

Закрытое акционерное общество

"АСТРА СТ"

ТЕРМИНАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ

СИСТЕМА «MIRAGE»

Описание применения

АСТР.51240-01 31 01

Листов 10

2006

АННОТАЦИЯ

Документ содержит общие сведения о Терминальной Вычислительной Системе Mirage, описание аппаратного и программного обеспечения, необходимого для её функционирования. Кратко описаны задачи и технические решения.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ.....	4
1.1 БАЗОВЫЕ ПРИНЦИПЫ.....	4
2. УСЛОВИЯ ПРИМЕНЕНИЯ.....	5
2.1 УСЛОВИЯ, НЕОБХОДИМЫЕ ДЛЯ ФУНКЦИОНИРОВАНИЯ ПРОГРАММЫ.....	5
2.2 ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ.....	5
2.3 ТРЕБОВАНИЯ К ЛОКАЛЬНОЙ СЕТИ.....	8
2.4 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.....	8
3. ОПИСАНИЕ ЗАДАЧИ.....	9
3.1 РЕШАЕМЫЕ ЗАДАЧИ.....	9
3.2 ИСПОЛЬЗУЕМЫЕ РЕШЕНИЯ.....	10

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Назначение данного программного продукта – построение сетевых многопользовательских многозадачных систем обработки информации с высоким классом защиты (до класса 1Б включительно), позволяющих обрабатывать информацию с грифом “СОВЕРШЕННО СЕКРЕТНО”.

1.1 Базовые принципы

Система Mirage основана на следующих базовых принципах:

- функционирование под управлением операционной системы Linux;
- использование в качестве хранилища служебных данных СУБД ЛИНТЕР;
- авторизация пользователей в том числе и по биометрическим параметрам;
- терминальный доступ к информации;
- механизмы изоляции файловых систем, дискреционного и мандатного контроля доступа.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Условия, необходимые для функционирования программы

Терминальная Вычислительная Система Mirage функционирует на одном или нескольких серверах, а также на одном или нескольких терминалах.

Система состоит из следующих функциональных компонентов:

- «Терминальный сервер»;
- «Сервер служебной базы данных»;
- «Сервер печати»;
- Терминалы.

«Терминальный сервер», «сервер служебной базы данных» и «сервер печати» – это программные комплексы, которые физически могут быть установлены на один или на разные компьютеры.

Каждый терминал – это отдельная рабочая станция.

Все рабочие станции и серверы должны быть связаны между собой локальной вычислительной сетью.

2.2 Требования к техническим средствам

В качестве поддерживаемой аппаратной платформы для серверов и терминалов была выбрана архитектура IBM PC, на основе процессоров с системой команд i386 и выше. Эта платформа наиболее распространена в настоящее время и практически не имеет альтернатив.

Требования к серверам

Для функционирования «Терминального сервера» должен использоваться наиболее производительный сервер. Минимально необходимая конфигурация:

- Процессор, i386-совместимый с тактовой частотой не менее 733 МГц.
- Оперативная память – не менее 512 Мб.
- Видеоадаптер – не менее 1 Мб видеопамати.
- Жесткие диски: IDE, SATA, SCSI – любые из поддерживаемых операционной системой, общим объемом не менее 80 Гб.

- Сетевые адаптеры: любые сетевые Ethernet контроллеры, работающие на скорости 100/1000 Мбит/сек и поддерживаемые операционной системой.

Для функционирования «Служебной базы данных» должен использоваться сервер с производительной дисковой подсистемой. Минимально необходимая конфигурация:

- Процессор, i386-совместимый с тактовой частотой не менее 400 МГц.
- Оперативная память – не менее 128 Мб.
- Видеоадаптер – не менее 1 Мб видеопамати.
- Жесткие диски: IDE, SATA, SCSI – любые из поддерживаемых операционной системой, общим объемом не менее 80 Гб.
- Сетевые адаптеры: любые сетевые Ethernet контроллеры, работающие на скорости 100/1000 Мбит/сек и поддерживаемые операционной системой.

Для функционирования «Сервера печати» может использоваться любой, даже не производительный сервер. Минимально необходимая конфигурация:

- Процессор, i386-совместимый с тактовой частотой не менее 400 МГц.
- Оперативная память – не менее 64 Мб.
- Видеоадаптер – не менее 1 Мб видеопамати.
- Жесткие диски: IDE, SATA, SCSI – любые из поддерживаемых операционной системой, общим объемом не менее 8 Гб.
- Сетевые адаптеры: любые сетевые Ethernet контроллеры, работающие на скорости 100/1000 Мбит/сек и поддерживаемые операционной системой.

Если «терминальный сервер», «служебная база данных» и «сервер печати» установлены на один сервер, то требования к такому серверу повышаются. Минимально необходимая конфигурация:

- Процессор, i386-совместимый с тактовой частотой не менее 733 МГц.
- Оперативная память – не менее 512 Мб.
- Видеоадаптер – не менее 1 Мб видеопамати.
- Жесткие диски: IDE, SATA, SCSI – любые из поддерживаемых операционной системой, общим объемом не менее 80 Гб.
- Сетевые адаптеры: любые сетевые Ethernet контроллеры, работающие на скорости

100/1000 Мбит/сек и поддерживаемые операционной системой.

