ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
майор С.Краснов

Лекция № 17

Тема: «СИСТЕМА ЗАЩИТЫ ОТ НСД ОС МСВС»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 201_ г.

Санкт-Петербург
201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Назначение, возможности и состав основного комплекса СЗИ ОС МСВС – 40 мин.
2. Назначение, возможности и состав дополнительного комплекса СЗИ ОС МСВС – 40 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml

2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области защиты ОС МС ВС.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов механизмах защиты ОС МС ВС.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите особенности защиты в ОС МС ВС?
2. Охарактеризуйте ОС МС ВС?
3. Перечислите основные задачи администратора безопасности в ОС МС ВС?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 15

Тема № 5 Механизмы защиты операционных систем

«КОМПЛЕКС «СИСТЕМА ЗАЩИТЫ ОТ НСД» ОС МСВС 3.0»

В. 1. Назначение, возможности и состав основного комплекса СЗИ ОС МСВС

Комплекс "Система защиты от НСД" предназначен для построения гибкой и многофункциональной системы защиты, при которой невозможно преднамеренное нарушение функционирования ОС МСВС 3.0, а также случайное или преднамеренное нарушение безопасности находящихся под управлением ОС МСВС 3.0 ресурсов системы.

Основой обеспечения безопасности ОС является создание механизмов контроля доступа к ресурсам системы. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Кроме того, комплекс "Система защиты от НСД" содержит *вспомогательные средства защиты*.

К этим средствам относятся:

- средства надзора,
- профилактического контроля,
- ревизии.

В совокупности механизмы контроля доступа и вспомогательные средства защиты образуют механизмы управления доступом.

При построении системы защиты, на основе комплекса "Система защиты от НСД" в ОС МСВС 3.0, вводятся понятия администратора безопасности и администратора аудита. Оба не могут влиять друг на друга. Администратор системы может управлять всей системой, включая настройку механизмов безопасности, а также производить настройки, заводить и удалять пользователей, ограничивать использование пользователями системных ресурсов. Администратор безопасности предназначен для управления механизмом мандатного управления доступом. Администратор аудита предназначен для управления политикой аудита.

Право изменять правила разграничения доступа (ПРД) предоставляется выделенным субъектам (администрации, службе безопасности и т.д.).

Комплекс "Система защиты от НСД" содержит совокупность программных элементов реализующих, механизмы управления доступом и обеспечивающих выполнение требований руководящих документов Государственной технической комиссии при президенте Российской Федерации ISBN 5-89354-009-03, а также Министерства Обороны Российской Федерации по защите информации от НСД.

В состав основного комплекса **"Система защиты от НСД"** (данная система защиты входит в состав базовой конфигурации ОС МСВС 3.0) входят две компоненты:

- комплект средств защиты от НСД (**КСЗИ НСД**);
- утилиты настройки средств защиты от НСД.

КСЗИ НСД содержит:

1. ядро ОС МСВС 3.0 со встроенной системой защиты,
2. утилиты для первоначальной инициализации системы защиты и задания первоначальных установок,
3. программу для протоколирования сообщений системы защиты,
4. программу контроля целостности файловой системы.

КСЗИ НСД предназначен для использования в составе системы обеспечения безопасности информации (СОБИ) в целях построения системы защиты информации от несанкционированного доступа. Автоматизированная система (АС) с КСЗИ НСД может

обрабатывать информацию с максимальной степенью секретности - «совершенно секретно», и имеет соответствующий класс защищенности АС-1Б в соответствии с требованиями ФСТЭК при МО РФ.

Комплект **КСЗИ НСД** обеспечивает:

- идентификацию и аутентификацию субъектов доступа;
- контроль целостности защищаемых ресурсов, программной среды и программных средств защиты информации от несанкционированного доступа;
- комплексное управление средствами защиты информации от несанкционированного доступа;
- комплексное управление доступом к защищаемым ресурсам;
- формирование, выдачу и оперативный контроль сигналов о несанкционированном доступе;
- регистрацию событий по доступу к защищаемым ресурсам.

