Операционная система МСВС

ОС МСВС (Мобильная Система Вооруженных Сил) – защищенная многопользовательская многозадачная ОС с разделением времени разработанная ВНИИНС на основе дистрибутива Red Hat Linux и отвечающая требованиям международных стандартов POSIX. Операционная система обеспечивает многоуровневую систему приоритетов с вытесняющей многозадачностью, виртуальную организацию памяти и сетевую поддержку; работает с многопроцессорными (SMP – symmetrical multiprocessing) и кластерными конфигурациями на платформах Intel, MIPS и SPARC. Работа с системой выполняется как в режиме командной строки, так и в режиме графического интерфейса.

Основное назначение ОС МСВС - управление ресурсами системы и процессами, использующими эти ресурсы при вычислениях. Используется для построения на ее основе защищенных информационных систем. Обладает развитыми средствами управления доступом пользователей к ресурсам ОС, включающими механизмы мандатного, дискреционного и ролевого управления доступом. Помимо развития средств защиты, совершенствования базовых функциональных возможностей и расширения поддержки современных устройств, для ОС МСВС были сделаны значительные доработки по части интерфейса пользователя и администратора системы, а также по русификации системы.

Таким образом, ОС МСВС, например, версии 3.0 - это универсальное инструментальное средство для управления техническими средствами и задачами. Это многопользовательская многозадачная ОС, которая может быть использована как в качестве базового ПО сервера, так и в качестве ОС графической рабочей станции. Область возможных приложений:

– в автоматизированных системах управления производством;
– в автоматизированных системах управления технологическим процессом;
– в информационных системах;
– в системах массового обслуживания;
– в системах сбора и анализа информации;
– в многопользовательских системах.

ОС МСВС 3.0 как программное изделие, поставляется в виде загрузочного модуля и комплекта эксплуатационной документации. Загрузочный модуль поставляется на CD-ROM, а комплект эксплуатационной документации на бумажном носителе.

Данная операционная система относится к системам класса UNIX. Это означает, что ОС МСВС 3.0 не только поддерживает многопользовательскую многозадачную работу в режиме разделения времени, но и имеет виртуальную организацию памяти, обладает сетевой прозрачностью.

При разработке ОС МСВС учитывался стандарт LSB (Linux Standard Base).

ОС МСВС может быть загружена как с внутренних устройств хранения, так и со сменных носителей.

МСВС 3.0 обладает встроенными средствами защиты от несанкционированного доступа, удовлетворяющими требованиям Руководящего документа Гостехкомиссии по классу 2 для средств вычислительной техники. Средства защиты включают мандатное управление доступом, списки контроля доступа, ролевую модель и развитые средства аудита (протоколирования событий).

Файловая система МСВС 3.0 поддерживает имена файлов длиной до 256 символов с возможностью русскоязычных имен файлов и каталогов, символьные ссылки, систему квот и списки прав доступа. Существует возможность монтирования файловых систем FAT и NTFS, а также ISO-9660 (компакт-диски). Механизм квотирования позволяет контролировать использование пользователями дискового пространства, количество запускаемых процессов и объем памяти, выделяемой каждому процессу.

В состав МСВС 3.0 входит графическая система на основе X Window. Для работы в графической среде поставляются два оконных менеджера: IceWM и KDE. Большинство

программ в МСВС ориентировано на работу в графической среде, что создает удобство для работы пользователей и для их перехода с Windows на МСВС.

МСВС 3.0 поставляется в конфигурации, которая, кроме ядра, включает набор дополнительных программных продуктов. Сама операционная система используется как базовый элемент организации автоматизированных рабочих мест (АРМ) и построения автоматизированных систем. Дополнительное программное обеспечение может устанавливаться по выбору, и ориентировано на максимальную автоматизацию управления и администрирования домена, что позволяет уменьшить затраты на обслуживание АРМов.

