Описание функциональных характеристик
ПО АСТД 37С
(в составе ОС «Циркон 37С» и ПО «Циркон 37Т»)

СОДЕРЖАНИЕ

1. Общие сведения

Программное обеспечение «Автоматизированная система терминального доступа 37С» имеет Заключение ФСБ России о соответствии программного обеспечения «Автоматизированная система терминального доступа 37С» «Требованиям к средствам защиты информации, содержащей сведения, составляющие государственную тайну, от несанкционированного доступа» и «Временным требованиям к программному обеспечению, используемому в автоматизированных системах ИТКС специального назначения».

ПО АСТД 37С предназначено для защиты от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну и имеющей степень секретности не выше «совершенно секретно», хранимой и обрабатываемой на серверах и рабочих станциях (автономных и в составе локальной вычислительной сети), включая доступ к виртуальной инфраструктуре, разворачиваемой на основе использования встроенного гипервизора.

В состав ПО АСТД 37С входят следующие компоненты:

- Операционная система «Циркон 37С» (ОС «Циркон 37С») СДЕМ.00100-01;
- Программное обеспечение терминального доступа «Циркон 37Т» (ПО «Циркон 37Т») СДЕМ.00099-01.

ПО АСТД 37С соответствует требованиям:

- «Требованиям к средствам защиты информации, содержащей сведения, составляющие государственную тайну, от несанкционированного доступа» по классу 1Б;
- «Временным требованиям к программному обеспечению, используемому в автоматизированных системах ИТКС специального назначения» в части контроля отсутствия недекларированных возможностей по 2 уровню контроля;
- Требованиям технического задания.

2. Назначение и область применения

ОС «Циркон 37С» – это многопользовательская, многозадачная операционная система, работающая как в режиме командной строки, так и в режиме графического интерфейса, выполняющая управление ресурсами системы (субъектами и объектами).

ОС «Циркон 37С» представляет собой гипервизор, обеспечивающий одновременное параллельное выполнение нескольких операционных систем на одном хост-компьютере. ОС «Циркон 37С» обеспечивает изоляцию виртуальных машин друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными виртуальными машинами и управление ресурсами.

Каждая виртуальная машина представляет собой отдельный процесс пользовательского пространства гипервизора со своим адресным пространством, а значит надежность изоляции виртуальных машин основана на надежности реализации механизмов (средств защиты информации), обеспечивающих невозможность доступа процессов одной виртуальной машины к объектам адресного пространства другой виртуальной машины, кроме как через внешнюю среду (сетевой интерфейс).

Для доступа пользователей к виртуальной инфраструктуре через терминальные устройства предусмотрено ПО «Циркон 37Т».

ПО «Циркон 37Т» состоит из серверной части, функционирующей под управлением ОС «Циркон 37С», которая реализует разграничение доступа пользователей к ресурсам разной степени конфиденциальности путем предоставления им возможности безопасной работы только с ресурсами выбранного пользовательского домена, а также терминальной части, функционирующей на терминальном устройстве.

Данное свойство реализуется за счет того, что:

- терминальное устройство имеет энергонезависимую память, защищенную от перезаписи, в которую на начальном этапе была записана программа-загрузчик (U-boot), которая с помощью протоколов DHCP и HTTP умеет находить в сети, скачивать и

проверять на подлинность PXE-образ (PXE-образ – это программное обеспечение терминального устройства, собираемое из той же базы исходных кодов, что и ОС «Циркон 37С», под архитектуру ARM, и упакованное в формат Flattened Image Tree (FIT-файл)). После скачивания и проверки управление передается на PXE-образ, который и будет работать до выключения терминального устройства;

- переключение между разными пользовательскими доменами происходит через выключение питания на терминале (происходящее при извлечении смарт-карты), таким образом, никакой остаточной информации на терминальном устройстве не остается;
- автоматический выбор домена осуществляется за счет соответствующей записи на пользовательской смарт-карте, т.е. у пользователя должно быть столько смарт-карт, сколько существует доменов, к которым он должен (может) иметь доступ.

Используемые смарт-карты: ACOS-16, ACOS-32 и ACOS-72.