В ОС МСВС создается база данных по файлам, в которой хранятся такие атрибуты как: размер, время создания, владелец, группа, права и т.д. Считается, что эти атрибуты должны оставаться неизменными в процессе нормальной жизнедеятельности системы, а любое изменение одного из них является сигналом опасности. Возможно, нарушитель подменил программу или внедрил в систему "троянца".

Обычной информации о файле недостаточно, злоумышленник может подделать и размер, и права, и владельца, и время создания файла. Для этого вводится еще дополнительная сигнатура - результат применения какой-нибудь односторонней функции к содержимому файла (подобно работе с паролями в UNIX). Сигнатур может быть несколько. Чаще всего применяется алгоритм MD5-Digest. Собственно, он сам предназначен для генерации 128-битных ключей и последующего применения в алгоритме шифрования RSA, но обладает замечательным свойством -при изменении исходных данных контрольная сумма существенно изменяется, и более того очень сложно выполнить такую модификацию файла, при которой контрольная сумма осталась бы неизменной.

Программа контроля целостности aide периодически проверяет соответствие данных базы с данными реальной файловой системы, и в случае обнаружения несоответствия администратору выдается предупреждение.

Синтаксис команды aide:

aide [опция]

Описание опций:

-check – проверить базу на непоследовательность данных. Необходимо предварительно создать базу перед данной процедурой. Это также действие по умолчанию. Без параметров aide выполняет проверку.

--init – создать базу данных. Необходимо создать базу и скопировать ее в определенное место перед использованием параметра -check.

-update – проверить базу данных и внести обновления, если это необходимо.

-config=conflgfile – считать конфигурационные данные из файла configfile, а не из файла aide.conf.

Ограничения на область применения

Ограничения на область применения не предъявляются.

Вторая компонента "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, а также

- утилиту для настройки программы контроля целостности файловой системы. (Примечание. Данная утилита в версиях ядра ОС МСВС 2.2.20 и 2.4.32 не функционирует).

Командами управления мандатными и дискреционными атрибутами файлов и процессов являются: **chmac, macid, ls** (некоторые опции), **ps** (некоторые опции), **chmod**.

Для настройки системы защиты можно воспользоваться следующими утилитами, имеющие графический интерфейс:auditadmin, fileadmin, macadmin, useradmin.

Программа **auditadmin** предназначена для настройки и управления системой аудита.

Программа **fileadmin** предназначена для настройки атрибутов доступа к файлам. В ОС МСВС 3.0 утилита позволяет назначить любому файлу мандатные и дискреционные права доступа в соответствии с его статусом.

Программа **macadmin** предназначена для формирования мандатной политики ОС МСВС 3.0. С её помощью определяется количество и состав уровней секретности и категории системы.

Программа **useradmin** предназначена для управления пользователями и группами ОС МСВС 3.0. Она позволяет управлять доступом пользователей в систему, формировать состав групп МСВС, а также назначать пользователям разрешенные мандатные атрибуты и другие, специфические для МСВС свойства.

Ограничения на область применения

«Утилиты настройки средств защиты от НСД» работают на ЭВМ под управлением ОС МСВС 3.0 с установленной и настроенной системой графического интерфейса. Утилита для настройки программы контроля целостности файловой системы не функционирует. Дополнительных ограничений на область применения не предъявляется.

В. 2. Назначение, возможности и состав дополнительного комплекса СЗИ ОС МСВС

Данный комплекс системы защиты информации не входит в состав базовой конфигурации ОС и поставляется отдельно на компакт диске.

В комплекс системы защиты информации входит:

- комплекс системы защиты информации (КСЗИ) от НСД,
- комплекс средств защиты информации от случайных воздействий и аварийных ситуаций (КСЗИ СВАС).

