50 1190 0101

Утвержден

РУСБ.10015-17-УД

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

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Описание применения

РУСБ.10015-17 31 01

Листов 38

2022

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-17 (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 ограниченного доступа, в том числе содержащую сведения, составляющие государственную тайну.

1.2. Основные характеристики

В состав ОС входят следующие компоненты:

- ядро ОС с поддержкой технологии виртуализации;
- 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 управления конфигурациями;
- 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 x86-64, а также поддержку периферийного оборудования;
- установку и функционирование на средствах вычислительной техники, оснащенных сенсорным устройством указания на чувствительной области экрана дисплея при помощи прикосновения (типа «touch-screen»);
- поддержку основных сетевых протоколов стека TCP/IP;
- создание защищенной среды виртуализации;
- организацию сетевого домена с централизованным хранением учетных записей;
- централизованное управление конфигурациями;
- поддержку отказоустойчивого режима работы;
- работу с мультимедийными данными;

- работу с реляционными базами данных;
- работу с электронной почтой;
- работу с гипертекстовыми данными;
- интеграцию включенного в ее состав комплекса программ 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.

1.4. Функции безопасности

Средства защиты информации (СЗИ) ОС обеспечивают:

- 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.

[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 x86-64 (AMD, Intel);
- оперативная память — не менее 1 ГБ;
- объем свободного дискового пространства — не менее 4 ГБ.

Для установки ОС с носителя требуется:

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

Для установки ОС по сети требуется:

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

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.10015-17 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 информационном ресурсе разработчика `wiki.astralinux.ru`.

2.4. Правовой аспект использования функций безопасности

Предоставляемое право использования функций ОС, включая указанные в 1.4 функции безопасности, определяется в заключаемых в соответствии с Гражданским кодексом Российской Федерации лицензионных договорах.

В зависимости от предоставленного пользователю права использования ОС на условиях простой (неисключительной) лицензии установлено несколько вариантов лицензирования, предусматривающих возможность комплексного использования функций безопасности ОС.

Соответствие варианта лицензирования и доступных функций безопасности приведено в таблице 1. Наименование уровней защищенности, для упрощения работы, совпадает с наименованием вариантов лицензирования, установленных в лицензионном договоре.

Таблица 1

Функция безопасности	Уровень защищенности		
	базовый	усиленный	максимальный
Замкнутая программная среда	Не доступно	Доступно (по умолчанию выключено)	Доступно (по умолчанию выключено)
Очистка освобождаемой внешней памяти	Не доступно	Доступно (по умолчанию выключено)	Доступно (по умолчанию выключено)
Мандатный контроль целостности	Не доступно	Доступно (по умолчанию включено)	Доступно (по умолчанию включено)
Мандатное управление доступом	Не доступно	Не доступно	Доступно (по умолчанию включено)
Идентификация и аутентификация	Доступно	Доступно	Доступно
Дискреционное управление доступом	Доступно	Доступно	Доступно
Регистрация событий безопасности	Доступно	Доступно	Доступно
Ограничение программной среды	Доступно	Доступно	Доступно
Изоляция процессов	Доступно	Доступно	Доступно
Защита памяти	Доступно	Доступно	Доступно
Контроль целостности	Доступно	Доступно	Доступно
Обеспечение надежного функционирования	Доступно	Доступно	Доступно
Фильтрация сетевого потока	Доступно	Доступно	Доступно
Маркировка документов	Не доступно	Не доступно	Доступно
Защита среды виртуализации	Доступно	Доступно	Доступно
Контроль подключения съемных машинных носителей информации	Доступно	Доступно	Доступно
Использование ядра hardened	Доступно	Доступно	Доступно

Выбор варианта лицензирования осуществляется пользователем, исходя из актуальных моделей нарушителя и угроз и других факторов.

Объем предоставленных лицензионным договором прав для использования функций безопасности ОС определяет возможность по достижению требуемых показателей защищенности автоматизированной (информационной) системы, в составе которой эксплуатируется ОС.

В программном обеспечении ОС в зависимости от выбранного варианта лицензирования пользователю предоставляется возможность установки и эксплуатации средств защиты, реализующих функции безопасности, путем выбора в меню программы установки соответствующего уровня защищенности.

