50 1190 0101

Утвержден

РУСБ.10265-01-УД

Подп. и дата	
Инв. № дубл	
Взам. инв. №	
Подп. и дата	
Инв. № подл	

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Описание применения

РУСБ.10265-01 31 01

Листов 33

2021

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10265-01 (далее по тексту — ОС).

В документе описаны назначение ОС, условия ее применения, описание задачи, приведены входные и выходные данные. Также приведены сведения по получению обновлений ОС.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

ОС предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

1.2. Основные характеристики

В состав ОС входят следующие компоненты:

- ядро ОС;
- средства установки и настройки ОС;
- системные и сервисные утилиты;
- базовые сетевые службы;
- средства организации единого пространства пользователей (ЕПП);
- программы защищенной графической подсистемы;
- средства управления программными пакетами;
- средства резервного копирования и восстановления данных;
- защищенный комплекс программ печати и учета документов;
- защищенный комплекс программ гипертекстовой обработки данных;
- защищенная система управления базами данных;
- защищенный комплекс программ электронной почты;
- пакет офисных программ.

1.3. Возможности

ОС предоставляет следующие возможности:

- установку и функционирование на средствах вычислительной техники с процессорной архитектурой «Эльбрус», а также поддержку периферийного оборудования;
- поддержку основных сетевых протоколов стека TCP/IP;
- организацию сетевого домена с централизованным хранением учетных записей;
- поддержку отказоустойчивого режима работы;
- работу с мультимедийными данными;
- работу с реляционными базами данных;
- работу с электронной почтой;
- работу с гипертекстовыми данными; интеграцию включенных в его состав программ защищенной графической подсистемы, пакета офисных программ и защищенного комплекса программ гипертекстовой обработки данных с дополнительно устанавливаемыми

сертифицированными ФСБ России средствами криптографической защиты конфиденциальной информации[1)] для:

- создания и проверки усиленной квалифицированной электронной подписи;
- криптографического преобразования канала передачи информации по протоколам прикладного уровня стека TCP/IP;
- обработку текстовых документов и электронных таблиц различных форматов.

[1)] Не допускается применение для защиты информации, содержащей сведения, составляющие государственную тайну.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

Для функционирования ОС необходима следующая минимальная конфигурация оборудования:

- аппаратная платформа — процессор с архитектурой Эльбрус-1С+, Эльбрус-8С, Эльбрус-8СВ [1)];
- оперативная память — не менее 1 ГБ;
- объем свободного дискового пространства — не менее 10 ГБ.

Для установки ОС требуется:

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

Для функционирования системы под управлением ОС наличие указанных устройств не обязательно.

2.2. Совместимость с оборудованием

Штатное, предусмотренное документацией, функционирование ОС обеспечивается только на рекомендованном изготовителем ОС совместимом оборудовании. Перечень рекомендуемого к применению оборудования, а также регламент сертификации на совместимость опубликованы на сайте `astralinux.ru`.

2.3. Порядок эксплуатации

Порядок установки, настройки и эксплуатации ОС осуществляется в соответствии с эксплуатационной документацией согласно РУСБ.10265-01 20 01 «Операционная система специального назначения «Astra Linux Special Edition». Ведомость эксплуатационных документов».

Дополнительная информация о порядке эксплуатации, а также варианты реализации отдельных решений с использованием ОС приведены в руководствах `man`, электронной справке из состава ОС и на официальном сайте `wiki.astralinux.ru`.

[1)] Поддержка процессора Эльбрус-8СВ введена оперативным обновлением № 20211019SE81.

3. ПОРЯДОК ОБНОВЛЕНИЯ ОС

В целях обеспечения соответствия изделия требованиям безопасности информации в части устранения недостатков и уязвимостей изделия осуществляется его техническая поддержка, предусматривающая выпуск очередных (плановых) обновлений (новых версий) и выпуск внеочередных (оперативных) обновлений.

3.1. Очередное (плановое) обновление

Очередное (плановое) обновление ОС представляет собой новую версию ОС и решает следующий комплекс задач:

- обеспечение поддержки современного оборудования;
- реализация новых функциональных возможностей программных средств (компонент) из состава ОС;
- устранение ошибок и повышение уровня защищенности;
- повышение удобства использования и управления компонентами ОС.

Лицензиаты (потребители) оповещаются о возможности и порядке получения очередного обновления ОС как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика `astralinux.ru`.

Получение очередного обновления ОС осуществляется установленным порядком при заключении соответствующего лицензионного договора (дополнения к имеющемуся лицензионному договору).

Контроль целостности потребителями очередного обновления ОС (входной контроль) осуществляется посредством подсчета контрольных сумм DVD-дисков. Значения контрольных сумм и порядок их вычисления определены в документе РУСБ.10265-01 30 01 «Операционная система специального назначения «Astra Linux Special Edition». Формуляр».

Дополнительный контроль целостности файлов, входящих в состав очередного обновления ОС, осуществляется:

- регламентно — средствами контроля целостности путем вычисления и сравнения контрольных сумм файлов ОС с эталонными значениями, указанными в файле `gostsums.txt`, размещенном на установочном диске ОС, в соответствии с описанием, приведенном в документе РУСБ.10265-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1»;
- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10265-01 97 01-1.

Доведение очередного обновления ОС до автоматизированных систем в защищенном исполнении Министерства обороны Российской Федерации осуществляется через

уполномоченный орган военного управления Министерства обороны Российской Федерации.

3.2. Внеочередное (оперативное) обновление

При получении сведений о наличии в компоненте ОС уязвимости или недостатка, которая может быть использована для нарушения установленных правил разграничения доступа к информации, разработчик ОС выпускает внеочередное обновление ОС.

Внеочередное обновление ОС может быть доступно в виде:

1) отдельных инструкций, содержащих сведения об обязательных к проведению при эксплуатации ОС организационно-технических мероприятиях;

2) отдельных файлов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ОС;

3) пакетов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ОС;

4) методических указаний по настройке и особенностям эксплуатации ОС с установленным внеочередным обновлением ОС.

