**Тема 7. Защищенность и отказоустойчивость ОС.**

**Лекция 23 «Защищенность и отказоустойчивость ОС».**

**Защищенность** – это защита операционной системы и самого компьютера от внешних и внутренних воздействий.

**Отказоустойчивость** — способность операционной системы восстанавливать свою работоспособность после сбоев как программного, так и аппаратного характера.

В идеале пользователь вообще не должен наблюдать никаких негативных последствий сбоев в работе операционной системы. **Сбои программного характера** могут возникать по различным причинам: например, вирусная атака, неосторожное обращение с системными файлами, конфликт драйверов устройств и многое другое. **Аппаратные сбои** могут возникать по причине несоблюдения условий эксплуатации оборудования, из-за некорректного монтажа плат на системную плату. **Безопасность (security)** - способность системы защищать данные от несанкционированного доступа. Многие компании обладают ценной информацией, которую они тщательно охраняют. Это информация может быть технической, коммерческой, финансовой, юридической и т.д.

По мере того как возрастают объемы информации, хранящейся в компьютерных системах, необходимость в защите информации становится все важнее. Таким образом, защита информации от несанкционированного доступа является главной заботой всех операционных систем. Термины «безопасность» и «защита» иногда смешиваются. Тем не менее, часто бывает полезно провести границу между общими проблемами, связанными с гарантированием того, что файлы не читаются и не модифицируются неавторизованными лицами, с одной стороны, и специфическими механизмами операционной системы, используемыми для обеспечения безопасности, с другой стороны.

**Защищенность** компьютера (локального), который работает автономно, решается средствами операционной системы – обслуживание дисков, проверка на вирус и т.д. В состав операционной системы должна входить высоконадежная вычислительная база TCB (Trusted Computing Base). Она состоит из большей части аппаратного обеспечения, части ядра операционной системы и пользовательских программ, обладающих правами администратора. К функциям ОС, которые должны быть частью TCB, относятся создание процесса, переключение процессов, управление картой памяти, некоторые вопросы управления файлами и каталогами, и управления вводом – выводом. Как правило, TCB создается как отдельный модуль.

Надежная операционная система строится на основе файловой организации данных, которая обладает свойством восстанавливаемость файловой системы. Это свойство, которое гарантирует, что в случае отказа питания или краха системы, все начатые файловые операции, в которых проводится запись данных файла на диск, будут успешно завершены или отменены без каких-либо отрицательных последствий для работоспособности файловой системы. К таким файловым системам относится файловая система NTFS.

С целью восстановления создается специальный системный файл – журнал транзакций (log file), который содержит данные о том, какая выполнялась файловая операция, с каким файлом или блоком данных, какое старое и новое значение данных блока. Эта информация используется для повторения действий с данными. Применяется упреждающее протоколирование, то есть запись данных вперед, которая заключается в том, что запись в журнал делается раньше, чем изменение данных. Только после успешной записи в журнал всей последовательности подопераций файловой операции, делаются изменения в самих данных. Если операция с файлом проведена успешно, то делается отметка о завершении транзакции. Обеспечивается восстановление только системной информации. В журнал транзакций записываются только действия с системными файлами, в том числе и при использовании дискового КЭШа. Сохранность данных пользователя не гарантируется, пользовательские данные, которые были записаны в кэш и не успели переписаться на диск восстановлению не подлежат.

**Отказоустойчивость** операционных систем связана с надежной работой аппаратуры. Для надежной работы аппаратуры в первую очередь необходимо стабильное электропитание. Следует применять бесперебойные источники питания, которые позволяют работать в течение некоторого времени после отключения электропитания, что позволяет завершить все операции с файлами, в том числе запись данных из кэш – памяти, и правильно завершить работу аппаратуры.

В 1988 году американский ученый Паттерсон и его коллеги предложили различные способы организации дисков для улучшения производительности или надежности дисковых операций. В результате был разработан новый класс устройств ввода–вывода, названный RAID – Redundant Array of Inexpensive Disks - массив независимых дисков с избыточностью. SLED (Single Large Expensive Disk - одиночный большой и дорогой дисковый накопитель). На компьютере, обычно сервере, устанавливается несколько жестких дисков и специальный RAID-контроллер, а весь набор дисков выглядит с точки зрения операционной системы как один большой (и дорогой) дисковый накопитель, работа с которым проводиться стандартными средствами, изменять программное обеспечение не нужно. Данные распределяются по дискам, что позволяет распараллеливать операции. Операционная система воспринимает их как один большой диск.