2.5. Особенности функционирования ОС на средствах вычислительной техники, оснащенных сенсорным экраном

Функционирование ОС на средствах вычислительной техники, оснащенных сенсорным устройством указания на чувствительной области экрана дисплея при помощи прикосновения (типа «touch-screen»), осуществляется:

1) в режиме «Планшетный» при необходимости применения мандатного управления доступом;

2) в режиме «Мобильный» при отсутствии необходимости применения мандатного управления доступом.

Режим «Планшетный» применяется на максимальном уровне защищенности.

Режим «Мобильный» применяется только на усиленном уровне защищенности.

3. ПОРЯДОК ОБНОВЛЕНИЯ

В целях реализации функций безопасности по управлению обновлениями функций СЗИ для ОС предусмотрен выпуск обновлений безопасности.

3.1. Получение обновления

Обновления безопасности размещаются на сайте предприятия-разработчика. Информирование о размещении обновлений безопасности осуществляется путем направления лицензиату уведомления способом, установленным в лицензионном договоре или в ином документе, содержащем порядок получения, контроля целостности и установки обновлений безопасности. В общем случае информирование осуществляется путем:

- выпуска бюллетеня безопасности, содержащего описание обновлений безопасности, способ их установки, а также эталонные значения, необходимые для контроля целостности обновлений безопасности;
- отправки лицензиату электронного письма, содержащего гиперссылку на бюллетень безопасности.

3.2. Контроль целостности обновления

Контроль целостности обновлений безопасности осуществляется:

- до установки обновлений — проведением вычисления и проверки электронной подписи обновлений безопасности с использованием открытого ключа предприятия-разработчика, опубликованного на его сайте, с использованием программного обеспечения КриптоПро CSP, поддерживающего проверку и выработку электронной подписи по ГОСТ Р 34.10-2012;
- до установки обновлений — проведением регламентного контроля целостности полученного файла обновлений безопасности с использованием функции хэширования по ГОСТ Р 34.11 и сравнением полученного значения с эталонным значением, указанным на сайте предприятия-разработчика, в соответствии с инструкцией, приведенной в бюллетене безопасности;
- после установки обновлений — проведением регламентного контроля целостности файлов обновлений безопасности с использованием функции хэширования по ГОСТ Р 34.11 (эталонное значение контрольных сумм файлов должно размещаться в специальном файле `gostsums.txt`, включенном в состав обновлений безопасности) в соответствии с описанием, приведенным в документе РУСБ.10015-17 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1»;

- после установки обновлений — проведением контроля включения в эксплуатируемом изделии режима замкнутой программной среды для динамического контроля целостности файлов обновлений безопасности с использованием электронной цифровой подписи по ГОСТ Р 34.10 в соответствии с описанием, приведенным в документе РУСБ.10015-17 97 01-1.

3.3. Установка обновления

Установка обновлений безопасности осуществляется в соответствии с инструкцией, изложенной в составе бюллетеня безопасности, опубликованного на сайте предприятия-разработчика. При этом используются встроенные средства изделия, а именно: `apt`, `dkpg` — в соответствии с документом РУСБ.10015-17 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1».

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 в соответствии с 4.1.1;
- идентификация и аутентификация в соответствии с 4.1.2;
- организация единого пространства пользователей (ЕПП) в соответствии с 4.1.3;
- дискреционное управление доступом в соответствии с 4.1.4;
- мандатное управление доступом в соответствии с 4.1.5;
- мандатный контроль доверия (целостности) в соответствии с 4.1.5;
- организация надежных вычислений (изоляция процессов) в соответствии с 4.1.6;
- обеспечение взаимодействия между процессами в соответствии с 4.1.6;
- регистрация событий безопасности (протоколирование) в соответствии с 4.1.7;
- очистка оперативной и внешней памяти в соответствии с 4.1.8;
- контроль целостности в соответствии с 4.1.9;