Они предназначены для использования в составе системы обеспечения безопасности.

Состав КСЗИ НСД включает:

1. Программное средство генерации паролей (ПС ГП);
2. Комплекс программ «Система печати»;
3. Программное средство ввода/вывода информации;
4. Программное обеспечение рабочего места администратора ОБИ (ПО РМ АОБИ);

Кроме этого в КСЗИ НСД дополнительно могут быть включены:

5. Антивирусные программы DrWeb для операционной системы ОС МСВС 3.0;
6. Аппаратно-программный модуль доверенной загрузки «Электронный замок» (средство контроля доступа к техническим средствам).

КСЗИ НСД обеспечивает:

- Идентификацию и аутентификацию пользователей;
- Контроль целостности защищаемых ресурсов, программной среды и программных средств защиты информации от НСД;
- комплексное управление средствами защиты информации от НСД;
- регистрацию событий по доступу к защищаемым ресурсам.

Рассмотрим состав основных СЗИ входящие в состав КСЗИ НСД ОС МСВС 3.0.

Программа генерации паролей предназначена для генерации и формирования паролей доступа пользователей к сети, файлам, базам данных и другим защищаемым ресурсам на рабочем месте, серверах и других объектах вычислительной техники автоматизированной системы.

Программа генерации паролей осуществляет:

- создание буквенно-цифровых, цифровых паролей длиной от 8 до 16 знаков;
- проверку полученных паролей на удовлетворение криптографическим и инженерно-криптографическим требованиям, предъявляемым к паролям;
- создание на магнитном носителе файла, содержащего сгенерированные пароли (в версии ядра 2.2.20 данная возможность не предусмотрена);
- распечатку карточек с паролями для выдачи пользователям;
- распечатку журнала учета выдачи карточек.

Комплекс программ "Система печати" (КП СП) - предназначен для организации печати документов в среде операционной системы МСВС 3.0 и предоставляет возможность работы с печатающими устройствами, входящими в состав автоматизированной системы в режиме печати с маркировкой твердых копий (с колонтитулами) и без нее, а также обеспечивает автоматическую регистрацию факта печати документов в журналах учета размножения документов различной степени секретности.

КП СП позволяет:

1. выводить на печать задания, создаваемые приложениями, функционирующими под управлением ОС МСВС 3.0, а также задания на печать создаваемые под управлением приложений, функционирующих под управлением ОС Windows Terminal Server Edition 4.0;
2. задавать два режима печати: с маркировкой твердого носителя или без маркировки;
3. в зависимости от заданного режима печати КП СП самостоятельно следит за направлением заданий на печать, на корректную очередь печати, а также осуществляет проверку корректности задаваемых параметров печати задания;
4. работать с журналами учета-размножения документов, выводимых на печать.

Для печати документов с использованием модуля станции печати (МСП) необходим подключенный станции печати, принтер, подготовленный к работе в соответствии с эксплуатационной документацией. Должна быть выполнена настройка ОС МСВС 3.0 для работы с данным принтером.

Утилита настройки модуля станции печати запускается в графическом режиме командой **printtool**. Рабочие станции, станция печати и средства защиты информации должны быть настроены для обеспечения сетевого взаимодействия. Во время печати документов должно быть подано электропитание на локальный принтер, и он должен находится в состоянии «ГОТОВ»**.**

Для печати документов с использованием модуля печати на локальный принтер (МЛП) необходим подключенный к автоматизированному рабочему месту (рабочей станции), принтер, подготовленный к работе в соответствии с эксплуатационной документацией на него. Должна быть выполнена настройка ОС МСВС 3.0 для работы с данным принтером. Во время печати документов должно быть подано электропитание на локальный принтер, и он должен находится в состоянии **«ГОТОВ».**

Перед использованием комплекса должна быть осуществлена установка и настройка программ МСП и МЛП.

Для выполнения КП СП необходимо выполнение демона печати lpd.