Лицензиаты (потребители) оповещаются о возможности и порядке получения внеочередного обновления ОС как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика `astralinux.ru`.

Разработчик установленным порядком организует доведение информации о выпуске внеочередного (оперативного) обновления до ФАУ «ГНИИИ ПТЗИ ФСТЭК России», являющегося оператором Банка данных угроз безопасности информации ФСТЭК России в установленном им формате.

Контроль целостности внеочередных обновлений ОС осуществляется с помощью контрольных сумм, рассчитанных с использованием программ подсчета контрольных сумм `gostsum` (для файлов) и `gostsum_from_deb` (для deb-пакетов) из состава ОС, а также утилиты `vimdiff` из состава ОС.

Дополнительный контроль целостности файлов, входящих в состав внеочередного обновления ОС, осуществляется:

- регламентно — средствами контроля целостности путем вычисления и сравнения контрольных сумм файлов ОС с эталонными значениями, указанными в файле `gostsums.txt`, входящем в состав внеочередного обновления ОС, в соответствии с описанием, приведенном в документе РУСБ.10265-01 97 01-1;

- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10265-01 97 01-1.

Источником внеочередного обновления ОС для информационных (автоматизированных) систем, находящихся в компетенции ФСТЭК России, является соответствующий раздел на официальном сайте разработчика ОС (`astralinux.ru/update`).

Внеочередное обновление ОС, содержащее в том числе информацию об устраненных недостатках и уязвимостях, подписывается усиленной квалифицированной электронной подписью изготовителя.

При распространении обновления по сетям связи его подлинность и целостность подтверждаются путем проверки усиленной квалифицированной электронной подписи изготовителя.

Доведение информации о возможности и порядке получения внеочередного обновления ОС до лицензиатов (потребителей) осуществляется как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на официальном сайте разработчика ОС `astralinux.ru`.

Доведение внеочередного обновления ОС до автоматизированных систем в защищенном исполнении Министерства обороны Российской Федерации осуществляется уполномоченным органом военного управления Министерства обороны Российской Федерации.

Информирование потребителей об окончании производства и (или) поддержки безопасности средства осуществляется с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика, информирование ФСТЭК России — официальным почтовым сообщением не позднее чем за один год до окончания производства и (или) поддержки безопасности средства.

4. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая ОС в процессе своего функционирования, — обеспечение интерфейса для доступа ПО к устройствам вычислительной системы посредством управления устройствами и вычислительными процессами и эффективного распределения вычислительных ресурсов между вычислительными процессами в соответствии с требованиями руководящих документов по обеспечению защиты информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну.

4.1. Классы решаемых задач

Для решения основной задачи функционирования ОС она декомпозируется на следующие классы задач:

- загрузка программ в ОП и управление их выполнением;
- обеспечение многозадачного режима функционирования (одновременного выполнения множества процессов);
- распределение ресурсов вычислительной системы между процессами;
- управление распределением ОП между процессами и организация виртуальной памяти;
- обеспечение доступа к данным на энергонезависимых носителях (НЖМД, оптические диски и пр.), организованным в виде некоторой ФС;
- выполнение по запросу программ низкоуровневых операций (ввод-вывод данных, выделение и освобождение памяти, запуск и завершение программ и т. д.);
- предоставление стандартизованного доступа программ к периферийным устройствам (устройствам ввода-вывода);
- поддержка стеков сетевых протоколов;
- обеспечение многопользовательского режима работы;
- обеспечение пользовательского интерфейса (4.1.1);
- идентификация и аутентификация (4.1.2);
- организация единого пространства пользователей (ЕПП) (4.1.3);
- дискреционное управление доступом (4.1.4);
- мандатное управление доступом (4.1.5);
- организация надежных вычислений (изоляция процессов) (4.1.6);
- обеспечение взаимодействия между процессами (4.1.6);
- регистрация событий безопасности (протоколирование) (4.1.7);
- очистка оперативной и внешней памяти (4.1.8);
- контроль целостности (4.1.9);
- ограничение программной среды (4.1.10);

- создание и проверка ЭП (4.1.11);
- маркировка документов (4.1.12);
- обеспечение работы в отказоустойчивом режиме (4.1.13);
- обеспечение надежного функционирования (4.1.14);
- обеспечение доступа к БД в соответствии с требованиями для разграничения доступа к информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну (4.1.15);
- обеспечение доступа к информации через сервер гипертекстовой обработки данных в соответствии с требованиями для разграничения доступа к информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну (4.1.16);
- обеспечение обмена сообщениями электронной почты в соответствии с требованиями для разграничения доступа к информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну (4.1.17).

4.1.1. Обеспечение пользовательского интерфейса

Решение задачи обеспечения графического пользовательского интерфейса основано на использовании системы X Window, которая имеет архитектуру «клиент-сервер». X-сервер отвечает за взаимодействие с дисплеем и устройствами ввода. Клиенты соединяются с X-сервером локально (с использованием сокетов) или удаленно (TCP/IP).

Для предотвращения реализации угроз нарушения конфиденциальности и целостности информации в обход мандатного управления доступом (4.1.5), в т. ч. с использованием механизмов «копирования-вставки» и «перетаскивания» (copy-paste и drag-and-drop), для переноса информации из секретного документа (окна) в несекретный в графической системе ОС реализован подход на основе полного разделения в соответствии с мандатным контекстом (сочетанием уровня и категорий). Подобный подход означает, что для каждого мандатного контекста запускается собственный X-сервер и, соответственно, графический сеанс. При графическом входе в систему пользователю предлагается в специальном диалоге выбрать мандатный контекст из доступных пользователю уровней и/или категорий. Далее графическая сессия будет выполняться в выбранном мандатном контексте. Одновременно пользователем может быть выполнено несколько входов с разными мандатными контекстами. Сессии изолированы, и передача информации между ними невозможна.