- ограничение программной среды в соответствии с 4.1.10;
- фильтрация сетевого потока в соответствии с 4.1.11;
- обеспечение работы в среде виртуализации (изоляция виртуальных машин, разграничение доступа виртуальных машин к ресурсам и т. д.) в соответствии с 4.1.12;
- создание и проверка ЭП в соответствии с 4.1.13;
- маркировка документов в соответствии с 4.1.14;
- обеспечение работы в отказоустойчивом режиме в соответствии с 4.1.15;
- обеспечение надежного функционирования в соответствии с 4.1.16;
- обеспечение доступа к БД в соответствии с требованиями для разграничения доступа к информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну, согласно 4.1.17;
- 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, согласно 4.1.18;
- обеспечение обмена сообщениями электронной почты в соответствии с требованиями для разграничения доступа к информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну, согласно 4.1.19.

4.1.1. Обеспечение пользовательского интерфейса

Решение задачи обеспечения графического пользовательского интерфейса основано на использовании X Window System, 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, 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 позволяет внутри графической сессии, выполняемой в определенном мандатном контексте, запускать приложения с другим 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;
- уровня конфиденциальности каждого окна;
- уровня конфиденциальности 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, 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, электронной почты, гипертекстовой обработки данных и печати;
- 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.

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, характеризующих 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 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

Решение задачи дискреционного управления доступом основано на реализации в ОС соответствующего механизма.

В ОС механизм дискреционного управления доступом обеспечивает проверку дискреционных ПРД, формируемых в виде базовых ПРД операционных систем 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 операционных систем 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. Мандатное управление доступом и мандатный контроль целостности

Решение задач мандатного управления доступом и мандатного контроля целостности в ОС выполняется соответствующими механизмами.

Мандатное управление доступом и мандатный контроль целостности (МКЦ) реализованы в ядре ОС и затрагивают следующие подсистемы:

- механизмы IPC;
- стек TCP/IP (IPv4, IPv6);
- ФС ext2/ext3/ext4/xfs;
- сетевые ФС CIFS, OCFS2, Ceph;
- ФС proc, tmpfs.

При описании мандатного управления доступом и мандатного контроля целостности используются следующие термины (в соответствии с ГОСТ Р 59453.1-2021):

- субъект доступа — компонент ОС (процесс, в т.ч. запущенный от имени пользователя), доступы которого регламентируются политиками управления доступом;
- объект доступа — компонент ОС (например, файл, сокет и др.), доступ к которому регламентируется политиками управления доступом;
- контейнер — составной компонент ОС (например, каталог и др.), доступ к которому регламентируется политиками управления доступом, состоящий из объектов или контейнеров, к которым по отдельности возможно осуществление управления доступом.

При этом сущностью называется компонент, являющийся объектом или контейнером.

Мандатное управление доступом обеспечивает защиту от угроз безопасности, связанных с возможностью преднамеренных или ошибочных действий пользователей по изменению прав доступа к сущностям, владельцами которых являются пользователи, что не запрещается методом дискреционного управления доступа.

Для реализации мандатного управления доступом используются классификационные метки доступа, назначаемые для каждого субъекта и сущности, — служебные атрибуты, представляющие собой комбинацию иерархических уровней конфиденциальности (степеней секретности) и неиерархических категорий конфиденциальности. Сущностям также могут быть присвоены дополнительные атрибуты для мандатного управления доступом.

Мандатное управление доступом позволяет минимизировать или исключить возможность реализации информационно-технических воздействий в результате получения

несанкционированного доступа к объектам защиты различных уровней конфиденциальности.

МКЦ обеспечивает защиту процессов высокого уровня целостности (системных и привилегированных) от несанкционированного доступа и управления, что позволяет исключить возможности повышения привилегий пользователей и управления такими процессами в случае использования дефектов/уязвимостей в программном обеспечении информационной системы.

Для реализации МКЦ субъектам (процессам, в т.ч. запущенным от имени пользователя) и сущностям (файлам, каталогам, сокетам и т.п.) присваиваются уровни целостности (метки целостности). Сущностям также могут быть присвоены дополнительные атрибуты для МКЦ.

Принятие решения о запрете или разрешении доступа субъекта к сущности принимается на основе типа операции (чтение/запись/исполнение), метки безопасности субъекта (классификационной метки и метки целостности) и метки безопасности сущности (классификационной метки и метки целостности), а также на основе присвоенных сущности дополнительных атрибутов для мандатного управления доступом и для МКЦ.

