Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 5.2 Desktop

Задание по безопасности

МСВСфера5.2_Desktop_ЗБ

Версия: 1.0

2009

Ссылки

[CAPP] Controlled Access Protection Profile, Issue 1.d, 8 October 1999
Безопасность информационных технологий. Управляемый доступ. Профиль защиты, 2002

[LSPP] Labeled Security Protection Profile, Issue 1.b, 8 October 1999
Безопасность информационных технологий. Меточная защита. Профиль защиты. (первая редакция) 2002

[RBACPP] Role-Based Access Control Protection Profile, Version 1.0, 30 July 1998

[GUIDE] ISO/IEC PDTR 15446 Title: Information technology – Security techniques – Guide for the production of protection profiles and security targets, ISO/IEC JTC 1/SC 27 N 2449, 2000- 01-04

ITSEC Information Technology Security Evaluation Criteria, Version 1.2, CEC, June 1991

SSHv2 Internet Draft: SSH Transport Layer Protocol; http://www.ietf.org/internet-drafts/draft-ietf- secsh-transport-24.txt

SSLv3 The SSL Protocol Version 3.0, http://wp.netscape.com/eng/ssl3/draft302.txt

[TCSEC] U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria

[X.509] ITU-T recommendation X.509 | ISO/IEC 9594-8: Information Technology - Open systems interconnection - the directory: public-key and attribute certificate frameworks

[ОК] ГОСТ Р ИСО/МЭК 15408–2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3.
Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, Part 1 to 3
htpp://www.commoncriteria.org/ri/FinalRI/Final_Interpretations

[ОМО] Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий, ФСТЭК России, 2005 (проект)
Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

[РД СВТ] Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992

Перечень сокращений

ACL	Access Control List (Список управления доступом)
AS	Advanced Desktop
CD	Compact Disc (Компакт-диск)
DAC	Discretionary Access Control (Дискреционное управление доступом)
RBAC	Role-Based Access Control (Управление доступом на основе ролей)
DVD	Digital Versatile Disc (Универсальный цифровой диск)
FSO	File System Object (Объект файловой системы)
FTP	File Transfer Protocol (Протокол передачи файлов)
IEC	International Electrotechnical Commission (Международная Электротехническая Комиссия)
IP	Internet Protocol (Межсетевой протокол)
IPC	Inter-Process Communication (Связь между процессами)
ISO	International Standards Organization (Международная организация по стандартизации)
MD5	Message Digest 5 (Алгоритм хэширования 5)
PAM	Pluggable Authentication Module (Подключаемый модуль аутентификации)
МСВСфера 5.2 Desktop	Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 5.2 Desktop
SSH	Secure Shell (Безопасная оболочка Shell)
TCP	Transmission Control Protocol (Протокол управления передачей)
UDP	User Datagram Protocol (Протокол пользовательских дейтаграмм)
VFS	Virtual File System (Виртуальная файловая система)
VMM	Virtual memory manager (Менеджер виртуальной памяти)
WS	Work station (Рабочая станция)
ЗБ	Задание по безопасности
ИТ	Информационная технология
ОДФ	Область действия ФБО
ОК	Общие критерии

ОО	Объект оценки
ОС	Операционная система
ОУД	Оценочный уровень доверия
ПБО	Политика безопасности организации
ПЗ	Профиль защиты
ПЗКД (CAPP)	Контролируемый (дискреционный) доступ, профиль защиты
ПЗОР (RBACPP)	Role-Based Access Control Protection Profile (Профиль защиты, основанный на ролях)
ПО	Программное обеспечение
СФБ	Стойкость функции безопасности
ФБ	Функция безопасности
ФБО	Функции безопасности ОО
ФТБ	Функциональное требование безопасности

Содержание

1 Введение

Настоящий документ представляет собой ЗБ для оценки клиентской операционной системы с интегрированными пользовательскими приложениями МСВСфера 5.2 Desktop (далее по тексту – МСВСфера 5.2 Desktop).

МСВСфера 5.2 Desktop является высокопроизводительной масштабируемой операционной системой на базе ядра Linux для использования на 32- и 64- разрядных аппаратных платформах.

ОО включает аппаратные средства и встроенное ПО, используемые для выполнения программных компонентов.

1.1 Идентификация ЗБ

Название ЗБ:	Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 5.2 Desktop Задание по безопасности.
Версия ЗБ:	Версия 1.0. 22 октября 2008
Обозначение ЗБ:	МСВСфера5.2_Desktop_ЗБ.
Идентификация ОО:	МСВСфера 5.2 Desktop
Уровень доверия:	ОУД2
Идентификация ОК:	ГОСТ Р ИСО/МЭК 15408–2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Часть 2: Функциональные требования безопасности, Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002. Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999. Расширения, определенные:

- Международными интерпретациями ОК (№ 065);
- Профилями защиты: ПЗКД (CAPP) и ПЗОР (RBACPP).

1.2 Аннотация ЗБ

Настоящее ЗБ предназначено для оценки по требованиям безопасности МСВСфера 5.2 Desktop.

МСВСфера 5.2 Desktop представляет собой удобно и гибко конфигурируемую ОС, основанную на ядре Linux, которая была разработана для обеспечения приемлемого уровня безопасности, обычно требуемого в среде коммерческого применения.

МСВСфера 5.2 Desktop может функционировать с использованием двух различных режимов, называемых режим дискреционного управления доступом (DAC). В режиме DAC модуль безопасности SELinux не реализует политику мандатного управления доступом и не распознает метки чувствительности субъектов и объектов. Модуль безопасности SELinux может быть или полностью заблокирован, или запущен с политикой, не использующей мандаты и метки чувствительности, такой как «целевая» или «строгая», которые лишь добавляют дополнительные ограничения к требованиям дискреционного управления доступом, не касающиеся роли администратора «root».

Несколько клиентов, на которых функционирует МСВСфера 5.2 Desktop, могут быть объединены в сетевую систему. Сетевые соединения могут быть защищены от нарушения конфиденциальности и целостности посредством ФБ, основанных на криптографических механизмах защиты, но эти вопросы находятся за рамками данного ЗБ и оценки.

Оценка фокусируется на использовании МСВСфера 5.2 Desktop в качестве клиента или сети клиентов. Кроме того, оценка предполагает эксплуатацию сети клиентов в невраждебной среде.

1.3 Соответствие ОК

Это ЗБ соответствует части 2 ОК с учетом интерпретаций и части 3 ОК с требуемым ОУД2.

1.4 Стойкость функции

Для данного ОО заявлена средняя стойкость функций безопасности (СФБ-средняя).

1.5 Структура

Структура документа соответствует требованиям части 1 ОК, приложение В.

Раздел 2 содержит описание ОО.

Раздел 3 содержит описание среды безопасности ОО.

Раздел 4 содержит описание целей безопасности.

Раздел 5 содержит описание требований безопасности ИТ.

Раздел 6 содержит краткую спецификацию ОО, включающую детализированную спецификацию функций безопасности ИТ.

Раздел 7 содержит утверждение о соответствии ПЗ.

Раздел 8 содержит обоснование целей безопасности, требований безопасности и краткой спецификации ОО.

1.6 Терминология

Этот подраздел содержит определения технических терминов, которые используются со специфичным для этого документа значением. Термины, определенные в ОК, здесь не повторяются, если не оговорено иное.

Административный пользователь: этот термин относится к пользователю в одной из определенных административных ролей ОО. ОО определяет перечень административных ролей, где каждая роль имеет конкретные административные полномочия. Разделение административных полномочий на различные роли позволяет создавать более управляемую эксплуатационную среду без необходимости иметь отдельного пользователя со всеми административными полномочиями.-

Аутентификационные данные: этот термин включает пароль для каждого пользователя ОС. Аутентификационные механизмы, использующие отличные от пароля аутентификационные данные, в оцениваемой конфигурации не рассматриваются.

Классификация: метка чувствительности, связанная с объектом.

Допуск: метка чувствительности, связанная с субъектом или пользователем.

Доминирование: метка чувствительности А *доминирует* над меткой чувствительности В, если иерархический уровень А больше или равен иерархическому уровню В, и набор категорий метки А является собственным или равным подмножеством набора категорий метки В.

Несравнимые: метки безопасности A и B являются *несравнимыми*, если A не доминирует над B, и B не доминирует над A, например, если ни один из наборов категории одной из меток не являются подмножеством другой.

Данные: произвольные разрядные последовательности в машинной памяти или на носителях данных.

Информация: любые данные, поддерживаемые клиентом, включая передающиеся между системами.

Поименованный объект: объекты, подчиненные управлению доступом, основанном на дискреционном или ролевом методе. Это понятие включает все объекты кроме объектов памяти.

Атрибуты безопасности поименованнного объекта: в МСВСфера 5.2 Desktop к таким атрибутам относятся тип объекта.

Объект: сущности в ОО, принадлежащие к одной из категорий: файловые системы, объекты IPC, объекты памяти и сетевые объекты. Процессы становятся объектами, когда они являются целью системных вызовов, относящихся к сигналам.

Продукт: программные компоненты, которые включает ОО.

Роль: перечень действий, которые может выполнять уполномоченный пользователь после назначения на роль.

Атрибуты безопасности: в соответствии с функциональным требованием FIA_ATD.1, термин «атрибуты безопасности», как минимум, включает: идентификатор пользователя; членство в группе; аутентификационные данные пользователя.

Субъект: существуют два класса субъектов в ОС МСВСфера 5.2 Desktop:

- едоверенный внутренний субъект – это процесс МСВСфера 5.2 Desktop, выполняющийся от имени некоторого пользователя вне ФБО (например, без привилегий).
- оверенный внутренний субъект – это процесс МСВСфера 5.2 Desktop, выполняющийся как часть ФБО (например – обслуживающие демоны и процесс, реализующий идентификацию и аутентификацию пользователей).

Система: совокупность аппаратных средств, компонентов встроенного ПО и ПО продукта ОС МСВСфера 5.2 Desktop, которые вместе связаны в сеть и сконфигурированы в пригодную для использования систему.

Объект оценки (ОО): Функции безопасности МСВСфера 5.2 Desktop.

Тип: ОО позволяет назначать определенный тип субъекту (процессу) и объекту и реализовать управление доступом, основанное на этих типах. Типы используются для управления доступом, основанного на модельной роли.

Пользователь: Любой индивидуум/лицо, которое имеет уникальный идентификатор пользователя и взаимодействует с продуктом.

Атрибуты безопасности пользователя: в соответствии с определенным в функциональном требовании FIA_ATD.1 термином. В «*атрибуты безопасности»* включаются, как минимум, следующие сущности: идентификатор пользователя, членство в группе, пользовательские аутентификационные данные и роли.

1.7 Соглашения

Общие критерии допускают выполнение определенных в части 2 ОК операций с функциональными компонентами. Соответственно в настоящем ЗБ при формулировании ФТБ используются операции **«итерация» «уточнение», «выбор»** и **«назначение».**

Операция «**итерация»** используется для повторного использования одного и того же функционального компонента с целью охватить различные аспекты одного и того же требования (например, идентифицировать несколько типов функций управления безопасностью). Результат операции **«итерация»** в настоящем ЗБ обозначается порядковым номером в круглых скобках вслед за кратким именем компонента.

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения. Результат операции **«уточнение»** в настоящем ЗБ обозначается **полужирным текстом.**

Операция **«выбор»** используется для выбора одного или нескольких элементов из перечня в формулировке требования. Результат операции **«выбор»** в настоящем ЗБ обозначается *подчеркнутым курсивным* текстом.

Операция **«назначение»** используется для присвоения конкретного значения ранее не конкретизированному параметру. Результат операции **«назначение»** в настоящем ЗБ обозначается заключением [значения параметра] в квадратные скобки

2 Описание ОО

Объектом оценки являются функции безопасности МСВСфера 5.2 Desktop.

МСВСфера 5.2 Desktop является универсальной, многопользовательской, многозадачной ОС, основанной на ядре Linux. Она предоставляет платформу для разнообразных приложений в государственной и коммерческой сфере. МСВСфера 5.2 Desktop доступна для широкого круга компьютерных систем.

Оценка МСВСфера 5.2 Desktop охватывает потенциально распределенную, но закрытую сеть клиентов на которых функционируют оцениваемые версии и конфигурации МСВСфера 5.2 Desktop . Платформы отобранных для оценки аппаратных средств состоят из машин, которые уже доступны на рынке и должны быть доступными продолжительное время после окончания оценки. Функции безопасности ОО состоят из функций МСВСфера 5.2 Desktop, которые выполняются в привилегированном режиме, плюс некоторые доверенные процессы. Эти функции осуществляют политику безопасности, определенную в данном ЗБ. Инструментальные средства и команды выполняются в непривилегированном режиме, который также часто используется административным пользователем, нуждающимся в безопасном и надежном способе управления системой. Но, подобно оценке других ОС, они не рассматриваются как часть ФБО.

Аппаратные средства и встроенное ПО BootProm предполагаются частью ОО.

В ОО включена инсталляция с CD-ROM и из раздела локального жесткого диска.

Средства администрирования ОС включают стандартные команды. Среда ОО включает приложения, которые не оцениваются, но используются как непривилегированные инструментальные средства для доступа к общим сервисам системы.

2.1 Предполагаемый метод использования

МСВСфера 5.2 Desktop может обеспечивать обслуживание нескольких пользователей одновременно. После успешного входа в систему пользователи имеют доступ в главную вычислительную среду, позволяющую запускать пользовательские приложения, создавать и получать доступ к файлам, задавать директивы пользователя на уровне оболочки командного процессора. МСВСфера 5.2 Desktop предоставляет адекватные механизмы для разграничения пользователей и защиты их данных.

Использование привилегированных команд ограничено и доступно только административным пользователям.

Как определено в разделе 1.2 этого документа, МСВСфера 5.2 Desktop может конфигурироваться для работы в режиме дискреционного управления доступом (DAC).

МСВСфера 5.2 Desktop предназначен для работы в сетевом окружении с другими экземплярами МСВСфера 5.2 Desktop, а также с иными совместимыми клиентскими системами одного и того же управляемого домена. Все эти системы должны конфигурироваться в соответствии с определенной общей политикой безопасности.

МСВСфера 5.2 Desktop разрешает использование многими пользователями одного или более процессоров, присоединенных внешних и запоминающих устройств для выполнения разнообразных функций, требующих управляемого распределенного доступа к данным, хранимым в системе. Такие инсталляции типичны для вычислительных систем рабочих групп или предприятий, к которым обращаются локальные пользователи, или компьютерных систем с иначе защищенным доступом.

Предполагается, что ответственность за сохранение данных, защищаемых МСВСфера 5.2 Desktop, может делегироваться пользователям ОО. Все данные находятся под управлением ОО. Данные сохраняются в поименованных объектах, и ОО может связать с каждым поименованным объектом описание прав доступа к этому объекту. Всем индивидуальным пользователям назначаются уникальные идентификаторы в рамках отдельной ведущей системы, которая формируется ОО. Этот идентификатор пользователя используется вместе с атрибутами и ролями, назначенными пользователю, как основание для решений по управлению доступом. ОО подтверждает подлинность предъявленного идентификатора пользователя до того, как разрешать ему выполнять дальнейшие действия. ОО внутри себя сопровождает ряд идентификаторов, связанных с процессами, которые получаются из уникального идентификатора пользователя, предъявляемого при входе в систему. Некоторые из этих идентификаторов могут изменяться во время выполнения процесса согласно политике, реализуемой ОО.

ОО предоставляет такие меры безопасности, при которых доступ к объектам данных осуществляется только в соответствии с ограничениями на доступ, наложенными на этот объект его владельцем, административными пользователями, типом и меткой чувствительности объекта. Права владения на поименованные объекты могут передаваться под контролем политики управления доступом.

На объекты данных могут быть назначены дискреционные права доступа (например, чтение, запись, выполнение) субъектов (пользователей). Как только субъекту предоставляется доступ к объекту, его содержание может быть свободно использовано для воздействия на другие доступные этому субъекту объекты.

МСВСфера 5.2 Desktop имеет существенные расширения элементов безопасности по сравнению со стандартными системами UNIX:

- списки управления доступом;
- реализацию доменов и типов;
- журналируемая файловая система (ext3);
- интегрированная аутентификационная структура (PAM);
- специализированная подсистема аудита, которая позволяет учитывать критичные события безопасности и предоставляет административному пользователю инструментальные средства конфигурирования подсистемы аудита и оценки записей аудита;
- базовые функции проверки комплекта оборудования позволяют по требованию административного пользователя проверять, правильно ли обеспечиваются основные функции безопасности аппаратных средств, на которые полагается ОО.