Графическая подсистема ОС все же позволяет внутри графической сессии, выполняемой в определенном мандатном контексте, запускать приложения с иным мандатным контекстом. При этом для предотвращения реализации угроз нарушения конфиденциальности и целостности информации в обход мандатного управления доступом используется специальный модуль-расширение X-сервера — `XPARSEC`. В модуле используется набор

«перехватчиков» («hooks»), предоставляемый встроенным расширением X-сервера — XACE. При получении запросов от клиента «перехватчики» XACE передают управление и параметры в XPARSEC, который анализирует аргументы запросов и в соответствии с установленными правилами разграничения доступа разрешает или запрещает выполнение запросов клиента. В ОС мандатный контекст считывается при каждом запросе клиента.

Для обеспечения возможности работы привилегированного клиента (менеджера окон), которому необходимо выполнять некоторые запросы к X-серверу независимо от мандатного контекста своей метки безопасности, в специальном файле (/etc/X11/trusted) размещается информация с указанием полного пути запуска. При локальном соединении X-сервер получает PID (идентификатор процесса) клиента, определяет путь запуска и привилегии клиента. Менеджер окон может получать метки безопасности окон и на основе реализованного в ОС специального расширения X-протокола выполнять привилегированные операции.

В состав графической подсистемы ОС входит рабочий стол пользователя Fly, интегрированный с внедренными в X-сервер механизмами защиты информации и обеспечивающий отображение:

- мандатного контекста сессии на панели задач;
- мандатного уровня каждого окна;
- мандатного уровня во всех приложениях рабочего стола;
- запуска приложения с разными мандатными контекстами;
- уровня доверенности окна для локальных и удаленных приложений (в удаленном режиме будут цветная рамка, соответствующая метке безопасности, и пунктирная).

Графическая подсистема ОС готова к работе с соблюдением мандатного управления доступом непосредственно после установки ОС без проведения дополнительных настроек.

4.1.2. Идентификация и аутентификация

Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма PAM, который представляет собой набор разделяемых библиотек (модулей), с помощью которых администратор может организовать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования PAM. Сценарии аутентификации описываются в конфигурационных файлах.

Если ОС не настроена для работы в ЕПП (4.1.3), то аутентификация осуществляется с помощью локальной БД пользователей. При использовании ЕПП аутентификация

пользователей осуществляется централизованно по протоколу Kerberos.

В ОС реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хэш-функции по ГОСТ Р 34.11-2012 (ГОСТ Р 34.11-94).

4.1.3. Организация единого пространства пользователей

Решение задачи организации ЕПП (создание домена) обеспечивает:

- сквозную аутентификацию в сети;
- централизацию хранения информации об окружении пользователей;
- централизацию хранения настроек системы защиты информации на сервере;
- интеграцию в домен защищенных серверов СУБД (4.1.15), электронной почты (4.1.17), гипертекстовой обработки данных (4.1.16) и печати (4.1.12);
- централизованную настройку правил регистрации событий безопасности в рамках домена;
- централизованный учет подключаемых устройств.

Сетевая аутентификация и централизация хранения информации об окружении пользователя подразумевает использование двух основных механизмов: поддержки кросс-платформенных серверных приложений для обеспечения безопасности NSS и PAM (см. 4.1.2).

Для реализации удаленной аутентификации используется служба каталогов LDAP в качестве источника данных для базовых системных служб на основе механизмов NSS и PAM. 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. Сетевые службы, поддерживающие возможность аутентификации пользователей, могут вместо локальных учетных записей использовать каталог LDAP. Администратор 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.

Сквозная доверенная аутентификация реализуется технологией Kerberos.

Централизация хранения информации об окружении пользователей подразумевает также и централизованное хранение домашних каталогов пользователей. Для этого используется сетевая защищенная ФС CIFS.

В среде ОС пользователю поставлен в соответствие ряд атрибутов, характеризую-

щих его мандатные права. Концепция ЕПП подразумевает хранение системной информации о пользователе (включая доступные мандатные уровни и категории) централизованно. В данном случае вся информация хранится в службе каталогов LDAP.

Информация о мандатных атрибутах пользователей (4.1.5) хранится локально в соответствующих конфигурационных файлах. При изменении конфигурации системы для использования в сетевом контексте мандатные права пользователей должны переместиться вслед за окружением пользователя (идентификаторы пользователей, групп, домашние каталоги и пр.) в службу каталогов LDAP. Доступ к мандатным атрибутам пользователей осуществляется с использованием программного интерфейса подсистемы безопасности PARSEC. Данный интерфейс позволяет получить из соответствующего конфигурационного файла информацию об источнике данных для мандатных СЗИ системы. По умолчанию используются локальные текстовые файлы. При работе ОС в сетевом контексте в качестве источника данных выступает служба каталогов LDAP. Переключение контекста производится путем правки соответствующего конфигурационного файла.

Для управления ЕПП в ОС включены службы ALD и FreeIPA, которые отличаются уровнями развертывания и масштабирования. Они базируются на технологиях LDAP, Kerberos и Samba, предоставляют графические интерфейсы управления и администрирования и автоматизированную настройку всех необходимых файлов конфигурации входящих в них служб.

4.1.4. Дискреционное управление доступом

В ОС механизм дискреционного управления доступом обеспечивает проверку дискреционных ПРД, формируемых в виде базовых ПРД ОС семейства Linux и представленных в виде идентификаторов субъектов (идентификатор пользователя (UID) и идентификатор группы (GID)), имеющих доступ к сущностям (чтение, запись, исполнение). Кроме того, для формирования дискреционных ПРД в ОС используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux.

В состав ОС входят защищенные комплексы программ: СУБД, электронной почты и гипертекстовой обработки данных.

В защищенных комплексах программ электронной почты и гипертекстовой обработки данных защищаемыми сущностями являются сущности ФС. Таким образом, дискреционное управление доступом к ним обеспечивается также, как и к прочим сущностям ФС.