**Существуют различные варианты организации совместной работы дисков.**

**Система RAID уровня 0** рассматривает весь диск, как разбитый на полосы, состоящие из одинакового числа секторов. Первый блок данных записывается на первый диск, второй блок на второй и т.д. Такой способ хранения называется чередующимся набором. Если надо считать целую полосу, то запрос на чтение разбивается на несколько и чтение проводится с дисков одновременно, но надежность ниже, чем у одного диска.

**Система RAID уровня 1** дублирует диски и называется зеркальным набором. Каждая запись записывается дважды, при чтении может использоваться любая копия. Отказоустойчивость очень хорошая, восстановление данных выполнить не сложно, но емкость дисков снижается вдвое.

**Система RAID уровня 5** работают полосами – чередующимися наборами данных. Если любой из дисков выйдет из строя, то потерянные байты можно восстановить по данным диска четности.

RAID 5 получил широкое распространение, в первую очередь благодаря своей экономичности. Объём дискового массива RAID 5 рассчитывается по формуле (n−1)×S, где n — число дисков в массиве, а S — объём диска (наименьшего, если диски имеют разный размер). Например, для массива из четырёх дисков по 500 гигабайт общий объём будет (4−1)×500 = 1500 гигабайт, то есть «теряется» 25 % против 50 % RAID 10. С увеличением количества дисков в массиве экономия (по сравнению с другими уровнями RAID, обладающими отказоустойчивостью) продолжает увеличиваться. RAID 5 обеспечивает высокую скорость чтения — выигрыш достигается за счёт независимых потоков данных с нескольких дисков массива, которые могут обрабатываться параллельно.

**Массив RAID 01 (RAID 0+1)** называют «зеркалом страйпов». Он представляет собой массив типа RAID 1, состоящий из двух вложенных массивов типа RAID 0. Количество дисков в обоих вложенных массивах RAID 0 должно быть одинаковым, из-за этой особенности данный тип может работать лишь с чётным количеством дисков. В зависимости от производителя RAID-контроллера, под RAID 0+1 может подразумеваться и другая конфигурация, кроме того, некоторые модели предлагают создание RAID 0+1 на нечётном количестве устройств, фактически реализуя под этим названием RAID 1E.

Как и в «чистом» RAID 1, полезный объём массива составляет половину суммарного объёма всех дисков (если это диски одинаковой ёмкости).

Отказоустойчивость у RAID 01 ниже, чем у RAID 10 при примерно одинаковой производительности и равном объёме, поэтому данный вид RAID практически не применяется.

**Массив RAID 10 (RAID 1+0)** — зеркалированный массив, данные в котором записываются последовательно на несколько дисков, как в RAID 0. Эта архитектура представляет собой массив типа RAID 0, сегментами которого вместо отдельных дисков являются массивы RAID 1. Соответственно, массив этого уровня должен содержать как минимум 4 диска (и всегда чётное количество). RAID 10 объединяет в себе высокую отказоустойчивость и производительность.

RAID 10 является достаточно надёжным вариантом для хранения данных в связи с тем, что весь массив RAID 10 будет выведен из строя только после выхода из строя всех накопителей в одном и том же массиве RAID 1. В общем массиве из 4 дисков при одном вышедшем из строя накопителе, шанс выхода из строя второго в одном и том же массиве равен 1/3×100=33 %.

**Основные выводы:**

1. Операционная система должна обладать механизмами защиты ресурсов и данных пользователей.
2. Операционная система должна обладать механизмами предотвращения программных и, по возможности, аппаратных сбоев.
3. Для того чтобы избежать потери данных и порчи оборудования, необходимо использовать специализированное программное обеспечение и соблюдать условия эксплуатации оборудования.
4. Защита данных может осуществляться как средствами самой операционной системы, так и с помощью специализированного программного обеспечения.