2.2 Краткое изложение свойств безопасности

Первичные свойства безопасности продукта:

- Идентификация и аутентификация;
- Аудит;
- Дискреционное управление доступом;
- Функциональные возможности повторного использования объекта;
- Администрирование безопасности;
- Безопасные связи;
- Защита ФБО.

Данные первичные свойства безопасности поддерживаются разделением домена и ссылаются на посредничество, которое всегда обеспечивает вызов этих свойств и невозможность их обхода.

Идентификация и аутентификация

МСВСфера 5.2 Desktop предоставляет идентификацию и аутентификацию пользователей, основанную на паролях, используя подключаемые аутентификационные модули (PAM). Качество используемых паролей может

определяться параметрами конфигурации, управляемыми МСВСфера 5.2 Desktop. Для режима доверенной загрузки МСВСфера 5.2 Desktop используется метод аутентификации, основанный на электронных ключах. Другие аутентификационные методы (например, аутентификация Kerberos,), поддерживаемые МСВСфера 5.2 Desktop в качестве подключаемых аутентификационных модулей, не являются частью оцениваемой конфигурации. Включаются функции аутентификации, обеспечивающие среднюю стойкость пароля, ограничивающие использование команды su и вход в систему для «root» конкретными терминалами.

При установлении сеансов пользователей программное обеспечение ФБО реализует ограничение набора активных ролей, доступных пользователю разрешенными ему ролями, и обеспечивает возможность установления сеансов только с непустым набором активных ролей.

Аудит

ОО предоставляет возможность аудита, которая позволяет генерировать записи аудита критичных событий безопасности. Административный пользователь может выбрать события аудита и пользователей, для которых аудит является активным. Список событий, подвергаемых аудиту, определен в разделах 5 и 6.

ОО обеспечивает инструментальные средства, помогающие административному пользователю извлекать из всех записей аудита, собранных ОО, конкретные записи о типах событий, связанных с конкретными пользователями, объектами файловой системы, временными интервалами. Записи аудита сохраняются в тексте ASCII, поэтому преобразование информации в читаемый формат не требуется.

Система аудита определяет, когда возможность записи в журнал аудита отсутствует при превышении конфигурируемых границ, и системный администратор может определить действия, которые необходимо предпринять при переполнении журнала: запись сообщения в системный журнал для администратора; переключение системы в однопользовательский режим (это предотвращает возможность работы всех пользователей, инициирующих действия, подвергаемые аудиту) или останов системы.

Функция аудита также предотвращает потерю записей аудита вследствие исчерпания внутренних буферов аудита. Выполнение процессов, пытающихся создавать записи аудита при уже заполненных внутренних буферах аудита, должно приостанавливаться, пока требуемые ресурсы снова не станут доступными. В

маловероятном случае невосполнимого исчерпания ресурсов, компонент аудита ядра инициирует панику ядра для предотвращения всех дальнейших событий аудита.

Дискреционное управление доступом

Дискреционное управление доступом (DAC) ограничивает доступ к объектам файловой системы, основываясь на Списках управления доступом (ACL), которые включают стандартные разрешения UNIX для идентификатора пользователя, группы и других атрибутов. Механизмы управления доступом также защищают объекты IPC от несанкционированного доступа.

МСВСфера 5.2 включает файловую систему ext3, которая поддерживает POSIX ACL. Эти ACL позволяют определять права доступа к файлам в файловой системе данного типа с детализацией до прав отдельного пользователя.

Объекты IPC используют биты разрешений для дискреционного управления доступом.

Повторное использование объекта

Объекты файловой системы, а также память и объекты IPC должны освобождаться прежде, чем их смогут повторно использовать процессы, принадлежащие различным пользователям.

Администрирование безопасности

Администрирование критичных параметров безопасности ОО выполняется административными пользователями. Для сопровождения системы используется ряд команд, которые требуют привилегий «root». Параметры безопасности сохраняются в конкретных файлах, которые обслуживаются механизмами управления доступом ОО и защищаются ими от несанкционированного доступа неадминистративных пользователей.

В режиме DAC и режиме MAC управление безопасностью может распределяться между различными ролями.

Защита ФБО

Во время функционирования ОО, ПО и данные ядра защищаются аппаратными механизмами защиты памяти. Память и компоненты управления процессами ядра обеспечивают запрет доступа пользовательского процесса к памяти ядра или памяти, принадлежащей другим процессам.

ПО и данные, не принадлежащие ядру, защищаются ФБО посредством DAC обрабатываются механизмами изоляции. В оцениваемой конфигурации зарезервирован идентификатор пользователя «root», которому принадлежат каталоги и файлы, определяющие конфигурацию ФБО. В целом, файлы и каталоги,

содержащие внутренние данные ФБО (например, файлы конфигурации, очереди пакетного задания), также защищаются от чтения в соответствии с разрешениями DAC.

ОО, включая аппаратные средства и компоненты встроенного ПО, должен быть физически защищен от несанкционированного доступа. Системное ядро выступает посредником для всех попыток доступа к аппаратным компонентам, защищенных от прямого доступа со стороны пользовательских программ. Пользовательский процесс может выполнять непривилегированные команды и читать или писать в память и регистры процессора в рамках, определенных ядром для пользовательского процесса, за исключением тех типов доступа, в которых ядро является посредником. Все другие типы доступа к аппаратным ресурсам со стороны пользовательских процессов могут выполняться только посредством запросов к ядру (в форме системных вызовов).

ОО предоставляет инструментарий, который позволяет административному пользователю проверять правильность функционирования используемого оборудования посредством выполнения тестов проверки системной памяти, особенностей защиты памяти центрального процессора и его правильного разделения между состояниями супервизор и пользователь.

2.3 Программное обеспечение

МСВСфера 5.2 Desktop и документация поставляются на DVD или через защищенный репозиторий.

Список пакетов (таблица 2.1), составляющих МСВСфера 5.2 Desktop в оцененной конфигурации, включает как пакеты, которые вносят свой вклад в ФБО, так и пакеты, которые содержат недоверенные пользовательские программы из дистрибутива. Следует отметить, что дополнительные недоверенные пользовательские программы могут устанавливаться и использоваться, если они не выполняют команды setuid или setgid для «root». Список содержит имена пакетов с номерами их версии.

Таблица 2.1 Список пакетов оцененной конфигурации ОО

Платформа x86	*Платформа x86_64*
a2ps-4.13b-57.2.el5.i386.rpm	a2ps-4.13b-57.2.el5.x86_64.rpm
acl-2.2.39-3.el5.i386.rpm	acl-2.2.39-3.el5.x86_64.rpm
acpid-1.0.4-5.i386.rpm	acpid-1.0.4-5.x86_64.rpm
alacarte-0.10.0-1.fc6.noarch.rpm	alacarte-0.10.0-1.fc6.noarch.rpm
alsa-lib-1.0.14-1.rc4.el5.i386.rpm	alsa-lib-1.0.14-1.rc4.el5.i386.rpm

alsa-utils-1.0.14-3.rc4.el5.i386.rpm	alsa-lib-1.0.14-1.rc4.el5.x86_64.rpm
amtu-1.0.6-1.el5.i386.rpm	alsa-utils-1.0.14-3.rc4.el5.x86_64.rpm
anacron-2.3-45.el5.i386.rpm	amtu-1.0.6-1.el5.x86_64.rpm
antlr-2.7.6-4jpp.2.i386.rpm	anacron-2.3-45.el5.x86_64.rpm
apmd-3.2.2-5.i386.rpm	antlr-2.7.6-4jpp.2.x86_64.rpm
apr-1.2.7-11.i386.rpm	apr-1.2.7-11.x86_64.rpm
apr-util-1.2.7-7.el5.i386.rpm	apr-util-1.2.7-7.el5.x86_64.rpm
aspell-0.60.3-7.1.i386.rpm	aspell-0.60.3-7.1.i386.rpm
aspell-en-6.0-2.1.i386.rpm	aspell-0.60.3-7.1.x86_64.rpm
aspell-ru-0.99f7-2.2.2.i386.rpm	aspell-en-6.0-2.1.x86_64.rpm
at-3.1.8-82.fc6.i386.rpm	aspell-ru-0.99f7-2.2.2.x86_64.rpm
atk-1.12.2-1.fc6.i386.rpm	at-3.1.8-82.fc6.x86_64.rpm
at-spi-1.7.11-3.el5.i386.rpm	atk-1.12.2-1.fc6.i386.rpm
attr-2.4.32-1.1.i386.rpm	atk-1.12.2-1.fc6.x86_64.rpm
audiofile-0.2.6-5.i386.rpm	at-spi-1.7.11-3.el5.i386.rpm
audit-1.6.5-9.el5.i386.rpm	at-spi-1.7.11-3.el5.x86_64.rpm
audit-libs-1.6.5-9.el5.i386.rpm	attr-2.4.32-1.1.x86_64.rpm
audit-libs-python-1.6.5-9.el5.i386.rpm	audiofile-0.2.6-5.i386.rpm
authconfig-5.3.21-3.el5.i386.rpm	audiofile-0.2.6-5.x86_64.rpm
authconfig-gtk-5.3.21-3.el5.i386.rpm	audit-1.6.5-9.el5.x86_64.rpm
autofs-5.0.1-0.rc2.88.i386.rpm	audit-libs-1.6.5-9.el5.i386.rpm
avahi-0.6.16-1.el5.i386.rpm	audit-libs-1.6.5-9.el5.x86_64.rpm
avahi-glib-0.6.16-1.el5.i386.rpm	audit-libs-python-1.6.5-9.el5.x86_64.rpm
basesystem-8.0-5.1.1.noarch.rpm	authconfig-5.3.21-3.el5.x86_64.rpm
bash-3.2-21.el5.i386.rpm	authconfig-gtk-5.3.21-3.el5.x86_64.rpm
bc-1.06-21.i386.rpm	autofs-5.0.1-0.rc2.88.x86_64.rpm
beecrypt-4.1.2-10.1.1.i386.rpm	avahi-0.6.16-1.el5.i386.rpm
bind-libs-9.3.4-6.P1.el5.i386.rpm	avahi-0.6.16-1.el5.x86_64.rpm
bind-utils-9.3.4-6.P1.el5.i386.rpm	avahi-glib-0.6.16-1.el5.i386.rpm
binutils-2.17.50.0.6-6.el5.i386.rpm	avahi-glib-0.6.16-1.el5.x86_64.rpm
bitmap-fonts-0.3-5.1.1.noarch.rpm	basesystem-8.0-5.1.1.noarch.rpm
bitstream-vera-fonts-1.10-7.noarch.rpm	bash-3.2-21.el5.x86_64.rpm
bluez-gnome-0.5-5.fc6.i386.rpm	bc-1.06-21.x86_64.rpm
bluez-libs-3.7-1.i386.rpm	beecrypt-4.1.2-10.1.1.x86_64.rpm
bluez-utils-3.7-2.i386.rpm	bind-libs-9.3.4-6.P1.el5.x86_64.rpm
brlapi-0.4.1-1.fc6.i386.rpm	bind-utils-9.3.4-6.P1.el5.x86_64.rpm
bsf-2.3.0-11jpp.1.i386.rpm	binutils-2.17.50.0.6-6.el5.x86_64.rpm
bsh-1.3.0-9jpp.1.i386.rpm	bitmap-fonts-0.3-5.1.1.noarch.rpm
bzip2-1.0.3-3.i386.rpm	bitstream-vera-fonts-1.10-7.noarch.rpm
bzip2-libs-1.0.3-3.i386.rpm	bluez-gnome-0.5-5.fc6.x86_64.rpm
cairo-1.2.4-5.el5.i386.rpm	bluez-libs-3.7-1.x86_64.rpm

ccid-1.0.1-6.el5.i386.rpm	bluez-utils-3.7-2.x86_64.rpm
cdparanoia-libs-alpha9.8-27.2.i386.rpm	brlapi-0.4.1-1.fc6.x86_64.rpm
cdrdao-1.2.1-2.i386.rpm	bsf-2.3.0-11jpp.1.x86_64.rpm
cdrecord-2.01-10.i386.rpm	bsh-1.3.0-9jpp.1.x86_64.rpm
checkpolicy-1.33.1-4.el5.i386.rpm	bzip2-1.0.3-3.x86_64.rpm
chkconfig-1.3.30.1-2.i386.rpm	bzip2-libs-1.0.3-3.i386.rpm
chkfontpath-1.10.1-1.1.i386.rpm	bzip2-libs-1.0.3-3.x86_64.rpm
comps-extras-11.1-1.1.noarch.rpm	cairo-1.2.4-5.el5.i386.rpm
conman-0.1.9.2-8.el5.i386.rpm	cairo-1.2.4-5.el5.x86_64.rpm
control-center-2.16.0-16.el5.i386.rpm	ccid-1.0.1-6.el5.x86_64.rpm
coolkey-1.1.0-6.el5.i386.rpm	cdparanoia-libs-alpha9.8-27.2.i386.rpm
coreutils-5.97-14.el5.i386.rpm	cdparanoia-libs-alpha9.8-27.2.x86_64.rpm
cpio-2.6-20.i386.rpm	cdrdao-1.2.1-2.x86_64.rpm
cpp-4.1.2-42.el5.i386.rpm	cdrecord-2.01-10.x86_64.rpm
cpuspeed-1.2.1-3.el5.i386.rpm	checkpolicy-1.33.1-4.el5.x86_64.rpm
cracklib-2.8.9-3.3.i386.rpm	chkconfig-1.3.30.1-2.x86_64.rpm
cracklib-dicts-2.8.9-3.3.i386.rpm	chkfontpath-1.10.1-1.1.x86_64.rpm
crash-4.0-5.0.3.i386.rpm	comps-extras-11.1-1.1.noarch.rpm
crontabs-1.10-8.noarch.rpm	conman-0.1.9.2-8.el5.x86_64.rpm
cryptsetup-luks-1.0.3-2.2.el5.i386.rpm	control-center-2.16.0-16.el5.i386.rpm
cups-1.2.4-11.18.el5.i386.rpm	control-center-2.16.0-16.el5.x86_64.rpm
cups-libs-1.2.4-11.18.el5.i386.rpm	coolkey-1.1.0-6.el5.i386.rpm
curl-7.15.5-2.el5.i386.rpm	coolkey-1.1.0-6.el5.x86_64.rpm
cyrus-sasl-2.1.22-4.i386.rpm	coreutils-5.97-14.el5.x86_64.rpm
cyrus-sasl-lib-2.1.22-4.i386.rpm	cpio-2.6-20.x86_64.rpm
cyrus-sasl-md5-2.1.22-4.i386.rpm	cpp-4.1.2-42.el5.x86_64.rpm
cyrus-sasl-plain-2.1.22-4.i386.rpm	cpuspeed-1.2.1-3.el5.x86_64.rpm
db4-4.3.29-9.fc6.i386.rpm	cracklib-2.8.9-3.3.i386.rpm
dbus-1.0.0-7.el5.i386.rpm	cracklib-2.8.9-3.3.x86_64.rpm
dbus-glib-0.70-5.i386.rpm	cracklib-dicts-2.8.9-3.3.x86_64.rpm
dbus-python-0.70-7.el5.i386.rpm	crash-4.0-5.0.3.x86_64.rpm
dbus-x11-1.0.0-7.el5.i386.rpm	crontabs-1.10-8.noarch.rpm
dcraw-0.0.20060521-1.1.i386.rpm	cryptsetup-luks-1.0.3-2.2.el5.i386.rpm
dejavu-lgc-fonts-2.10-1.noarch.rpm	cryptsetup-luks-1.0.3-2.2.el5.x86_64.rpm
Deployment_Guide-en-US-5.2-9.noarch.rpm	cups-1.2.4-11.18.el5.x86_64.rpm
Deployment_Guide-ru-RU-5.2-9.noarch.rpm	cups-libs-1.2.4-11.18.el5.i386.rpm
desktop-backgrounds-basic-2.0-37.noarch.rpm	cups-libs-1.2.4-11.18.el5.x86_64.rpm
desktop-file-utils-0.10-7.i386.rpm	curl-7.15.5-2.el5.x86_64.rpm
desktop-printing-0.19-20.1.el5.i386.rpm	cyrus-sasl-2.1.22-4.x86_64.rpm
device-mapper-1.02.24-1.el5.i386.rpm	cyrus-sasl-lib-2.1.22-4.i386.rpm
device-mapper-event-1.02.24-1.el5.i386.rpm	cyrus-sasl-lib-2.1.22-4.x86_64.rpm