4.1.5. Мандатные управление доступом и контроль целостности

Механизмы мандатного управления доступом и мандатного контроля целостности реализованы в ядре ОС и затрагивают следующие подсистемы:

- механизмы IPC;

- стек TCP/IP (IPv4);
- ФС ext2/ext3/ext4;
- сетевые ФС CIFS;
- ФС proc, tmpfs.

В механизме мандатного управления доступом определены следующие термины:

- субъект мандатного доступа — тот, кто выполняет операции, подлежащие мандатному контролю (пользователь или процесс);
- сущность (объект) мандатного доступа — то, с чем выполняются операции, подлежащие мандатному контролю (файл, каталог и т.д.);
- контейнер — структурированная сущность доступа, т.е. сущность (каталог ФС), которая может содержать другие сущности доступа (каталоги или файлы).

Сущностям и субъектам присваиваются следующие мандатные атрибуты:

- иерархический уровень конфиденциальности (уровень конфиденциальности) — определяет степень секретности документа (сущности) и соответствующий уровень доступа к этому документу, назначенный персоналу (субъекту). Субъекту с определенным уровнем конфиденциальности разрешено читать только документы с таким же уровнем конфиденциальности или ниже и запрещено читать документы с более высоким уровнем конфиденциальности. А также персоналу с более высоким уровнем конфиденциальности запрещено передавать (преднамеренно или случайно) документы высокого уровня конфиденциальности персоналу с более низким уровнем конфиденциальности;
- неиерархическая категория конфиденциальности (категории конфиденциальности) — разделение по категориям конфиденциальности. Персонал, работающий с первой категорией конфиденциальности, имеет соответствующую категорию конфиденциальности. При этом, не имея вторую категорию конфиденциальности, персонал не может иметь доступ к материалам второй категории конфиденциальности, а также не может передавать материалы первой категории конфиденциальности персоналу, не имеющему первую категорию конфиденциальности. Доступ может быть предоставлен одновременно к нескольким категориям конфиденциальности;
- уровень целостности (неиерархический уровень целостности и иерархический (линейный) уровень целостности) — субъект, работающий на некотором уровне целостности, может записывать (изменять) только сущности своего или более низкого уровня целостности. Иерархический уровень целостности в ОС зарезервирован, и на уровне пользователя не поддерживается его использование;
- дополнительные мандатные атрибуты управления доступом — являются необязательными атрибутами и позволяют уточнять или изменять правила мандатного

доступа для отдельных контейнеров, субъектов или сущностей.

Мандатные атрибуты субъекта/сущности объединяются в мандатный контекст этого субъекта/сущности.

Путем использования уровней и категорий конфиденциальности обеспечивается защита от несанкционированного доступа к информации в части:

1) невозможности прочитать информацию, к которой не предоставлен доступ:
   а) нижним уровням конфиденциальности запрещено читать информацию с верхних уровней конфиденциальности;
   б) всем запрещено читать информацию, на которую нет разрешенной категории конфиденциальности;
2) невозможности передать информацию тому, кому не предоставлен доступ:
   а) верхним уровням конфиденциальности запрещено записывать свою информацию на нижние уровни конфиденциальности;
   б) всем запрещено передавать информацию тем, у кого нет соответствующей категории конфиденциальности.

Принятие решения о запрете или разрешении доступа субъекта к сущности принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности субъекта и мандатного контекста безопасности сущности.

Реализация мандатного управления доступом и мандатного контроля целостности в ОС описана в документе РУСБ.10265-01 97 01-1.

Система Linux-привилегий ОС, предназначенная для передачи отдельным пользователям прав выполнения определенных административных действий, расширена PARSEC-привилегиями. Данные привилегии относятся к системе PARSEC и обеспечивают работу с механизмом мандатного управление доступом.

PARSEC-привилегии наследуются процессами от своих «родителей». Процессы, запущенные от имени суперпользователя, независимо от наличия у них привилегий, имеют возможность осуществлять все перечисленные привилегированные действия. Перечень и описание PARSEC-привилегий приведены в РУСБ.10265-01 97 01-1.

В качестве основной сетевой ФС используется CIFS, которая является расширением SMB и поддерживает атрибуты ФС UNIX и имеет ограниченную поддержку расширенных атрибутов. Данная ФС широко распространена и работает в гетерогенных сетях (поддерживается многими ОС), а также поддерживает аутентификацию средствами PAM и Kerberos (см. 4.1.2).

Взаимодействие при помощи сетевого протокола IPv4 (IPv6) осуществляется через программный интерфейс сущностей доступа, являющихся элементами межпроцессного и сетевого взаимодействия (например, сетевых сокетов), которые обеспечивают обмен

данными между процессами в рамках одной или нескольких ОС, объединенных в локальную вычислительную сеть.

Для поддержки мандатного уравления доступом в сетевые пакеты протокола IPv4 (IPv6) внедряются классификационные метки. Порядок присвоения классификационных меток и их формат соответствует национальному стандарту ГОСТ Р 58256-2018. Прием сетевых пакетов подчиняется мандатным ПРД. Следует отметить, что метка сокета может иметь тип, позволяющий создавать сетевые сервисы, принимающие соединения с любыми уровнями секретности.

При необходимости для обеспечения целостности заголовка IP-пакетов, содержащего классификационную метку, допускается применение программного средства OpenVPN. Описание использования OpenVPN приведено в документе РУСБ.10265-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1».

Отсутствие метки на сущности доступа эквивалентно нулевой метке безопасности. Таким образом, ядро ОС, в которой все сущности и субъекты доступа имеют уровень секретности «несекретно», функционирует аналогично стандартному ядру ОС Linux.

Для ряда сетевых сервисов (сервера LDAP, DNS, Kerberos и т. д.) необходимо обеспечить возможность их работы с клиентами, имеющими разный мандатный контекст безопасности, без внесения изменений в исходные тексты сервиса.