ПО АСТД 37С может функционировать самостоятельно на рабочей станции пользователя (рис. 1), а также может использоваться для построения виртуальной инфраструктуры с подключением терминальных устройств (рис. 2).

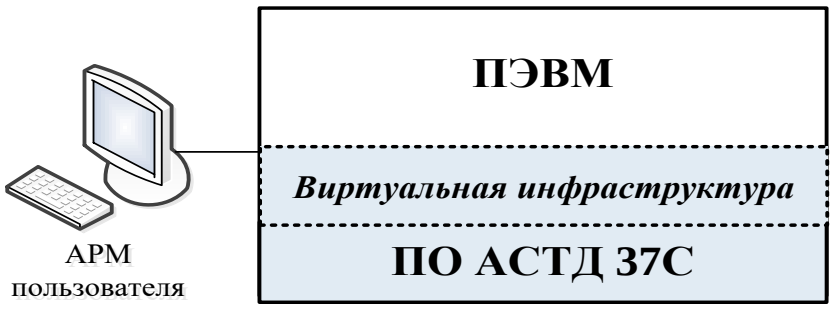

Рис. 1 – Использование ПО АСТД 37С
в качестве хостовой операционной системы на АРМ пользователя

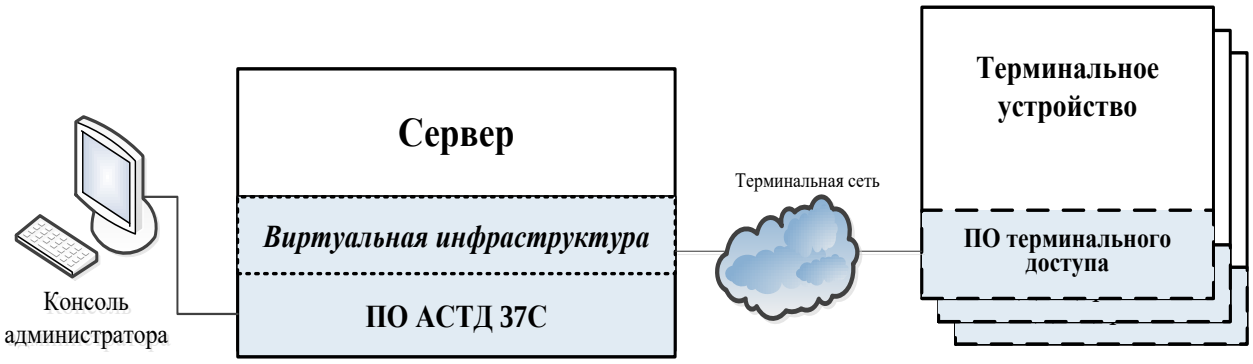

Рис. 2 – Использование ПО АСТД 37С для построения виртуальной инфраструктуры с подключением терминальных устройств

3. Функциональные характеристики

ПО АСТД 37С предоставляет привилегированным пользователям средства по установке, настройке и сопровождению нескольких виртуальных машин на одной вычислительной платформе.

ПО АСТД 37С поддерживает установку и функционирование на современных серверах и рабочих станциях на платформах с процессорной архитектурой x86-64 (AMD, Intel), а также поддержку современного периферийного оборудования.

Возможности ПО АСТД 37С:

- масштабируемость (возможность работы на аппаратных платформах в большом диапазоне вычислительных ресурсов: тактовой частоты процессора, оперативной и дисковой памяти, периферийного оборудования);
- многозадачность (множество задач может выполняться одновременно и множество устройств может быть доступно в одно и то же время, т.е. обеспечивается возможность параллельной/псевдопараллельной обработки нескольких процессов);
- многопользовательский режим (системой могут пользоваться одновременно несколько пользователей);
- поддержка файловых систем (Ext3, Ext2, XFS, FAT, NTFS, SMB, NFS);
- работа с внешними устройствами;
- поддержка графического интерфейса;
- выполнение прикладных программ (выполнение программы начинается с создания в памяти ее образа и связанных с процессом структур ядра, инициализации и передачи управления инструкциям программы. Завершение программы ведет к освобождению памяти и соответствующих структур ядра. Образ программы в памяти содержит, как минимум, сегменты инструкций и данных, созданные

компилятором, а также стек для хранения автоматических переменных при выполнении программы);