device-mapper-multipath-0.4.7-17.el5.i386.rpm	cyrus-sasl-md5-2.1.22-4.x86_64.rpm
dhcdbd-2.2-1.el5.i386.rpm	cyrus-sasl-plain-2.1.22-4.i386.rpm
dhclient-3.0.5-13.el5.i386.rpm	cyrus-sasl-plain-2.1.22-4.x86_64.rpm
dhcpv6-client-1.0.10-4.el5.i386.rpm	db4-4.3.29-9.fc6.i386.rpm
diffutils-2.8.1-15.2.3.el5.i386.rpm	db4-4.3.29-9.fc6.x86_64.rpm
dmidecode-2.7-1.28.2.el5.i386.rpm	dbus-1.0.0-7.el5.i386.rpm
dmraid-1.0.0.rc13-9.el5.i386.rpm	dbus-1.0.0-7.el5.x86_64.rpm
docbook-dtds-1.0-30.1.noarch.rpm	dbus-glib-0.70-5.i386.rpm
dos2unix-3.1-27.1.i386.rpm	dbus-glib-0.70-5.x86_64.rpm
dosfstools-2.11-6.2.el5.i386.rpm	dbus-python-0.70-7.el5.x86_64.rpm
dump-0.4b41-2.fc6.i386.rpm	dbus-x11-1.0.0-7.el5.x86_64.rpm
dvd+rw-tools-7.0-0.el5.3.i386.rpm	dcraw-0.0.20060521-1.1.x86_64.rpm
e2fsprogs-1.39-15.el5.i386.rpm	dejavu-lgc-fonts-2.10-1.noarch.rpm
e2fsprogs-libs-1.39-15.el5.i386.rpm	Deployment_Guide-en-US-5.2-9.noarch.rpm
ecryptfs-utils-41-1.el5.i386.rpm	Deployment_Guide-ru-RU-5.2-9.noarch.rpm
ed-0.2-38.2.2.i386.rpm	desktop-backgrounds-basic-2.0-37.noarch.rpm
eel2-2.16.1-1.el5.i386.rpm	desktop-file-utils-0.10-7.x86_64.rpm
eject-2.1.5-4.2.el5.i386.rpm	desktop-printing-0.19-20.1.el5.x86_64.rpm
ekiga-2.0.2-7.0.2.i386.rpm	device-mapper-1.02.24-1.el5.i386.rpm
elfutils-libelf-0.125-3.el5.i386.rpm	device-mapper-1.02.24-1.el5.x86_64.rpm
emacs-21.4-20.el5.i386.rpm	device-mapper-event-1.02.24-1.el5.x86_64.rpm
emacs-common-21.4-20.el5.i386.rpm	device-mapper-multipath-0.4.7-17.el5.x86_64.rpm
emacs-leim-21.4-20.el5.i386.rpm	dhcdbd-2.2-1.el5.x86_64.rpm
emacspeak-23.0-3.el5.noarch.rpm	dhclient-3.0.5-13.el5.x86_64.rpm
enscript-1.6.4-4.1.el5.i386.rpm	dhcpv6-client-1.0.10-4.el5.x86_64.rpm
eog-2.16.0.1-6.el5.i386.rpm	diffutils-2.8.1-15.2.3.el5.x86_64.rpm
esc-1.0.0-33.el5.i386.rpm	dmidecode-2.7-1.28.2.el5.x86_64.rpm
esound-0.2.36-3.i386.rpm	dmraid-1.0.0.rc13-9.el5.x86_64.rpm
ethtool-5-1.el5.i386.rpm	docbook-dtds-1.0-30.1.noarch.rpm
evince-0.6.0-8.el5.i386.rpm	dos2unix-3.1-27.1.x86_64.rpm
evolution-2.12.3-8.el5.i386.rpm	dosfstools-2.11-6.2.el5.x86_64.rpm
evolution-connector-2.12.3-4.el5.i386.rpm	dump-0.4b41-2.fc6.x86_64.rpm
evolution-data-server-1.12.3-6.el5.i386.rpm	dvd+rw-tools-7.0-0.el5.3.x86_64.rpm
evolution-webcal-2.7.1-6.i386.rpm	e2fsprogs-1.39-15.el5.x86_64.rpm
expat-1.95.8-8.2.1.i386.rpm	e2fsprogs-libs-1.39-15.el5.i386.rpm
fbset-2.1-22.i386.rpm	e2fsprogs-libs-1.39-15.el5.x86_64.rpm
festival-1.95-5.2.1.i386.rpm	ecryptfs-utils-41-1.el5.i386.rpm
file-4.17-13.i386.rpm	ecryptfs-utils-41-1.el5.x86_64.rpm

file-roller-2.16.0-2.fc6.i386.rpm	ed-0.2-38.2.2.x86_64.rpm
filesystem-2.4.0-1.i386.rpm	eel2-2.16.1-1.el5.i386.rpm
findutils-4.2.27-4.1.i386.rpm	eel2-2.16.1-1.el5.x86_64.rpm
finger-0.17-32.2.1.1.i386.rpm	eject-2.1.5-4.2.el5.x86_64.rpm
firefox-3.0-0.beta5.6.el5.i386.rpm	ekiga-2.0.2-7.0.2.x86_64.rpm
firstboot-1.4.27.7-1.sphere.i386.rpm	elfutils-libelf-0.125-3.el5.x86_64.rpm
firstboot-custom-1.0.0-2.sphere.2.i386.rpm	emacs-21.4-20.el5.x86_64.rpm
firstboot-tui-1.4.27.7-1.sphere.i386.rpm	emacs-common-21.4-20.el5.x86_64.rpm
flac-1.1.2-28.el5_0.1.i386.rpm	emacs-leim-21.4-20.el5.x86_64.rpm
fontconfig-2.4.1-7.el5.i386.rpm	emacspeak-23.0-3.el5.noarch.rpm
fonts-KOI8-R-100dpi-1.0-9.1.1.noarch.rpm	enscript-1.6.4-4.1.el5.x86_64.rpm
fonts-KOI8-R-1.0-9.1.1.noarch.rpm	eog-2.16.0.1-6.el5.x86_64.rpm
fonts-KOI8-R-75dpi-1.0-9.1.1.noarch.rpm	esc-1.0.0-33.el5.x86_64.rpm
foomatic-3.0.2-38.1.el5.i386.rpm	esound-0.2.36-3.i386.rpm
freeglut-2.4.0-7.1.el5.i386.rpm	esound-0.2.36-3.x86_64.rpm
freetype-2.2.1-19.el5.i386.rpm	ethtool-5-1.el5.x86_64.rpm
ftp-0.17-33.fc6.i386.rpm	evince-0.6.0-8.el5.x86_64.rpm
gail-1.9.2-1.fc6.i386.rpm	evolution-2.12.3-8.el5.i386.rpm
gamin-0.1.7-8.el5.i386.rpm	evolution-2.12.3-8.el5.x86_64.rpm
gamin-python-0.1.7-8.el5.i386.rpm	evolution-connector-2.12.3-4.el5.x86_64.rpm
gawk-3.1.5-14.el5.i386.rpm	evolution-data-server-1.12.3-6.el5.i386.rpm
gcalctool-5.8.25-1.el5.i386.rpm	evolution-data-server-1.12.3-6.el5.x86_64.rpm
GConf2-2.14.0-9.el5.i386.rpm	evolution-webcal-2.7.1-6.x86_64.rpm
gd-2.0.33-9.4.el5_1.1.i386.rpm	expat-1.95.8-8.2.1.i386.rpm
gdbm-1.8.0-26.2.1.i386.rpm	expat-1.95.8-8.2.1.x86_64.rpm
gdk-pixbuf-0.22.0-25.el5.i386.rpm	fbset-2.1-22.x86_64.rpm
gdm-2.16.0-46.el5.i386.rpm	file-4.17-13.x86_64.rpm
gedit-2.16.0-9.el5.i386.rpm	file-roller-2.16.0-2.fc6.x86_64.rpm
gettext-0.14.6-4.el5.i386.rpm	filesystem-2.4.0-1.x86_64.rpm
ghostscript-8.15.2-9.1.el5_1.1.i386.rpm	findutils-4.2.27-4.1.x86_64.rpm
ghostscript-fonts-5.50-13.1.1.noarch.rpm	finger-0.17-32.2.1.1.x86_64.rpm
giflib-4.1.3-7.1.el5.1.i386.rpm	firefox-3.0-0.beta5.6.el5.i386.rpm
gimp-2.2.13-2.0.7.el5.i386.rpm	firefox-3.0-0.beta5.6.el5.x86_64.rpm
gimp-data-extras-2.0.1-1.1.1.noarch.rpm	firstboot-1.4.27.7-1.sphere.x86_64.rpm
gimp-help-2-0.1.0.10.1.1.noarch.rpm	firstboot-custom-1.0.0-2.sphere.2.x86_64.rpm
gimp-libs-2.2.13-2.0.7.el5.i386.rpm	firstboot-tui-1.4.27.7-1.sphere.x86_64.rpm
gimp-print-4.2.7-22.i386.rpm	flac-1.1.2-28.el5_0.1.x86_64.rpm
gimp-print-plugin-4.2.7-22.i386.rpm	fontconfig-2.4.1-7.el5.i386.rpm

gimp-print-utils-4.2.7-22.i386.rpm	fontconfig-2.4.1-7.el5.x86_64.rpm
gjdoc-0.7.7-12.el5.i386.rpm	fonts-KOI8-R-100dpi-1.0-9.1.1.noarch.rpm
glib-1.2.10-20.el5.i386.rpm	fonts-KOI8-R-1.0-9.1.1.noarch.rpm
glib2-2.12.3-2.fc6.i386.rpm	fonts-KOI8-R-75dpi-1.0-9.1.1.noarch.rpm
glibc-2.5-24.i686.rpm	foomatic-3.0.2-38.1.el5.x86_64.rpm
glibc-common-2.5-24.i386.rpm	freeglut-2.4.0-7.1.el5.i386.rpm
glx-utils-6.5.1-7.5.el5.i386.rpm	freeglut-2.4.0-7.1.el5.x86_64.rpm
gnome-applets-2.16.0.1-19.el5.i386.rpm	freetype-2.2.1-19.el5.i386.rpm
gnome-audio-2.0.0-3.1.1.noarch.rpm	freetype-2.2.1-19.el5.x86_64.rpm
gnome-backgrounds-2.15.92-1.fc6.noarch.rpm	ftp-0.17-33.fc6.x86_64.rpm
gnome-desktop-2.16.0-1.fc6.i386.rpm	gail-1.9.2-1.fc6.i386.rpm
gnome-doc-utils-0.8.0-2.fc6.noarch.rpm	gail-1.9.2-1.fc6.x86_64.rpm
gnome-icon-theme-2.16.0.1-4.el5.noarch.rpm	gamin-0.1.7-8.el5.i386.rpm
gnome-keyring-0.6.0-1.fc6.i386.rpm	gamin-0.1.7-8.el5.x86_64.rpm
gnome-mag-0.13.1-1.fc6.i386.rpm	gamin-python-0.1.7-8.el5.x86_64.rpm
gnome-media-2.16.1-3.el5.i386.rpm	gawk-3.1.5-14.el5.x86_64.rpm
gnome-menus-2.16.0-2.fc6.i386.rpm	gcalctool-5.8.25-1.el5.x86_64.rpm
gnome-mime-data-2.4.2-3.1.i386.rpm	GConf2-2.14.0-9.el5.i386.rpm
gnome-mount-0.5-3.el5.i386.rpm	GConf2-2.14.0-9.el5.x86_64.rpm
gnome-netstatus-2.12.0-5.el5.i386.rpm	gd-2.0.33-9.4.el5_1.1.x86_64.rpm
gnome-panel-2.16.1-7.el5.i386.rpm	gdbm-1.8.0-26.2.1.x86_64.rpm
gnome-pilot-2.0.13-16.i386.rpm	gdk-pixbuf-0.22.0-25.el5.x86_64.rpm
gnome-power-manager-2.16.0-9.el5.i386.rpm	gdm-2.16.0-46.el5.x86_64.rpm
gnome-python2-2.16.0-1.fc6.i386.rpm	gedit-2.16.0-9.el5.x86_64.rpm
gnome-python2-applet-2.16.0-2.el5.i386.rpm	gettext-0.14.6-4.el5.x86_64.rpm
gnome-python2-bonobo-2.16.0-1.fc6.i386.rpm	ghostscript-8.15.2-9.1.el5_1.1.i386.rpm
gnome-python2-canvas-2.16.0-1.fc6.i386.rpm	ghostscript-8.15.2-9.1.el5_1.1.x86_64.rpm
gnome-python2-desktop-2.16.0-2.el5.i386.rpm	ghostscript-fonts-5.50-13.1.1.noarch.rpm
gnome-python2-extras-2.14.2-6.el5.i386.rpm	giflib-4.1.3-7.1.el5.1.x86_64.rpm
gnome-python2-gconf-2.16.0-1.fc6.i386.rpm	gimp-2.2.13-2.0.7.el5.x86_64.rpm
gnome-python2-gnomeprint-2.16.0-2.el5.i386.rpm	gimp-data-extras-2.0.1-1.1.1.noarch.rpm
gnome-python2-gnomevfs-2.16.0-1.fc6.i386.rpm	gimp-help-2-0.1.0.10.1.1.noarch.rpm
gnome-python2-gtksourceview-2.16.0-2.el5.i386.rpm	gimp-libs-2.2.13-2.0.7.el5.x86_64.rpm
gnome-python2-libegg-2.14.2-6.el5.i386.rpm	gimp-print-4.2.7-22.x86_64.rpm
gnome-screensaver-2.16.1-8.el5.i386.rpm	gimp-print-plugin-4.2.7-22.x86_64.rpm
gnome-session-2.16.0-6.el5.i386.rpm	gimp-print-utils-4.2.7-22.x86_64.rpm
gnome-speech-0.4.5-1.fc6.i386.rpm	gjdoc-0.7.7-12.el5.x86_64.rpm
gnome-spell-1.0.7-3.1.i386.rpm	glib-1.2.10-20.el5.i386.rpm
gnome-system-monitor-2.16.0-3.el5.i386.rpm	glib-1.2.10-20.el5.x86_64.rpm
gnome-terminal-2.16.0-3.el5.i386.rpm	glib2-2.12.3-2.fc6.i386.rpm
gnome-themes-2.16.0-1.fc6.noarch.rpm	glib2-2.12.3-2.fc6.x86_64.rpm

gnome-user-docs-2.16.0-2.fc6.noarch.rpm	glibc-2.5-24.i686.rpm
gnome-user-share-0.10-6.el5.i386.rpm	glibc-2.5-24.x86_64.rpm
gnome-utils-2.16.0-5.el5.i386.rpm	glibc-common-2.5-24.x86_64.rpm
gnome-vfs2-2.16.2-4.el5.i386.rpm	glx-utils-6.5.1-7.5.el5.x86_64.rpm
gnome-vfs2-smb-2.16.2-4.el5.i386.rpm	gnome-applets-2.16.0.1-19.el5.x86_64.rpm
gnome-volume-manager-2.15.0-5.el5.i386.rpm	gnome-audio-2.0.0-3.1.1.noarch.rpm
gnupg-1.4.5-13.i386.rpm	gnome-backgrounds-2.15.92-1.fc6.noarch.rpm
gnutls-1.4.1-2.i386.rpm	gnome-desktop-2.16.0-1.fc6.i386.rpm
gok-1.2.0-2.el5.i386.rpm	gnome-desktop-2.16.0-1.fc6.x86_64.rpm
gphoto2-2.2.0-3.el5.i386.rpm	gnome-doc-utils-0.8.0-2.fc6.noarch.rpm
gpm-1.20.1-74.1.i386.rpm	gnome-icon-theme-2.16.0.1-4.el5.noarch.rpm
grep-2.5.1-54.2.el5.i386.rpm	gnome-keyring-0.6.0-1.fc6.i386.rpm
groff-1.18.1.1-11.1.i386.rpm	gnome-keyring-0.6.0-1.fc6.x86_64.rpm
grub-0.97-13.2.i386.rpm	gnome-mag-0.13.1-1.fc6.i386.rpm
gstreamer-0.10.9-3.el5.i386.rpm	gnome-mag-0.13.1-1.fc6.x86_64.rpm
gstreamer-plugins-base-0.10.9-6.el5.i386.rpm	gnome-media-2.16.1-3.el5.i386.rpm
gstreamer-plugins-good-0.10.4-4.el5.i386.rpm	gnome-media-2.16.1-3.el5.x86_64.rpm
gstreamer-tools-0.10.9-3.el5.i386.rpm	gnome-menus-2.16.0-2.fc6.i386.rpm
gthumb-2.7.8-8.el5.i386.rpm	gnome-menus-2.16.0-2.fc6.x86_64.rpm
gtk+-1.2.10-56.el5.i386.rpm	gnome-mime-data-2.4.2-3.1.x86_64.rpm
gtk2-2.10.4-20.el5.i386.rpm	gnome-mount-0.5-3.el5.x86_64.rpm
gtk2-engines-2.8.0-3.el5.i386.rpm	gnome-netstatus-2.12.0-5.el5.x86_64.rpm
gtkhtml2-2.11.0-3.i386.rpm	gnome-panel-2.16.1-7.el5.i386.rpm
gtkhtml3-3.16.3-1.el5.i386.rpm	gnome-panel-2.16.1-7.el5.x86_64.rpm
gtksourceview-1.8.0-1.fc6.i386.rpm	gnome-pilot-2.0.13-16.i386.rpm
gtkspell-2.0.11-2.1.i386.rpm	gnome-pilot-2.0.13-16.x86_64.rpm
gucharmap-1.8.0-1.fc6.i386.rpm	gnome-power-manager-2.16.0-9.el5.x86_64.rpm
gzip-1.3.5-10.el5.i386.rpm	gnome-python2-2.16.0-1.fc6.x86_64.rpm
hal-0.5.8.1-35.el5.i386.rpm	gnome-python2-applet-2.16.0-2.el5.x86_64.rpm
hal-cups-utils-0.6.2-5.2.el5.i386.rpm	gnome-python2-bonobo-2.16.0-1.fc6.x86_64.rpm
hdparm-6.6-2.i386.rpm	gnome-python2-canvas-2.16.0-1.fc6.x86_64.rpm
hesiod-3.1.0-8.i386.rpm	gnome-python2-desktop-2.16.0-2.el5.x86_64.rpm
hicolor-icon-theme-0.9-2.1.noarch.rpm	gnome-python2-extras-2.14.2-6.el5.x86_64.rpm