Реализация мандатного управления доступом и мандатного контроля целостности в ОС описана в документе РУСБ.10015-17 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 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.10015-17 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.

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.10015-17 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 операционной системы семейства 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 и электронной почты 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

Решение задачи изоляции процессов основано на архитектуре ядра ОС.

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.

Также в ОС реализован механизм контейнеризации, обеспечивающий режим изоляции процессов на уровне операционной системы, описание которого приведено в 4.1.12.

4.1.7. Регистрация событий безопасности

Решение задачи регистрации событий безопасности в ОС реализовано на основе расширенной подсистемы протоколирования, осуществляющей регистрацию событий в двоичные файлы с использованием сервиса `auditd`.

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.

4.1.8. 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

Для решения задач контроля целостности используется библиотека `libgost`, в которой для вычисления контрольных сумм 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. По умолчанию используются функции хэширования в соответствии с ГОСТ Р 34.11-2012. Использование функции в соответствии с ГОСТ Р 34.11-94 сохранено для совместимости.

Библиотека `libgost` используется в средствах подсчета контрольных сумм файлов и оптических дисков, контроля соответствия дистрибутиву и регламентного контроля целостности, модулях аутентификации.

Контроль соответствия дистрибутиву обеспечивается методом подсчета контрольных сумм и их сравнения с эталонными значениями.

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 из состава ОС предоставляют возможность создавать замкнутую программную среду (ЗПС). Использование ЗПС обеспечивает динамический контроль неизменности (целостности) и подлинности файлов и предназначено для выявления фактов несанкционированного изменения файлов формата ELF и других файлов (в т. ч. относящихся к КСЗ) и предотвращения загрузки измененных файлов формата ELF и открытия других измененных файлов.

Контроль целостности реализован в невыгружаемом модуле ядра ОС `digsig_verif` и производится на основе проверки ЭЦП[1)] , внедренной в исполняемые файлы и разделяемые библиотеки формата ELF, входящие в состав ОС и устанавливаемого СПО, и в расширенные атрибуты файловой системы. ЭЦП реализована в соответствии с ГОСТ Р 34.10-2012 (256 бит) и ГОСТ Р 34.10-2001 (256 бит), использование ГОСТ Р 34.10-2001 в ОС сохранено для совместимости.

Контроль целостности исполняемых файлов и разделяемых библиотек формата ELF 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).

Контроль целостности файлов на основе ЭЦП в расширенных атрибутах файловой системы 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);

[1)] Электронная цифровая подпись — строка бит, полученная в результате процесса формирования подписи (применяется для подписи средствами ОС исполняемых файлов с использованием функции хэширования на базе асимметричного криптографического алгоритма.

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.10015-17 97 01-1

4.1.11. Фильтрация сетевого потока

В ОС реализована возможность фильтрации сетевых потоков, позволяющая:

- осуществлять фильтрацию входящих и/или исходящих сетевых потоков;
- осуществлять фильтрацию сетевых потоков на основе атрибутов безопасности субъектов доступа и информации;
- разрешать/запрещать сетевой поток на основе установленных правил фильтрации.

Сетевые соединения идентифицированы в ОС как объекты доступа, на которые распространяются следующие функции безопасности:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- изоляция процессов;
- ограничение программной среды;
- защита памяти;
- контроль целостности.

4.1.12. Обеспечение работы в среде виртуализации

ОС разработана с учетом применения встроенных средств защиты в виртуальной инфраструктуре и предоставляет возможность создания защищенной среды виртуализации. Виртуальные машины идентифицированы в ОС как объекты доступа, на которые распространяются следующие функции безопасности:

- идентификация и аутентификация;
- управление доступом;

- регистрация событий безопасности;
- изоляция процессов;
- ограничение программной среды;
- защита памяти;
- контроль целостности.

Ядро ОС поддерживает технологию KVM (Kernel-based Virtual Machine), обеспечивающую создание и функционирование виртуальной инфраструктуры. Технология KVM включает в себя специальный модуль ядра KVM и средство создания виртуального программно-аппаратного окружения QEMU.

