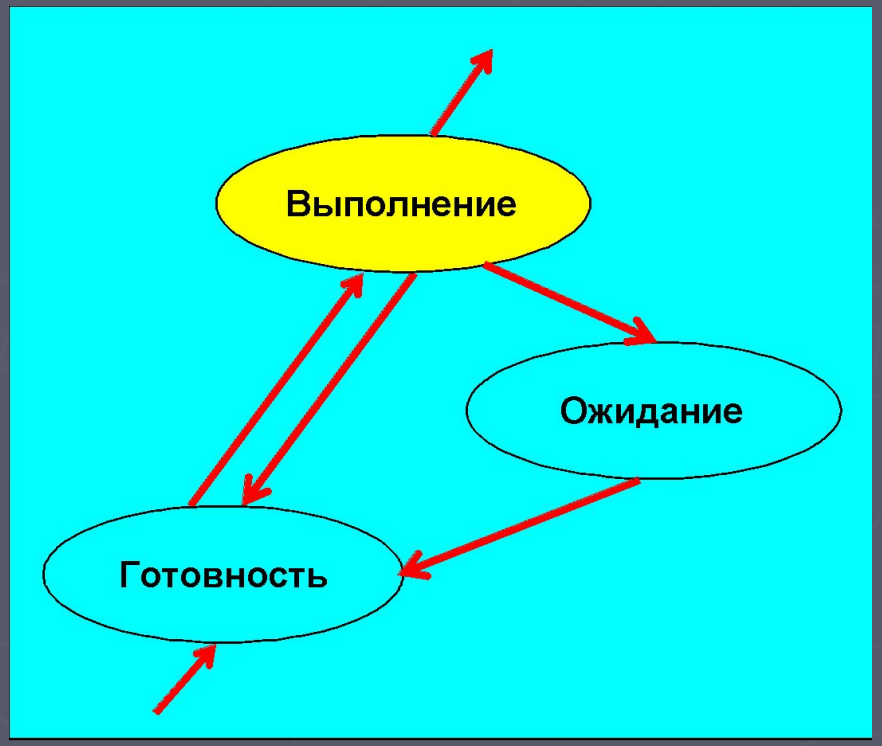
Относительные приоритеты

В системах с относительными приоритетами активный процесс выполняется до тех пор, пока он сам не покинет процессор, перейдя в состояние **ожидание** (или же произойдет ошибка, или процесс завершится).



Абсолютные приоритеты

В системах с абсолютными приоритетами выполнение активного процесса прерывается еще при одном условии: если в очереди готовых процессов появился процесс, приоритет которого выше приоритета активного процесса. В этом случае прерванный процесс переходит в состояние готовности



Вытесняющие и невытесняющие алгоритмы планирования

Невытесняющая многозадачность - это способ планирования процессов, при котором активный процесс выполняется до тех пор, пока он сам, по собственной инициативе, не отдаст управление планировщику операционной системы для того, чтобы тот выбрал из очереди другой, готовый к выполнению процесс.

Вытесняющая многозадачность - это такой способ, при котором решение о переключении процессора с выполнения одного процесса на выполнение другого процесса принимается планировщиком операционной системы, а не самой активной задачей.

При вытесняющей многозадачности механизм планирования задач целиком сосредоточен в операционной системе, и программист пишет свое приложение, не заботясь о том, что оно будет выполняться параллельно с другими задачами. При этом операционная система выполняет следующие функции:

- определяет момент снятия с выполнения активной задачи;
- запоминает ее контекст;
- выбирает из очереди готовых задач следующую и запускает ее на выполнение, загружая ее контекст.

При невытесняющей многозадачности механизм планирования распределен между системой и прикладными программами.

Прикладная программа, получив управление от операционной системы, сама определяет момент завершения своей очередной итерации и передает управление операционной системе с помощью какого-либо системного вызова, а операционная система формирует очереди задач и выбирает в соответствии с некоторым алгоритмом (например, с учетом приоритетов) следующую задачу на выполнение.

Такой механизм создает проблемы и для пользователей, и для разработчиков.

Процессы Windows XP

rundll32.exe

Утилита командной строки в среде Windows, выполняет следующую задачу - запуск библиотеки (DLL - Dynamic Link Library) как приложения, в том числе позволяя запускать некоторые функции, скомпилированные в DLL-файлах.

cisvc.exe (Microsoft Index Service Helper)

Контролирует использование памяти процессом CIDAEMON.exe и предотвращает проблемы, связанные с нехваткой памяти. Не рекомендуется завершать работу процесса, если вы используете службу индексации на локальном компьютере.

cisvc.exe

Файл cisvc.exe всегда расположен в каталоге C:WindowsSystem32. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. В настоящее время известно несколько вирусов (например, VBS.Spiltron@mm, VBS.Ypsan.E@mm, W32.HLLW.Gaobot.EE и другие), использующих имя csrss.exe для сокрытия своего присутствия в системе.