Обеспечение мандатного управления доступом в защищенных комплексах программ гипертекстовой обработки данных (см. 4.1.16) и электронной почты (см. 4.1.17) реализовано на основе программного интерфейса библиотек подсистемы безопасности PARSEC. На серверах комплексов программ гипертекстовой обработки данных и электронной почты при обработке запросов на соединение выполняется получение мандатного контекста соединения, унаследованного от субъекта (процесса). Сокет сервера, ожидающий входящих запросов на соединение, работает в контексте процесса, имеющего привилегию для приема соединений с любыми уровнями секретности.

После установки соединения и успешного прохождения процедуры идентификации и аутентификации пользователя процесс сервера, обрабатывающий запросы пользователя, переключается в контекст безопасности пользователя, сбрасывает привилегии, обрабатывает запросы пользователя и завершается.

В комплексе программ гипертекстовой обработки данных пользователь получает доступ к ресурсам, являющимся сущностями ФС. Комплекс программ электронной почты использует технологию maildir, обеспечивающую хранение почтовых сообщений в виде отдельных сущностей ФС. Создаваемые файлы почтовых сообщений маркируются метками безопасности, унаследованными от процесса-создателя. Таким образом, в обоих комплексах

программ ресурсы, к которым осуществляется доступ от имени серверных процессов, обрабатывающих запросы пользователей, являются сущностями ФС. Следовательно, доступ к защищаемым ресурсам при приеме и обработке запросов пользователей в процессе функционирования серверов комплексов программ гипертекстовой обработки данных и электронной почты подчиняется мандатным ПРД.

4.1.6. Изоляция процессов

Ядро ОС обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и работает процессор) преобразуются в разные физические для разных адресных пространств. Процесс не может несанкционированным образом получить доступ к пространству другого процесса, т. к. непривилегированный пользовательский процесс лишен возможности работать с физической памятью напрямую.

Механизм разделяемой памяти является санкционированным способом получить нескольким процессам доступ к одному и тому же участку памяти и находится под контролем дискреционных и мандатных ПРД.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной защиты. Страницы пространства ядра являются привилегированными, и доступ к ним из непривилегированного кода вызывает исключение процессора, которое обрабатывается корректным образом ядром ОС. Единственным санкционированным способом доступа к ядру ОС из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

4.1.7. Регистрация событий безопасности

В ОС реализована расширенная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы с использованием сервиса `parlogd`.

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования. Данный программный интерфейс применен для регистрации событий в СУБД PostgreSQL (4.1.15.3).

4.1.8. Очистка оперативной и внешней памяти

Решение задачи очистки ОП основано на архитектуре ядра ОС, которое гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено ПРД. Это означает, что средства взаимодействия между процессами

контролируются с помощью ПРД, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Решение задачи очистки памяти на внешних носителях основано на реализации механизма, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа названного механизма снижает скорость выполнения операций удаления и усечения размера файла. Механизм является настраиваемым и позволяет обеспечить работу ФС ОС (Ext2/Ext3/Ext4/XFS) в одном из следующих режимов:

- данные любых удаляемых/урезаемых файлов в пределах заданной ФС предварительно очищаются маскирующей последовательностью;
- данные ФС освобождаются обычным образом (без предварительного маскирования).

Режим работы ФС может быть выбран администратором ОС и задан в виде параметра монтирования ФС.

Кроме того, в ОС реализован механизм включения очистки активных разделов страничного обмена.

4.1.9. Контроль целостности

Решение задач контроля целостности основано на использовании библиотеки `libgost`, в которой реализованы функции хэширования в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. Данная библиотека используется в средствах контроля целостности дистрибутива и средствах контроля целостности ФС.

Контроль целостности дистрибутива обеспечивается методом расчета его контрольной суммы и сравнения полученного значения с эталонным значением контрольной суммы.

Контроль целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств, который предоставляет возможность периодического (с использованием системного планировщика заданий `cron`) вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки `libgost` и контроль целостности связанных с файлами атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования).

4.1.10. Ограничение программной среды

4.1.10.1. Замкнутая программная среда

Инструменты замкнутой программной среды (ЗПС) предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав

устанавливаемого СПО, и в расширенные атрибуты файловой системы.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС `digsig_verif`, который является не выгружаемым модулем ядра Linux и может функционировать в одном из следующих режимов:

1) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

2) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в СПО);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС `digsig_verif` и может функционировать в одном из следующих режимов:

1) запрещается открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП;

2) открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой системы);

3) ЭЦП при открытии файлов не проверяется.

4.1.10.2. Системные ограничения и блокировки

Дополнительно в ОС реализованы механизмы, позволяющие устанавливать системные ограничения и блокировки действий пользователя. Основными механизмами блокировки являются:

- запрет установки бита исполнения;
- блокировка консоли для пользователей;
- блокировка интерпретаторов;
- блокировка макросов;
- блокировка трассировки ptrace;
- блокировка клавиш SysRq.

Полный перечень ограничивающих функций безопасности и их описание приведены в РУСБ.10265-01 97 01-1

4.1.11. Сервис электронной подписи

Возможность создания и проверки усиленной квалифицированной электронной подписи (сервис электронной подписи (СЭП)) обеспечивается использованием комплекса

программ защищенной графической подсистемы и пакета офисных программ, интегрированных с дополнительно устанавливаемыми сертифицированными ФСБ России средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, не содержащей сведения, составляющие государственную тайну.

ВНИМАНИЕ! СЭП предоставляется программами, функционирующими в условиях политики разграничения доступа, не допускающей их применение совместно с СКЗИ в режиме обработки сведений, составляющих государственную тайну.

ВНИМАНИЕ! Эксплуатация СКЗИ в составе информационных систем должна осуществляться в соответствии с правилами пользования СКЗИ и указаниями, определенными в формуляре (или иных эксплуатационных документах) на СКЗИ.

