50 1190 0101

Утвержден

РУСБ.10015-01-УД

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

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Описание применения

РУСБ.10015-01 31 01

Листов 40

2024

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (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 применения в составе информационных (автоматизированных) систем в целях обработки и защиты[1)] информации любой категории доступа[2)] — общедоступной информации, а также информации, доступ к которой ограничен федеральными законами (информации ограниченного доступа).

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 управления конфигурациями;
- средства резервного копирования и восстановления данных;
- средства виртуализации;
- средства контейнеризации;
- средства контроля подключения съемных машинных носителей информации;
- защищенный комплекс программ печати и учета документов;
- защищенный комплекс программ гипертекстовой обработки данных;
- защищенная система управления базами данных (ЗСУБД);
- защищенный комплекс программ электронной почты;
- пакет офисных программ.

ЗСУБД является неотъемлемым программным модулем ОС, разработанным на основе СУБД Tantor Basic, которая реализована с использованием СУБД PostgreSQL.

[1)] От несанкционированного доступа.

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

1.3. Возможности

ОС предоставляет следующие возможности:

1) установку и функционирование на средствах вычислительной техники с процессорной архитектурой x86-64, а также поддержку периферийного оборудования;

2) установку и функционирование на средствах вычислительной техники, оснащенных сенсорным устройством указания на чувствительной области экрана дисплея при помощи прикосновения (типа «touch-screen»);

3) поддержку основных сетевых протоколов стека TCP/IP;

4) создание защищенной среды виртуализации;

5) организацию сетевого домена с централизованным хранением учетных записей;

6) централизованное управление конфигурациями;

7) поддержку отказоустойчивого режима работы;

8) работу с мультимедийными данными;

9) работу с реляционными базами данных;

10) работу с электронной почтой;

11) работу с гипертекстовыми данными;

12) интеграцию включенного в ее состав комплекса программ с дополнительно устанавливаемыми сертифицированными ФСБ России средствами криптографической защиты конфиденциальной информации[1)] для:

а) создания и проверки усиленной квалифицированной электронной подписи;

б) криптографического преобразования канала передачи информации по протоколам прикладного уровня стека TCP/IP;

13) обработку текстовых документов и электронных таблиц различных форматов;

14) 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 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 с носителя дополнительно требуется:

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

Для установки по сети дополнительно требуется:

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

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.10015-01 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 информационном ресурсе разработчика `wiki.astralinux.ru`.

2.4. Правовой аспект использования функций безопасности

Предоставляемое право использования функций ОС, включая 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 доступно несколько вариантов лицензирования, предусматривающих возможность комплексного использования функций безопасности 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.

Определение требуемого уровня защищенности осуществляется пользователем исходя из актуальных моделей нарушителя и угроз и других факторов.

Соответствие уровня защищенности и доступных функций безопасности приведено в таблице 1. Наименование уровней защищенности, для упрощения работы, указывается вместе с вариантом лицензирования в наименовании лицензии и в иных правоустанавливающих документах.

Таблица 1

Функция безопасности	Уровень защищенности		
	базовый	усиленный	максимальный
Замкнутая программная среда	Недоступно	Доступно (по умолчанию выключено)	Доступно (по умолчанию выключено)
Очистка памяти	Недоступно	Доступно, в т.ч. для ЗСУБД (по умолчанию выключено)	Доступно, в т.ч. для ЗСУБД (по умолчанию выключено)
Мандатный контроль целостности	Недоступно	Доступно (по умолчанию включено)	Доступно (по умолчанию включено)
Мандатное управление доступом	Недоступно	Недоступно	Доступно, в т.ч. для ЗСУБД (по умолчанию включено)
Идентификация и аутентификация	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД
Дискреционное управление доступом	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД

Окончание таблицы 1

Функция безопасности	Уровень защищенности		
	базовый	усиленный	максимальный
Регистрация событий безопасности	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД
Ограничение программной среды	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД	Доступно, в т.ч. для ЗСУБД
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	Недоступно	Недоступно	Доступно (по умолчанию включено)
Контроль подключения съемных машинных носителей информации	Недоступно	Доступно	Доступно
Защита среды виртуализации	Доступно	Доступно	Доступно
Защита изолированных программных сред (контейнеров)	Доступно	Доступно	Доступно
Обеспечение доступности ЗСУБД	Доступно	Доступно	Доступно
Обеспечение производительности ЗСУБД	Доступно	Доступно	Доступно
Ролевое управление доступом в ЗСУБД	Доступно	Доступно	Доступно

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.