При инсталляции администратору предлагается выбрать либо один из стандартных типов инсталляции, либо настраиваемую инсталляцию. Стандартные типы используются при установке на стандартные рабочие места и охватывают основные типовые варианты организации рабочих мест на базе ОС МСВС 3.0. При выборе настраиваемой инсталляции можно установить МСВС 3.0 на компьютер с другой операционной системой, например, Windows NT.

В состав МСВС 3.0 входит единая система документации (ЕСД) с информацией о разных аспектах функционирования системы. ЕСД состоит из сервера документации и базы данных, содержащей тексты описаний, доступ к которым возможен через браузеры. МСВС 3.0 русифицирована в алфавитно-цифровом и в графическом режимах. Поддерживаются виртуальные терминалы, переключение между которыми осуществляется с помощью комбинации клавиш <Alt><Fn>.

Ключевым моментом с точки зрения целостности системы является операция регистрации новых пользователей МСВС, когда определяются атрибуты пользователя, включая атрибуты безопасности, в соответствии с которыми система управления доступом будет контролировать работу пользователя. Основу для мандатной модели составляет информация, вводимая при регистрации нового пользователя.

Для реализации дискреционного управления доступом используются традиционные для Unix механизмы бит прав доступа и списков прав доступа (ACL – Access Control List). Оба механизма реализуются на уровне файловой системы МСВС 3.0 и служат для задания прав доступа к объектам файловой системы. С помощью списков ACL можно задавать права на уровне отдельных пользователей и/или групп пользователей, и достичь нужной детализации в задании прав.

Особенность МСВС 3.0 – децентрализация функций суперпользователя. Задача администрирования системы разделена на несколько частей, для выполнения которых существуют администраторы конфигурирования, безопасности и аудита. Каждый из администраторов отвечает за выполнение своих задач, например, администратор конфигурирования управляет файловыми системами, сетевыми интерфейсами, настройкой системных служб и т. п. Администратор безопасности отвечает за политику безопасности и контролирует настройки системы.

В состав МСВС 3.0 входит служба печати, позволяющая осуществлять печать документов в соответствии с требованиями, предъявляемыми к защищенным системам. Среди особенностей системы печати МСВС 3.0, отличающих ее от аналогичных систем, является поддержка механизма мандатного управления доступом, которая позволяет на этапе формирования задания на печать определить уровень конфиденциальности документа и автоматически направить задание на определенный принтер в соответствии с правилами печати данной организации.

Важным элементом системы защиты МСВС 3.0 является система идентификации/аутентификации. Для успешной аутентификации пользователю необходимо ввести правильный пароль. Для осуществления мониторинга компьютеров домена применяется система контроля функционирования (КФ), состоящая из сервера и специальных агентов. Агенты устанавливаются на компьютеры домена и сообщают серверу об их состоянии. Система КФ позволяет получать информацию о различных аспектах функционирования компьютеров

(состояние процессов, дисковой подсистемы, подсистем ядра) и контролировать работоспособность сетевых служб.

МСВС 3.0 используется для создания доменов, на основе которых создаются защищенные автоматизированные системы. Физически домен реализуется в виде локальной сети компьютеров, большинство из которых служит для организации рабочих мест пользователей. Некоторые из них необходимы для организации ресурсов общего пользования, таких как файловый сервер, сервер баз данных, сервер печати, почтовый сервер. Логически домен МСВС представляет собой множество компьютеров, реализующих единую политику безопасности и образующих единое пространство администрирования.

На рабочем месте администратора безопасности поддерживается база данных с информацией о всех пользователях домена, включающая их учетную запись, расширенную информацию (например, должность, название/номер отдела), а также имя его компьютера и всех серверов, к которым он имеет доступ.

Таким образом, учетная запись является единой для данного пользователя в рамках домена МСВС и именно через нее происходит управление доступом пользователя к информационным ресурсам домена.