KVM использует технологию аппаратной виртуализации, поддерживаемую 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.

В архитектуре KVM виртуальная машина выполняется как обычный процесс ОС, на который распространяется действие мер по идентификации и аутентификации субъектов и объектов доступа в полном объеме возможностей функций безопасности ОС.

Управление средой виртуализации обеспечивается утилитой `virsh` с использованием программного интерфейса `libvirt`.

Libvirt — программное обеспечение сервера виртуализации, которое обеспечивает способ управления виртуальными машинами и другими функциями виртуализации, такими как управление хранилищем и сетевым интерфейсом, доступ к которому также ограничивается в соответствии с установленной в ОС политикой разграничения доступа.

Утилита `virsh` предназначена для управления гостевыми системами и гипервизором, использует программный интерфейс сервера виртуализации `libvirt` и служит альтернативой графическому менеджеру виртуальных машин. Непривилегированные пользователи могут выполнять доступ только в режиме чтения. С помощью `virsh` можно исполнять сценарии для виртуальных машин.

Разграничение доступа к гипервизору, средствам управления компонентами виртуальной инфраструктуры (утилита `virsh` с использованием программного интерфейса `libvirt`), к виртуальным машинам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, к виртуальному аппаратному обеспечению, являющимся объектом доступа, а также контроль запуска виртуальных машин на основе заданных правил реализуется средствами ОС с использованием механизмов дискреционной и мандатной политики управления доступом.

При доступе к виртуальным машинам различается доступ к серверу виртуализации libvirt для управления виртуальными машинами и доступ пользователя непосредственно к рабочему столу виртуальной машины.

Доступ к серверу виртуализации `libvirt` для управления виртуальными машинами и доступ непосредственно к рабочему столу виртуальной машины осуществляется только после прохождения идентификации и аутентификации пользователей.

Поддержка дискреционного и мандатного управления доступом к виртуальным машинам в сервере виртуализации реализуется средствами ОС с помощью драйвера доступа parsec, специально разработанного с использованием прикладного программного интерфейса драйверов доступа `libvirt`.

Для хранения конфигурации и параметров виртуальных машин используются `xml`-файлы описания конфигурации виртуальных машин. В файле конфигурации задается состав аппаратных средств, которые необходимо эмулировать для данной виртуальной машины, а также параметры использования ресурсов сервера виртуализации (процессора, оперативной памяти и других физических устройств).

При создании виртуальной машины задаются конфигурационные параметры и создается файл-образ загрузочного диска виртуальной машины. Формат файла-образа зависит от выбранного средства эмуляции аппаратного обеспечения. В ОС используются средства эмуляции аппаратного обеспечения на основе QEMU. Кроме того, существует возможность конвертирования форматов образов других средств эмуляции аппаратного обеспечения.

При запуске виртуальной машины сервер виртуализации `libvirt` подготавливает необходимую для функционирования виртуальной машины инфраструктуру и формирует соответствующий набор параметров запуска средства эмуляции аппаратного обеспечения QEMU. После подготовительных действий производится порождения процесса ОС, в рамках которого будет функционировать виртуальная машина. Каждая запускаемая виртуальная машина функционирует от имени учетной записи запустившего ее пользователя и с его мандатными атрибутами безопасности.

Для обеспечения безопасности функционирования виртуальных машин сервер виртуализации `libvirt` использует концепцию драйверов безопасности. Данная концепция представляет собой специальный программный интерфейс для создания модулей безопасности, используемых для настройки окружения и инфраструктуры запуска и функционирования виртуальных машин в условиях их изоляции и мандатного управления доступом.

Выполнение требований по защите информации при функционировании виртуальных машин достигается совместным использованием модуля дискреционного управления доступом `dac` и специально разработанного модуля мандатного и дискреционного управления доступом `parsec`, взаимодействующего с подсистемой безопасности ОС.

Поддержка функционирования виртуальной машины в режиме запрета модификации ее файлов-образов осуществляется специальными способами запуска виртуальной машины, реализованными в ОС, при которых основной файл-образ защищается от записи. В зависимости от выбранного режима используется создание физической копии или различные варианты создания снимков файл-образов с последующим их удалением после завершения работы виртуальной машины.

