Документ, содержащий описание функциональных характеристик «Операционной системы специального назначения «Astra Linux Special Edition» для ЭВМ на базе процессорной архитектуры «MIPS»

Описание программы

Листов 27

2025

АННОТАЦИЯ

Настоящий документ является описанием программы операционной системы специального назначения «Astra Linux Special Edition MIPS» (далее по тексту — ОС).

В документе приведены общие сведения, функциональное назначение и логическая структура ОС, используемые технические средства, вызов и загрузка, входные и выходные данные.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование программы: Операционная система специального назначения «Astra Linux Special Edition MIPS».

1.2. ОС написана на следующих языках программирования: ассемблер, Perl, C, C++, shell, Python.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1. Назначение

ОС предназначена для применения в составе информационных (автоматизированных) систем в целях обработки и защиты[1)] информации любой категории доступа[2)] — общедоступной информации, а также информации, доступ к которой ограничен федеральными законами (информации ограниченного доступа).

2.2. Классы решаемых задач

2.2.1. ОС обеспечивает решение следующих классов задач (предоставляет следующие функциональные возможности):

- установка и функционирование на средствах вычислительной техники с процессорной архитектурой x86-64, а также поддержка периферийного оборудования;
- установку и функционирование на средствах вычислительной техники, оснащенных сенсорным устройством указания на чувствительной области экрана дисплея при помощи прикосновения (типа «touch-screen»);
- поддержка основных сетевых протоколов стека TCP/IP;
- создание защищенной среды виртуализации;
- организация сетевого домена с централизованным хранением учетных записей;
- работа с мультимедийными данными;
- работа с реляционными базами данных (БД);
- работа с электронной почтой;
- работа с гипертекстовыми данными;
- обработка текстовых документов и электронных таблиц различных форматов;
- поддержка прикладного программного интерфейса для взаимодействия со встроенными в ОС средствами защиты информации (СЗИ) от несанкционированного доступа (НСД).

2.2.2. Основой обеспечения безопасности ОС является создание механизмов контроля доступа к ее ресурсам. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Кроме того, к СЗИ от НСД принадлежат вспомогательные инструменты. К ним относятся средства надзора, профилактического контроля и ревизии. В совокупности механизмы контроля доступа и вспомогательные СЗИ образуют механизмы управления доступом.

---

1) От несанкционированного доступа.

2) В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (статья 5, пункт 2).

2.2.3. Комплекс средств защиты ОС обеспечивает решение следующих классов задач по защите информации от НСД:

- идентификацию и аутентификацию;
- дискреционное управление доступом;
- мандатное управление доступом;
- регистрацию событий безопасности;
- ограничение программной среды;
- изоляцию процессов;
- защиту памяти;
- контроль целостности;
- обеспечение надежного функционирования;
- фильтрацию сетевого потока;
- маркировку документов;
- защиту среды виртуализации;
- контроль подключения съемных машинных носителей информации (защиту ввода-вывода на отчуждаемый физический носитель информации).

2.2.4. Организация сетевого домена реализуется средствами создания единого пространства пользователей (ЕПП), которые обеспечивают:

- сквозную аутентификацию в сети;
- централизацию хранения информации об окружении пользователей;
- централизацию хранения настроек системы защиты информации на сервере;
- интеграцию в домен защищенных серверов: системы управления базами данных (СУБД); печати и маркировки CUPS, гипертекстовой обработки данных Apache и электронной почты на основе Dovecot и Exim4;
- централизованный аудит событий безопасности в рамках домена.

2.2.5. Функционал ОС поддерживает создание кластерной файловой системы с обеспечением ее отказоустойчивости (отказоустойчивый кластер). Для создания отказоустойчивого кластера используются пакеты Pacemaker, Corosync и Keepalived, а также Ceph для создания отказоустойчивой распределенной файловой системы.

В отказоустойчивом кластере и отказоустойчивой распределенной файловой системе при выходе из строя одного из серверов сохраняется доступность сервисов и информа- ции.

2.2.6. ОС является русифицированной системой. Русский язык поддерживается как в алфавитно-цифровом, так и в графическом режимах. Файловая система (ФС) ОС поддерживает имена файлов длиной до 256 символов с возможностью создания русскоязычных

имен файлов и каталогов, символьные ссылки, систему квот и ACL. Существует возможность монтирования ФС FAT и ISO-9660 (компакт-дисков).

2.3. Функциональное ограничение на применение ОС

ОС предназначена для использования на аппаратной платформе с процессорной архитектурой x86-64. Минимальная конфигурация компьютера, на котором функционирует ОС, приведена в разделе 5.

3. ЛОГИЧЕСКАЯ СТРУКТУРА

Структура ОС представлена на рис. 1.