Для построения защищенной автоматизированной системы на базе МСВС 3.0 с возможностью временной совместимости с NT разработана система терминального доступа. Она позволяет организовать в МСВС работу с Windows-приложениями следующим образом: серверы файлов и печати, а также клиентские места строятся на базе МСВС 3.0, а для работы с Windows-приложениями выделяется сервер приложений на базе NT Terminal Server Edition. Одно из достоинств этого варианта – это гибкость в организации работы пользователей, которые получают возможность работать одновременно в двух операционных средах и использовать приложения каждой из них. Недостаток – необходимость создания сервера приложений со специальным доступом, что приводит ограничениям в политике безопасности.

Структура ОС МСВС

В состав ОС МСВС входят четыре комплекса:
– Базовая конфигурация ОС
– Система защиты от НСД
– ОС МСВС – 3.0
– Система графического интерфейса

Комплекс «Базовая конфигурация ОС»

Данный комплекс предназначен для выполнения основных функций ОС и по существу является самой ОС, в которой отсутствуют система графического интерфейса, система защиты от несанкционированного доступа и средства разработки.

Комплекс «Базовая конфигурация ОС» может иметь самостоятельное применение в тех случаях, когда пользователь не нуждается в специальных средствах защиты информации, средствах разработки программ и вся работа пользователя осуществляется в режиме командной строки. Для функционирования этого комплекса требуется значительно меньше вычислительных ресурсов, чем для функционирования ОС МСВС 3.0.

Комплекс «Система графического интерфейса»

Комплекс «Система графического интерфейса» предназначен для организации выполнения прикладных задач в режиме графического интерфейса.

Для МСВС 3.0, как и для всех ОС семейства UNIX стандартом графического интерфейса является система X-Window System (далее по тексту X-Window).

Система графического интерфейса (СГИ) обеспечивает многооконный графический режим работы в среде ОС МСВС в режиме разделения времени, который разрешает

одновременное использование на одном экране нескольких прикладных программ, находящихся на одном или нескольких узлах локальной вычислительной сети (ЛВС).

СГИ предлагает различные методы работы с цветовыми возможностями, что позволяет создавать программы, не требующие изменений при работе с дисплеями различных типов. Предусмотрена также возможность передачи данных между прикладными программами. Для взаимодействия с выполняющимися программами пользователь может использовать манипулятор «мышь» (далее по тексту - «мышь») и клавиатуру. Движение «мыши» отображается на экране с помощью курсора, который может изменять свою форму и цвет при перемещении из одного окна в другое, тем самым, отражая особенности задач, решаемых с помощью конкретного окна.

СГИ является мощным средством для разработки и создания современного графического интерфейса отдельных прикладных программ и при этом дает возможность отображать на одном экране графического дисплея результаты решения прикладных программ, выполняющихся на различных узлах ЛВС.

Комплекс «Система защиты от НСД»

Комплекс «Система защиты от НСД» предназначен для обеспечения информационной безопасности.

В состав комплекса «Система защиты от НСД» входят два компонента:

- Средства защиты от НСД;
- Утилиты настройки средств защиты от НСД.

Компонент «Средства защиты от НСД» обеспечивает работу средств защиты и содержит:

ядро ОС МСВС со встроенной системой защиты;

утилиты для первоначальной инициализации системы защиты и задания первоначальных установок;

программу для протоколирования сообщений системы защиты и программу контроля целостности файловой системы.

Компонент «Утилиты настройки средств защиты от НСД» обеспечивает настройку средств защиты и содержит:

– утилиты для настройки параметров межсетевых экранов;

– утилиты для настройки системы защиты ОС МСВС 3.0;

– руководства пользователя для системы «man» по утилитам администрирования и системным вызовам ядра, относящимся к системе защиты;

– утилиту для настройки программы контроля целостности файловой системы.

Комплекс «Средства разработки»

Комплекс «Средства разработки» (СР) предназначен для разработки прикладных программ. В состав комплекса «Средства разработки» входят компиляторы для нескольких современных языков программирования, утилиты обеспечения работы программиста в среде ОС МСВС 3.0 и библиотеки средств разработки.