СЭП обеспечивает создание и проверку ЭП электронных документов в соответствии с ГОСТ Р 34.10-2012. Предоставление пользователю СЭП осуществляется путем вызова соответствующих пунктов основного меню рабочего стола и меню файлового менеджера `fly-fm` с последующим формированием запросов к СКЗИ для создания и проверки ЭП.

4.1.12. Маркировка документов

Решение задачи маркировки документов при выводе на печать основано на использовании в ОС защищенного сервера печати CUPS, который обеспечивает маркировку выводимых на печать документов. Мандатные атрибуты автоматически связываются с заданием для печати на основе мандатного контекста получаемого сетевого соединения. Вывод на печать документов без маркировки субъектами доступа, работающими в ненулевом мандатном контексте, невозможен.

Для разрешения серверу CUPS обрабатывать задания печати, формируемые в ненулевом мандатном контексте, необходимо от имени администратора выполнить определенные действия, определяющие возможный мандатный контекст, в котором могут формироваться задания для печати на конкретном принтере.

Маркировка документов осуществляется на основе следующих модифицируемых файлов шаблонов:

- файл шаблона, содержащий информацию об атрибутах маркировки и их положении на странице при печати документа;
- файл шаблона, содержащий информацию об атрибутах маркировки оборота последнего листа документа и их положении на странице при печати пяти и менее экземпляров документа;
- файл шаблона, содержащий информацию об атрибутах маркировки оборота последнего листа документа и их положении на странице при печати более пяти экземпляров документа.

4.1.13. Обеспечение работы в отказоустойчивом режиме

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 информации.

Более подробная информация приведена в документе РУСБ.10265-01 95 01-1.

4.1.14. Обеспечение надежного функционирования

Для решения задачи обеспечения надежного функционирования в ОС реализованы средства резервного копирования и восстановления после сбоев и отказов оборудования.

Средства обеспечения надежного функционирования предоставляют следующие возможности:

- автоматическое выполнение в процессе перезагрузки после сбоя программы проверки и восстановления ФС;
- резервное копирование и восстановление ОС;
- резервное копирование и восстановление СУБД.

Более подробная информация приведена в документах РУСБ.10265-01 95 01-1 и РУСБ.10265-01 97 01-1.

4.1.15. Обеспечение доступа к БД

Решение задачи обеспечения доступа к БД реализовано с использованием защищенного комплекса программ СУБД на основе объектно-реляционной СУБД PostgreSQL, доработанной в соответствии с требованием интеграции с ОС в части мандатного управления доступом к информации и содержащей реализацию ДП-модели управления доступом и информационными потоками. Данная ДП-модель описывает все аспекты дискреционного, мандатного и ролевого управления доступом с учетом безопасности информационных потоков.

4.1.15.1. Дискреционное управление доступом в защищенной СУБД

В качестве защищенной СУБД в составе ОС используется PostgreSQL, доработанная в соответствии с требованием интеграции с ОС в части мандатного управления доступом к информации.

СУБД PostgreSQL является объектно-реляционной. На низком уровне данные хранятся в отношениях (таблицах, видах), и доступ к данным разграничивается в понятиях реляционной СУБД.

Сущности (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.

С каждым типом объектов БД ассоциируется определенный набор типов доступа (возможных операций). Для каждого объекта явно задается список разрешенных для каждого из поименованных субъектов БД (пользователей, групп или ролей) типов доступа (т. е. ACL). И в дальнейшем при разборе запроса к БД осуществляется проверка возможности предоставления доступа субъекта к объекту типа, соответствующего запросу.

В PostgreSQL объектами дискреционного управления доступом могут быть столбцы таблицы, поскольку они однозначно идентифицируются по составному имени таблицы и столбца, т.к. имя столбца внутри таблицы является уникальным.

В то же время отдельная строка таблицы не является однозначно идентифицируемым объектом, и в общем случае дискреционные и любые другие правила разграничения доступа к ней применены быть не могут. Поскольку каждая строка идентифицируется только набором содержимого своих полей, то разработчику потребуется выбрать ту или иную процедуру идентификации строк в БД, например, создание первичного ключа или создание физического уникального идентификатора строки в БД.

Дополнительно для ограничения набора данных, выдаваемых пользователю, можно применять входящую в PostgreSQL систему фильтрации строк (POLICY) под названием ROW LEVEL SECURITY — фильтровать строки, выдаваемые из таблицы указанному пользователю (пользователям) на основании вычисления заданного логического выражения.

В рамках дискреционных ПРД определены следующие операции над таблицами и хранящимися в них данными:

- `SELECT` — чтение данных из таблицы;
- `INSERT` — вставка новых данных в таблицу;
- `DELETE` — удаление некоторых/всех данных в таблице;
- `UPDATE` — изменение данных в таблице;
- `REFERENCES` — использование данных таблицы для внешних ключей;
- `TRIGGER` — создание и назначение для таблицы триггеров;
- `TRUNCATE` — очистка таблицы (удаление всех данных).

Для более гибкой работы с данными в СУБД введены объекты БД СУБД PostgreSQL. Описание объектов БД СУБД PostgreSQ, а также средств управления дискреционными ПРД к данным объектам приведены в документе РУСБ.10265-01 97 01-1.

4.1.15.2. Мандатное управление доступом в защищенной СУБД

В основе механизма мандатного управления доступом лежит управление доступом к защищаемым ресурсам БД на основе иерархических и не иерархических атрибутов доступа. Это позволяет реализовать многоуровневую защиту с обеспечением разграничения доступа пользователей к защищаемым ресурсам БД и управление потоками информации. В качестве иерархических и не иерархических атрибутов доступа при использовании СУБД в ОС используются метки безопасности ОС.

СУБД PostgreSQL не имеет собственного механизма назначения, хранения и модификации меток безопасности пользователей и использует для этого механизмы ОС.