3. ПОРЯДОК ОБНОВЛЕНИЯ ОС

В целях обеспечения соответствия ОС требованиям безопасности информации в части устранения недекларированных возможностей и уязвимостей ОС осуществляется ее техническая поддержка, предусматривающая выпуск очередного и оперативного обновлений.

Техническая поддержка осуществляется на протяжении всего срока, указанного в Государственном реестре сертифицированных средств защиты информации ФСТЭК России, и предполагает выпуск и последовательное применение потребителем очередных и соответствующих им оперативных обновлений, что обеспечивает возможность нейтрализации актуальных угроз безопасности информации.

Порядок выпуска и доведения обновлений ОС до потребителей установлен:

- для информационных (автоматизированных) систем, находящихся в компетенции ФСТЭК России, в настоящем документе;
- для информационных (автоматизированных) систем, находящихся в компетенции Министерства обороны Российской Федерации, в документе «Регламент организации работ по устранению уязвимостей и выпуску обновлений безопасности...», утвержденном начальником 8 Управления Генерального штаба Вооруженных Сил Российской Федерации и согласованным с заказывающими и довольствующими органами военного управления[1)] (далее по тексту — Регламент).

Информирование потребителей об окончании производства и (или) поддержки безопасности ОС осуществляется с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам) и путем размещения соответствующей информации на сайте изготовителя.

Информирование ФСТЭК России — официальным почтовым сообщением не позднее чем за один год до окончания производства и (или) поддержки безопасности ОС.

3.1. Очередное обновление

Очередное обновление представляет собой заводские экземпляры ОС, изготовленные в соответствии с конструкторской (программной) и технологической документацией, действующей на момент изготовления, с внесенными в нее порядком, установленным ГОСТ 2.503-2013, плановыми изменениями.

Очередное обновление решает следующий комплекс задач:

- устранение критических и некритических уязвимостей;
- обеспечение усовершенствования (модернизации) конструкции;

[1)] Настоящий документ содержит основные положения Регламента.

- поддержка современного оборудования;
- реализация новых функциональных возможностей;
- обеспечение соответствия актуальным требованиям безопасности информации;
- повышение удобства использования, управления компонентами ОС и другие.

Очередное обновление предоставляется пользователям при заключении соответствующего лицензионного договора или дополнения к имеющемуся лицензионному договору, а также в соответствии с положениями «Лицензионного соглашения с конечным пользователем по использованию операционной системы специального назначения «Astra Linux Special Edition».

Информация о выпуске очередного обновления ОС размещается на официальном сайте `wiki.astralinux.ru` и в личном кабинете пользователя, а также доводится до лицензиатов (потребителей) с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам).

В целях поддержания информационных (автоматизированных) систем в безопасном состоянии, обеспечения их работоспособности совместно с современным оборудованием и увеличения срока эксплуатации, рекомендуется на постоянной основе планировать и организовывать проведение мероприятий по применению очередного обновления ОС.

3.2. Оперативное обновление

3.2.1. Общая информация о выпуске оперативного обновления

Оперативное обновление решает задачу оперативного устранения уязвимостей в экземплярах ОС, находящихся в эксплуатации, а также реализации (совершенствования) необходимых функциональных возможностей ОС.

Общий порядок работ по выпуску оперативного обновления:

1) поиск в доступных источниках информации об уязвимостях ОС, в том числе в программных компонентах;

2) получение сведений об уязвимостях от потребителей;

3) проведение испытаний по выявлению уязвимостей, в том числе по выявлению уязвимостей и недекларированных возможностей в соответствии с ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и другими стандартами серии «Защита информации. Разработка безопасного программного обеспечения», а также методическими документами ФСТЭК России;

4) разработка компенсирующих мер по защите информации или ограничений по применению ОС, снижающих возможность эксплуатации уязвимостей;

5) доведение информации об уязвимостях ОС, а также о компенсирующих мерах по защите информации или ограничений по применению ОС до потребителей средства, ФСТЭК России и БДУ ФСТЭК России;

6) устранение уязвимостей путем доработки ОС или ее отдельных компонентов, принятие иных мер, снижающих возможность эксплуатации уязвимостей;

7) тестирование (испытания) доработанной ОС или отдельных компонентов на предмет устранения влияния обновлений на функции безопасности, подтверждения устранения уязвимостей, невнесения новых уязвимостей;

8) доведение отдельных доработанных программных компонентов из состава ОС или кумулятивного обновления программного обеспечения ОС до потребителей.