hpijs-1.6.7-4.1.el5_0.3.i386.rpm	gnome-python2-gconf-2.16.0-1.fc6.x86_64.rpm
hplip-1.6.7-4.1.el5_0.3.i386.rpm	gnome-python2-gnomeprint-2.16.0-2.el5.x86_64.rpm
hsqldb-1.8.0.9-1jpp.2.i386.rpm	gnome-python2-gnomevfs-2.16.0-1.fc6.x86_64.rpm
htmlview-4.0.0-2.el5.noarch.rpm	gnome-python2-gtksourceview-2.16.0-2.el5.x86_64.rpm
httpd-2.2.3-11.el5_1.3.i386.rpm	gnome-python2-libegg-2.14.2-6.el5.x86_64.rpm
hwdata-0.213.6-1.el5.noarch.rpm	gnome-screensaver-2.16.1-8.el5.x86_64.rpm
ifd-egate-0.05-15.i386.rpm	gnome-session-2.16.0-6.el5.x86_64.rpm
ImageMagick-6.2.8.0-4.el5_1.1.i386.rpm	gnome-speech-0.4.5-1.fc6.x86_64.rpm
im-chooser-0.3.3-6.el5.i386.rpm	gnome-spell-1.0.7-3.1.x86_64.rpm
info-4.8-14.el5.i386.rpm	gnome-system-monitor-2.16.0-3.el5.x86_64.rpm
initscripts-8.45.19.EL-1.i386.rpm	gnome-terminal-2.16.0-3.el5.x86_64.rpm
iproute-2.6.18-7.el5.i386.rpm	gnome-themes-2.16.0-1.fc6.noarch.rpm
ipsec-tools-0.6.5-9.el5.i386.rpm	gnome-user-docs-2.16.0-2.fc6.noarch.rpm
iptables-1.3.5-4.el5.i386.rpm	gnome-user-share-0.10-6.el5.x86_64.rpm
iptables-ipv6-1.3.5-4.el5.i386.rpm	gnome-utils-2.16.0-5.el5.i386.rpm
iptstate-1.4-1.1.2.2.i386.rpm	gnome-utils-2.16.0-5.el5.x86_64.rpm
iputils-20020927-43.el5.i386.rpm	gnome-vfs2-2.16.2-4.el5.i386.rpm
irda-utils-0.9.17-2.fc6.i386.rpm	gnome-vfs2-2.16.2-4.el5.x86_64.rpm
irqbalance-0.55-10.el5.i386.rpm	gnome-vfs2-smb-2.16.2-4.el5.x86_64.rpm
isdn4k-utils-3.2-51.el5.i386.rpm	gnome-volume-manager-2.15.0-5.el5.x86_64.rpm
java-1.4.2-gcj-compat-1.4.2.0-40jpp.115.i386.rpm	gnupg-1.4.5-13.x86_64.rpm
jpackage-utils-1.7.3-1jpp.2.el5.noarch.rpm	gnutls-1.4.1-2.i386.rpm
jwhois-3.2.3-8.el5.i386.rpm	gnutls-1.4.1-2.x86_64.rpm
kbd-1.12-20.el5.i386.rpm	gok-1.2.0-2.el5.x86_64.rpm
kernel-2.6.18-92.el5.i686.rpm	gphoto2-2.2.0-3.el5.x86_64.rpm
keyutils-libs-1.2-1.el5.i386.rpm	gpm-1.20.1-74.1.i386.rpm
kpartx-0.4.7-17.el5.i386.rpm	gpm-1.20.1-74.1.x86_64.rpm
krb5-auth-dialog-0.7-1.i386.rpm	grep-2.5.1-54.2.el5.x86_64.rpm
krb5-libs-1.6.1-25.el5.i386.rpm	groff-1.18.1.1-11.1.x86_64.rpm
krb5-workstation-1.6.1-25.el5.i386.rpm	grub-0.97-13.2.x86_64.rpm
kudzu-1.2.57.1.17-1.i386.rpm	gstreamer-0.10.9-3.el5.i386.rpm
launchmail-4.0.0-2.el5.noarch.rpm	gstreamer-0.10.9-3.el5.x86_64.rpm
lcms-1.15-1.2.2.i386.rpm	gstreamer-plugins-base-0.10.9-

	6.el5.i386.rpm
less-394-5.el5.i386.rpm	gstreamer-plugins-base-0.10.9-6.el5.x86_64.rpm
lftp-3.5.1-2.fc6.i386.rpm	gstreamer-plugins-good-0.10.4-4.el5.x86_64.rpm
libacl-2.2.39-3.el5.i386.rpm	gstreamer-tools-0.10.9-3.el5.x86_64.rpm
libaio-0.3.106-3.2.i386.rpm	gthumb-2.7.8-8.el5.x86_64.rpm
libart_lgpl-2.3.17-4.i386.rpm	gtk+-1.2.10-56.el5.i386.rpm
libattr-2.4.32-1.1.i386.rpm	gtk+-1.2.10-56.el5.x86_64.rpm
libavc1394-0.5.3-1.fc6.i386.rpm	gtk2-2.10.4-20.el5.i386.rpm
libbonobo-2.16.0-1.fc6.i386.rpm	gtk2-2.10.4-20.el5.x86_64.rpm
libbonoboui-2.16.0-1.fc6.i386.rpm	gtk2-engines-2.8.0-3.el5.i386.rpm
libcap-1.10-26.i386.rpm	gtk2-engines-2.8.0-3.el5.x86_64.rpm
libcroco-0.6.1-2.1.i386.rpm	gtkhtml2-2.11.0-3.x86_64.rpm
libdaemon-0.10-5.el5.i386.rpm	gtkhtml3-3.16.3-1.el5.i386.rpm
libdmx-1.0.2-3.1.i386.rpm	gtkhtml3-3.16.3-1.el5.x86_64.rpm
libdrm-2.0.2-1.1.i386.rpm	gtksourceview-1.8.0-1.fc6.x86_64.rpm
libdv-0.104-4.fc6.1.i386.rpm	gtkspell-2.0.11-2.1.i386.rpm
liberation-fonts-1.0-1.el5.noarch.rpm	gtkspell-2.0.11-2.1.x86_64.rpm
libevent-1.1a-3.2.1.i386.rpm	gucharmap-1.8.0-1.fc6.x86_64.rpm
libexif-0.6.13-4.0.2.el5_1.1.i386.rpm	gzip-1.3.5-10.el5.x86_64.rpm
libfontenc-1.0.2-2.2.el5.i386.rpm	hal-0.5.8.1-35.el5.i386.rpm
libFS-1.0.0-3.1.i386.rpm	hal-0.5.8.1-35.el5.x86_64.rpm
libgail-gnome-1.1.3-1.2.1.i386.rpm	hal-cups-utils-0.6.2-5.2.el5.x86_64.rpm
libgcc-4.1.2-42.el5.i386.rpm	hdparm-6.6-2.x86_64.rpm
libgcj-4.1.2-42.el5.i386.rpm	hesiod-3.1.0-8.x86_64.rpm
libgcrypt-1.2.3-1.i386.rpm	hicolor-icon-theme-0.9-2.1.noarch.rpm
libglade2-2.6.0-2.i386.rpm	hpijs-1.6.7-4.1.el5_0.3.x86_64.rpm
libgnome-2.16.0-6.el5.i386.rpm	hplip-1.6.7-4.1.el5_0.3.x86_64.rpm
libgnomecanvas-2.14.0-4.1.i386.rpm	hsqldb-1.8.0.9-1jpp.2.x86_64.rpm
libgnomecups-0.2.2-8.i386.rpm	htmlview-4.0.0-2.el5.noarch.rpm
libgnomeprint22-2.12.1-10.el5.i386.rpm	httpd-2.2.3-11.el5_1.3.x86_64.rpm
libgnomeprintui22-2.12.1-6.i386.rpm	hwdata-0.213.6-1.el5.noarch.rpm
libgnomeui-2.16.0-5.el5.i386.rpm	ifd-egate-0.05-15.x86_64.rpm
libgpg-error-1.4-2.i386.rpm	ImageMagick-6.2.8.0-4.el5_1.1.i386.rpm
libgsf-1.14.1-6.1.i386.rpm	ImageMagick-6.2.8.0-4.el5_1.1.x86_64.rpm
libgssapi-0.10-2.i386.rpm	im-chooser-0.3.3-6.el5.x86_64.rpm
libgtop2-2.14.4-3.el5.i386.rpm	info-4.8-14.el5.x86_64.rpm
libhugetlbfs-1.2-5.el5.i386.rpm	initscripts-8.45.19.EL-1.x86_64.rpm
libICE-1.0.1-2.1.i386.rpm	iproute-2.6.18-7.el5.x86_64.rpm
libicu-3.6-5.11.1.i386.rpm	ipsec-tools-0.6.5-9.el5.x86_64.rpm

libIDL-0.8.7-1.fc6.i386.rpm	iptables-1.3.5-4.el5.x86_64.rpm
libidn-0.6.5-1.1.i386.rpm	iptables-ipv6-1.3.5-4.el5.x86_64.rpm
libiec61883-1.0.0-11.fc6.i386.rpm	iptstate-1.4-1.1.2.2.x86_64.rpm
libieee1284-0.2.9-4.el5.i386.rpm	iputils-20020927-43.el5.x86_64.rpm
libjpeg-6b-37.i386.rpm	irda-utils-0.9.17-2.fc6.x86_64.rpm
libmng-1.0.9-5.1.i386.rpm	irqbalance-0.55-10.el5.x86_64.rpm
libnl-1.0-0.10.pre5.5.i386.rpm	isdn4k-utils-3.2-51.el5.x86_64.rpm
libnotify-0.4.2-6.el5.i386.rpm	java-1.4.2-gcj-compat-1.4.2.0-40jpp.115.x86_64.rpm
libogg-1.1.3-3.el5.i386.rpm	jpackage-utils-1.7.3-1jpp.2.el5.noarch.rpm
liboil-0.3.8-2.1.i386.rpm	jwhois-3.2.3-8.el5.x86_64.rpm
libpcap-0.9.4-12.el5.i386.rpm	kbd-1.12-20.el5.x86_64.rpm
libpng-1.2.10-7.1.el5_0.1.i386.rpm	kernel-2.6.18-92.el5.x86_64.rpm
libpurple-2.3.1-1.el5.i386.rpm	keyutils-libs-1.2-1.el5.i386.rpm
libraw1394-1.3.0-1.el5.i386.rpm	keyutils-libs-1.2-1.el5.x86_64.rpm
librsvg2-2.16.1-1.el5.i386.rpm	kpartx-0.4.7-17.el5.x86_64.rpm
libsane-hpaio-1.6.7-4.1.el5_0.3.i386.rpm	krb5-auth-dialog-0.7-1.x86_64.rpm
libselinux-1.33.4-5.el5.i386.rpm	krb5-libs-1.6.1-25.el5.i386.rpm
libselinux-python-1.33.4-5.el5.i386.rpm	krb5-libs-1.6.1-25.el5.x86_64.rpm
libsemanage-1.9.1-3.el5.i386.rpm	krb5-workstation-1.6.1-25.el5.x86_64.rpm
libsepol-1.15.2-1.el5.i386.rpm	kudzu-1.2.57.1.17-1.x86_64.rpm
libsilc-1.0.2-2.fc6.i386.rpm	launchmail-4.0.0-2.el5.noarch.rpm
libSM-1.0.1-3.1.i386.rpm	lcms-1.15-1.2.2.i386.rpm
libsoup-2.2.98-2.el5.i386.rpm	lcms-1.15-1.2.2.x86_64.rpm
libstdc++-4.1.2-42.el5.i386.rpm	less-394-5.el5.x86_64.rpm
libsysfs-2.0.0-6.i386.rpm	lftp-3.5.1-2.fc6.x86_64.rpm
libtermcap-2.0.8-46.1.i386.rpm	libacl-2.2.39-3.el5.i386.rpm
libtheora-1.0alpha7-1.i386.rpm	libacl-2.2.39-3.el5.x86_64.rpm
libtiff-3.8.2-7.el5.i386.rpm	libaio-0.3.106-3.2.i386.rpm
libusb-0.1.12-5.1.i386.rpm	libaio-0.3.106-3.2.x86_64.rpm
libuser-0.54.7-2.el5.5.i386.rpm	libart_lgpl-2.3.17-4.i386.rpm
libutempter-1.1.4-3.fc6.i386.rpm	libart_lgpl-2.3.17-4.x86_64.rpm
libvolume_id-095-14.16.el5.i386.rpm	libattr-2.4.32-1.1.i386.rpm
libvorbis-1.1.2-3.el5.0.i386.rpm	libattr-2.4.32-1.1.x86_64.rpm
libwmf-0.2.8.4-10.1.i386.rpm	libavc1394-0.5.3-1.fc6.x86_64.rpm
libwnck-2.16.0-4.fc6.i386.rpm	libbonobo-2.16.0-1.fc6.i386.rpm
libwpd-0.8.7-3.el5.i386.rpm	libbonobo-2.16.0-1.fc6.x86_64.rpm
libwvstreams-4.2.2-2.1.i386.rpm	libbonoboui-2.16.0-1.fc6.i386.rpm
libX11-1.0.3-9.el5.i386.rpm	libbonoboui-2.16.0-1.fc6.x86_64.rpm
libXau-1.0.1-3.1.i386.rpm	libcap-1.10-26.i386.rpm
libXaw-1.0.2-8.1.i386.rpm	libcap-1.10-26.x86_64.rpm