При печати документов с грифами секретности «**Секретно**» и «**Сов. секретно**», пользователям путем использования организационных мер должно быть запрещено понижение грифа секретности документов при формировании задания на печать и печать

данных документов на принтерах, подключенных к АРМ (рабочим станциям) в качестве локальных.

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, принятыми в данной организации. Каждый напечатанный лист автоматически маркируется учетными атрибутами документа, включающими фамилию пользователя, распечатавшего документ и имя компьютера, с которого было отправлено задание на печать. Одним из достоинств системы печати является ее инвариантность по отношению к приложениям, которые обращаются к службе печати. Это означает, что она не привязана к существующим приложениям и не изменяется при появлении новых приложений. Как следствие, приложения, выводящие на печать, должны учитывать маркировку листов и оставлять для этого свободное место. Факт печати регистрируется в специальном журнале учета размножения печатных документов. Для работы с этим журналом используется специальная программа, позволяющая просматривать, редактировать некоторые поля записей и распечатывать их.

Программное средство ввода-вывода информации предназначено для организации информационного обмена между ПЭВМ, посредством переносимых накопителей (НЖМД, НГМД, лазерных дисков) и автоматизации процесса установки мандатных и дискреционных атрибутов на копируемые файлы.

Программное средство ввода-вывода информации обеспечивает выполнение следующих функций:

- выбор переносимой файловой системы из списка, представленного в файле */etc/fstab* и её автоматическое монтирование;
- копирование выбранных файлов из переносимой файловой системы на локальную в файловую систему (импорт);
- автоматическую установку заданных мандатных и дискреционных атрибутов на импортируемые файлы;
- синхронизацию содержимого выбранных директорий на локальной и переносимой файловой системе.

Запуск программного средства ввода-вывода информации осуществляется только от имени администратора. В графическом режиме запустить команду **psio**. Вид программы показан на рисунке 8.1.