В реляционной модели в качестве структуры, обладающей меткой, необходимо выбрать кортеж, поскольку именно на этом уровне детализации осуществляются операции чтения-записи информации в СУБД. При этом местом хранения метки может быть выбран только сам кортеж, так метка будет неразрывно связана с данными, содержащимися в кортеже. Кроме этого, метка также может быть определена для таких объектов БД, к которым применимы виды доступа на чтение-запись данных, а именно таблицы и виды. В этом случае метки объектов располагаются в записи системной таблицы, непосредственно описывающей защищаемый объект.

В связи с тем, что в PostgreSQL объектами защиты являются столбцы, выполнена реализация мандатных ПРД для столбцов объектов. В этом случае метки безопасности столбцов объектов также располагаются в записи соответствующей системной таблицы, непосредственно описывающей защищаемый столбец. Мандатные ПРД столбцов и самого объекта не могут быть применены одновременно. Режим применения мандатных ПРД только к самому объекту или только к его столбцам может быть задан для каждого объекта в отдельности. Защита на уровне записей может использоваться в любом случае.

При наличии меток безопасности на сам объект, его столбец и непосредственно строку возможны следующие варианты использования мандатных ПРД (на примере таблиц):

- метки безопасности отсутствуют — мандатные ПРД не применяются. В этом случае метка безопасности объекта не установлена, метки безопасности столбцов не установлены, а сам объект создан без защиты строк. СУБД функционирует в штатном режиме защиты с использованием только дискреционных ПРД;
- метками безопасности защищаются только записи. Метка безопасности объекта не установлена, метки безопасности столбцов не установлены, а сам объект создан с защитой строк. Дискреционные ПРД применяются перед выполнением запроса. Мандатные ПРД применяются только на уровне записей. Создание записей разрешено всем субъектам, при этом записи наследуют метку безопасности субъекта. Операции чтения и модификации осуществляются над множествами записей, доступных субъ-

екту по мандатным ПРД. Проверка мандатных ПРД осуществляется после успешного применения дискреционных ПРД, нарушение безопасности не возникает;

- метками безопасности защищается только объект. Метка безопасности объекта установлена, метки безопасности столбцов не установлены, а сам объект создан без защиты строк. Мандатные ПРД применяются только на уровне объекта, все данные, содержащиеся в объекте, рассматриваются как имеющие метку безопасности объекта. Создание записей разрешено субъектам с метками безопасности, над которыми доминирует метка безопасности объекта, при этом записи наследуют метку безопасности субъекта. Операции чтения и модификации осуществляются по мандатным ПРД к объекту. Мандатные ПРД применяются только в случае успешной проверки дискреционных ПРД, которые к столбцам объекта применяются только при отсутствии явного разрешения на доступ к самой таблице;
- метками безопасности защищается объект и его записи. Метка безопасности объекта установлена, метки безопасности столбцов не установлены, а сам объект создан с защитой строк. Аналогично предыдущему варианту создание записей разрешено субъектам с метками безопасности, над которыми доминирует метка безопасности объекта, при этом записи наследуют метку безопасности субъекта. Мандатные ПРД применяются как на уровне объекта, так и на уровне записей. Операции модификации возможны только над данными, имеющими метку безопасности, равную метке безопасности таблицы;
- метками безопасности защищаются столбцы объекта. Метка безопасности объекта не установлена, метки безопасности столбцов установлены, а сам объект создан без защиты строк. При этом мандатные ПРД применяются на уровне столбцов. Субъект может читать из столбцов, над метками безопасности которых доминирует его метка безопасности, вставлять данные в столбцы, чьи метки безопасности доминируют над его, и модифицировать те, чьи метки безопасности равны его метке безопасности. Операции удаления невозможны при наличии разных меток безопасности на столбцы, т. к. операция применяется ко всей строке. Это связано с тем, что операция удаления интерпретируется как последовательное предоставление доступа на чтение и на запись, что возможно только при равенстве меток безопасности субъекта и объекта. В случае, когда столбцы имеют разные метки безопасности, данное условие выполниться не может. Операция удаления доступна только для администратора и пользователей, обладающих привилегиями игнорирования мандатного управления доступом;
- метками безопасности защищаются столбцы и записи объекта. В этом случае метка безопасности объекта не установлена, метки безопасности столбцов установлены,

а сам объект создан с защитой строк. При этом мандатные ПРД применяются как на уровне столбцов, так и на уровне записей. Субъект может вставлять данные в столбцы, чьи метки безопасности доминируют над его, при этом записи наследуют метку безопасности субъекта. Операции чтения и модификации осуществляются над множеством записей, доступных субъекту по мандатным ПРД на записи, и только по столбцам, доступных по мандатным ПРД на столбцы.

Описание применения мандатного разграничения доступа в СУБД PostgreSQL приведено в документе РУСБ.10265-01 97 01-1.

4.1.15.3. Регистрация событий в защищенной СУБД

Решение задачи регистрации событий в защищенной СУБД обеспечивается на основе использования реализованной в ОС расширенной подсистемы протоколирования (см. 4.1.7). Настройка подсистемы регистрации событий в защищенной СУБД обеспечивается конфигурационным файлом `pg_audit.conf` конкретного кластера данных.

В этом конфигурационном файле можно задать списки успешных (success events mask) и неуспешных (failure events mask) типов запросов на доступ, которые будут регистрироваться в журнале СУБД и подсистеме аудита ОС для отдельных пользователей и по умолчанию. Списки типов запросов на доступ задаются в виде шестнадцатеричных чисел, в которых каждому типу запроса соответствует установленный (для регистрируемых запросов) или сброшенный (для не регистрируемых запросов) бит:

- на добавление/изменение/удаление пользователей и групп (`SUBJECT`) соответствует нулевой бит (шестнадцатеричное значение — 1);
- на изменение конфигурации, влияющей на доступ к данным (запрос на изменение значения переменной `ac_session_maclabel`) (`CONFIGURATION`), соответствует первый бит (шестнадцатеричное значение — 2);
- на изменение прав доступа к объектам БД (`RIGHTS`) соответствует второй бит (шестнадцатеричное значение — 4);
- на выборку информации из БД (`SELECT`) соответствует четвертый бит (шестнадцатеричное значение — 10);
- на добавление информации в БД (`INSERT`) соответствует пятый бит (шестнадцатеричное значение — 20);
- на изменение информации в БД (`UPDATE`) соответствует шестой бит (шестнадцатеричное значение — 40);
- на удаление информации из БД (`DELETE`) соответствует седьмой бит (шестнадцатеричное значение — 80);
- на очистку данных (`TRUNCATE`) соответствует восьмой бит (шестнадцатеричное значение — 100);