Управление доступом внутри гостевой операционной системы реализуется встроенными средствами защиты информации из состава операционной системы или сертифицированными наложенными средствами защиты информации (в случае использования в качестве гостевой операционной системы несертифицированную по требованиям безопасности информации операционную систему).

ОС обеспечивает функционирование виртуальных машин (виртуальной инфраструктуры) в условиях мандатного и дискреционного управления доступом при межпроцессном и сетевом взаимодействии, включая взаимодействие между виртуальными машинами по сетевому протоколу IPv4 (IPv6) в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих виртуальных машин.

Управление потоками информации, в том числе при взаимодействии между гостевыми операционными системами, осуществляется на основе классификационных меток, установленных в соответствии с национальным стандартом ГОСТ Р 58256-2018.

Также в ОС реализован механизм контейнеризации, обеспечивающий режим изоляции процессов на уровне ядра операционной системы. Использование данного механизма позволяет запускать приложение и необходимый ему минимум системных библиотек в полностью изолированном контейнере, соединяющемся с хостовой ОС при помощи определенных интерфейсов. Процессы, запущенные внутри контейнера, изолированы от процессов других контейнеров и процессов хостовой ОС, что предотвращает воздействие на них потенциально вредоносного кода, выполняемого в контейнере.

Контейнеры идентифицированы в ОС как объекты доступа, на которые распространяются следующие функции безопасности:

- управление доступом;
- изоляция процессов;
- ограничение программной среды.

4.1.13. Сервис электронной подписи

Комплекс программ из состава ОС предоставляет сервис электронной подписи (СЭП), обеспечивающий интеграцию с дополнительно устанавливаемыми сертифицирован-

ными ФСБ России средствами криптографической защиты информации[1] (СКЗИ) в целях создания и проверки усиленной квалифицированной электронной подписи.

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[2] электронных документов в соответствии с ГОСТ Р 34.10-2012 средствами сертифицированных СКЗИ.

4.1.14. 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.

---

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

[2] Электронная подпись (в соответствии с № 63-ФЗ от 06.04.2011) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (является юридически значимой).

4.1.15. 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.10015-17 95 01-1.

4.1.16. 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.10015-17 95 01-1 и РУСБ.10015-17 97 01-1.

4.1.17. 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 и информационными потоками.

ОС совместно с СУБД предоставляет следующие функции защиты информации:

- аудит безопасности;
- ролевое, дискреционное и мандатное управление доступом;
- восстановление информации (резервное копирование);
- определение атрибутов пользователей;
- аутентификация субъектов доступа до разрешения любого действия, выполняемого при посредничестве функций безопасности от имени любого пользователя;
- идентификация пользователей до разрешения любого действия;

- связывание «пользователь-субъект», предусматривающее ассоциирование атрибутов безопасности пользователя с субъектами доступа и управление изменениями атрибутов безопасности пользователей;
- идентификация объектов доступа до разрешения любого действия;
- контроль доступа (обращений) средствами монитора обращений из состава ОС, проверка правомочности обращений на основе установленных политик мандатной, дискреционной и ролевой политики управления доступом;
- ограничение сеансов пользователя.

4.1.17.1. Идентификация и аутентификация

В ходе аутентификации осуществляется проверка сервером СУБД подлинности клиента и последующего определения наличия для клиентского приложения (для пользователя, который запускает клиентское приложение) права на соединение с БД от имени указанного пользователя БД.

PostgreSQL предлагает несколько различных методов аутентификации. Метод, используемый для аутентификации клиентского соединения, может быть выбран на основе адреса узла сети клиента, БД и пользователя.

Имена пользователей СУБД PostgreSQL логически отделены от имен пользователей ОС, в которой запущен сервер СУБД. При реализации требований по защите информации от несанкционированного доступа установлена необходимость обеспечения соответствия пользователей СУБД учетным записям в ОС. При настройке аутентификации в СУБД следует использовать только методы аутентификации, в которых осуществляется подобное сопоставление.

При попытке соединения с сервером СУБД клиентское приложение указывает пользователя СУБД PostgreSQL, от имени которого осуществляется подключение. В пределах окружения SQL активное имя пользователя СУБД определяет права на объекты БД.