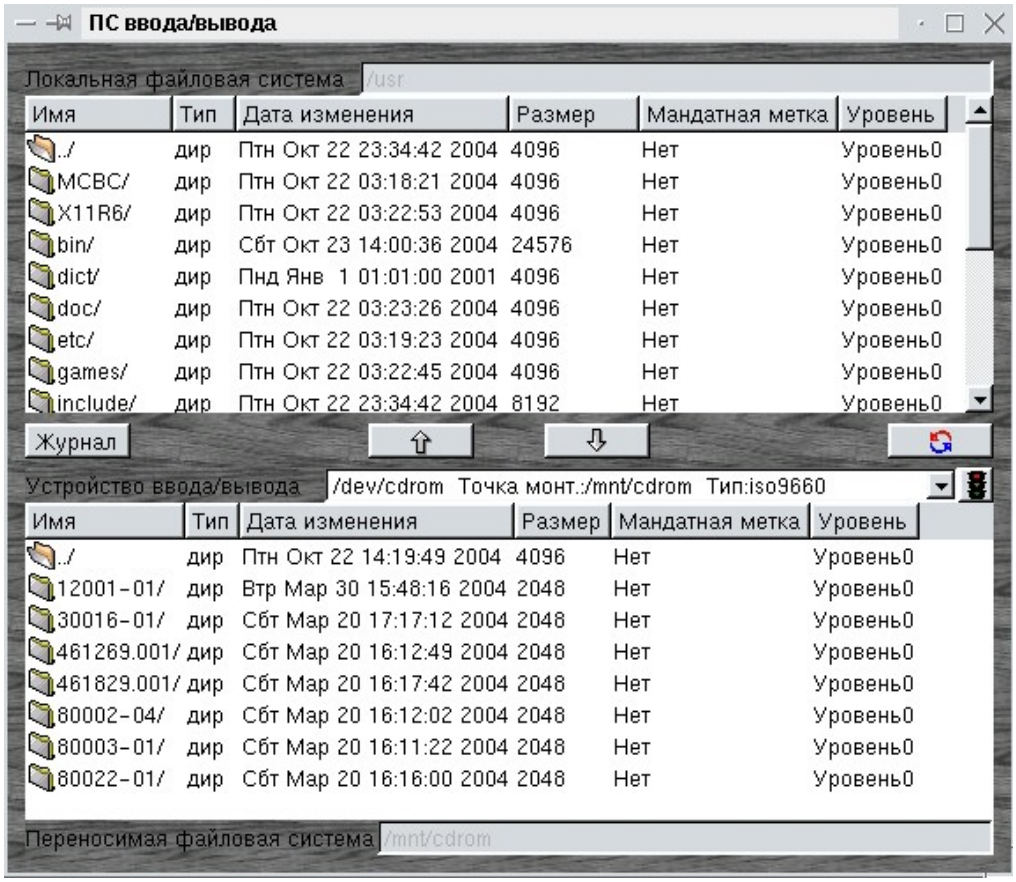

Рисунок 8.1 - Программное средство ввода-вывода информации

Программное обеспечение рабочего места администратора обеспечения безопасности информации (ПО РМ АОБИ)

ПО РМ АОБИ предназначено для:

- обеспечения централизованного контроля доступа в АС;
- идентификации и проверки подлинности субъектов доступа при входе в систему по идентификатору и паролю;
- идентификацию ПЭВМ, узлов сети, программ, томов, каталогов, файлов по именам;
- формирования учетных записей пользователей;
- установки и модификации меток конфиденциальности субъектов доступа, тиражирования производимых настроек политики безопасности на определенные администратором безопасности рабочие станции из состава АС;
- блокировки на вход ПЭВМ всех пользователей при совершении несанкционированного доступа на данной ПЭВМ;
- регистрации запуска (завершения) всех программ и процессов в АС, которые не входят с вписок разрешенных к запуску;
- регистрации попыток доступа программных средств к защищаемым файлам, список которых определяется администратором безопасности;
- регистрации попыток доступа программных средств к защищаемым устройствам, список которых определяется администратором безопасности;
- регистрации действий администратора безопасности по изменению полномочий субъектов доступа и статуса объектов доступа;
- контроля целостности файлов, список которых определяется администратором безопасности, при запуске системы по именам и контрольным суммам;
- периодического контроля целостности файлов по именам и контрольным суммам в процессе работы ОС, периоды определяются администратором.

ПО РМ АОБИ предполагает ведение домена безопасности. Домен безопасности определяет список станций, входящих в него, и ведение централизованной базы пользователей и групп (создание, редактирование и удаление пользователей). С помощью

ПО РМ АОБИ обеспечивается задача единой политики безопасности в рамках домена безопасности.

С помощью агентов домена осуществляет контроль событий НСД. Контроль правильность выполнения данных операций осуществляется на уровне ОС. В случае выявления НСД агент домена безопасности передает информацию серверу домена безопасности, который осуществляет ведение общего централизованного журнала НСД в рамках домена.

В состав ПО рабочего места администратора ОБИ входит:

1. Утилита настройки и администрирования сервера контроля функционирования.
2. Визуальная система администрирования для просмотра журналов событий АРМ клиентов ПО РМ АОБИ.
3. В комплект поставки ПО РМ АС входит WEB-сервер, который устанавливается одновременно с СКФ. Несмотря на то, что сам СКФ в процессе работы не использует возможности WEB-сервера, WEB-сервер необходим для обеспечения доступа администратора к информации, собираемой и обрабатываемой СКФ, посредством WEB-браузера.
4. Сервер домена безопасности ОС МСВС 3.0 входит в состав ПО РМ АОБИ и является его основным компонентом.
5. Агент домена безопасности ОС МСВС 3.0 входит в состав ПО РМ АОБИ и устанавливается на все клиентские АРМ для обеспечения взаимодействия с сервером ПО РМ АОБИ.
6. ПО РМ АС использует в процессе работы **DNS**-сервер, поэтому его необходимо установить и настроить, а также сконфигурировать **DNS**-клиентов.