Explorer.exe

Графическая оболочка операционной системы Microsoft Windows, включающая меню пуск, рабочий стол, панель инструментов и файловый менеджер. В случае удаления этого процесса, исчезнет из виду графический интерфейс для Windows.

Explorer.exe

Файл Explorer.exe расположен в папке C:Windows. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. Наиболее распространенные вирусы, использующие для сокрытия имя Explorer.exe – W32.MyDoom, w32.Codered, BKDR_ZAPCHAST.

vsmon.exe

Процесс принадлежащий персональному межсетевому экрану ZoneAlarm. Он используется для контроля интернет трафика и создания предупреждений в зависимости от настроек безопасности пользователя.

spoolsv.exe

Отвечает за обработку процессов печати на локальном компьютере в операционных системах Microsoft Windows. В случае завершения процесса spoolsv.exe, локальный пользователь не сможет распечатывать задания на локальном принтере.

spoolsv.exe

Файл spoolsv.exe всегда расположен в C:WindowsSystem32 директории. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. В настоящее время известно несколько вирусов (например Backdoor.Ciadoor.B, VBS.Masscal.Worm, Hacktool.Privshell и другие), использующих имя spoolsv.exe для сокрытия своего присутствия в системе.

LSASS.EXE

Является сервером аутентификации локальной защиты, создающим процесс, ответственный за проверку пользователей для службы Winlogon. Данный процесс использует пакеты аутентификации, такие как Msgina.dll. Если аутентификация успешна, процесс Lsass создает маркер доступа пользователя, который используется для запуска пользовательской оболочки. Другие процессы, инициализируемые пользователем, наследуют данный маркер.

CSRSS.EXE

Часть пользовательской Win32 подсистемы. SRSS - сокращение от "client/server run-time subsystem" (клиент/серверная подсистема). csrss отвечает за консольные приложения, создание/удаление потоков и за 16-битную виртуальную среду MS-DOS.

Файл csrss.exe всегда расположен в каталоге C:\Windows\System32/. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. В настоящее время известно несколько десятков вирусов (например Trojan.Webus, W32.Dalbug.Worm, Spyware.LoverSpy и множество других), использующих имя csrss.exe для сокрытия своего присутствия в системе.

SMSS.EXE

Данный процесс представляет подсистему менеджера сеансов. Данная подсистема является ответственной за запуск пользовательского сеанса. Этот процесс инициализируется системным потоком и ответствен за различные действия, включая запуск процессов Winlogon и Win32 (Csrss.exe) и установку системных переменных. После запуска данных процессов процесс Smss ожидает их завершения. При "нормальном" завершении процессов система корректно завершает работу. Если процессы завершаются аварийно, процесс Smss.exe заставляет систему прекратить отвечать на запросы. Этот процесс нельзя завершить из менеджера задач.

Файл smss.exe расположен в каталоге c:windowsSystem32. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. Наиболее распространенные вирусы, использующие для сокрытия своего присутствия в системе имя smss.exe – W32.Dalbug.Worm, Adware.DreamAd, Win32. Brontok, Win32 Sober, Win32.Landis и другие.

Ctfmon.exe

Управляет технологиями альтернативного ввода данных. Он запускает языковую панель в системной трее при старте операционной системы, и работает в фоновом режиме даже после закрытия всех программ пакета Microsoft Office, независимо от того, запускались ли программы Office XP.

Ctfmon.exe

Программа Ctfmon.exe активирует процессор текстового ввода компонента «Альтернативный ввод данных» и языковую панель Microsoft Office. Программа производит мониторинг активных окон и предоставляет поддержку клавиатуры, перевода, распознавания речи и рукописных символов, а также других технологий альтернативного ввода данных. Удалять Ctfmon.exe не рекомендуется, потому что это может вызвать проблемы в работе программ пакета Microsoft Office.

Файл Ctfmon.exe всегда расположен в C:\Windows\System32. В случае обнаружения этого файла в любом другом каталоге он должен быть незамедлительно удален. В настоящее время известно множество вирусов (например W32.Snow.A, Spyware.UltraKeylogger, Trojan.Satiloler и другие), использующих имя Ctfmon.exe для сокрытия своего присутствия в системе.