Корректная работа с СУБД предполагает использование механизма ЕПП. Для обеспечения сквозной аутентификации пользователей ЕПП в СУБД необходимо в качестве метода аутентификации указать `gss` и провести соответствующую настройку сервера и клиента СУБД PostgreSQL.

Для авторизации через PAM пользователь, от которого работает СУБД PostgreSQL, должен иметь права на чтение информации из БД пользователей и обладать сведениями о мандатных метках и привилегиях.

4.1.17.2. Управление доступом

Дискреционное управление доступом к данным объектно-реляционной СУБД PostgreSQL из состава ОС обеспечивается в понятиях реляционной СУБД. С каждым типом объектов БД ассоциируется определенный набор типов доступа (возможных операций). Для

каждого объекта 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. При выполнении любого запроса пользователя (субъекта БД) к защищаемому ресурсу (объекту БД) выполняется дискреционное управление доступом на основе установленных пользователю прав. Для каждой выполняемой операции производится проверка наличия права у пользователя на выполнение данной конкретной операции.

В СУБД PostgreSQL для управления правами на доступ к БД используется концепция ролей — ролевое управление доступом. Под ролью понимается пользователь или группа пользователей БД. Роли могут являться владельцами объектов БД и могут назначать привилегии на управление объектами для других ролей, имеющих доступ к данными объектам.

Система привилегий СУБД PostgreSQL предназначена для передачи отдельным пользователям прав выполнения определенных административных действий. Обычный пользователь системы не имеет дополнительных привилегий. Привилегии являются подклассом атрибутов пользователя СУБД PostgreSQL.

Роли СУБД концептуально отличаются от пользователей ОС. Каждое подключение к серверу СУБД осуществляется от имени определенной роли, которая определяет первичные права доступа для команд, используемых в контексте подключения. Имя роли, используемое при подключении к БД, определяется клиентом в запросе на соединение способом. Набор ролей СУБД, от имени которых клиент может осуществить подключение, определяется значениями параметров аутентификации клиента. Роли СУБД назначается набор атрибутов, определяющих ее права и взаимодействующих с системой аутентификации клиента.

В основе механизма мандатного управления доступом в защищенной СУБД из состава ОС лежит управление доступом к защищаемым ресурсам БД на основе иерархических и неиерархических меток доступа. В качестве иерархических и неиерархических меток доступа при использовании СУБД в ОС используются метки конфиденциальности или метки безопасности ОС. СУБД PostgreSQL не имеет собственного механизма назначения, хранения и модификации меток пользователей и использует для этого механизмы ОС.

Системный каталог (метаданные) рассматривается как самостоятельная БД, реализованная с помощью средств СУБД. При этом все операции с этой БД осуществляются либо с помощью специальных конструкций языка запросов SQL или привилегированным пользователем в специальном режиме. Таким образом, мандатное управление доступом применяется ко всем объектам БД. Метки системных объектов располагаются в записях таблиц системного каталога, непосредственно описывающих защищаемый объект.

Проверка мандатных прав доступа к объектам СУБД осуществляется одновременно с проверкой дискреционных прав доступа к ним.

В ОС каждый пользователь может иметь множество меток, которое задается минимальной и максимальной метками диапазона. Чтобы поддержать эту модель в СУБД PostgreSQL каждой сессии пользователя назначаются три метки: максимальная, минимальная и текущая.

Их начальная инициализация осуществляется по определенному алгоритму. При возникновении ситуации с несовместимостью меток или выходом за пределы диапазона, процесс аутентификации клиента прерывается и доступ к БД блокируется.

Описание применения дискреционного управления доступом и мандатного управления доступом в СУБД PostgreSQL приведено в документе РУСБ.10015-17 97 01-1.

4.1.17.3. Регистрация событий безопасности

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования, применяемый для регистрации событий в СУБД PostgreSQL.