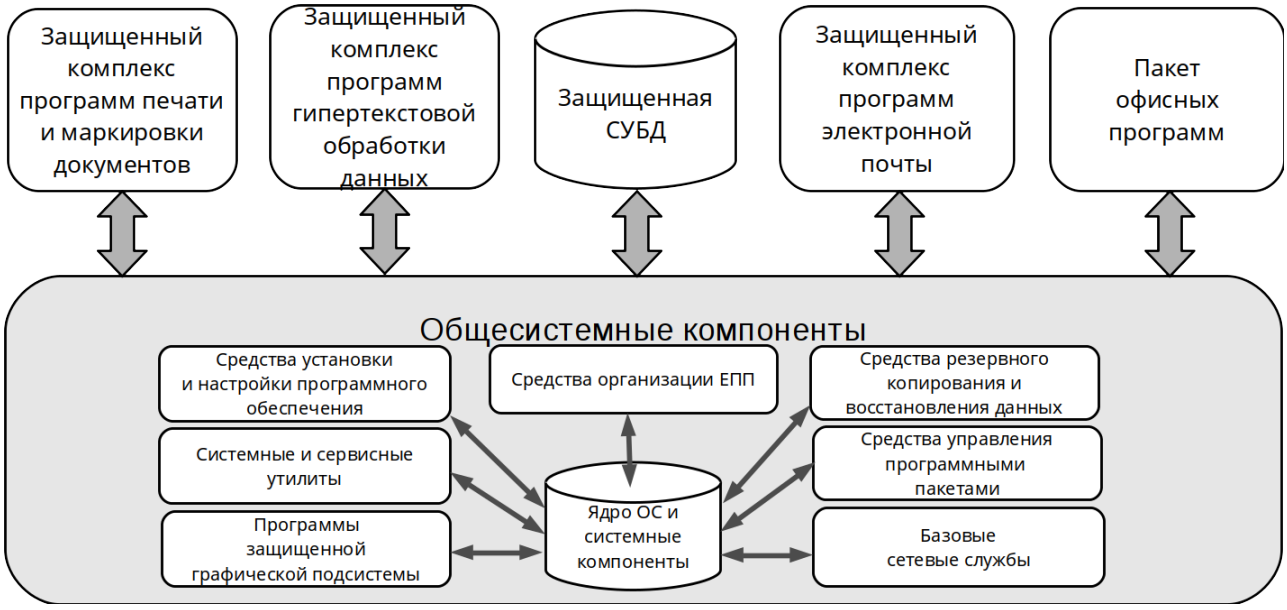

Рис. 1

3.1. Общесистемные компоненты

3.1.1. Ядро ОС и системные компоненты

ОС является Linux-подобной операционной системой, в которой используется ядро операционной системы Linux.

Ядро ОС состоит из следующих основных подсистем:

- управление процессами;
- взаимодействие между процессами;
- управление памятью;
- управление ФС;
- модуль виртуализации;
- управление операциями ввода-вывода;
- сетевая подсистема.

Все подсистемы контролируют доступ к системным ресурсам.

Модуль виртуализации используется для изоляции и управления виртуальными гостевыми машинами. Модуль виртуализации реализован на базе технологии KVM (Kernel-based Virtual Machine), которая включает специальный модуль ядра KVM и средство создания виртуального аппаратного окружения QEMU. KVM использует технологию аппаратной виртуализации, поддерживаемую современными процессорами от Intel и AMD и известную под названиями Intel-VT и AMD-V. Используя загруженный в память модуль ядра, KVM, с помощью драйвера пользовательского режима (который представляет собой модифицированный драйвер от QEMU), эмулирует слой аппаратного обеспечения,

в среде которого могут создаваться и запускаться виртуальные машины. Управление средой виртуализации обеспечивается утилитой virsh с использованием программного интерфейса libvirt.

3.1.2. Средства установки и настройки ОС

Средства установки и настройки ОС обеспечивают:

- локальную и сетевую загрузку ОС с внешних носителей информации;
- автоматическое обнаружение с последующей возможностью ручного выбора средств ядра для поддержки оборудования, входящего в состав или обслуживаемого компьютером;
- выбор и подготовку носителей устройства для размещения компонентов ОС;
- установку компонентов ОС на устройство;
- предварительную настройку основных компонентов ОС;
- поддержку полуавтоматического и автоматического (с минимальным участием пользователя) режимов установки и настройки ОС;
- управление составом компонентов ОС в процессе ее функционирования.

При локальной загрузке с внешнего носителя требуется поддержка от BIOS целевого компьютера возможности выбора данного типа носителя в качестве загрузочного.

Для сетевой загрузки необходима поддержка протокола PXE сетевым интерфейсом целевого компьютера и наличие сетевого сервера с настроенными службами TFTP, BOOTP, FTP или HTTP.