libXcursor-1.1.7-1.1.i386.rpm	libcroco-0.6.1-2.1.i386.rpm
libXdamage-1.0.3-2.1.i386.rpm	libcroco-0.6.1-2.1.x86_64.rpm
libXdmcp-1.0.1-2.1.i386.rpm	libdaemon-0.10-5.el5.i386.rpm
libXevie-1.0.1-3.1.i386.rpm	libdaemon-0.10-5.el5.x86_64.rpm
libXext-1.0.1-2.1.i386.rpm	libdmx-1.0.2-3.1.x86_64.rpm
libXfixes-4.0.1-2.1.i386.rpm	libdrm-2.0.2-1.1.i386.rpm
libXfont-1.2.2-1.0.3.el5_1.i386.rpm	libdrm-2.0.2-1.1.x86_64.rpm
libXfontcache-1.0.2-3.1.i386.rpm	libdv-0.104-4.fc6.1.x86_64.rpm
libXft-2.1.10-1.1.i386.rpm	liberation-fonts-1.0-1.el5.noarch.rpm
libXi-1.0.1-3.1.i386.rpm	libevent-1.1a-3.2.1.x86_64.rpm
libXinerama-1.0.1-2.1.i386.rpm	libexif-0.6.13-4.0.2.el5_1.1.x86_64.rpm
libxkbfile-1.0.3-3.1.i386.rpm	libfontenc-1.0.2-2.2.el5.x86_64.rpm
libxklavier-3.0-3.el5.i386.rpm	libFS-1.0.0-3.1.x86_64.rpm
libxml2-2.6.26-2.1.2.1.i386.rpm	libgail-gnome-1.1.3-1.2.1.x86_64.rpm
libxml2-python-2.6.26-2.1.2.1.i386.rpm	libgcc-4.1.2-42.el5.i386.rpm
libXmu-1.0.2-5.i386.rpm	libgcc-4.1.2-42.el5.x86_64.rpm
libXp-1.0.0-8.1.el5.i386.rpm	libgcj-4.1.2-42.el5.i386.rpm
libXpm-3.5.5-3.i386.rpm	libgcj-4.1.2-42.el5.x86_64.rpm
libXrandr-1.1.1-3.1.i386.rpm	libgcrypt-1.2.3-1.i386.rpm
libXrender-0.9.1-3.1.i386.rpm	libgcrypt-1.2.3-1.x86_64.rpm
libXres-1.0.1-3.1.i386.rpm	libglade2-2.6.0-2.i386.rpm
libXScrnSaver-1.1.0-3.1.i386.rpm	libglade2-2.6.0-2.x86_64.rpm
libxslt-1.1.17-2.i386.rpm	libgnome-2.16.0-6.el5.i386.rpm
libXt-1.0.2-3.1.fc6.i386.rpm	libgnome-2.16.0-6.el5.x86_64.rpm
libXTrap-1.0.0-3.1.i386.rpm	libgnomecanvas-2.14.0-4.1.i386.rpm
libXtst-1.0.1-3.1.i386.rpm	libgnomecanvas-2.14.0-4.1.x86_64.rpm
libXv-1.0.1-4.1.i386.rpm	libgnomecups-0.2.2-8.i386.rpm
libXxf86dga-1.0.1-3.1.i386.rpm	libgnomecups-0.2.2-8.x86_64.rpm
libXxf86misc-1.0.1-3.1.i386.rpm	libgnomeprint22-2.12.1-10.el5.i386.rpm
libXxf86vm-1.0.1-3.1.i386.rpm	libgnomeprint22-2.12.1-10.el5.x86_64.rpm
linuxwacom-0.7.4.3-2.el5.i386.rpm	libgnomeprintui22-2.12.1-6.i386.rpm
lockdev-1.0.1-10.i386.rpm	libgnomeprintui22-2.12.1-6.x86_64.rpm
logrotate-3.7.4-8.i386.rpm	libgnomeui-2.16.0-5.el5.i386.rpm
logwatch-7.3-6.el5.noarch.rpm	libgnomeui-2.16.0-5.el5.x86_64.rpm
lrzsz-0.12.20-22.1.i386.rpm	libgpg-error-1.4-2.i386.rpm
lsof-4.78-3.i386.rpm	libgpg-error-1.4-2.x86_64.rpm
lvm2-2.02.32-4.el5.i386.rpm	libgsf-1.14.1-6.1.i386.rpm
m2crypto-0.16-6.el5.2.i386.rpm	libgsf-1.14.1-6.1.x86_64.rpm
m4-1.4.5-3.el5.1.i386.rpm	libgssapi-0.10-2.x86_64.rpm
mailcap-2.1.23-1.fc6.noarch.rpm	libgtop2-2.14.4-3.el5.i386.rpm
mailx-8.1.1-44.2.2.i386.rpm	libgtop2-2.14.4-3.el5.x86_64.rpm

make-3.81-3.el5.i386.rpm	libhugetlbfs-1.2-5.el5.i386.rpm
MAKEDEV-3.23-1.2.i386.rpm	libhugetlbfs-1.2-5.el5.x86_64.rpm
man-1.6d-1.1.i386.rpm	libICE-1.0.1-2.1.i386.rpm
man-pages-2.39-10.el5.noarch.rpm	libICE-1.0.1-2.1.x86_64.rpm
man-pages-ru-0.97-1.1.1.noarch.rpm	libicu-3.6-5.11.1.x86_64.rpm
mcstrans-0.2.7-1.el5.i386.rpm	libIDL-0.8.7-1.fc6.i386.rpm
mdadm-2.6.4-1.el5.i386.rpm	libIDL-0.8.7-1.fc6.x86_64.rpm
meanwhile-1.0.2-5.el5.i386.rpm	libidn-0.6.5-1.1.x86_64.rpm
mesa-libGL-6.5.1-7.5.el5.i386.rpm	libiec61883-1.0.0-11.fc6.x86_64.rpm
mesa-libGLU-6.5.1-7.5.el5.i386.rpm	libieee1284-0.2.9-4.el5.x86_64.rpm
metacity-2.16.0-10.el5.i386.rpm	libjpeg-6b-37.i386.rpm
microcode_ctl-1.17-1.47.el5.i386.rpm	libjpeg-6b-37.x86_64.rpm
mingetty-1.07-5.2.2.i386.rpm	libmng-1.0.9-5.1.x86_64.rpm
minicom-2.1-3.i386.rpm	libnl-1.0-0.10.pre5.5.x86_64.rpm
mkbootdisk-1.5.3-2.1.i386.rpm	libnotify-0.4.2-6.el5.i386.rpm
mkinitrd-5.1.19.6-28.i386.rpm	libnotify-0.4.2-6.el5.x86_64.rpm
mkisofs-2.01-10.i386.rpm	libogg-1.1.3-3.el5.i386.rpm
mktemp-1.5-23.2.2.i386.rpm	libogg-1.1.3-3.el5.x86_64.rpm
mlocate-0.15-1.el5.i386.rpm	liboil-0.3.8-2.1.i386.rpm
module-init-tools-3.3-0.pre3.1.37.el5.i386.rpm	liboil-0.3.8-2.1.x86_64.rpm
mozldap-6.0.5-1.el5.i386.rpm	libpcap-0.9.4-12.el5.x86_64.rpm
mtools-3.9.10-2.fc6.i386.rpm	libpng-1.2.10-7.1.el5_0.1.i386.rpm
nano-1.3.12-1.1.i386.rpm	libpng-1.2.10-7.1.el5_0.1.x86_64.rpm
nash-5.1.19.6-28.i386.rpm	libpurple-2.3.1-1.el5.i386.rpm
nautilus-2.16.2-7.el5.i386.rpm	libpurple-2.3.1-1.el5.x86_64.rpm
nautilus-cd-burner-2.16.0-7.el5.i386.rpm	libraw1394-1.3.0-1.el5.x86_64.rpm
nautilus-extensions-2.16.2-7.el5.i386.rpm	librsvg2-2.16.1-1.el5.i386.rpm
nautilus-open-terminal-0.6-6.el5.i386.rpm	librsvg2-2.16.1-1.el5.x86_64.rpm
nautilus-sendto-0.7-5.fc6.i386.rpm	libsane-hpaio-1.6.7-4.1.el5_0.3.x86_64.rpm
nc-1.84-10.fc6.i386.rpm	libselinux-1.33.4-5.el5.i386.rpm
ncurses-5.5-24.20060715.i386.rpm	libselinux-1.33.4-5.el5.x86_64.rpm
netpbm-10.35-6.fc6.i386.rpm	libselinux-python-1.33.4-5.el5.x86_64.rpm
netpbm-progs-10.35-6.fc6.i386.rpm	libsemanage-1.9.1-3.el5.x86_64.rpm
net-snmp-libs-5.3.1-24.el5.i386.rpm	libsepol-1.15.2-1.el5.i386.rpm
net-tools-1.60-78.el5.i386.rpm	libsepol-1.15.2-1.el5.x86_64.rpm
NetworkManager-0.6.4-8.el5.i386.rpm	libsilc-1.0.2-2.fc6.i386.rpm
NetworkManager-glib-0.6.4-8.el5.i386.rpm	libsilc-1.0.2-2.fc6.x86_64.rpm
NetworkManager-gnome-0.6.4-8.el5.i386.rpm	libSM-1.0.1-3.1.i386.rpm
newt-0.52.2-10.el5.i386.rpm	libSM-1.0.1-3.1.x86_64.rpm
nfs-utils-1.0.9-33.el5.i386.rpm	libsoup-2.2.98-2.el5.i386.rpm
nfs-utils-lib-1.0.8-7.2.z2.i386.rpm	libsoup-2.2.98-2.el5.x86_64.rpm

notification-daemon-0.3.5-9.el5.i386.rpm	libstdc++-4.1.2-42.el5.i386.rpm
notify-python-0.1.0-3.fc6.i386.rpm	libstdc++-4.1.2-42.el5.x86_64.rpm
nscd-2.5-24.i386.rpm	libsysfs-2.0.0-6.x86_64.rpm
nspluginwrapper-0.9.91.5-21.el5.i386.rpm	libtermcap-2.0.8-46.1.i386.rpm
nspr-4.7.0.99.2-1.el5.i386.rpm	libtermcap-2.0.8-46.1.x86_64.rpm
nss-3.11.99.5-2.el5.i386.rpm	libtheora-1.0alpha7-1.i386.rpm
nss_db-2.2-35.3.i386.rpm	libtheora-1.0alpha7-1.x86_64.rpm
nss_ldap-253-12.el5.i386.rpm	libtiff-3.8.2-7.el5.i386.rpm
nss-tools-3.11.99.5-2.el5.i386.rpm	libtiff-3.8.2-7.el5.x86_64.rpm
ntp-4.2.2p1-8.el5.i386.rpm	libusb-0.1.12-5.1.i386.rpm
ntsysv-1.3.30.1-2.i386.rpm	libusb-0.1.12-5.1.x86_64.rpm
oddjob-0.27-9.el5.i386.rpm	libuser-0.54.7-2.el5.5.x86_64.rpm
oddjob-libs-0.27-9.el5.i386.rpm	libutempter-1.1.4-3.fc6.i386.rpm
opal-2.2.2-1.1.0.1.i386.rpm	libutempter-1.1.4-3.fc6.x86_64.rpm
OpenIPMI-2.0.6-6.el5.i386.rpm	libvolume_id-095-14.16.el5.i386.rpm
OpenIPMI-libs-2.0.6-6.el5.i386.rpm	libvolume_id-095-14.16.el5.x86_64.rpm
openjade-1.3.2-27.i386.rpm	libvorbis-1.1.2-3.el5.0.i386.rpm
openldap-2.3.27-8.el5_1.3.i386.rpm	libvorbis-1.1.2-3.el5.0.x86_64.rpm
openoffice.org-calc-2.3.0-6.5.el5.i386.rpm	libwmf-0.2.8.4-10.1.i386.rpm
openoffice.org-core-2.3.0-6.5.el5.i386.rpm	libwmf-0.2.8.4-10.1.x86_64.rpm
openoffice.org-draw-2.3.0-6.5.el5.i386.rpm	libwnck-2.16.0-4.fc6.i386.rpm
openoffice.org-graphicfilter-2.3.0-6.5.el5.i386.rpm	libwnck-2.16.0-4.fc6.x86_64.rpm
openoffice.org-impress-2.3.0-6.5.el5.i386.rpm	libwpd-0.8.7-3.el5.x86_64.rpm
openoffice.org-langpack-ru-2.3.0-6.5.el5.i386.rpm	libwvstreams-4.2.2-2.1.x86_64.rpm
openoffice.org-math-2.3.0-6.5.el5.i386.rpm	libX11-1.0.3-9.el5.i386.rpm
openoffice.org-writer-2.3.0-6.5.el5.i386.rpm	libX11-1.0.3-9.el5.x86_64.rpm
openoffice.org-xsltfilter-2.3.0-6.5.el5.i386.rpm	libXau-1.0.1-3.1.i386.rpm
opensp-1.5.2-4.i386.rpm	libXau-1.0.1-3.1.x86_64.rpm
openssh-4.3p2-26.el5.i386.rpm	libXaw-1.0.2-8.1.x86_64.rpm
openssh-askpass-4.3p2-26.el5.i386.rpm	libXcursor-1.1.7-1.1.i386.rpm
openssh-clients-4.3p2-26.el5.i386.rpm	libXcursor-1.1.7-1.1.x86_64.rpm
openssh-server-4.3p2-26.el5.i386.rpm	libXdamage-1.0.3-2.1.i386.rpm
openssl-0.9.8b-10.el5.i686.rpm	libXdamage-1.0.3-2.1.x86_64.rpm
ORBit2-2.14.3-4.el5.i386.rpm	libXdmcp-1.0.1-2.1.i386.rpm
orca-1.0.0-5.el5.i386.rpm	libXdmcp-1.0.1-2.1.x86_64.rpm
pam-0.99.6.2-3.27.el5.i386.rpm	libXevie-1.0.1-3.1.i386.rpm
pam_ccreds-3-5.i386.rpm	libXevie-1.0.1-3.1.x86_64.rpm
pam_krb5-2.2.14-1.i386.rpm	libXext-1.0.1-2.1.i386.rpm
pam_passwdqc-1.0.2-1.2.2.i386.rpm	libXext-1.0.1-2.1.x86_64.rpm
pam_pkcs11-0.5.3-23.i386.rpm	libXfixes-4.0.1-2.1.i386.rpm
pam_smb-1.1.7-7.2.1.i386.rpm	libXfixes-4.0.1-2.1.x86_64.rpm

pango-1.14.9-3.el5.i386.rpm	libXfont-1.2.2-1.0.3.el5_1.x86_64.rpm
paps-0.6.6-17.el5.i386.rpm	libXfontcache-1.0.2-3.1.x86_64.rpm
parted-1.8.1-17.el5.i386.rpm	libXft-2.1.10-1.1.i386.rpm
passwd-0.73-1.i386.rpm	libXft-2.1.10-1.1.x86_64.rpm
patch-2.5.4-29.2.2.i386.rpm	libXi-1.0.1-3.1.i386.rpm
pax-3.4-1.2.2.i386.rpm	libXi-1.0.1-3.1.x86_64.rpm
pciutils-2.2.3-5.i386.rpm	libXinerama-1.0.1-2.1.i386.rpm
pcmciautils-014-5.i386.rpm	libXinerama-1.0.1-2.1.x86_64.rpm
pcre-6.6-2.el5_1.7.i386.rpm	libxkbfile-1.0.3-3.1.i386.rpm
pcsc-lite-1.4.4-0.1.el5.i386.rpm	libxkbfile-1.0.3-3.1.x86_64.rpm
pcsc-lite-libs-1.4.4-0.1.el5.i386.rpm	libxklavier-3.0-3.el5.i386.rpm
perl-5.8.8-10.el5_0.2.i386.rpm	libxklavier-3.0-3.el5.x86_64.rpm
perl-Compress-Zlib-1.42-1.fc6.i386.rpm	libxml2-2.6.26-2.1.2.1.i386.rpm
perl-HTML-Parser-3.55-1.fc6.i386.rpm	libxml2-2.6.26-2.1.2.1.x86_64.rpm
perl-HTML-Tagset-3.10-2.1.1.noarch.rpm	libxml2-python-2.6.26-2.1.2.1.x86_64.rpm
perl-libwww-perl-5.805-1.1.1.noarch.rpm	libXmu-1.0.2-5.x86_64.rpm
perl-String-CRC32-1.4-2.fc6.i386.rpm	libXp-1.0.0-8.1.el5.i386.rpm
perl-URI-1.35-3.noarch.rpm	libXp-1.0.0-8.1.el5.x86_64.rpm
pidgin-2.3.1-1.el5.i386.rpm	libXpm-3.5.5-3.x86_64.rpm
pilot-link-0.11.8-16.i386.rpm	libXrandr-1.1.1-3.1.i386.rpm
pinfo-0.6.9-1.fc6.i386.rpm	libXrandr-1.1.1-3.1.x86_64.rpm
pirut-1.3.28-13.el5.noarch.rpm	libXrender-0.9.1-3.1.i386.rpm
pkgconfig-0.21-2.el5.i386.rpm	libXrender-0.9.1-3.1.x86_64.rpm
pkinit-nss-0.7.3-1.el5.i386.rpm	libXres-1.0.1-3.1.i386.rpm
planner-0.14-3.i386.rpm	libXres-1.0.1-3.1.x86_64.rpm
pm-utils-0.99.3-6.el5.19.i386.rpm	libXScrnSaver-1.1.0-3.1.i386.rpm
policycoreutils-1.33.12-14.el5.i386.rpm	libXScrnSaver-1.1.0-3.1.x86_64.rpm
policycoreutils-gui-1.33.12-14.el5.i386.rpm	libxslt-1.1.17-2.x86_64.rpm
poppler-0.5.4-4.4.el5_1.i386.rpm	libXt-1.0.2-3.1.fc6.i386.rpm
popt-1.10.2-48.el5.i386.rpm	libXt-1.0.2-3.1.fc6.x86_64.rpm
portmap-4.0-65.2.2.1.i386.rpm	libXTrap-1.0.0-3.1.x86_64.rpm
postgresql-libs-8.1.11-1.el5_1.1.i386.rpm	libXtst-1.0.1-3.1.i386.rpm
ppp-2.4.4-1.el5.i386.rpm	libXtst-1.0.1-3.1.x86_64.rpm
prelink-0.3.9-2.1.i386.rpm	libXv-1.0.1-4.1.i386.rpm
procmail-3.22-17.1.i386.rpm	libXv-1.0.1-4.1.x86_64.rpm
procps-3.2.7-9.el5.i386.rpm	libXxf86dga-1.0.1-3.1.x86_64.rpm
psacct-6.3.2-41.1.i386.rpm	libXxf86misc-1.0.1-3.1.i386.rpm
psgml-1.2.5-4.3.noarch.rpm	libXxf86misc-1.0.1-3.1.x86_64.rpm
psmisc-22.2-6.i386.rpm	libXxf86vm-1.0.1-3.1.i386.rpm
psutils-1.17-26.1.i386.rpm	libXxf86vm-1.0.1-3.1.x86_64.rpm
pwlib-1.10.1-7.0.1.el5.i386.rpm	linuxwacom-0.7.4.3-2.el5.x86_64.rpm