Оперативное обновление представляет собой бюллетень, который может быть доступен в виде:

- инструкций и методических указаний по настройке и особенностям эксплуатации ОС, содержащих сведения о компенсирующих мерах или ограничениях по применению ОС при эксплуатации;

- отдельных программных компонентов из состава ОС, в которые внесены изменения с целью устранения уязвимостей, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов оперативного обновления;

- кумулятивного оперативного обновления, представляющее собой файл с программным обеспечением установочного диска ОС очередного обновления из комплекта поставки с внесенными изменениями, а также информации, содержащей сведения о контрольных суммах всех файлов обновления, указания по установке, настройке и особенностям эксплуатации ОС с установленными обновлениями безопасности.

Сроки устранения уязвимостей установлены в соответствии с документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) и составляют:

- разработку компенсирующих мер по защите информации или ограничений по применению ОС, а также доведение информации о таких мерах и ограничениях до потребителей в срок до 48 часов с момента выявления уязвимости;

- доработку ОС, в том числе разработку обновлений программного обеспечения ОС, или разработку мер по защите информации, нейтрализующих недостаток, в срок до 60 дней с момента выявления (подтверждения) уязвимости.

В рамках работ по организации процессов управления уязвимостями на объектах информатизации в целях устранения уязвимостей программного обеспечения, входящего в состав установочного диска ОС, в приоритетном порядке применяется оперативное обновление

ОС. Не допускается применение обновлений такого программного обеспечения из открытых источников.

Для минимизации вероятности эксплуатации уязвимостей до выпуска и применения оперативного обновления необходимо использовать средства защиты ОС, реализующие сертифицированные функции безопасности. Возможности ОС для защиты от типовых угроз безопасности информации приведены в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

3.2.2. Порядок доведения оперативного обновления

Оперативные обновления представляют собой отдельные программные документы, не предусматривающие внесения изменений в комплект поставки очередного обновления, характеристики которого подтверждены сертификатом соответствия требованиям по безопасности информации. Сертификат соответствия очередного обновления ОС, поставляемого потребителям в комплектности в соответствии с формуляром, является действующим вне зависимости от выпуска и применения оперативного обновления.

Оперативное обновление предоставляется пользователям на безвозмездной основе.

Лицензиаты (потребители) оповещаются о выпуске и возможности получения обновления с использованием контактной информации, указанной в лицензионных договорах и дополнениях к ним, путем размещения соответствующей информации на официальном сайте и через личный кабинет пользователя.

Оперативное обновление не является самостоятельным программным изделием. Серийное производство и поставка (в том числе на материальных носителях) оперативного обновления не предусмотрены.

Доведение оперативного обновления до потребителей осуществляется:

- для информационных (автоматизированных) систем, находящихся в компетенции ФСТЭК России, — изготовителем ОС путем распространения по сетям связи. Источником получения оперативного обновления, подписанного усиленной квалифицированной электронной подписью изготовителя, является официальный информационный ресурс изготовителя;
- для информационных (автоматизированных) систем, находящихся в компетенции Министерства обороны Российской Федерации, — изготовителем ОС путем распространения по сетям связи. Источником получения оперативного обновления, подписанного усиленной квалифицированной электронной подписью изготовителя, является информационный ресурс изготовителя. Оперативное обновление также может быть размещено в интерактивной системе (витрине) Министерства обороны Российской Федерации, доступ к которой предоставляется организациям, включая

предприятия оборонно-промышленного комплекса, осуществляющим выполнение опытно-конструкторских и иных работ в интересах Министерства обороны Российской Федерации.

3.2.3. Порядок применения оперативного обновления

Контроль целостности обновлений безопасности в составе информационных (автоматизированных) систем потребителей осуществляется следующим порядком:

- до установки обновления — проведением проверки электронной подписи обновления;
- до установки обновления — проведением контроля целостности образа установочного диска оперативного обновления путем подсчета его контрольной суммы и сравнения с контрольной суммой, указанной в бюллетене;
- после установки обновления — проведением контроля целостности с использованием функции хеширования и автоматической сверки полученного значения с эталонным, указанным в специальном файле с контрольными суммами `gostsums.txt`, входящем в состав оперативного обновления.