Общая характеристика файловой системы МСВС

ОС МСВС использует файловую систему, которая сейчас повсеместно используется для файлов общедоступных операционных систем GNU/Linux и называется «расширенная файловая система номер два» - Ext3fs (Second Extended Filesystem) или проще ext3. Многие годы ext3 была файловой системой в GNU/Linux, принятой по умолчанию. ext3 заменила собой Extended File System 2. Ext3fs поддерживает обычные стандарты для файловых систем Unix-типа. По своей концепции она предназначена для развития, обеспечивая при этом большую устойчивость от ошибок и хорошую производительность.

Эта файловая система осуществляет поддержку файловых систем других ОС, при этом ОС МСВС способна быть как клиентом, так и сервером сетевой файловой системы NFS (Network File System). Данная файловая система соответствует стандарту

FHS(FilesystemHierarchyStandard), разработанному для UNIX-подобных систем, при этом ОС МСВС использует стандартную схему разделов диска и может разделять жесткий диск с другими системами, в т.ч. с DOS. Имеется загрузчик, который позволяет выборочно загружать требуемую ОС с диска. Поддерживает большое число файловых систем, в том числе: FAT16 (DOS), FAT32 (Windows 95/98), NTFS (NT) в режиме чтения, ISO 9660 (CD-ROM).

Из ОС МСВС обычным образом можно работать с разделами жестких дисков и дискетами, содержащими файловые системы других ОС, в т.ч. DOS, Windows 95, Minix, Xenix, Coherent, файловые системы System V. Файловые системы DoubleSpace, HPFS-2 (OS/2) и Amiga доступны в режиме только чтения. Файловые системы DoubleSpace/Stacked и т.п. становятся доступными на чтение и на запись в ОС МСВС при работе эмулятора DOS.

Файловая система ОС МСВС поддерживает все стандартные форматы CD ROM.

ОС МСВС поддерживает файловую систему UMS DOS, что дает возможность устанавливать ОС МСВС прямо в файловую систему DOS без переделывания разделов на жестком диске.

Основой контроля функционирования ОС МСВС является каталог /proc, который иногда называют собственно файловой системой /proc. Это виртуальная файловая система, которая не занимает места на диске и предоставляет удобный способ получения информации о загруженной системе. Большинство программ реально получают информацию из файлов в /proc и интерпретируют их своим способом, а затем отображают, по аналогии со всеми другими программами, которые отображают информацию о процессах.

Файловая система /proc - хороший источник информации об аппаратных средствах, а некоторые программы являются только интерфейсами к информации, содержащейся в /proc.

Существует также специальный подкаталог /proc/sys. Он позволяет изменять некоторые параметры ядра ОС МСВС в реальном режиме времени или отображать их.

Файловая система /proc содержит информацию о процессах. Если просмотреть содержимое каталога файловая система /proc, можно увидеть много каталогов, названиями которых являются номера. Эти каталоги содержат информацию о всех запущенных в данный момент процессах в системе, например: /proc/1/; /proc/302/; /proc/451/; /proc/496/; /proc/556/; /proc/633/; /proc/127/; /proc/317/; /proc/452/; /proc/497/; /proc/557/; /proc/718/.

Необходимо иметь ввиду, что каждый пользователь может увидеть информацию только о своих собственных процессах.

Каждый каталог файловой системы содержит одинаковые входы. Вот краткое описание некоторых из них:

1.cmdline: это (псевдо) файл, который содержит целую командную строку, использованную для вызова процесса. Он не отформатирован: нет пробелов между программой и ее аргументами, и нет разделителя в конце строки.

2.cwd: это символическая ссылка на текущий рабочий каталог (следует из имени) процесса.

3.environ. Этот файл содержит все переменные окружения, определенные для процесса, в форме VARIABLE=value. Подобно cmdline, вывод не форматирован вообще: нет разделителей между различными переменными, и нет разделителя в конце.