pycairo-1.2.0-1.1.i386.rpm	lockdev-1.0.1-10.x86_64.rpm
pygobject2-2.12.1-5.el5.i386.rpm	logrotate-3.7.4-8.x86_64.rpm
pygtk2-2.10.1-12.el5.i386.rpm	logwatch-7.3-6.el5.noarch.rpm
pygtk2-libglade-2.10.1-12.el5.i386.rpm	lrzsz-0.12.20-22.1.x86_64.rpm
pyOpenSSL-0.6-1.p24.7.2.2.i386.rpm	lsof-4.78-3.x86_64.rpm
pyorbit-2.14.1-1.1.i386.rpm	lvm2-2.02.32-4.el5.x86_64.rpm
PyQt-3.16-4.i386.rpm	m2crypto-0.16-6.el5.2.x86_64.rpm
python-2.4.3-21.el5.i386.rpm	m4-1.4.5-3.el5.1.x86_64.rpm
python-elementtree-1.2.6-5.i386.rpm	mailcap-2.1.23-1.fc6.noarch.rpm
python-iniparse-0.2.3-4.el5.noarch.rpm	mailx-8.1.1-44.2.2.x86_64.rpm
python-ldap-2.2.0-2.1.i386.rpm	make-3.81-3.el5.x86_64.rpm
python-numeric-23.7-2.2.2.i386.rpm	MAKEDEV-3.23-1.2.x86_64.rpm
python-sqlite-1.1.7-1.2.1.i386.rpm	man-1.6d-1.1.x86_64.rpm
python-urlgrabber-3.1.0-2.noarch.rpm	man-pages-2.39-10.el5.noarch.rpm
pyxf86config-0.3.31-2.fc6.i386.rpm	man-pages-ru-0.97-1.1.1.noarch.rpm
PyXML-0.8.4-4.i386.rpm	mcelog-0.7-1.22.fc6.x86_64.rpm
qt-3.3.6-23.el5.i386.rpm	mcstrans-0.2.7-1.el5.x86_64.rpm
quota-3.13-1.2.3.2.el5.i386.rpm	mdadm-2.6.4-1.el5.x86_64.rpm
rdist-6.1.5-44.i386.rpm	meanwhile-1.0.2-5.el5.i386.rpm
readahead-1.3-7.el5.i386.rpm	meanwhile-1.0.2-5.el5.x86_64.rpm
readline-5.1-1.1.i386.rpm	mesa-libGL-6.5.1-7.5.el5.i386.rpm
redhat-artwork-5.0.10-sphere.i386.rpm	mesa-libGL-6.5.1-7.5.el5.x86_64.rpm
redhat-logos-4.9.99-12.noarch.rpm	mesa-libGLU-6.5.1-7.5.el5.i386.rpm
redhat-lsb-3.1-12.3.EL.i386.rpm	mesa-libGLU-6.5.1-7.5.el5.x86_64.rpm
redhat-menus-6.7.8-2.el5.noarch.rpm	metacity-2.16.0-10.el5.i386.rpm
redhat-release-5Client-5.2.0.4.i386.rpm	metacity-2.16.0-10.el5.x86_64.rpm
redhat-release-notes-5Client-12.i386.rpm	microcode_ctl-1.17-1.47.el5.x86_64.rpm
rhel-instnum-1.0.8-1.el5.noarch.rpm	mingetty-1.07-5.2.2.x86_64.rpm
rhgb-0.16.4-8.sphere.3.i386.rpm	minicom-2.1-3.x86_64.rpm
rhn-check-0.4.17-8.el5.noarch.rpm	mkbootdisk-1.5.3-2.1.x86_64.rpm
rhn-client-tools-0.4.17-8.el5.noarch.rpm	mkinitrd-5.1.19.6-28.i386.rpm
rhnlib-2.2.5-1.el5.noarch.rpm	mkinitrd-5.1.19.6-28.x86_64.rpm
rhnsd-4.6.1-1.el5.i386.rpm	mkisofs-2.01-10.x86_64.rpm
rhn-setup-0.4.17-8.el5.noarch.rpm	mktemp-1.5-23.2.2.x86_64.rpm
rhn-setup-gnome-0.4.17-8.el5.noarch.rpm	mlocate-0.15-1.el5.x86_64.rpm
rhpl-0.194.1-1.i386.rpm	module-init-tools-3.3-0.pre3.1.37.el5.x86_64.rpm
rhpxl-0.41.1-6.el5.i386.rpm	mozldap-6.0.5-1.el5.x86_64.rpm
rmt-0.4b41-2.fc6.i386.rpm	mtools-3.9.10-2.fc6.x86_64.rpm
rng-utils-2.0-1.14.1.fc6.i386.rpm	nano-1.3.12-1.1.x86_64.rpm
rootfiles-8.1-1.1.1.noarch.rpm	nash-5.1.19.6-28.x86_64.rpm

rpm-4.4.2-48.el5.i386.rpm	nautilus-2.16.2-7.el5.x86_64.rpm
rpm-libs-4.4.2-48.el5.i386.rpm	nautilus-cd-burner-2.16.0-7.el5.i386.rpm
rpm-python-4.4.2-48.el5.i386.rpm	nautilus-cd-burner-2.16.0-7.el5.x86_64.rpm
rp-pppoe-3.5-32.1.i386.rpm	nautilus-extensions-2.16.2-7.el5.i386.rpm
rsh-0.17-38.el5.i386.rpm	nautilus-extensions-2.16.2-7.el5.x86_64.rpm
rsync-2.6.8-3.1.i386.rpm	nautilus-open-terminal-0.6-6.el5.x86_64.rpm
sabayon-apply-2.12.4-5.el5.i386.rpm	nautilus-sendto-0.7-5.fc6.x86_64.rpm
samba-client-3.0.28-0.el5.8.i386.rpm	nc-1.84-10.fc6.x86_64.rpm
samba-common-3.0.28-0.el5.8.i386.rpm	ncurses-5.5-24.20060715.i386.rpm
sane-backends-1.0.18-5.el5.i386.rpm	ncurses-5.5-24.20060715.x86_64.rpm
sane-backends-libs-1.0.18-5.el5.i386.rpm	netpbm-10.35-6.fc6.x86_64.rpm
sane-frontends-1.0.14-1.2.2.i386.rpm	netpbm-progs-10.35-6.fc6.x86_64.rpm
scrollkeeper-0.3.14-9.el5.i386.rpm	net-snmp-libs-5.3.1-24.el5.x86_64.rpm
SDL-1.2.10-8.el5.i386.rpm	net-tools-1.60-78.el5.x86_64.rpm
sed-4.1.5-5.fc6.i386.rpm	NetworkManager-0.6.4-8.el5.x86_64.rpm
selinux-policy-2.4.6-137.el5.noarch.rpm	NetworkManager-glib-0.6.4-8.el5.i386.rpm
selinux-policy-targeted-2.4.6-137.el5.noarch.rpm	NetworkManager-glib-0.6.4-8.el5.x86_64.rpm
sendmail-8.13.8-2.el5.i386.rpm	NetworkManager-gnome-0.6.4-8.el5.x86_64.rpm
setarch-2.0-1.1.i386.rpm	newt-0.52.2-10.el5.x86_64.rpm
setools-3.0-3.el5.i386.rpm	nfs-utils-1.0.9-33.el5.x86_64.rpm
setserial-2.17-19.2.2.i386.rpm	nfs-utils-lib-1.0.8-7.2.z2.x86_64.rpm
setup-2.5.58-1.el5.noarch.rpm	notification-daemon-0.3.5-9.el5.x86_64.rpm
setuptool-1.19.2-1.i386.rpm	notify-python-0.1.0-3.fc6.x86_64.rpm
sgml-common-0.6.3-18.noarch.rpm	nscd-2.5-24.x86_64.rpm
shadow-utils-4.0.17-13.el5.i386.rpm	nspluginwrapper-0.9.91.5-21.el5.i386.rpm
shared-mime-info-0.19-5.el5.i386.rpm	nspluginwrapper-0.9.91.5-21.el5.x86_64.rpm
sip-4.4.5-3.i386.rpm	nspr-4.7.0.99.2-1.el5.i386.rpm
slang-2.0.6-4.el5.i386.rpm	nspr-4.7.0.99.2-1.el5.x86_64.rpm
smartmontools-5.36-4.el5.i386.rpm	nss-3.11.99.5-2.el5.i386.rpm
sos-1.7-9.2.el5.noarch.rpm	nss-3.11.99.5-2.el5.x86_64.rpm
sox-12.18.1-1.i386.rpm	nss_db-2.2-35.3.i386.rpm
specspo-13-1.el5.noarch.rpm	nss_db-2.2-35.3.x86_64.rpm
speex-1.0.5-4.el5_1.1.i386.rpm	nss_ldap-253-12.el5.i386.rpm
sqlite-3.3.6-2.i386.rpm	nss_ldap-253-12.el5.x86_64.rpm
startup-notification-0.8-4.1.i386.rpm	nss-tools-3.11.99.5-2.el5.x86_64.rpm
stunnel-4.15-2.i386.rpm	ntp-4.2.2p1-8.el5.x86_64.rpm
su-desktop-profile-0.1-2.el5.noarch.rpm	

sudo-1.6.8p12-12.el5.i386.rpm	ntsysv-1.3.30.1-2.x86_64.rpm
svrcore-4.0.4-3.el5.i386.rpm	oddjob-0.27-9.el5.x86_64.rpm
symlinks-1.2-24.2.2.i386.rpm	oddjob-libs-0.27-9.el5.x86_64.rpm
synaptics-0.14.4-8.fc6.i386.rpm	opal-2.2.2-1.1.0.1.x86_64.rpm
sysfsutils-2.0.0-6.i386.rpm	OpenIPMI-2.0.6-6.el5.x86_64.rpm
sysklogd-1.4.1-44.el5.i386.rpm	OpenIPMI-libs-2.0.6-6.el5.x86_64.rpm
syslinux-3.11-4.i386.rpm	openjade-1.3.2-27.x86_64.rpm
system-config-date-1.8.12-3.el5.noarch.rpm	openldap-2.3.27-8.el5_1.3.i386.rpm
system-config-display-1.0.48-2.el5.noarch.rpm	openldap-2.3.27-8.el5_1.3.x86_64.rpm
system-config-keyboard-1.2.11-1.el5.noarch.rpm	openoffice.org-calc-2.3.0-6.5.el5.x86_64.rpm
system-config-language-1.1.18-2.el5.noarch.rpm	openoffice.org-core-2.3.0-6.5.el5.x86_64.rpm
system-config-network-1.3.99.10-2.el5.noarch.rpm	openoffice.org-draw-2.3.0-6.5.el5.x86_64.rpm
system-config-network-tui-1.3.99.10-2.el5.noarch.rpm	openoffice.org-graphicfilter-2.3.0-6.5.el5.x86_64.rpm
system-config-printer-0.7.32.8-1.el5.i386.rpm	openoffice.org-impress-2.3.0-6.5.el5.x86_64.rpm
system-config-printer-libs-0.7.32.8-1.el5.i386.rpm	openoffice.org-langpack-ru-2.3.0-6.5.el5.x86_64.rpm
system-config-securitylevel-1.6.29.1-2.1.el5.i386.rpm	openoffice.org-math-2.3.0-6.5.el5.x86_64.rpm
system-config-securitylevel-tui-1.6.29.1-2.1.el5.i386.rpm	openoffice.org-writer-2.3.0-6.5.el5.x86_64.rpm
system-config-services-0.9.4-1.el5.noarch.rpm	openoffice.org-xsltfilter-2.3.0-6.5.el5.x86_64.rpm
system-config-soundcard-2.0.6-1.el5.noarch.rpm	opensp-1.5.2-4.x86_64.rpm
system-config-users-1.2.51-4.el5.noarch.rpm	openssh-4.3p2-26.el5.x86_64.rpm
SysVinit-2.86-14.i386.rpm	openssh-askpass-4.3p2-26.el5.x86_64.rpm
talk-0.17-29.2.2.i386.rpm	openssh-clients-4.3p2-26.el5.x86_64.rpm
tango-icon-theme-0.8.1-2.fc10.noarch.rpm	
tar-1.15.1-23.0.1.el5.i386.rpm	openssh-server-4.3p2-26.el5.x86_64.rpm
tcl-8.4.13-3.fc6.i386.rpm	openssl-0.9.8b-10.el5.i686.rpm
tclx-8.4.0-5.fc6.i386.rpm	openssl-0.9.8b-10.el5.x86_64.rpm
tcpdump-3.9.4-12.el5.i386.rpm	ORBit2-2.14.3-4.el5.i386.rpm
tcp_wrappers-7.6-40.4.el5.i386.rpm	ORBit2-2.14.3-4.el5.x86_64.rpm
tcsh-6.14-12.el5.i386.rpm	orca-1.0.0-5.el5.x86_64.rpm
telnet-0.17-39.el5.i386.rpm	pam-0.99.6.2-3.27.el5.i386.rpm
termcap-5.5-1.20060701.1.noarch.rpm	pam-0.99.6.2-3.27.el5.x86_64.rpm
time-1.7-27.2.2.i386.rpm	pam_ccreds-3-5.i386.rpm