3.1.3. Системные и сервисные утилиты

Системные и сервисные утилиты обеспечивают:

- первоначальную инициализацию системы;
- работу с файлами;
- поддержку учетных записей пользователей и групп;
- планирование;
- работу с печатающими устройствами;
- работу с сетевыми службами;
- поддержку отказоустойчивого режима работы;
- поддержку русской раскладки клавиатуры;
- работу с текстовыми файлами;
- интерпретацию команд;
- выдачу пользовательских инструкций.
- задание, управление, просмотр мандатных атрибутов доступа в файловом менеджере;

- регистрацию выдачи документов на печать;
- контроль целостности мандатных атрибутов объектов ФС.

3.1.4. Базовые сетевые службы

Сетевые службы предназначены для выполнения определенных функций в рамках базовых сетевых протоколов.

Стек протоколов TCP/IP — набор сетевых протоколов разных уровней модели сетевого взаимодействия.

DHCP — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

DNS — распределенная система для получения информации о доменах. Используется для получения IP-адреса по имени хоста (компьютера или устройства), информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

FTP — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

TFTP — используется для первоначальной загрузки бездисковых рабочих станций. TFTP не содержит возможностей аутентификации (хотя возможна фильтрация по IP-адресу) и основан на транспортном протоколе UDP.

SMTP — сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

IMAP — протокол прикладного уровня для доступа к электронной почте.

HTTP — протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер». Обмен сообщениями идет по обыкновенной схеме: «запрос-ответ». Для идентификации ресурсов HTTP используют глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния.

NTP — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

SSH — сетевой протокол сеансового уровня, позволяющий производить удаленное управление ОС и туннелирование TCP-соединений (например, для передачи файлов).

NFS — протокол сетевого доступа к ФС. Основан на протоколе вызова удаленных процедур (ONC RPC, RFC 1057, RFC 1831). Позволяет подключать (монтировать) удаленные ФС через сеть.

SMB — сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия.

LDAP — сетевой протокол прикладного уровня для доступа к службе каталогов X.500, обеспечивающей централизованное хранение информации, организованной в иерархической древовидной форме.

Kerberos — сетевой протокол аутентификации, позволяющий передавать данные через незащищенные сети для безопасной идентификации. Технология Kerberos позволяет обеспечить доверенную сквозную аутентификацию.

3.1.5. Средства организации ЕПП

Для организации домена в состав ОС входят средства создания ЕПП, которые обеспечивают:

- сквозную аутентификацию в сети;
- централизацию хранения информации об окружении пользователей;
- централизацию хранения настроек системы защиты информации на сервере;
- интеграцию в домен защищенных серверов: СУБД, маркировки документов, выводимых на печать, CUPS, электронной почты Dovecot, Exim и гипертекстовой обработки данных Apache;
- централизованный аудит событий безопасности в рамках домена.

Сетевая аутентификация и централизация хранения информации об окружении пользователя используют два основных механизма: поддержки кросс-платформенных серверных приложений для обеспечения безопасности NSS и PAM.

Для реализации удаленной аутентификации в качестве источника данных для базовых системных служб на основе механизмов NSS и PAM используется служба каталогов LDAP. В результате вся служебная информация пользователей сети может располагаться на выделенном сервере в распределенной гетерогенной сетевой среде. Добавление новых сетевых пользователей в этом случае производится централизованно на сервере службы каталогов.

Администратор сети может централизованно управлять конфигурацией сети, включая разграничение доступа к сетевым службам. Благодаря предоставлению информации LDAP в иерархической древовидной форме разграничение доступа в рамках службы каталогов LDAP может быть основано на введении доменов. В качестве домена в данном случае будет выступать поддерево службы каталогов LDAP. Служба каталогов LDAP позволяет разграничивать доступ пользователей к разным поддеревьям каталога, хотя по умолчанию в ОС реализуется схема одного домена.

Для обеспечения сквозной доверенной аутентификации используется технология Kerberos.

Централизация хранения информации об окружении пользователей предоставляет возможность для централизованного хранения домашних каталогов пользователей. Для этого используется сетевая защищенная файловая система (СЗФС), работающая по

протоколу SMB/CIFS. Протокол СЗФС содержит в себе сообщения, которые передают информацию о мандатных атрибутах (атрибутах безопасности), а также сообщения для передачи метки безопасности субъекта доступа.

СЗФС состоит из сервера и клиента. Сервер представляет собой расширенный сервер Samba и выполняет следующие задачи:

- управление разделяемыми ресурсами;
- контроль доступа к разделяемым ресурсам на основе информации о полномочиях клиента и его мандатных атрибутах.

Клиент представляет собой сетевую ФС в составе системы управления файлами ядра ОС и реализует интерфейс между виртуальной ФС ядра и сервером СЗФС. Клиент СЗФС выполняет следующие задачи:

- отображение каталогов и файлов смонтированного сетевого ресурса;
- передача на сервер дополнительной информации о классификационной метке пользователя (процесса), работающего с разделяемым ресурсом.