4.exe: это символическая ссылка на соответствующий запущенному процессу выполняемый файл.

5.fd: этот подкаталог содержит список файловых дескрипторов, открытых процессом в данный момент.

6.maps: когда вы выводите содержимое именованной команды, вы можете видеть части адресного пространства процесса, которые в текущий момент отображаются в файле. Слева направо это поля: адресное пространство, связанное с этим отображением, права отображения, смещение с начала файла, где начинаются отображения, старший и младший номер (в шестнадцатиричном формате) устройства, где хранится файл отображения, номер узла файла и, последнее, имя файла. Когда устройство обозначено как 0 и нет номера узла и имени файла - это анонимное отображение.

7.root: Это символическая ссылка на корневой каталог, используемый процессом.

8.status: этот файл содержит различную информацию о процессе: название выполняемой программы, его текущее состояние, использование им памяти, и другое.

Если вывести список каталога fd для какого-либо процесса, мы получим список файловых дескрипторов, открытых процессом. Каждый открытый дескриптор обозначен символической ссылкой, именем каждого номера дескриптора, и указателем на файл, открытый этим дескриптором.

Кроме каталогов, связанных с различными процессами, /proc также содержит информацию об аппаратном обеспечении ЭВМ. Список файлов каталога /proc показывает, например, список прерываний, используемых системой на данный момент, а также периферийных устройств, которые держат их; список адресных интервалов ввода-вывода, занятых в настоящее время и другую информацию, позволяющую обнаружить конфликты в системе.

Сетевые возможности ОС МСВС

ОС МСВС является сетевой операционной системой, в которой содержатся сетевые службы, реализующие функционально полный набор протоколов TCP/IP для организации работы в ЛВС (по протоколу Ethernet) и распределенных сетях (по протоколам SLIP, PUP и PPP).

Основные характеристики операционной системы МСВС

Базовая защищенная операционная система *МСВС*, как и любая другая ОС, представляет собой совокупность программных средств, обеспечивающих управление аппаратными ресурсами вычислительной системы и взаимодействие программных процессов с аппаратурой, другими процессами и пользователями. Вместе с тем, она имеет ряд особенностей.

Являясь мобильной, многопользовательской, многозадачной операционной системой, она поддерживает симметричные многопроцессорные архитектуры, способна работать как в режиме командной строки, так и в режиме графического интерфейса и может быть использована как в качестве базового ПО сервера, так и в качестве ОС графической рабочей станции.

Проанализируем данные характеристики подробнее.

1.) Мобильность

Мобильность - это способность ОС работать на разных платформах, и при этом корректно выполнять все свои функции. Мобильность ОС *МСВС* дает возможность нескольким ЭВМ разных типов (ЭВМ с процессорами *INTEL 486* или *PENTIUM, SPARC* и *MIPS*) под управлением ОС *МСВС* четко и эффективно взаимодействовать без каких-либо дополнительных коммуникационных устройств.

2.) Масштабируемость

Масштабируемость ОС *МСВС* означает возможность работы на аппаратных платформах в большом диапазоне вычислительных ресурсов: тактовой частоты процессора, оперативной и дисковой памяти, периферийного оборудования.

3.) Многозадачность

Многозадачность ОС *МСВС* означает, что множество задач может выполняться одновременно и множество устройств может быть доступно в одно и то же время.

4.) Многопользовательский режим

ОС *МСВС* обеспечивает полный многопользовательский режим. Это означает, что системой могут пользоваться одновременно сразу несколько пользователей.

5.) Поддержка режима многопроцессорных вычислений

Технология *Symmetric Multiprocessing* (*SMP*) - симметричных многопроцессорных вычислений подразумевает, что процессоры равны между собой и выполнение приложений осуществляется в распределенном режиме.