tk-8.4.13-5.el5_1.1.i386.rpm	pam_ccreds-3-5.x86_64.rpm
tmpwatch-2.9.7-1.1.el5.1.i386.rpm	pam_krb5-2.2.14-1.i386.rpm
tomcat5-jsp-2.0-api-5.5.23-0jpp.7.el5.i386.rpm	pam_krb5-2.2.14-1.x86_64.rpm
tomcat5-servlet-2.4-api-5.5.23-0jpp.7.el5.i386.rpm	pam_passwdqc-1.0.2-1.2.2.i386.rpm
traceroute-2.0.1-3.el5.i386.rpm	pam_passwdqc-1.0.2-1.2.2.x86_64.rpm
tree-1.5.0-4.i386.rpm	pam_pkcs11-0.5.3-23.i386.rpm
ttmkfdir-3.0.9-23.el5.i386.rpm	pam_pkcs11-0.5.3-23.x86_64.rpm
tzdata-2007k-2.el5.noarch.rpm	pam_smb-1.1.7-7.2.1.i386.rpm
udev-095-14.16.el5.i386.rpm	pam_smb-1.1.7-7.2.1.x86_64.rpm
udftools-1.0.0b3-0.1.el5.i386.rpm	pango-1.14.9-3.el5.i386.rpm
unix2dos-2.2-26.2.2.i386.rpm	pango-1.14.9-3.el5.x86_64.rpm
unixODBC-2.2.11-7.1.i386.rpm	paps-0.6.6-17.el5.x86_64.rpm
unzip-5.52-2.2.1.i386.rpm	parted-1.8.1-17.el5.i386.rpm
urw-fonts-2.3-6.1.1.noarch.rpm	parted-1.8.1-17.el5.x86_64.rpm
usbutils-0.71-2.1.i386.rpm	passwd-0.73-1.x86_64.rpm
usermode-1.88-3.el5.1.i386.rpm	patch-2.5.4-29.2.2.x86_64.rpm
usermode-gtk-1.88-3.el5.1.i386.rpm	pax-3.4-1.2.2.x86_64.rpm
util-linux-2.13-0.47.el5.i386.rpm	pciutils-2.2.3-5.x86_64.rpm
vconfig-1.9-2.1.i386.rpm	pcmciautils-014-5.x86_64.rpm
vim-common-7.0.109-3.el5.3.i386.rpm	pcre-6.6-2.el5_1.7.x86_64.rpm
vim-enhanced-7.0.109-3.el5.3.i386.rpm	pcsc-lite-1.4.4-0.1.el5.x86_64.rpm
vim-minimal-7.0.109-3.el5.3.i386.rpm	pcsc-lite-libs-1.4.4-0.1.el5.x86_64.rpm
vino-2.13.5-6.el5.i386.rpm	perl-5.8.8-10.el5_0.2.x86_64.rpm
vixie-cron-4.1-72.el5.i386.rpm	perl-Compress-Zlib-1.42-1.fc6.x86_64.rpm
vnc-server-4.1.2-9.el5.i386.rpm	perl-HTML-Parser-3.55-1.fc6.x86_64.rpm
vte-0.14.0-2.el5.i386.rpm	perl-HTML-Tagset-3.10-2.1.1.noarch.rpm
wdaemon-0.13-1.i386.rpm	perl-libwww-perl-5.805-1.1.1.noarch.rpm
wget-1.10.2-7.el5.i386.rpm	perl-String-CRC32-1.4-2.fc6.x86_64.rpm
which-2.16-7.i386.rpm	perl-URI-1.35-3.noarch.rpm
wireless-tools-28-2.el5.i386.rpm	pidgin-2.3.1-1.el5.i386.rpm
words-3.0-9.noarch.rpm	pidgin-2.3.1-1.el5.x86_64.rpm
wpa_supplicant-0.4.8-10.2.el5.i386.rpm	pilot-link-0.11.8-16.i386.rpm
wvdial-1.54.0-5.2.2.1.i386.rpm	pilot-link-0.11.8-16.x86_64.rpm
xalan-j2-2.7.0-6jpp.1.i386.rpm	pinfo-0.6.9-1.fc6.x86_64.rpm
Xaw3d-1.5E-10.1.i386.rpm	pirut-1.3.28-13.el5.noarch.rpm
xerces-j2-2.7.1-7jpp.2.i386.rpm	pkgconfig-0.21-2.el5.x86_64.rpm
xkeyboard-config-0.8-7.fc6.noarch.rpm	pkinit-nss-0.7.3-1.el5.x86_64.rpm
xml-common-0.6.3-18.noarch.rpm	planner-0.14-3.x86_64.rpm
xml-commons-1.3.02-0.b2.7jpp.10.i386.rpm	pm-utils-0.99.3-6.el5.19.x86_64.rpm
xml-commons-apis-1.3.02-0.b2.7jpp.10.i386.rpm	policycoreutils-1.33.12-14.el5.x86_64.rpm
xml-commons-resolver-1.1-1jpp.12.i386.rpm	policycoreutils-gui-1.33.12-

	14.el5.x86_64.rpm
xorg-x11-apps-7.1-4.0.1.el5.i386.rpm	poppler-0.5.4-4.4.el5_1.x86_64.rpm
xorg-x11-drivers-7.1-4.1.el5.i386.rpm	popt-1.10.2-48.el5.i386.rpm
xorg-x11-drv-acecad-1.1.0-2.1.i386.rpm	popt-1.10.2-48.el5.x86_64.rpm
xorg-x11-drv-aiptek-1.0.1-2.i386.rpm	portmap-4.0-65.2.2.1.x86_64.rpm
xorg-x11-drv-apm-1.1.1-2.1.i386.rpm	postgresql-libs-8.1.11-1.el5_1.1.x86_64.rpm
xorg-x11-drv-ark-0.6.0-2.1.i386.rpm	ppp-2.4.4-1.el5.x86_64.rpm
xorg-x11-drv-ast-0.81.0-3.i386.rpm	prelink-0.3.9-2.1.x86_64.rpm
xorg-x11-drv-ati-6.6.3-3.13.el5.i386.rpm	procmail-3.22-17.1.x86_64.rpm
xorg-x11-drv-calcomp-1.1.0-1.1.i386.rpm	procps-3.2.7-9.el5.x86_64.rpm
xorg-x11-drv-chips-1.1.1-2.1.i386.rpm	psacct-6.3.2-41.1.x86_64.rpm
xorg-x11-drv-cirrus-1.1.0-2.fc6.i386.rpm	psgml-1.2.5-4.3.noarch.rpm
xorg-x11-drv-citron-2.2.0-1.1.i386.rpm	psmisc-22.2-6.x86_64.rpm
xorg-x11-drv-cyrix-1.1.0-4.i386.rpm	psutils-1.17-26.1.x86_64.rpm
xorg-x11-drv-digitaledge-1.1.0-1.1.i386.rpm	pwlib-1.10.1-7.0.1.el5.x86_64.rpm
xorg-x11-drv-dmc-1.1.0-2.i386.rpm	pycairo-1.2.0-1.1.x86_64.rpm
xorg-x11-drv-dummy-0.2.0-2.1.i386.rpm	pygobject2-2.12.1-5.el5.x86_64.rpm
xorg-x11-drv-dynapro-1.1.0-2.i386.rpm	pygtk2-2.10.1-12.el5.x86_64.rpm
xorg-x11-drv-elo2300-1.1.0-1.1.i386.rpm	pygtk2-libglade-2.10.1-12.el5.x86_64.rpm
xorg-x11-drv-elographics-1.1.0-1.1.i386.rpm	pyOpenSSL-0.6-1.p24.7.2.2.x86_64.rpm
xorg-x11-drv-evdev-1.0.0.5-3.el5.i386.rpm	pyorbit-2.14.1-1.1.x86_64.rpm
xorg-x11-drv-fbdev-0.3.0-2.i386.rpm	PyQt-3.16-4.x86_64.rpm
xorg-x11-drv-fpit-1.1.0-1.1.i386.rpm	python-2.4.3-21.el5.x86_64.rpm
xorg-x11-drv-glint-1.1.1-4.1.i386.rpm	python-elementtree-1.2.6-5.x86_64.rpm
xorg-x11-drv-hyperpen-1.1.0-2.i386.rpm	python-iniparse-0.2.3-4.el5.noarch.rpm
xorg-x11-drv-i128-1.2.0-4.i386.rpm	python-ldap-2.2.0-2.1.x86_64.rpm
xorg-x11-drv-i740-1.1.0-2.1.i386.rpm	python-numeric-23.7-2.2.2.x86_64.rpm
xorg-x11-drv-i810-1.6.5-9.13.el5.i386.rpm	python-sqlite-1.1.7-1.2.1.x86_64.rpm
xorg-x11-drv-jamstudio-1.1.0-1.1.i386.rpm	python-urlgrabber-3.1.0-2.noarch.rpm
xorg-x11-drv-joystick-1.1.0-1.1.i386.rpm	pyxf86config-0.3.31-2.fc6.x86_64.rpm
xorg-x11-drv-keyboard-1.1.0-3.i386.rpm	PyXML-0.8.4-4.x86_64.rpm
xorg-x11-drv-magellan-1.1.0-1.1.i386.rpm	qt-3.3.6-23.el5.x86_64.rpm
xorg-x11-drv-magictouch-1.0.0.5-2.1.i386.rpm	quota-3.13-1.2.3.2.el5.x86_64.rpm
xorg-x11-drv-mga-1.4.2-7.el5.i386.rpm	rdist-6.1.5-44.x86_64.rpm
xorg-x11-drv-microtouch-1.1.0-1.1.i386.rpm	readahead-1.3-7.el5.x86_64.rpm
xorg-x11-drv-mouse-1.1.1-1.1.i386.rpm	readline-5.1-1.1.i386.rpm
xorg-x11-drv-mutouch-1.1.0-2.i386.rpm	readline-5.1-1.1.x86_64.rpm
xorg-x11-drv-neomagic-1.1.1-2.1.i386.rpm	redhat-artwork-5.0.10-sphere.x86_64.rpm
xorg-x11-drv-nsc-2.8.1-2.1.i386.rpm	redhat-logos-4.9.99-12.noarch.rpm
xorg-x11-drv-nv-2.1.6-6.el5.i386.rpm	redhat-lsb-3.1-12.3.EL.i386.rpm
xorg-x11-drv-palmax-1.1.0-1.1.i386.rpm	redhat-lsb-3.1-12.3.EL.x86_64.rpm

xorg-x11-drv-penmount-1.1.0-2.1.i386.rpm	redhat-menus-6.7.8-2.el5.noarch.rpm
xorg-x11-drv-rendition-4.1.0-3.1.i386.rpm	redhat-release-5Client-5.2.0.4.x86_64.rpm
xorg-x11-drv-s3-0.4.1-2.1.i386.rpm	redhat-release-notes-5Client-12.x86_64.rpm
xorg-x11-drv-s3virge-1.9.1-2.1.i386.rpm	rhel-instnum-1.0.8-1.el5.noarch.rpm
xorg-x11-drv-savage-2.1.1-5.fc6.i386.rpm	rhgb-0.16.4-8.sphere.3.x86_64.rpm
xorg-x11-drv-siliconmotion-1.4.1-2.1.i386.rpm	rhn-check-0.4.17-8.el5.noarch.rpm
xorg-x11-drv-sis-0.9.1-7.1.el5.i386.rpm	rhn-client-tools-0.4.17-8.el5.noarch.rpm
xorg-x11-drv-sisusb-0.8.1-4.1.i386.rpm	rhnlib-2.2.5-1.el5.noarch.rpm
xorg-x11-drv-spaceorb-1.1.0-1.1.i386.rpm	rhnsd-4.6.1-1.el5.x86_64.rpm
xorg-x11-drv-summa-1.1.0-1.1.i386.rpm	rhn-setup-0.4.17-8.el5.noarch.rpm
xorg-x11-drv-tdfx-1.2.1-3.1.i386.rpm	rhn-setup-gnome-0.4.17-8.el5.noarch.rpm
xorg-x11-drv-tek4957-1.1.0-1.1.i386.rpm	rhpl-0.194.1-1.x86_64.rpm
xorg-x11-drv-trident-1.2.1-3.fc6.i386.rpm	rhpxl-0.41.1-6.el5.x86_64.rpm
xorg-x11-drv-tseng-1.1.0-3.1.i386.rpm	rmt-0.4b41-2.fc6.x86_64.rpm
xorg-x11-drv-ur98-1.1.0-1.1.i386.rpm	rng-utils-2.0-1.14.1.fc6.x86_64.rpm
xorg-x11-drv-v4l-0.1.1-4.i386.rpm	rootfiles-8.1-1.1.1.noarch.rpm
xorg-x11-drv-vesa-1.3.0-8.1.el5.i386.rpm	rpm-4.4.2-48.el5.x86_64.rpm
xorg-x11-drv-vga-4.1.0-2.1.i386.rpm	rpm-libs-4.4.2-48.el5.x86_64.rpm
xorg-x11-drv-via-0.2.1-9.i386.rpm	rpm-python-4.4.2-48.el5.x86_64.rpm
xorg-x11-drv-vmmouse-12.4.0-2.1.i386.rpm	rp-pppoe-3.5-32.1.x86_64.rpm
xorg-x11-drv-vmware-10.13.0-2.1.i386.rpm	rsh-0.17-38.el5.x86_64.rpm
xorg-x11-drv-void-1.1.0-3.1.i386.rpm	rsync-2.6.8-3.1.x86_64.rpm
xorg-x11-drv-voodoo-1.1.0-3.1.i386.rpm	sabayon-apply-2.12.4-5.el5.x86_64.rpm
xorg-x11-filesystem-7.1-2.fc6.noarch.rpm	samba-client-3.0.28-0.el5.8.x86_64.rpm
xorg-x11-fonts-100dpi-7.1-2.1.el5.noarch.rpm	samba-common-3.0.28-0.el5.8.x86_64.rpm
xorg-x11-fonts-75dpi-7.1-2.1.el5.noarch.rpm	sane-backends-1.0.18-5.el5.x86_64.rpm
xorg-x11-fonts-base-7.1-2.1.el5.noarch.rpm	sane-backends-libs-1.0.18-5.el5.x86_64.rpm
xorg-x11-fonts-cyrillic-7.1-2.1.el5.noarch.rpm	sane-frontends-1.0.14-1.2.2.x86_64.rpm
xorg-x11-fonts-ISO8859-1-100dpi-7.1-2.1.el5.noarch.rpm	scrollkeeper-0.3.14-9.el5.x86_64.rpm
xorg-x11-fonts-ISO8859-1-75dpi-7.1-2.1.el5.noarch.rpm	SDL-1.2.10-8.el5.x86_64.rpm
xorg-x11-fonts-misc-7.1-2.1.el5.noarch.rpm	sed-4.1.5-5.fc6.x86_64.rpm
xorg-x11-fonts-truetype-7.1-2.1.el5.noarch.rpm	selinux-policy-2.4.6-137.el5.noarch.rpm
xorg-x11-fonts-Type1-7.1-2.1.el5.noarch.rpm	selinux-policy-targeted-2.4.6-137.el5.noarch.rpm
xorg-x11-font-utils-7.1-2.i386.rpm	sendmail-8.13.8-2.el5.x86_64.rpm
xorg-x11-server-utils-7.1-4.fc6.i386.rpm	setarch-2.0-1.1.x86_64.rpm
xorg-x11-server-Xnest-1.1.1-48.41.el5.i386.rpm	setools-3.0-3.el5.x86_64.rpm
xorg-x11-server-Xorg-1.1.1-48.41.el5.i386.rpm	setserial-2.17-19.2.2.x86_64.rpm

xorg-x11-twm-1.0.1-3.1.i386.rpm	setup-2.5.58-1.el5.noarch.rpm
xorg-x11-utils-7.1-2.fc6.i386.rpm	setuptool-1.19.2-1.x86_64.rpm
xorg-x11-xauth-1.0.1-2.1.i386.rpm	sgml-common-0.6.3-18.noarch.rpm
xorg-x11-xfs-1.0.2-4.i386.rpm	shadow-utils-4.0.17-13.el5.x86_64.rpm
xorg-x11-xinit-1.0.2-15.el5.i386.rpm	shared-mime-info-0.19-5.el5.x86_64.rpm
xorg-x11-xkb-utils-1.0.2-2.1.i386.rpm	sip-4.4.5-3.x86_64.rpm
xrestop-0.2-6.2.2.i386.rpm	slang-2.0.6-4.el5.x86_64.rpm
xsane-0.991-5.el5.i386.rpm	smartmontools-5.36-4.el5.x86_64.rpm
xsane-gimp-0.991-5.el5.i386.rpm	sos-1.7-9.2.el5.noarch.rpm
xsri-2.1.0-10.fc6.i386.rpm	sox-12.18.1-1.x86_64.rpm
xterm-215-5.el5.i386.rpm	specspo-13-1.el5.noarch.rpm
xulrunner-1.9-0.beta5.6.el5.i386.rpm	speex-1.0.5-4.el5_1.1.x86_64.rpm
yelp-2.16.0-18.el5.i386.rpm	sqlite-3.3.6-2.x86_64.rpm
ypbind-1.19-8.el5.i386.rpm	startup-notification-0.8-4.1.i386.rpm
yp-tools-2.9-0.1.i386.rpm	startup-notification-0.8-4.1.x86_64.rpm
yum-3.2.8-9.el5.noarch.rpm	stunnel-4.15-2.x86_64.rpm
yum-metadata-parser-1.1.2-2.el5.i386.rpm	su-desktop-profile-0.1-2.el5.noarch.rpm
yum-rhn-plugin-0.5.3-6.el5.noarch.rpm	sudo-1.6.8p12-12.el5.x86_64.rpm
yum-security-1.1.10-9.el5.noarch.rpm	svrcore-4.0.4-3.el5.i386.rpm
yum-updatesd-0.9-2.el5.noarch.rpm	svrcore-4.0.4-3.el5.x86_64.rpm
zenity-2.16.0-2.el5.i386.rpm	symlinks-1.2-24.2.2.x86_64.rpm
zip-2.31-1.2.2.i386.rpm	synaptics-0.14.4-8.fc6.x86_64.rpm
zlib-1.2.3-3.i386.rpm	sysfsutils-2.0.0-6.x86_64.rpm
	sysklogd-1.4.1-44.el5.x86_64.rpm
	syslinux-3.11-4.x86_64.rpm
	system-config-date-1.8.12-3.el5.noarch.rpm
	system-config-display-1.0.48-2.el5.noarch.rpm
	system-config-keyboard-1.2.11-1.el5.noarch.rpm
	system-config-language-1.1.18-2.el5.noarch.rpm
	system-config-network-1.3.99.10-2.el5.noarch.rpm
	system-config-network-tui-1.3.99.10-2.el5.noarch.rpm
	system-config-printer-0.7.32.8-1.el5.x86_64.rpm
	system-config-printer-libs-0.7.32.8-1.el5.x86_64.rpm