В среде ОС пользователю поставлен в соответствие ряд атрибутов, характеризующих его права доступа. Концепция ЕПП подразумевает хранение системной информации о пользователе (включая доступные уровни и категории конфиденциальности и уровни целостности) централизованно. В данном случае вся информация хранится в службе каталогов LDAP.

Для управления ЕПП в ОС используется программное обеспечение FreeIPA, являющееся надстройкой над технологиями LDAP, Kerberos, CIFS и обеспечивающее автоматическую настройку всех необходимых файлов конфигурации служб, реализующих перечисленные технологии, а также предоставляет интерфейс управления и администрирования.

Настройка окружения пользователя при входе в систему обеспечивается PAM-модулем, который выполняет следующие функции:

- получение параметров окружения пользователя с сервера домена;
- проверка возможности входа пользователя на данный компьютер по списку разрешенных пользователю компьютеров;
- проверка возможности использования пользователем типа ФС его домашнего каталога;
- настройка параметров окружения пользователя;
- монтирование домашнего каталога пользователя;
- включение доменного пользователя в заданные локальные группы.

Для управления службой FreeIPA и администрирования ЕПП предназначены инструменты командной сроки `astra-freeipa-server` и `astra-freeipa-client`, а также графические утилиты `fly-admin-freeipa-server` и `fly-admin-freeipa-client`.

3.1.6. Программы защищенной графической подсистемы

В качестве программ защищенной графической подсистемы используется графический сервер Xorg и оконный менеджер Fly.

Xorg — оконная система, обеспечивающая стандартные инструменты и протоколы для построения графического интерфейса пользователя.

Fly — полнофункциональный рабочий стол, который состоит из оконного менеджера (`fly-wm`) и набора пользовательских и административных графических утилит.

Дополнительно к своим стандартным функциональным возможностям графическая подсистема обеспечивает:

- корректную работу в рамках мандатного управления доступом;
- визуальную индикацию уровней и категорий конфиденциальности и уровней целостности.

3.1.7. Средства резервного копирования и восстановления данных

Средства резервного копирования и восстановления данных обеспечивают надежное функционирование ОС.

В качестве программы для резервного копирования используется Bacula.

Она обеспечивает поддержку сохранения расширенных атрибутов каталогов и файлов и, при необходимости, их последующее восстановление.

Bacula — сетевая клиент-серверная система резервного копирования и восстановления данных, которая позволяет сохранять данные с компьютеров сети на устройства записи (например, на жесткие или DVD-диски), а также искать и восстанавливать утерянные данные.

Компоненты системы такие как: управляющий директор, СУБД, сервер хранения, сервер доступа к ФС, монитор и консоль — выделены в отдельные процессы (могут быть в нескольких экземплярах) и расположены в различных узлах сети. При этом сохраняется возможность единой точки управления и мониторинга. Компоненты могут быть разнесены в нужные места сети или удаленных сетей.

Процесс резервирования автоматизирован с помощью единого планировщика. Возможно параллельное выполнение нескольких заданий, включая запись в один том.

В системе имеется отдельная процедура резервного копирования с целью восстановления «с нуля». При этом восстанавливаются не только данные, но и большая часть системной информации (разбиение на разделы, LVM).

Основным интерфейсом программы является командная строка, также имеется графический интерфейс.

В системе есть собственная система аутентификации и авторизации для администраторов с возможностью разбивки по ролям и областям ответственности, учет действий пользователей.

Средства программы Bacula обеспечивают возможность сохранения параметров меток безопасности при резервном копировании и восстановлении.

Команды `tar`, `cpio`, `gzip` представляют собой традиционные инструменты создания резервных копий и архивирования ФС. При создании архива командами `tar` и `gzip` передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно.

При создании архива с помощью команды `cpio` ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов ОС, поименованные каналы и т. п.).

3.1.8. Средства управления программными пакетами

В ОС используются программные пакеты (далее по тексту — пакеты) с расширением `.deb`. Для управления пакетами в режиме командной строки (или в эмуляторе терминала в графическом режиме) предназначены набор команд нижнего уровня `dpkg` и комплекс программ высокого уровня `apt-get`, `apt-cache` и `aptitude`. В графическом режиме управлять пакетами можно с помощью программы Synaptic (универсальная графическая оболочка для `apt`).

По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами (за исключением некоторых случаев получения информации о пакетах) необходимы права администратора.

Средства управления пакетами обеспечивают возможность автоматизированной установки обновлений ОС.

3.2. Защищенный комплекс программ печати и маркировки документов

Служба печати из состава ОС позволяет осуществлять печать документов в соответствии с требованиями, предъявляемыми к защищенным ОС.