6.) Возможность поддержки кластерной структуры

ОС *MCBC* обеспечивает возможность поддержки кластерной структуры. Основная идея кластерной технологии - объединение нескольких ЭВМ в единую систему-кластер, которая эффективно использовала бы возможности всех входящих в нее ЭВМ. Простейший пример - это объединение двух серверов и разделяемой файловой библиотеки. Такой кластер позволяет почти вдвое увеличить быстродействие системы, так как программы будут вычисляться параллельно на различных ЭВМ. В этом случае кластерное программное обеспечение должно равномерно распределять нагрузку между серверами, чтобы наиболее эффективно использовать возможности кластера.

Поддержка кластерных структур возможна с помощью специальных программ, работающих под управлением ОС *MCBC*.

7.) Виртуальная память

ОС *MCBC* может использовать часть жесткого магнитного диска как виртуальную память, которая увеличивает эффективность вычислительной системы, сохраняя активные процессы в оперативной памяти и располагая редко используемые или неактивные части памяти на диске.

8.) Поддержка нескольких файловых систем

Файловые системы, поддерживаемые ОС *MCBC*:

DOS FAT;

VFAT (Win-95);

ISO 9660 CD-ROM;

Microsoft Joliet CD-ROM extension;

*NTFS (*чтение*);*

Second Extended FS (ext3);

NFSu SMB-FS и др.

9.) Поддержка графических интерфейсов

Графические интерфейсы упрощают работу пользователя. Система графического интерфейса ОС *MCBC* обеспечивает многооконный графический режим работы, предоставляя пользователю возможность одновременного взаимодействия с несколькими прикладными программами, каждая из которых представлена на экране одним или более окнами.

10.) Защищенность

В ОС *MCBC* имеется как средства защиты общего назначения, так и специальные средства защиты от несанкционированного доступа.

11.) Среда для разработки приложений

ОС *MCBC* - это удобная среда для разработки приложений, так как предоставляет прикладным программистам множество современных средств разработки и отладки программ, в том числе широкий спектр компиляторов современных языков программирования (Ассемблер, C, C++, Perl), утилиты и библиотеки средств разработки (Qt).

12.) Поддержка режима клиент/сервер

Технология клиент/сервер - это распределение прикладной программы по двум логически различным компонентам, каждый из которых решает свои задачи. Клиент посылает на сервер запросы на выполнение определенной работы, а сервер обрабатывает запросы и возвращает результаты клиенту.

13.) Возможность поддержки режима распределенных вычислений

Распределенные вычисления - это технология, которая предполагает распределение работ между несколькими ЭВМ (один из видов систем клиент/сервер).

14.) Поддержка стандартов POSIX

Стандарт ISO/IEC 9945 состоит из нескольких частей под общим названием «Информационная технология - Интерфейс мобильной операционной системы» (POSIX).

ОС МСВС разработана в соответствии с требованиями международного стандарта ISO/IEC 9945-1 и ISO/IEC 9945-2.

15.) Поддержка сетевых протоколов *TCP/IP*

16.) Поддержка сетевых протоколов *IPX* и *SMB*.

17.) Поддержка протоколов канального уровня

ОС *MCBC* обеспечивает поддержку протоколов канального уровня, таких как *Ethernet, SLIP, PLIP* и *PPP*. Ethernet- это протокол канального уровня ЛВС *Ethernet. SLIP* и *PPP* - это протоколы канального уровня распределенных сетей для работы по последовательному порту. *PLIP* - это протокол канального уровня распределенных сетей для работы по параллельному порту.

18.) Поддержка протоколов верхних уровней

ОС *MCBC* обеспечивает поддержку протоколов верхних уровней, таких как *FTP, TELNET, SMTP, NFS, NIS+* и *DNS*. Это протоколы прикладного уровня, используемые в соответствующих сетевых приложениях.

19.) Поддержка режима управления электропитанием

Расширенный режим управления электропитанием и сохранения энергии позволяет экономить электроэнергию и продлить срок службы мониторов и ЭВМ.

По материалам статей

http://gistechnik.ru/pub/3-publik/65-mcbc.html

http://www.osp.ru/os/2001/10/180520/