Применение оперативных обновлений обусловлено следующими требованиями:

- требованиями, предъявляемыми к защите информации в информационных системах, обрабатывающих информацию ограниченного доступа, а именно необходимости реализации мер по контролю защищенности информации (меры группы «АНЗ»), предусматривающими выявление и оперативное устранение уязвимостей;
- требованиями, устанавливающими порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, в соответствии с которыми при проведении аттестационных испытаний органом по аттестации проводится анализ уязвимостей, таким образом отсутствие уязвимостей является условием положительных результатов аттестационных испытаний и достигается путем применения обновлений безопасности программного обеспечения информационной системы, в том числе средств защиты информации.

В рамках аттестации или при реализации мер по обеспечению целостности информационных систем, функционирующих под управлением ОС, в целях подтверждения целостности, подлинности и неизменности сертифицированного программного обеспечения ОС необходимо:

1) указать номер бюллетеня, содержащего оперативное обновление, в разделе «Сведения о бюллетенях» формуляра ОС или в паспорте средства вычислительной техники, функционирующего под управлением ОС;

2) провести контроль целостности установочного диска ОС (или его образа) из комплекта поставки путем подсчета его контрольной суммы и сравнения с контрольной суммой, указанной в формуляре ОС;

3) провести контроль целостности образа установочного диска ОС с внесенными оперативным обновлением изменениями путем подсчета его контрольной суммы и сравнения с контрольной суммой, указанной в бюллетене безопасности;

4) провести контроль целостности файлов программного обеспечения ОС, реализующего сертифицированные функции безопасности информации, после применения оперативного обновления путем подсчета контрольных сумм файлов утилитой `fly-admin-int-check` или `astra-int-check` с применением шаблона проверки со списком файлов, реализующих функции безопасности, в соответствии с описанием, приведенным в документе РУСБ.10015-01 97 01-1.

Совпадение контрольных сумм является достаточным подтверждением использования в информационной системе сертифицированного программного обеспечения ОС.

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 нормативных документов по обеспечению защиты информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну.

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

- 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.

Также ОС реализует функции безопасности информации, перечень которых определен в документах РУСБ.10015-01 30 01 «Операционная система специального назначения «Astra Linux Special Edition». Формуляр» и РУСБ.10015-01 30 02 «Операционная система специального назначения «Astra Linux Special Edition». Формуляр».

Реализация функций безопасности ОС основана на следующих основных положениях:

1) при моделировании и описании управления доступом в ОС на основе ГОСТ Р 59453.1-2021 используются следующие термины:

а) субъект доступа — активный компонент ОС (например, процесс, запущенный от имени учетной записи пользователя), доступы которого регламентируются политиками управления доступом;

б) сущность (объект доступа) — пассивный компонент ОС, доступ к которому регламентируется политиками управления доступом, при этом используются следующие виды сущностей (объектов доступа):

- сущность-объект (объект) — пассивный компонент ОС (например, файл, сетевое соединение (файл-сокет), устройство (файл-устройство), файл-образ виртуальной машины или контейнера, как средства изоляции программной среды), доступ к которому регламентируется политиками управления доступом, к частям которого по отдельности управление доступом не осуществляется;

- сущность-контейнер (контейнер) — пассивный составной компонент ОС (например, каталог, том), доступ к которому регламентируется политиками управления доступом, состоящий из сущностей-объектов или сущностей-контейнеров, к которым по отдельности возможно осуществление управления доступом;

2) с каждым пользователем системы связан уникальный численный идентификатор — идентификатор пользователя (UID), который однозначно соотносится с записью в БД пользователей, содержащей информацию о пользователях, включая их реальные и системные имена. БД пользователей поддерживается и управляется системным администратором. UID является ярлыком субъекта (номинальный субъект), которым система пользуется для определения прав доступа. БД пользователей в ОС может быть как локальной для системы, так и являться частью ЕПП, функционирующего на основе протокола LDAP;

3) каждый пользователь входит в одну или более групп. Группа — это список пользователей системы, имеющий собственный идентификатор (GID). Поскольку группа объединяет несколько пользователей системы, в терминах политики безопасности она соответствует понятию «множественный субъект». GID является ярлыком множественного субъекта, которых у номинального субъекта может быть более одного. Таким образом, одному UID соответствует список GID;