В ОС используется защищенный комплекс программ печати на базе доработанного сервера печати CUPS. Комплекс обеспечивает:

- управление заданиями на печать;
- выполнение команд администратора (пользователя из группы, указанной в значении параметра `SystemGroup` в файле `/etc/cups/cups-files.conf`);

- предоставление информации о состоянии принтеров локальным и удаленным программам;
- выдачу информационных сообщений пользователям.

При поступлении задания на печать считывается метка безопасности сетевого соединения и копируется в атрибут задания. Если метка безопасности задания является нулевой, то печать выполняется без маркировки.

Если метка безопасности задания ненулевая, но не входит в множество разрешенных меток для данного принтера, заданных атрибутами `mac-printer-mac-min` и `mac-printer-mac-max`, то задание не принимается и возвращается ошибка.

Если метка безопасности задания ненулевая и входит в множество разрешенных меток для принтера, то задание принудительно переводится в состояние «отложено», в котором ожидается маркировка. Задание, подлежащее маркировке, блокируется для использования другими пользователями.

Маркировка печатных листов осуществляется «наложением» маркеров с атрибутами задания, включающими:

- уровень конфиденциальности документа;
- номер экземпляра;
- количество листов в экземпляре;
- дату вывода документа на печать;
- номер каждого входящего документа;
- имя исполнителя;
- имя пользователя, производившего печать на станции печати.

При выполнении маркировки проводится проверка наличия атрибутов задания `copies` и `job-name` и при их отсутствии они присваиваются с помощью стандартного запроса `Set-Job-Attributes`. Затем с помощью запроса `MAC-Get-Info` выполняется получение списка переменных маркировки, указанных в качестве значения атрибута `mac-marker-vars`, и на основе полученного списка запрашиваются значения переменных маркировки у пользователя. Полученные значения переменных маркировки присваиваются в качестве атрибутов задания с помощью запроса `MAC-Set-Job-Attributes`. После присвоения всех атрибутов выполняется маркировка с помощью запроса `MAC-Mark-Document`. Документ, подлежащий маркировке, из своего формата преобразуется в PostScript с помощью цепочки фильтров, которая строится динамически. Для задания создается файл с переменными маркировки, включающими атрибуты задания, данные пользователя и др. Дополнительно, если был отправлен на печать документ в формате PDF, запускается исполняемый модуль `pdfhelper` для определения формата и ориентации PDF-документов и добавления в файл с переменными маркировки соответствующих сведений.

Для маркируемого документа с использованием исполняемых модулей `fonarik` и `psmarker` на основе PostScript-файла оригинального задания, файла с переменными маркировки и шаблона маркера создаются маркированный PostScript-файл основного документа и PostScript-файл «фонарика». Затем промаркированные PostScript-файлы преобразуются в PDF и для них создаются два унаследованных задания на печать (маркированный документ и «фонарик»).

Выполнить печать маркированных документов может пользователь, имеющий соответствующие полномочия.

Переменные маркировки и шаблон маркера может быть изменен администратором.

Реализованное решение представляет настраиваемый механизм маркировки, инвариантный к типу входных данных и модели принтера.

3.3. Защищенный комплекс программ гипертекстовой обработки данных

Защищенный комплекс программ гипертекстовой обработки данных — это программное обеспечение (ПО), осуществляющее взаимодействие по HTTP-протоколу между сервером и браузерами: прием запросов, поиск указанных файлов и передача их содержимого, выполнение приложений на сервере и передача клиенту результатов их выполнения. Комплекс представлен web-севером Apache2 и браузерами Firefox и Chromium.

Возможности защищенного комплекса программ гипертекстовой обработки данных:

- интеграция с ядром ОС и системными компонентами для обеспечения мандатного управления доступом;
- реализация мандатного управления доступом к файлам, содержащим гипертекстовую информацию и скрипты, на основе классификационных меток;
- регистрация попыток доступа к файлам, содержащим гипертекстовую информацию и скрипты.

3.4. Защищенная СУБД

В качестве защищенной СУБД в составе ОС используется СУБД «Тантор» (в исполнении Basic), доработанной в соответствии с требованием интеграции с ОС в части защиты информации, в том числе мандатного управления доступом (реализована с использованием СУБД PostgreSQL).

СУБД предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным.

СУБД построена на основе открытой архитектуры и поддерживает большинство современных технологий организации, хранения и управления данными на основе реляционной модели, включая стандартные и расширенные инструкции SQL, хранимые процедуры, вложенные запросы, управление транзакциями, расширенный состав типов хранимых

данных и использование типов, определенных пользователем. Помимо этого, СУБД обеспечивает хранение и работу с XML документами и поддерживает полнотекстовый поиск.

Входящий в состав СУБД набор программных средств позволяет решать следующие задачи:

- управление схемами данных и самими данными, хранящимися в СУБД;
- поддержка конфиденциальности хранимых данных;
- поддержка целостности хранящихся данных;
- контроль функционирования СУБД и входящих в нее СЗИ;
- обеспечение средств копирования и восстановления БД;
- предоставление прикладных программных интерфейсов.