В СУБД PostgreSQL для настройки режима работы подсистемы регистрации событий используются конфигурационный параметр `ac_audit_mode` файла `postgresql.conf`. Настройка подсистемы сообщений аудита в СУБД PostgreSQL обеспечивается конфигурационным файлом `pg_audit.conf` конкретного кластера данных. В этом конфигурационном файле задаются списки успешных и неуспешных типов запросов на доступ, которые будут регистрироваться в журнале СУБД и подсистеме аудита ОС для отдельных пользователей и по умолчанию. Информация о соединении пользователей с БД и разъединении с ней регистрируется всегда.

В СУБД PostgreSQL маска регистрации событий устанавливается в процессе авторизации пользователя согласно выбранному режиму работы подсистемы регистрации событий и находится в атрибуте сессии `ac_session_audit`.

При этом реализован следующий порядок применения настроек регистрации событий:

- настройки для конкретной роли и конкретной базы данных;
- настройки для конкретной роли;
- настройки для конкретной базы данных;
- для всех остальных.

4.1.17.4. Обеспечение надежного функционирования

В случае возникновения ошибок в хранящихся данных, нарушения целостности или в случае программного и/или аппаратного сбоя сервера СУБД необходимо проведение процедуры восстановления БД. При этом в зависимости от тяжести повреждений может

осуществляться как сохранение существующего кластера БД с последующим его восстановлением, так и восстановление из резервных копий, созданных в процессе регулярного проведения регламентных работ.

В PostgreSQL существуют три подхода к резервному копированию данных:

- SQL-дамп;
- резервное копирование на уровне ФС;
- непрерывное архивирование.

СУБД PostgreSQL из состава ОС содержит ряд стандартных средств резервного копирования и восстановления БД. К ним относятся утилиты `pg_dump`, `pg_dumpall`, `pg_restore` и, в том числе, интерактивный терминал `psql`, с помощью которого могут быть восстановлены резервные копии, сохраненные в виде скрипта SQL.

Для создания и восстановления резервных копий баз данных с мандатными атрибутами необходимо, чтобы пользователь имел соответствующие привилегии. Для создания резервной копии БД в виде файла в текстовом или других форматах используется утилита `pg_dump`, которая создает согласованную копию, даже если БД используется, при этом доступ к БД других пользователей не блокируется.

Резервная копия может создаваться в виде скрипта или форматах упакованного файла. Скрипт резервной копии представляет собой текст, содержащий последовательность SQL-команд, необходимых для воссоздания БД до состояния, в котором она была сохранена. Для восстановления из скрипта он подается на вход утилиты `psql`. Скрипт может быть использован для воссоздания БД на другом сервере или архитектуре, а также на других СУБД при внесении в него небольших изменений.

Утилита `pg_dumpall` используется для создания резервной копии всего кластера в виде скрипта.

Скрипт содержит SQL-команды и может быть подан в дальнейшем на вход утилиты `psql` для восстановления. Операция осуществляется последовательным вызовом утилиты `pg_dump` для каждой БД кластера. Кроме этого, `pg_dumpall` сохраняет глобальные объекты, единые для всех БД (`pg_dump` подобные объекты не сохраняет). Данные объекты включают в себя информацию о пользователях и группах и такие свойства, как права доступа, применяемые для всех БД в целом.

Для восстановления архивов резервных копий БД, полученных с помощью утилиты `pg_dump`, используется утилита `pg_restore`. Она выполняет команды, необходимые для воссоздания БД до состояния на момент времени создания резервной копии. Архивные файлы так же позволяют выбирать с помощью утилиты `pg_restore`, что именно восстанавливать, менять порядок восстанавливаемых элементов. Файлы архивов являются переносимыми между разными архитектурами.

Утилита `pg_restore` может функционировать в двух режимах. При указании БД архив восстанавливается непосредственно в нее. В другом случае скрипт, содержащий необходимые для пересоздания БД SQL-команды, создается и выводится в файл или стандартный поток вывода.

4.1.18. 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 средствами расширенной подсистемы безопасности PARSEC.

В защищенном комплексе программ гипертекстовой обработки обеспечено функционирование в ЕПП.

4.1.19. 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:

- 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.

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.

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 доступа
СЗИ — средства 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)
NTP — Network Time Protocol (протокол сетевого времени)
NSS — Name Service Switch (диспетчер службы имен)
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					