4) роль действительного (работающего с сущностями) субъекта играет процесс. Каждому процессу присваивается единственный UID, являющийся идентификатором запустившего процесс номинального субъекта, т. е. пользователя. Процесс, порожденный некоторым процессом пользователя, наследует UID родительского процесса. Таким образом, все процессы, запускаемые пользователем, имеют его идентификатор. Все процессы, принадлежащие пользователю, образуют сеанс пользователя. Первый процесс сеанса пользователя порождается после прохождения процедур идентификации и аутентификации. При обращении процесса к сущности доступ предоставляется по результатам процедуры авторизации, т. е. обработки запроса на основе мандатных и дискреционных ПРД;

5) механизм ПРД реализован в ядре ОС, что обеспечивает его правильное функционирование при использовании любых компонентов, предоставляемых ОС. Реализация мандатного управления доступом затрагивает все подсистемы ядра, в которых

реализовано дискреционное управление доступом. При этом оба вида управления доступом функционируют параллельно, не влияя на принятие решений друг друга (непротиворечивость). Доступ разрешается в том случае, если он возможен с учетом дискреционных и мандатных ПРД. Запрещается в случае, если доступ запрещен хотя бы одним из видов ПРД (дискреционным или мандатным).

4.1. 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 кли-

ента. 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.

4.2. 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 хеш-функции по ГОСТ Р 34.11-2012 (ГОСТ Р 34.11-94).

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.3. 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 серверов ЗСУБД, защищенной электронной почты, защищенной 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 включено программное обеспечение FreeIPA. Программное обеспечение FreeIPA базируется на технологиях LDAP, Kerberos и Samba, предоставляет графический интерфейс управления и администрирования и автоматизированную настройку всех необходимых конфигурационных файлов входящих в него служб.

Более подробная информация приведена в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1».

4.4. 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 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.

Более подробная информация приведена в документах РУСБ.10015-01 97 01-1.

4.5. 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.

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.10015-01 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 возмож-

ность осуществлять все перечисленные привилегированные действия. Перечень и описание PARSEC-привилегий приведены в РУСБ.10015-01 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.

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.10015-01 95 01-1.

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.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.6. 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 контейнеризации приведено в 4.12.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.7. Регистрация событий безопасности

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

Также в ОС реализована подсистема регистрации событий, выполняющая регистрацию событий безопасности с учетом требований ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации». Подсистема регистрации событий обеспечивает сбор информации о событиях, в том числе о событиях безопасности, из различных источников (служба `auditd`, собственные подключаемые модули, файлы, прикладное ПО и др.) и предоставляет инструменты для просмотра собранных данных и реагирования на события.

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования. Данный программный интерфейс применен для регистрации событий в ЗСУБД.

Более подробная информация о регистрации событий безопасности приведена в документе РУСБ.10015-01 97 01-1. Информация о регистрации событий безопасности в ЗСУБД приведена в документе РУСБ.10015-01 97 01-3 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 3. Защищенная СУБД».

4.8. 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.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.9. Контроль целостности

Для решения задач контроля целостности используется библиотека `libgost`, в которой для вычисления контрольных сумм реализованы функции хеширования в соответствии с ГОСТ Р 34.11-2012 с длиной хеш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хеш-кода 512 бит и ГОСТ Р 34.11-94. По умолчанию используются функции хеширования 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).

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.10. Ограничение программной среды

4.10.1. 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 несанкци-

онированного изменения исполняемых файлов и других файлов (в т. ч. относящихся к КСЗ), предотвращения загрузки измененных исполняемых файлов, а также открытия других измененных файлов.

Контроль целостности реализован в невыгружаемом модуле ядра ОС `digsig_verif` и производится на основе проверки:

- цифровой подписи, внедренной в файл;
- цифровой подписи, содержащейся в расширенных атрибутах файловой системы файла;
- отсоединенной цифровой подписи (содержащейся в отдельном файле).

Цифровая подпись 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.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.10.2. 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.10015-01 97 01-1.

4.11. 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.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.12. Создание и защита среды виртуализации

ОС разработана с учетом применения встроенных средств защиты в виртуальной инфраструктуре, включает в свой состав ядро с поддержкой технологии виртуализации и предоставляет возможность создания и защиты среды виртуализации с обеспечением выполнения следующих функций безопасности:

- доверенная загрузка виртуальных машин;
- контроль целостности;
- регистрация событий безопасности;
- управление доступом;
- резервное копирование;
- управление потоками информации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей;
- централизованное управление образами виртуальных машин и виртуальными машинами.