Возможности защищенной СУБД:

- автоматическая маркировка создаваемых объектов БД, отражающая уровень их конфиденциальности;
- регистрация попыток доступа к объектам БД;
- регистрация действий по изменению правил разграничения доступа к объектам БД.

ПО СУБД основано на архитектуре «клиент-сервер» и содержит все необходимые компоненты для решения поставленных задач, а именно:

- сервер СУБД;
- набор утилит администрирования для поддержки целостности, контроля функционирования, обеспечения резервного копирования и восстановления БД, средства управления схемами данных;
- набор прикладных программных интерфейсов для доступа к БД из прикладных программ и расширения возможностей сервера.

Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц существуют другие объекты БД (виды, процедуры и т. п.), которые предоставляют доступ к данным, хранящимся в таблицах.
П р и м е ч а н и е. Корректная работа с СУБД предполагает использование механизма ЕПП.

СУБД состоит из следующих компонентов:

- `postgresql` — сервисная служба, реализующая непосредственно сервер БД;
- `libpq` — клиентская библиотека, предоставляющая доступ к серверу СУБД;
- набор серверных утилит для управления работой сервера и создания кластеров БД;
- набор клиентских утилит для создания и управления БД.

Для работы СУБД на диске выделяется область для хранения БД, называемая кластером БД. Кластер БД управляется одним экземпляром сервера СУБД. Настройка работы отдельного экземпляра сервера СУБД также определяется в рамках кластера соответствующими конфигурационными файлами.

Более подробное описание СУБД приведено в документе РУСБ.10015-01 97 01-3 «Операционная система специального назначения «Astra Linux Special Edition MIPS». Руководство по КСЗ. Часть 3».

3.5. Защищенный комплекс программ электронной почты

В качестве защищенного комплекса программ электронной почты используется сервер электронной почты, состоящий из агента передачи электронной почты Exim4, агента доставки электронной почты Dovecot и клиента электронной почты Thunderbird.

Возможности защищенного комплекса программ электронной почты:

- интеграция с ядром ОС и базовыми библиотеками для обеспечения разграничения доступа;
- реализация мандатного управления доступом к почтовым сообщениям;
- автоматическая маркировка создаваемых почтовых сообщений, отражающих уровень их конфиденциальности;
- регистрация попыток доступа к почтовым сообщениям.

Защищенный комплекс программ электронной почты состоит из следующих компонентов:

- агент передачи сообщений Exim4;
- агент доставки сообщений Dovecot;
- клиент электронной почты Mozilla Thunderbird.

Агент передачи электронной почты использует протокол SMTP и обеспечивает решение следующих задач:

- доставку исходящей почты от авторизованных клиентов до сервера, который является целевым для обработки почтового домена получателя;
- прием и обработку почтовых сообщений доменов, для которых он является целевым;
- передачу входящих почтовых сообщений для обработки агентом доставки электронной почты.

Агент доставки электронной почты предназначен для решения задач по обслуживанию почтового каталога и предоставления удаленного доступа к почтовому ящику по протоколу IMAP (протокол POP3 отключен). Серверная часть в защищенном исполнении использует в качестве почтового хранилища MailDir.

Клиент электронной почты — прикладное ПО, устанавливаемое на рабочем месте пользователя и предназначенное для получения, написания, отправки и хранения сообщений электронной почты пользователя.

3.6. Пакет офисных программ

Пакет офисных программ LibreOffice предоставляет инструменты для решения всех типов офисных задач, таких как написание текстов, работа с электронными таблицами и создание графических объектов и презентаций.

LibreOffice состоит из шести компонентов:

- Текст LibreOffice — текстовый редактор и редактор web-страниц;
- Таблица LibreOffice — редактор электронных таблиц;
- Презентация LibreOffice — средство создания и демонстрации презентации;
- Рисунок LibreOffice — векторный редактор;
- Математика LibreOffice — редактор для создания и редактирования формул.

Также к офисным средствам относятся: текстовый редактор Kate, просмотрщик PDF-файлов Okular, словарь-переводчик GoldenDict и утилита `fly-notes` («Заметки»).

3.7. Алгоритм функционирования

В состав ОС входят программные средства, предназначенные для использования в автоматизированных системах. Большая часть программ предоставляет функциональные возможности, не связанные с защитой информации от НСД.

Для использования ОС в защищенных автоматизированных системах должны применяться программные средства из состава ОС, реализующие функции по защите информации от НСД. Описание работы и настройки данных программных средств приведено в РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition MIPS». Руководство по КСЗ. Часть 1».

4. ПРОЦЕСС РАЗРАБОТКИ ОС

Разработка ОС производится в замкнутом автоматизированном производственном цикле. Источниками пакетов ОС являются собственные разработки и ПО с открытым исходным текстом.