Драйвер ограничения полномочий суперпользователя должен быть установлен на все ЭВМ домена безопасности МСВС 3.0, включая ЭВМ сервера ПО РМ АОБИ.

Ограничения на область применения

Дополнительный КСЗИ НСД работает на ЭВМ под управлением ОС МСВС 3.0 с установленной и настроенной системой графического интерфейса. Дополнительных ограничений на область применения не предъявляется.

Комплекс средств защиты информации от случайных воздействий и аварийных ситуаций

Комплекс средств защиты информации от случайных воздействий и аварийных ситуаций (КСЗИ СВАС) это набор утилит для автоматизации рутинных действий администратора системы по предотвращению нештатных ситуаций и предназначен для защиты критической информации от случайных воздействий и аварийных ситуаций на рабочих станциях, работающих под управлением ОС МСВС 3.0. Для решения задачи были использованы стандартные библиотеки и компилятор из состава ОС МСВС 3.0.

В состав входят программные компоненты, обеспечивающие удобные средства администрирования в графической среде. В качестве входных данных в КСЗИ СВАС выступает вся информация, полученная от входных устройств, таких, например, как «мышь» и клавиатура. Выходными данными КСЗИ СВАС являются вся графическая информация на дисплее, файлы с сохраненными заданиями, файлы с сохранённой информацией.

Конфигурирование и функционирование отдельных компонент комплекса происходит независимо друг от друга.

ФУНКЦИИ КСЗИ СВАС позволяют обеспечивать:

- централизованное управление конфигурацией программных средств автоматизированной системы;
- процесс централизованной установки и обновления программного обеспечения, резервного копирования и восстановления критической информации, а также удаленного восстановления программного обеспечения рабочих мест.

- управление конфигурацией источника бесперебойного питания.

Минимальная конфигурация оборудования должна обеспечить работу ОС МСВС 3.0 в графическом режиме и иметь свободное место на жестком магнитном диске для установки пакетов программ.

СОСТАВ КСЗИ СВАС:

- средство управления конфигурацией ПО;
- средство удаленного восстановления ПО;
- средство управления резервным копированием;
- средство управления источником бесперебойного питания;
- программное средство рабочего места администратора сети (ПО РМ АС).

Средство управления конфигурацией ПО предназначено для удаленного администрирования рабочей станции сети. Запускается на удаленном компьютере через сетевые сервисы с компьютера администратора и позволяет в удобной графической среде получать доступ к основным административным ресурсам удаленной станции.

Средство удаленного восстановления ПО предназначено для организации и управления централизованной установкой и обновления набора программного обеспечения на рабочих станциях сети. Средство удаленного восстановления ПО реализовано на базе модели клиент/сервер и состоит из трех частей:

- серверная часть;
- клиентская часть;
- система администрирования серверной части.

Принцип обмена данными между ЭВМ клиента СУВ ПО и ЭВМ сервера СУВ ПО заключается в том, что программа клиента СУВ ПО посылает программе сервера СУВ ПО запросы по указанному порту (по умолчанию – порт 8002) в виде текстовой строки «LIST», а в ответ получает список доступных дистрибутивов также в текстовом виде. Для обмена дистрибутивами программного обеспечения используется сетевая файловая система (NFS, Network File System), причем программа клиента СУВ ПО автоматически устанавливает все доступные пакеты, заявленные в каталоге дистрибутивов.

Файлы дистрибутивов ПО хранятся на ЭВМ сервера СУВ ПО в виде rpm-пакетов, что

позволяет программе-клиенту СУВ ПО использовать все реализованные в ОС МСВС 3.0

механизмы по работе с базой данных RPM.