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.

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.

Описание средств виртуализации приведено в документе РУСБ.10015-01 95 01-1.

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 раз- личные 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.

Более подробная информация приведена в документах РУСБ.10015-01 95 01-1 и РУСБ.10015-01 97 01-1.

4.13. Создание и защита изолированных программных сред (контейнеров)

ОС содержит программные средства (средства контейнеризации), реализующие создание и функционирование изолированных программных сред, с обеспечением выполнения следующих функций безопасности:

- изоляция контейнеров;
- выявление уязвимостей в образах контейнеров;
- проверка корректности конфигурации контейнеров;
- контроль целостности контейнеров и их образов;
- регистрация событий безопасности;
- идентификация и аутентификация пользователей.

Средства контейнеризации реализуют функциональные возможности по созданию образов контейнеров, формированию среды выполнения контейнеров и обеспечения выполнения их процессов, запуску контейнера и управление данным контейнером.

В состав ОС входит программное обеспечение Docker для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации.

Подробно функции описаны в документах РУСБ.10015-01 95 01-1 и РУСБ.10015-01 97 01-1.

4.14. Сервис электронной подписи

Комплекс программ из состава ОС предоставляет сервис электронной подписи (СЭП), обеспечивающий интеграцию с дополнительно устанавливаемыми сертифицированными ФСБ России средствами криптографической защиты информации[1)] (СКЗИ) в целях создания и проверки усиленной квалифицированной электронной подписи[2)] .

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.

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

[2)] Электронная подпись (ЭП) (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).

СЭП обеспечивает создание и проверку электронной подписи электронных документов в соответствии с ГОСТ Р 34.10-2012 средствами сертифицированных СКЗИ.

Более подробная информация приведена в документах РУСБ.10015-01 97 01-1 и РУСБ.10015-01 93 01 «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».

4.15. 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.

Более подробная информация приведена в документе РУСБ.10015-01 97 01-1.

4.16. 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.10015-01 95 01-1.

4.17. 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 ЗСУБД.

Более подробная информация приведена в документах РУСБ.10015-01 95 01-1, РУСБ.10015-01 97 01-1 и РУСБ.10015-01 97 01-3.

4.18. Создание и защита баз данных

ЗСУБД реализована на основе СУБД Tantor и доработана в целях интеграции со средствами защиты информации ОС, в том числе в соответствии с требованием интеграции с ОС в части мандатного управления доступом к информации. ЗСУБД содержит реализацию ДП-модели управления доступом и информационными потоками. Данная ДП-модель описывает все аспекты дискреционного, мандатного и ролевого управления доступом и информационными потоками. Все программные компоненты ЗСУБД включены в состав ОС.

ЗСУБД 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.

ЗСУБД имеет клиент-серверную архитектуру. Сеанс состоит из следующих сотрудничающих процессов (программ):

- серверный процесс, который управляет файлами базы данных, принимает подключения к базе данных от клиентских приложений и выполняет действия с базой данных от имени клиентов;
- клиентское приложение пользователя, выполняющее операции с базой данных. Клиентские приложения могут представлять собой как инструмент с текстовым интерфейсом, так и графическое приложение, веб-сервер, который обращается к

базе данных для отображения веб-страниц, или специализированный инструмент для обслуживания базы данных.

Клиент и сервер могут находиться на разных хостах. В этом случае они обмениваются данными по сетевому соединению TCP/IP. Сервер ЗСУБД может обрабатывать несколько одновременных подключений от клиентов.

ЗСУБД предоставляет следующие возможности:

- управление данными во внешней памяти;
- управление данными в оперативной памяти;
- выполнение запросов и манипулирования данными (DML/DDL);
- поддержка большого количества символьных кодировок
- управление транзакциями;
- журнализация изменений;
- репликация;
- работа в составе отказоустойчивого кластера с механизмом переключения нагрузки на основной узел кластера.

Дискреционное управление доступом к данным объектно-реляционной ЗСУБД обеспечивается в понятиях реляционной ЗСУБД. 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.