- работа в режиме командной строки (в режиме командной строки ОС «Циркон 37С» предлагает пользователю ввести команду (общего назначения, для работы с файлами, для обработки текста, для работы с сетью и др.), которая принимается и обрабатывается интерпретатором команд. Интерпретатор команд обеспечивает интерфейс между пользователем и ОС;
- администрирование системы (администрирование системы осуществляется администратором системы, который должен выполнять такие основные задачи, как: настройка устройств, управление профилями пользователей, создание резервных копий, включение/выключение системы, обеспечение безопасности системы, ведение системного журнала и т. д. Настройка устройств предусматривает настройку локальных и сетевых ресурсов, таких как принтеры, модемы и др. Управление пользователями означает добавление, удаление пользователей и определение их привилегий. Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможных сбоев в работе ОС. Завершение работы ОС «Циркон 37С» предполагает корректное выключение системы, позволяющее избежать потери информации и сбоев файловой системы. Ведение системного журнала необходимо для регистрации событий в ОС «Циркон 37С»);
- поддержка основных сетевых протоколов (DHCP, DNS, FTP, HTTP, IMAP, NFS, NTP, SMB, SMTP, SSH, TCP/IP, TFTP);
- администрирование сети (выполнение ряда процедур, которые необходимы для поддержки сети в работоспособном состоянии. В отличие от других сетевых функций администрирование связано с операциями, выполняемыми в сети уже после ее развертывания. По этой причине все задачи и вопросы администрирования сети должны

быть учтены во время разработки и установки сети, а решаться непосредственно в процессе функционирования. К основным задачам сетевого администратора относятся установка и конфигурирование помеченных доменов, серверов и рабочих станций, создание и поддержка пользовательских бюджетов, поддержка работоспособности системы, установка программного обеспечения на рабочих станциях и оказание помощи пользователям в решении их проблем);

- работу с электронной почтой.

Средства защиты информации ПО АСТД 37С обеспечивают:

- идентификацию и аутентификацию;
- мандатный контроль доступа;
- дискреционный контроль доступа;
- изоляцию процессов;
- контроль целостности;
- регистрацию и учет;
- запуск выбранной операционной системы;
- защиту виртуальной инфраструктуры;
- противодействие использованию уязвимостей;
- маскирование информации;
- математические алгоритмы, используемые в механизмах аутентификации;
- очистку памяти.

ПО АСТД 37С обеспечивает решение следующих задач:

- эффективное управление ресурсами средств вычислительной техники;
- предоставление удобных средств взаимодействия с автоматизированными системами;
- защита обрабатываемой информации;
- использование мультимедийных возможностей оборудования;
- оптимизация повседневной деятельности пользователя;
- реализация сетевой функциональности;
- реализация сервисной функциональности;
- наглядное отображение обрабатываемой информации.

Выполнение поставленных задач достигается за счет:

- использования современных наработок в области создания ОС;
- применения эргономичного графического интерфейса пользователя;
- наличия различных механизмов защиты и средств управления защитой;
- поддержки широкого перечня сетевых протоколов;
- использования специальных служб, реализующих сервисные функции.

4. Входные и выходные данные

Входными данными ОС являются:

- действия пользователя в графическом интерфейсе (нажатие кнопок, заполнение полей, выбор пунктов в списках и т.д.);
- команды, вводимые пользователем в консоли;
- системные конфигурационные файлы;
- информация, получаемая по сетевым интерфейсам.

Выходными данными ОС являются:

- данные, отображаемые средствами графического интерфейса;
- результаты выполнения команд пользователя, выводимые в консоль;
- файлы и документы в различных форматах, созданные при помощи текстовых, табличных, графических и иных редакторов;
- записи в системных журналах;
- информация, отправляемая по сетевым интерфейсам.

АКЦИОНЕРНОЕ ОБЩЕСТВО
"МНОГОПРОФИЛЬНОЕ
ВНЕДРЕНЧЕСКОЕ ПРЕДПРИЯТИЕ
"СВЕМЕЛ"

127254, г. Москва, Огородный пр., д. 5, стр.5
Тел/Факс: +7(495) 926-7187, +7(499) 750-7065
E-mail: post@swemel.ru