Серверная часть оснащена визуальной системой администрирования для графической среды, которая представляет собой удобный интерактивный инструмент, позволяющий управлять конфигурацией сервера дистрибутивов на уровне групп, клиентов и rpm-пакетов. При добавлении или удалении клиента система администрирования автоматически вносит соответствующие изменения в файл */etc/exports*, который используется **NFS** при предоставлении полномочий клиентам, монтирующим удаленную файловую систему.

Средство управления резервным копированием предназначено для управления централизованным созданием резервных копий критической информации с возможностью ее последующего восстановления в удобной графической среде. При выполнении планового резервного копирования используется сервис **CRON.**

Средство управления источником бесперебойного питания (ИБП) предназначено для управления конфигурацией источников бесперебойного питания в удобной графической среде. Работа средства базируется на использовании агента ИБП, отвечающего за взаимодействие с ИБП.

Программное средство рабочего места администратора сети (ПО РМ АС) - это рабочая среда, в которой одновременно выполняется несколько модулей, обеспечивающих одновременный контроль текущего состояния контролируемых устройств и служб и

формирующих данные о состоянии контролируемых устройств и служб в виде **html-**страниц. С помощью данных модулей ПО РМ АС позволяет контролировать как программные службы, так и аппаратуру, собирая данные по её использованию и состоянию.

Параллельно с этим, ПО РМ АС позволяет выполнять настройку параметров контроля с использованием возможностей графического оконного менеджера ОС МСВС 3.0. Для этого имеются модули администрирования как СКФ, так и АКФ.

ПО РМ АС используется - администратором системы для осуществления оперативного контроля над узлами администрируемой сети, позволяет ему своевременно вмешиваться в процесс работы узла.

ПО РМ АС обеспечивает выполнение следующих функций:

1. Организация непрерывного контроля за состоянием узлов администрируемой сети.
2. Обеспечение администратора средствами настройки контроля над узлами сети.
3. Вывод информации о текущей настройке в графическом виде.
4. Обеспечение администратора информацией о предыдущих состояниях контролируемых узлов сети.
5. Ведение и работу с журналом сообщений.
6. Обеспечение вывода информации в удобном для восприятия виде в виде **html-**страниц, и в частности по следующим пунктам:
   - информации о нахождении функционирующих рабочих станций в составе ЛВС (есть связь с рабочей станцией или отсутствует);
   - информации о состоянии дискового пространства рабочих станций;
   - информации о загрузке процессора;
   - информации о времени включения и времени непрерывной работы рабочих станций;
   - информации о состоянии интересующих администратора процессов в системе рабочих станций (запущены, остановлены);
   - информации о состоянии операционной системы в целом, т.е. сбор сведений о сообщениях ядра или системных сообщениях характеризующих сбой или неисправность в процессе работы;
   - информации о состоянии источника бесперебойного питания, если средство управления ИБП установлено на рабочей станции;
   - информации о состоянии сетевых сервисов на рабочих станциях.

ПО РМ АС представляет собой программу, работающую под управлением операционной системы ОС МСВС 3.0 и состоящую из 2-х основных частей:

- сервер контроля функционирования (далее по тексту - СКФ), установленный на машине администратора.

- агент контроля функционирования (далее по тексту АКФ), установленный на машинах пользователей.

УСЛОВИЯ ПРИМЕНЕНИЯ И ОГРАНИЧЕНИЯ КСЗИ СВАС

Технические средства

Для установки и работы с КСЗИ СВАС рекомендуются следующие технические средства:

- свободное место на жестком диске — не менее 20 Мбайт;
- устройство чтения компакт-дисков.

Программные средства

КСЗИ СВАС функционирует на ЭВМ под управлением ОС МСВС 3.0 с установленной и настроенной системой графического интерфейса и настроенными средствами межсетевого взаимодействия.

Ограничения на область применения

КСЗИ СВАС работает на ЭВМ под управлением ОС МСВС 3.0 с установленной и настроенной системой графического интерфейса. Дополнительных ограничений на область применения не предъявляется.