В ЗСУБД для управления правами на доступ к БД используется концепция ролей — ролевое управление доступом. Система привилегий ЗСУБД предназначена для передачи отдельным пользователям прав выполнения определенных административных действий. Обычный пользователь системы не имеет дополнительных привилегий.

Роли ЗСУБД отличаются от пользователей ОС. Каждое подключение к серверу ЗСУБД осуществляется от имени определенной роли, которая определяет первичные права доступа для команд, используемых в контексте подключения. Роли ЗСУБД назначается набор атрибутов, определяющих ее права и взаимодействующих с системой аутентификации клиента.

В основе механизма мандатного управления доступом в ЗСУБД лежит управление доступом к защищаемым ресурсам БД на основе иерархических и неиерархических меток доступа. Это позволяет реализовать многоуровневую защиту с обеспечением разграничения доступа

пользователей к защищаемым ресурсам БД и управление потоками информации. В качестве иерархических и неиерархических меток доступа при использовании ЗСУБД в ОС используются метки безопасности ОС. ЗСУБД не имеет собственного механизма назначения, хранения и модификации меток пользователей и использует для этого механизмы ОС. Проверка мандатных прав доступа к объектам ЗСУБД осуществляется одновременно с проверкой дискреционных прав доступа к ним.

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

При попытке соединения с сервером ЗСУБД клиентское приложение указывает пользователя ЗСУБД, от имени которого осуществляется подключение. В пределах окружения SQL активное имя пользователя ЗСУБД определяет права на объекты БД. Корректная работа с ЗСУБД предполагает использование механизма ЕПП.

В ЗСУБД реализована возможность контроля целостности конфигурации ЗСУБД, БД, процедур, хранимых в БД.

ЗСУБД функционирует в отказоустойчивом кластере, обеспечивающем её доступность, за счет одновременного функционирования нескольких экземпляров ЗСУБД.

С применением сертифицированных функций ОС ЗСУБД обеспечивает удаление БД и журналов, используемых ЗСУБД, путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями, а также блокирование загрузки в адресное пространство ЗСУБД программного обеспечения, не включенного в перечень (список) программного обеспечения, разрешенного для выполнения.

В случае возникновения ошибок в хранящихся данных, нарушения целостности или в случае программного и/или аппаратного сбоя сервера ЗСУБД 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. Резервное копирование и восстановление осуществляется с использованием утилит `pg_dump`, `pg_dumpall` и `pg_restore`, а также методов физического резервного копирования, таких как `pg_basebackup`. Для регистрации событий безопасности и действий пользователей в ЗСУБД используется `pgAudit`.

Более подробная информация и описание ЗСУБД приведены в документе РУСБ.10015-01 97 01-3.

4.19. 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.

Более подробная информация приведена в документе РУСБ.10015-01 95 01-1.

4.20. 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 обслуживания 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.

Более подробная информация приведена в документе РУСБ.10015-01 95 01-1.

5. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

5.1. Входными данными для ОС являются:

- обращение субъектов доступа (пользователей, процессов) 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 и т. п.

ПЕРЕЧЕНЬ ТЕРМИНОВ

Хеш — строка бит, являющаяся выходным результатом функции хеширования.

Цифровая подпись — результат преобразования хеша для его защиты от несанкционированного доступа с использованием закрытого ключа (не предназначена для криптографической защиты информации).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных
ЕПП — единое пространство пользователей
ЗСУБД — защищенная система управления базами данных
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

ACL — Access Control List (список контроля доступа)
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 сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		Все				РУСБ.14.03-11 от 20.10.11			
2		Все				РУСБ.14.04-13 от 21.03.13			
3		Все				РУСБ.14.05-14 от 19.11.14			
4		Все				РУСБ.14.02-16 от 17.02.16			
5		Все				РУСБ.14.03-17 от 05.04.17			
6		Все				РУСБ.14.02-18 от 11.04.18			
7		Все				РУСБ.14.03-18 от 19.04.18			
8		Все				РУСБ.08-20 от 18.02.20			
9		Все				РУСБ.20-20 от 23.07.20			
10		Все				РУСБ.06-21 от 01.04.21			
11		Все				РУСБ.12-21 от 30.07.21			
12		Все				РУСБ.10-22 от 03.11.22			
13		Все				РУСБ.03-23 от 26.04.23			
14		Все				РУСБ.14-23 от 26.12.23			
15		Все				РУСБ.02-24 от 25.03.24			
16		Все				РУСБ.04-24 от 01.07.24			