Собственные разработки в части, касающейся графической подсистемы, СЗИ, комплекса печати и маркировки, программы установки и всех разрабатываемых и дорабатываемых пакетов из состава ОС, ведутся с использованием системы контроля версий GIT на выделенном сервере.

Автоматизированная система формирует репозиторий исходных текстов ОС и производит сборку бинарных пакетов из исходных текстов. Из собранных пакетов формируется бинарный репозиторий, в котором выполняется цифровая подпись библиотек и исполняемых файлов.

В дальнейшем автоматизированная система генерирует образы установочных дисков, производит установку собранной ОС и осуществляет автоматизированное тестирование основных подсистем ОС. Отчеты, полученные в результате тестирования, обрабатываются специалистами и все замечания фиксируются в системе сбора и контроля ошибок Jira.

Схема по организации процесса разработки ОС приведена на рис. 2.

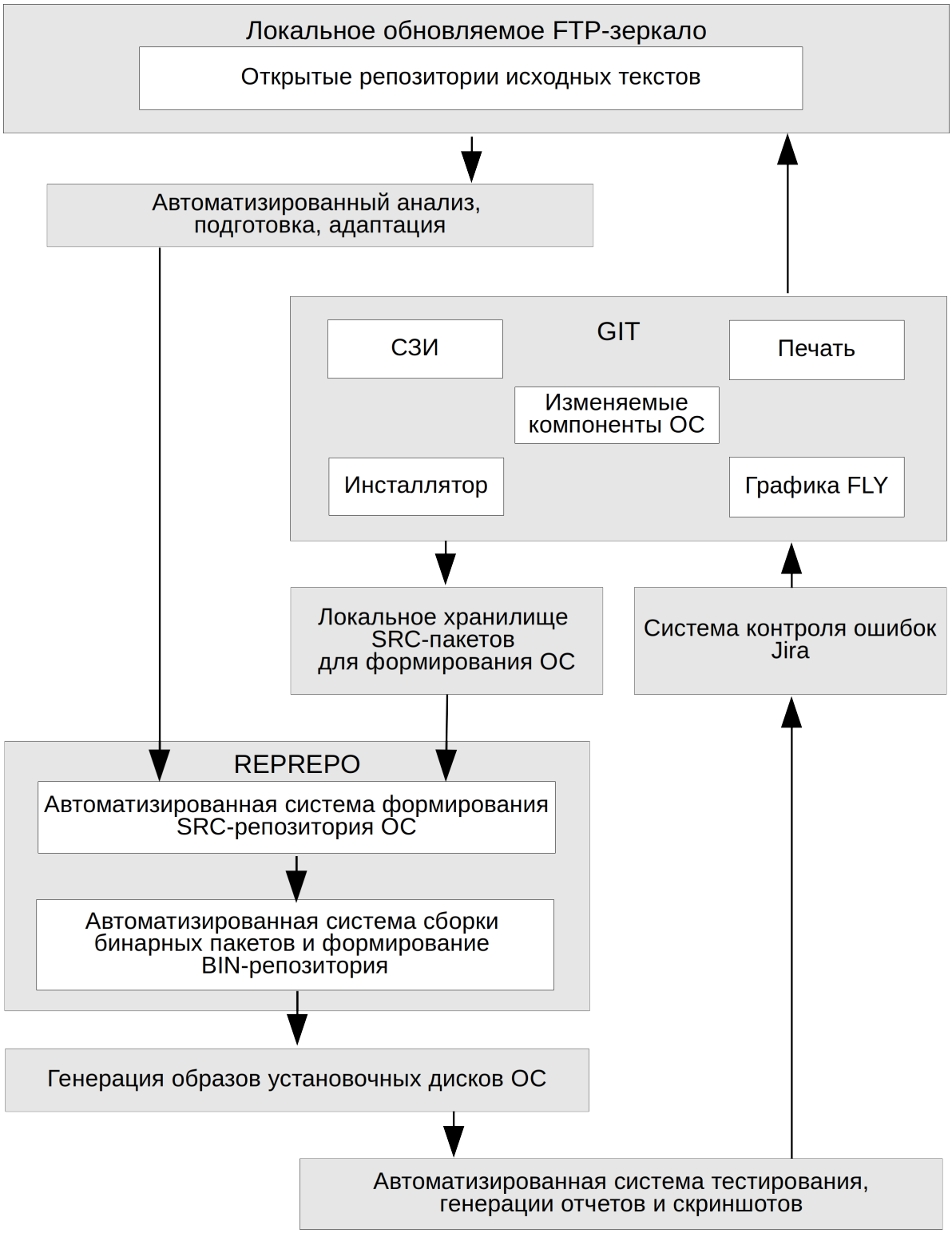
Локальное обновляемое FTP-зеркало
Открытые репозитории исходных текстов
Автоматизированный анализ, подготовка, адаптация
GIT
СЗИ
Печать
Изменяемые компоненты ОС
Инсталлятор
Графика FLY
Локальное хранилище SRC-пакетов для формирования ОС
Система контроля ошибок Jira
REPREPO
Автоматизированная система формирования SRC-репозитория ОС
Автоматизированная система сборки бинарных пакетов и формирование BIN-репозитория
Генерация образов установочных дисков ОС
Автоматизированная система тестирования, генерации отчетов и скриншотов