Требования к терминалам

В качестве терминалов могут использоваться как обычные персональные компьютеры, так и специализированные системные боксы, отличающиеся:

- малыми размерами;
- ограниченным набором периферийных устройств;
- пониженным энергопотреблением;
- меньшей производительностью.

К конфигурации терминала предъявляются следующие требования:

- Процессор, i386-совместимый с тактовой частотой не менее 200 МГц.
- Оперативная память – не менее 32 Мб.
- Видеоадаптер – не менее 2 Мб видеопамати.
- Жесткие диски – не нужны.
- Сетевые адаптеры: любые сетевые Ethernet контроллеры, работающие на скорости 10/100/1000 Мбит/сек и поддерживаемые операционной системой.

Помимо этого, к терминалу предъявляются особые требования, поскольку на него устанавливается «агент загрузки терминала». Это небольшая программа 32 Кб, которая обеспечивает авторизацию пользователя, загрузку образа ОС с сервера по сети и ее запуск. Агент может быть установлен:

- в ПЗУ BootROM на сетевом адаптере;
- как дополнительный модуль в ПЗУ BIOS материнской платы (только для Award BIOS);
- в загрузочной области FLASH-диска, установленного в терминал.

Соответственно терминал должен быть оборудован либо разъемом для ПЗУ BootROM, либо FLASH-диском, либо иметь съемное ПЗУ с BIOS типа Award.

Требования к принтерам

Система поддерживает следующие типы принтеров:

1. USB Postscript (подключается локально к серверу печати);
2. IP PCL (подключается удаленно через сеть);
3. Windows PCL (подключается удаленно через сервер с ОС Windows).

2.3 Требования к локальной сети

Локальная сеть должна быть построена на протоколах Ethernet.

Должна обеспечиваться пропускная способность:

- от сетевого оборудования к серверу – не менее 100 Мбит/сек;
- от сетевого оборудования к терминалу – не менее 10 Мбит/сек.

2.4 Требования к программному обеспечению

На сервере должно быть установлено следующее программное обеспечение:

- Операционная система Linux с ядром версии 2.4.22 (Рекомендуемый дистрибутив: ASP Linux 9.2);
- Графический сервер Xvnc версии 4.0 (из пакета vncserver);
- Графическая среда Gnome версии 2.4.1;
- Графическая библиотека Qt версии 3.1.

На терминале не требуется никакого программного обеспечения, т.к. на него устанавливается агент загрузки терминала.

3. ОПИСАНИЕ ЗАДАЧИ

3.1 Решаемые задачи

Защита информации. Основное назначение системы – защита от несанкционированного доступа к информации.

Различные уровни конфиденциальности информации. Обрабатываемая в системе информация может иметь разную степень защиты. При этом пользователи должны получать доступ к конфиденциальной информации только при наличии необходимого уровня допуска.

Многопользовательский режим работы. Система должна поддерживать одновременную работу нескольких пользователей. При этом пользователи не должны влиять на работу друг друга. Кроме того, необходим механизм для обмена информацией между пользователями, работающими над одной задачей.

Различные категории пользователей. У разных сотрудников могут быть различные привилегии для управления системой. Должны различаться: обычные пользователи, администраторы системы и администраторы безопасности.

Надежная идентификация. Помимо обычных способов идентификации должна обеспечиваться идентификация пользователей по биометрическим параметрам.

Графический интерфейс. Взаимодействие пользователя с системой должно производиться посредством стандартного графического интерфейса с использованием рабочего стола, окон, меню, ярлыков и пр.

Централизованное хранение информации. Файлы пользователей должны быть сосредоточены в одном месте для обеспечения возможности оперативного резервирования и восстановления информации.

Централизованное администрирование. Необходим единый механизм для оперативной установки и обновления программного обеспечения для всех пользователей. Кроме того, у администраторов должен быть удобный интерфейс для управления и контроля системы.

3.2 Используемые решения

В системе используется технология терминального доступа к данным. В качестве АРМ пользователей используются терминалы – аппаратно ограниченные рабочие станции без каких бы то ни было средств вывода и собственных накопителей информации. Пользователи, работая на терминале, фактически работают на сервере терминального доступа. При этом терминал получает с сервера и отображает на экране изображение рабочего сеанса, и отправляет на сервер данные с устройств ввода (клавиатура и мышь). Таким образом хранение, обработка, ввод/вывод информации осуществляются централизованно – на сервере.

В системе Mirage используются следующие технологии:

- Загрузка терминалов по сети – на терминалах нет никакой информации, даже свою ОС они загружают с сервера;
- Био-идентификация пользователей – поддерживается несколько схем авторизации, кроме стандартного логина и пароля можно использовать отпечатки пальцев (решение с использованием библиотеки BioLink);
- Терминальный доступ к приложениям – работая на терминале пользователь видит свой рабочий стол и программы, хотя все это исполняется на сервере;
- Замкнутая программная среда – пользователь не сможет запустить ни одно приложение, если не записано явное разрешение в матрице доступа;
- Ограниченная файловая система – все пользователи работают на одном сервере, но каждый – в своей изолированной файловой системе;
- Контроль ввода-вывода – на терминале недоступен вывод данных на носители или устройства, а на сервере ввод/вывод информации полностью контролируется;
- Защищенная СУБД «ЛИНТЕР» – информация о всех пользователях и совершаемых ими действиях сохраняется в служебной базе данных, реализуемой средствами сертифицированной СУБД.