- на задание колонки таблицы в качестве внешнего ключа (REFERENCES) соответствует десятый бит (шестнадцатеричное значение — 400);
- на добавление триггера к таблице (TRIGGER) соответствует одиннадцатый бит (шестнадцатеричное значение — 800);
- на запуск хранимой процедуры или триггера (EXECUTE) соответствует двенадцатый бит (шестнадцатеричное значение — 1000);
- на использование объекта БД (USAGE) соответствует тринадцатый бит (шестнадцатеричное значение — 2000);
- на создание объектов в БД (CREATE) соответствует шестнадцатый бит (шестнадцатеричное значение — 10000);
- на создание временных объектов в БД (CREATE) соответствует семнадцатый бит (шестнадцатеричное значение — 20000);
- на удаление объектов БД (DROP) соответствует восемнадцатый бит (шестнадцатеричное значение — 40000);
- на изменение объекта БД (ALTER) соответствует девятнадцатый бит (шестнадцатеричное значение — 80000).

Информация о соединении пользователей с БД (CONNECT) и разъединении с ней (DISCONNECT) регистрируется всегда.

4.1.16. Гипертекстовая обработка данных

Решение задачи гипертекстовой обработки данных основано на использовании защищенного комплекса программ гипертекстовой обработки данных, который включает web-сервер Apache2 и браузер Mozilla Firefox, доработанные для интеграции с ядром ОС и базовыми библиотеками с целью обеспечения мандатного управления доступом при организации удаленного доступа к информационным ресурсам в информационных и управляющих системах, в которых осуществляется хранение, обработка и передача конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну.

Web-сервер защищенного комплекса программ гипертекстовой обработки запускается как сервис ОС. При обслуживании запросов пользователей осуществляется переключение в мандатный контекст безопасности пользователя. Информационные ресурсы, к которым осуществляется доступ, хранятся как объекты ФС. Таким образом, доступ к защищаемой информации разграничивается средства расширенной подсистемы безопасности PARSEC.

В защищенном комплексе программ гипертекстовой обработки обеспечено функционирование в ЕПП (см. 4.1.3).

4.1.17. Обмен сообщениями электронной почты

В качестве защищенного комплекса программ электронной почты используется сервер электронной почты, состоящий из агента передачи электронной почты (Mail Transfer Agent, MTA) Exim4, агента доставки электронной почты (Mail Delivery Agent, MDA) Dovecot и клиента электронной почты (Mail User Agent, MUA) Mozilla Thunderbird, доработанных для реализации следующих дополнительных функциональных возможностей:

- интеграции с ядром ОС и базовыми библиотеками для обеспечения разграничения доступа;
- реализации мандатного управления доступом к почтовым сообщениям;
- автоматической маркировки создаваемых почтовых сообщений, отражающих уровень их конфиденциальности;
- регистрации попыток доступа к почтовым сообщениям.

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

1) доставку исходящей почты от авторизованных клиентов до сервера, который является целевым для обработки почтового домена получателя;

2) прием и обработку почтовых сообщений доменов, для которых он является целевым;

3) 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.

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

В защищенном комплексе программ электронной почты обеспечено функционирование в ЕПП (см. 4.1.3).

5. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

5.1. Входными данными для ОС являются:

- обращение субъектов доступа (процессов и команд СУБД) 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.

5.2. Выходными данными для ОС является результат использования субъектом доступа защищаемой сущности, предоставленного ему в соответствии с установленными ПРД. К таким результатам могут относиться: запуск программы, редактирование файла, создание сокетов, добавление данных в БД и т. п.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных
ЕПП — единое пространство пользователей
НЖМД — накопитель на жестком магнитном диске
ОП — оперативная память
ОС — операционная система специального назначения «Astra Linux Special Edition»
ПО — программное обеспечение
ПРД — правила разграничения доступом
СЗИ — средства защиты информации
СКЗИ — средства криптографической защиты информации
СПО — специальное программное обеспечение
СУБД — система управления базами данных
СЭП — сервис электронной подписи
ФС — файловая система
ЭП — электронная подпись (в соответствии с № 63-ФЗ от 06.04.2011)
ЭЦП — электронная цифровая подпись (в соответствии с ГОСТ Р 34.10-2012)

ACL — Access Control List (список контроля доступа)
ALD — Astra Linux Directory (единое пространство пользователей)
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)
GID — Group Identifier (идентификатор группы)
HTTP — HyperText Transfer Protocol (протокол передачи гипертекста)
IP — Internet Protocol (межсетевой протокол)
IPC — InterProcess Communication (межпроцессное взаимодействие)
IMAP — Internet Message Access Protocol (протокол доступа к сообщениям в сети Интернет)
LDAP — Lightweight Directory Access Protocol (легковесный протокол доступа к сервисам каталогов)
NFS — Network File System (сетевая файловая система)
NSS — Name Service Switch (диспетчер службы имен)
NTP — Network Time Protocol (протокол сетевого времени)
PAM — Pluggable Authentication Modules (подключаемые модули аутентификации)

PID — Process Identifier (идентификатор процесса)

SMB — Server Message Block (блок сообщений сервера)

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

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)

UID — User Identifier (идентификатор пользователя)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопро-водительного документа и дата	Подпись	Дата
	изменен-ных	заменен-ных	новых	аннулиро-ванных					
1		Все				РУСБ.14.09-18			25.12.18
2		Все				РУСБ.15-20			01.06.20
3		Все				РУСБ.15-21			15.10.21