Рис. 2

5. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

5.1. Для функционирования необходима следующая минимальная конфигурация оборудования:

- аппаратная платформа — процессор с архитектурой x86-64 (AMD, Intel);
- оперативная память — не менее 1218 МБ;
- объем свободного дискового пространства — не менее 12 ГБ.

Для установки с носителя дополнительно требуется:

- стандартный монитор;
- устройство чтения DVD-дисков или USB-интерфейс.

Для установки по сети дополнительно требуется:

- сетевая карта;
- поддержка в UEFI/BIOS возможности установки по сети;
- стандартный монитор (при ручной установке по сети).

6. ВЫЗОВ И ЗАГРУЗКА

6.1. Загрузку ядра ОС в память и передачу ему управления осуществляет системный загрузчик. Вызов системного загрузчика и передачу ему управления выполняет BIOS автоматически после включения компьютера.

7. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

7.1. Входными данными для ОС являются:

- обращение субъектов доступа (процессов и команд) к защищаемым именованным сущностям — файлам (программам, библиотекам, файлам с пользовательской и служебной информацией), каталогам, специальным файлам (устройствам, ссылкам, каналам FIFO и т. п.), БД и их элементам (таблицам, записям, полям записей, триггерам и т. п.), а также средствам IPC (портам, сокетам, семафорам);
- атрибуты, определяющие полномочия субъектов доступа и правила разграничения доступа к сущностям.

7.2. Выходными данными для ОС является результат использования субъектом доступа защищаемой сущности (объекта доступа), предоставленной ему в соответствии с установленными правилами разграничения доступа, либо отказ в предоставлении доступа к сущности в связи с отсутствием соответствующих полномочий и привилегий.

К результатам использования субъектом доступа защищаемой сущности могут относиться:

- запуск программы;
- редактирование файла;
- создание сокетов;
- добавление данных в БД и т. п.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных

ЕПП — единое пространство пользователей

НСД — несанкционированный доступ

ОС — операционная система специального назначения «Astra Linux Special Edition MIPS»

ПО — программное обеспечение

СЗИ — средства защиты информации

СЗФС — сетевая защищенная файловая система

СУБД — система управления базами данных

ФС — файловая система

ACL — Access Control List (список контроля доступа)

ANSI — American National Standards Institute (Американский национальный институт стандартов)

BIOS — Basic Input/Output System (базовая система ввода-вывода)

BOOTP — Bootstrap Protocol (простой протокол динамической конфигурации хоста)

CIFS — Common Internet File System (общий протокол доступа к файлам Интернет)

DHCP — Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)

DNS — Domain Name System (система доменных имен)

FIFO — First-In, First-Out (первым пришел — первым обслужен — дисциплина очереди)

FTP — File Transfer Protocol (протокол передачи файлов)

HTTP — HyperText Transfer Protocol (протокол передачи гипертекста)

IMAP — Internet Message Access Protocol (протокол доступа к сообщениям в сети Интернет)

IP — Internet Protocol (межсетевой протокол)

LDAP — Lightweight Directory Access Protocol (легковесный протокол доступа к сервисам каталогов)

LVM — Logical Volume Manager (менеджер логических томов)

NFS — Network File System (сетевая файловая система)

NSS — Name Service Switch (диспетчер службы имен)

NTP — Network Time Protocol (протокол сетевого времени)

ONC — Open Network Computing (открытая сетевая обработка)

PAM — Pluggable Authentication Modules (подключаемые модули аутентификации)

PXE — Preboot Execution Environment (среда для загрузки компьютеров с помощью сетевой карты без использования жестких дисков, компакт-дисков и других устройств, применяемых при загрузке операционной системы)

RFC — Request For Comments (общее название технических стандартов сети

Интернет)

RPC — Remote Procedure Call (удаленный вызов процедур)

SMB — Server Message Block (блок сообщений сервера)

SMTP — Simple Mail Transfer Protocol (простой протокол электронной почты)

SQL — Structured Query Language (язык структурированных запросов)

SSH — Secure Shell Protocol (протокол защищенной передачи информации)

TCP— Transmission Control Protocol (протокол управления передачей данных)

TFTP — Trivial File Transfer Protocol (простейший протокол передачи файлов)

URI — Uniform Resource Identifier (универсальный идентификатор ресурса)