	system-config-securitylevel-1.6.29.1-2.1.el5.x86_64.rpm
	system-config-securitylevel-tui-1.6.29.1-2.1.el5.x86_64.rpm
	system-config-services-0.9.4-1.el5.noarch.rpm
	system-config-soundcard-2.0.6-1.el5.noarch.rpm
	system-config-users-1.2.51-4.el5.noarch.rpm
	SysVinit-2.86-14.x86_64.rpm
	talk-0.17-29.2.2.x86_64.rpm
	tango-icon-theme-0.8.1-2.fc10.noarch.rpm
	tar-1.15.1-23.0.1.el5.x86_64.rpm
	tcl-8.4.13-3.fc6.x86_64.rpm
	tclx-8.4.0-5.fc6.x86_64.rpm
	tcpdump-3.9.4-12.el5.x86_64.rpm
	tcp_wrappers-7.6-40.4.el5.i386.rpm
	tcp_wrappers-7.6-40.4.el5.x86_64.rpm
	tcsh-6.14-12.el5.x86_64.rpm
	telnet-0.17-39.el5.x86_64.rpm
	termcap-5.5-1.20060701.1.noarch.rpm
	time-1.7-27.2.2.x86_64.rpm
	tk-8.4.13-5.el5_1.1.x86_64.rpm
	tmpwatch-2.9.7-1.1.el5.1.x86_64.rpm
	tomcat5-jsp-2.0-api-5.5.23-0jpp.7.el5.x86_64.rpm
	tomcat5-servlet-2.4-api-5.5.23-0jpp.7.el5.x86_64.rpm
	traceroute-2.0.1-3.el5.x86_64.rpm
	tree-1.5.0-4.x86_64.rpm
	ttmkfdir-3.0.9-23.el5.x86_64.rpm
	tzdata-2007k-2.el5.noarch.rpm
	udev-095-14.16.el5.x86_64.rpm
	udftools-1.0.0b3-0.1.el5.x86_64.rpm
	unix2dos-2.2-26.2.2.x86_64.rpm

	unixODBC-2.2.11-7.1.i386.rpm
	unixODBC-2.2.11-7.1.x86_64.rpm
	unzip-5.52-2.2.1.x86_64.rpm
	urw-fonts-2.3-6.1.1.noarch.rpm
	usbutils-0.71-2.1.x86_64.rpm
	usermode-1.88-3.el5.1.x86_64.rpm
	usermode-gtk-1.88-3.el5.1.x86_64.rpm
	util-linux-2.13-0.47.el5.x86_64.rpm
	vconfig-1.9-2.1.x86_64.rpm
	vim-common-7.0.109-3.el5.3.x86_64.rpm
	vim-enhanced-7.0.109-3.el5.3.x86_64.rpm
	vim-minimal-7.0.109-3.el5.3.x86_64.rpm
	vino-2.13.5-6.el5.x86_64.rpm
	vixie-cron-4.1-72.el5.x86_64.rpm
	vnc-server-4.1.2-9.el5.x86_64.rpm
	vte-0.14.0-2.el5.x86_64.rpm
	wdaemon-0.13-1.x86_64.rpm
	wget-1.10.2-7.el5.x86_64.rpm
	which-2.16-7.x86_64.rpm
	wireless-tools-28-2.el5.i386.rpm
	wireless-tools-28-2.el5.x86_64.rpm
	words-3.0-9.noarch.rpm
	wpa_supplicant-0.4.8-10.2.el5.x86_64.rpm
	wvdial-1.54.0-5.2.2.1.x86_64.rpm
	xalan-j2-2.7.0-6jpp.1.x86_64.rpm
	Xaw3d-1.5E-10.1.x86_64.rpm
	xerces-j2-2.7.1-7jpp.2.x86_64.rpm
	xkeyboard-config-0.8-7.fc6.noarch.rpm
	xml-common-0.6.3-18.noarch.rpm
	xml-commons-1.3.02-0.b2.7jpp.10.x86_64.rpm
	xml-commons-apis-1.3.02-0.b2.7jpp.10.x86_64.rpm
	xml-commons-resolver-1.1-1jpp.12.x86_64.rpm

	xorg-x11-apps-7.1-4.0.1.el5.x86_64.rpm
	xorg-x11-drivers-7.1-4.1.el5.x86_64.rpm
	xorg-x11-drv-acecad-1.1.0-2.1.x86_64.rpm
	xorg-x11-drv-aiptek-1.0.1-2.x86_64.rpm
	xorg-x11-drv-ast-0.81.0-3.x86_64.rpm
	xorg-x11-drv-ati-6.6.3-3.13.el5.x86_64.rpm
	xorg-x11-drv-calcomp-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-cirrus-1.1.0-2.fc6.x86_64.rpm
	xorg-x11-drv-citron-2.2.0-1.1.x86_64.rpm
	xorg-x11-drv-digitaledge-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-dmc-1.1.0-2.x86_64.rpm
	xorg-x11-drv-dummy-0.2.0-2.1.x86_64.rpm
	xorg-x11-drv-dynapro-1.1.0-2.x86_64.rpm
	xorg-x11-drv-elo2300-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-elographics-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-evdev-1.0.0.5-3.el5.x86_64.rpm
	xorg-x11-drv-fbdev-0.3.0-2.x86_64.rpm
	xorg-x11-drv-fpit-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-hyperpen-1.1.0-2.x86_64.rpm
	xorg-x11-drv-i810-1.6.5-9.13.el5.x86_64.rpm
	xorg-x11-drv-jamstudio-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-joystick-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-keyboard-1.1.0-3.x86_64.rpm
	xorg-x11-drv-magellan-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-magictouch-1.0.0.5-2.1.x86_64.rpm
	xorg-x11-drv-mga-1.4.2-7.el5.x86_64.rpm
	xorg-x11-drv-microtouch-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-mouse-1.1.1-1.1.x86_64.rpm
	xorg-x11-drv-mutouch-1.1.0-2.x86_64.rpm

	xorg-x11-drv-nv-2.1.6-6.el5.x86_64.rpm
	xorg-x11-drv-palmax-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-penmount-1.1.0-2.1.x86_64.rpm
	xorg-x11-drv-s3-0.4.1-2.1.x86_64.rpm
	xorg-x11-drv-s3virge-1.9.1-2.1.x86_64.rpm
	xorg-x11-drv-savage-2.1.1-5.fc6.x86_64.rpm
	xorg-x11-drv-siliconmotion-1.4.1-2.1.x86_64.rpm
	xorg-x11-drv-sis-0.9.1-7.1.el5.x86_64.rpm
	xorg-x11-drv-sisusb-0.8.1-4.1.x86_64.rpm
	xorg-x11-drv-spaceorb-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-summa-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-tdfx-1.2.1-3.1.x86_64.rpm
	xorg-x11-drv-tek4957-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-trident-1.2.1-3.fc6.x86_64.rpm
	xorg-x11-drv-ur98-1.1.0-1.1.x86_64.rpm
	xorg-x11-drv-vesa-1.3.0-8.1.el5.x86_64.rpm
	xorg-x11-drv-vga-4.1.0-2.1.x86_64.rpm
	xorg-x11-drv-via-0.2.1-9.x86_64.rpm
	xorg-x11-drv-vmmouse-12.4.0-2.1.x86_64.rpm
	xorg-x11-drv-vmware-10.13.0-2.1.x86_64.rpm
	xorg-x11-drv-void-1.1.0-3.1.x86_64.rpm
	xorg-x11-drv-voodoo-1.1.0-3.1.x86_64.rpm
	xorg-x11-filesystem-7.1-2.fc6.noarch.rpm
	xorg-x11-fonts-100dpi-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-75dpi-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-base-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-cyrillic-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-ISO8859-1-100dpi-7.1-2.1.el5.noarch.rpm

	xorg-x11-fonts-ISO8859-1-75dpi-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-misc-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-truetype-7.1-2.1.el5.noarch.rpm
	xorg-x11-fonts-Type1-7.1-2.1.el5.noarch.rpm
	xorg-x11-font-utils-7.1-2.x86_64.rpm
	xorg-x11-server-utils-7.1-4.fc6.x86_64.rpm
	xorg-x11-server-Xnest-1.1.1-48.41.el5.x86_64.rpm
	xorg-x11-server-Xorg-1.1.1-48.41.el5.x86_64.rpm
	xorg-x11-twm-1.0.1-3.1.x86_64.rpm
	xorg-x11-utils-7.1-2.fc6.x86_64.rpm
	xorg-x11-xauth-1.0.1-2.1.x86_64.rpm
	xorg-x11-xfs-1.0.2-4.x86_64.rpm
	xorg-x11-xinit-1.0.2-15.el5.x86_64.rpm
	xorg-x11-xkb-utils-1.0.2-2.1.x86_64.rpm
	xrestop-0.2-6.2.2.x86_64.rpm
	xsane-0.991-5.el5.x86_64.rpm
	xsane-gimp-0.991-5.el5.x86_64.rpm
	xsri-2.1.0-10.fc6.x86_64.rpm
	xterm-215-5.el5.x86_64.rpm
	xulrunner-1.9-0.beta5.6.el5.i386.rpm
	xulrunner-1.9-0.beta5.6.el5.x86_64.rpm
	yelp-2.16.0-18.el5.x86_64.rpm
	ypbind-1.19-8.el5.x86_64.rpm
	yp-tools-2.9-0.1.x86_64.rpm
	yum-3.2.8-9.el5.noarch.rpm
	yum-metadata-parser-1.1.2-2.el5.x86_64.rpm
	yum-rhn-plugin-0.5.3-6.el5.noarch.rpm
	yum-security-1.1.10-9.el5.noarch.rpm
	yum-updatesd-0.9-2.el5.noarch.rpm
	zenity-2.16.0-2.el5.x86_64.rpm

	zip-2.31-1.2.2.x86_64.rpm
	zlib-1.2.3-3.i386.rpm
	zlib-1.2.3-3.x86_64.rpm

2.4 Конфигурации

Оцениваемые конфигурации определяются следующим образом:

- Оцениваемый по ОК набор пакетов должен быть выбран во время установки в соответствии с описанием Руководства по оцениваемой конфигурации и установлен соответствующим образом.
- ОО поддерживает использование протоколов IPv4 и IPv6, и они оба рассматриваются в оцениваемой конфигурации.
- Поддерживается инсталляция как с компакт-диска, так и с определенного раздела жесткого диска.
- По умолчанию для подсистемы идентификации и аутентификации принимается конфигурация, основанная на модулях PAM, определяющих парольную аутентификацию. Поддержка других аутентификационных возможностей (например, смарт-карты) в оцениваемую конфигурацию не включается.
- Если используется системная консоль, она должна быть непосредственно связана с ОО и так же, как ОО, физически защищена.
- ОО поддерживает работу в режиме DAC. Программная конфигурация для обоих режимов идентична и различается только модулями безопасности SELinux и файлами политики для этих модулей.
- ОО включает единственную клиентскую машину (далее «клиент ОО»), на которой функционирует системное ПО, перечисленное в списке пакетов в подразделе 2.3, и аппаратные средства, перечисленные в пункте 2.4.2.

2.4.1 Файловые системы

ОО обеспечивает поддержку файловых систем следующих типов:

- журналируемая файловая система Ext3;
- файловая система ISO 9660 для дисководов CD и DVD ROM;
- файловая система процесса procfs (/proc), представляет процессы/задачи как файлы и каталоги, содержащие оперативную информацию о состоянии каждого процесса в системе. Решения на доступ процесса

определяются атрибутами DAC, выведенными из атрибутов DAC основного процесса. На конкретные объекты в этой файловой системе налагаются дополнительные ограничения;

- файловая система sysfs, используемая для экспорта и обработки информации, не относящейся к процессам ядра, например информация драйвера конкретного устройства;
- временная файловая система tmpfs, базирующаяся на оперативной памяти;
- файловая система devpts, используемая для работы терминальных псевдоустройств;
- виртуальная файловая система rootfs, временно используемая в процессе запуска системы;
- файловая система binfmt_misc регистрации файлов смешанного двоичного формата, используемая для конфигурирования интерпретаторов по информации заголовков выполняемых двоичных файлов;
- файловая система selinuxfsc усиленной безопасности Linux, используемая для конфигурирования системы selinux и для обеспечения API политики SELinux в программах пользовательского пространства.

2.4.2 Аппаратные средства ОО

Аппаратные средства, на которых функционируют программные компоненты ОО, считаются частью ОО. ОО может включать любую из аппаратных платформ на основе 32 – и 64 – разрядных процессоров Intel и AMD.

2.4.3 Среда ОО

Несколько систем ОО могут быть связаны в сеть, и отдельные сети могут быть объединены мостами и/или маршрутизаторами, или системами ОО, которые действуют как маршрутизаторы и/или шлюзы. Каждый из клиентов ОО и каждая из систем ОО реализует свою собственную политику безопасности. ОО не включает каких-либо функций синхронизации для этих политик. В результате, отдельный пользователь может иметь учетные записи пользователя на каждой из этих систем с различными идентификаторами пользователя, различными ролями и другими отличительными атрибутами. (Метод синхронизации может использоваться факультативно, но он не является частью ОО и не должен использовать методы, которые противоречат требованиям ОО). Если к сети присоединяются другие системы, они должны конфигурироваться и администрироваться с теми же самыми

полномочиями и в соответствии с политикой безопасности, которая не противоречит политике безопасности ОО. Все связи между сетями, основанными на ОО, и недоверенными сетями (например, Интернет) должны быть защищены соответствующими мерами, включая межсетевые экраны, предотвращающие нападения из недоверенных сетей. Эти средства защиты являются частью среды ОО.

3 Среда безопасности ОО

3.1 Введение

Описание среды безопасности ОО содержит аспекты безопасности среды, в которой предполагается развертывание и использование ОО ожидаемым способом. В описании среды безопасности ОО идентифицируется список предположений, сделанных для эксплуатационной среды (включая физические и процедурные меры), и намеченный метод использования ОО, определяются угрозы, которым продукт должен противостоять, и политики безопасности организации, которым продукт должен подчиняться.

3.2 Угрозы

Предполагаемые угрозы безопасности приведены ниже.

3.2.1 ИТ-активы

Активы, которые необходимо защищать, включают информацию, сохраняемую, обрабатываемую или передаваемую ОО. Используемый здесь термин «информация», относится ко всем поддерживаемым клиентом данным, включая находящиеся в пути между системами.

ОО противостоит общей угрозе несанкционированного доступа, которая включает раскрытие, модификацию и уничтожение информации.

3.2.2 Источники угроз

Источником угроз обычно являются нарушители, которые подразделяются на:

- неуполномоченных пользователей ОО, у которых нет прав на доступ к системе;
- уполномоченных пользователей ОО, у которых есть права на доступ к системе.

Источником угроз предполагается хорошо организованное и управляемое сообщество пользователей в невраждебных производственных условиях. Следовательно, ОО защищает от угроз безопасности через посредство уязвимостей, которые могли бы использоваться в предполагаемой среде ОО, подвергаемого экспертизе и оценке со средним уровнем усилий. В соответствии с требуемой стойкостью функций безопасности, ОО защищает от прямого или преднамеренного нарушения своей безопасности нарушителями, обладающими низким потенциалом нападения.

3.2.3 Угрозы, которым противостоит ОО

Ниже сгруппированы угрозы, которым противостоит ОО. Угрозам, которым ОО не противостоит, противостоят механизмы среды или другие внешние механизмы.

T.UAUSER Нарушитель (возможно, но не обязательно, неуполномоченный пользователь ОО) может выдать себя за уполномоченного пользователя ОО. Это угроза со стороны уполномоченного пользователя, который пробует выдать себя за какого-либо другого уполномоченного пользователя, не обладая знаниями о его аутентификационной информации.

T.UAACCESS Уполномоченный пользователь ОО может получить доступ к информационным ресурсам, не имея разрешения на данный тип доступа от владельца или ответственного за информационный ресурс.

T.COMPROT Нарушитель (возможно, но не обязательно, неуполномоченный пользователь ОО) может прервать сетевое соединение между ОО и другим доверенным ИТ-продуктом (который также может быть реализацией ОО) для чтения или изменения информации, передаваемой между ними с использованием определенных протоколов (SSH или SSL), способом, не обнаруживаемым ни ОО, ни другим доверенным ИТ-продуктом.

T.OPERATE Компрометация ИТ-активов может произойти из-за неправильного администрирования и эксплуатации ОО.

T.ROLEDEV Разработка и назначение ролей пользователей может производиться способом, подрывающим безопасность ОО.

3.2.4 Угрозы, которым противостоит среда ОО

В среде ОО необходимо противостоять следующим угрозам системе:

TE.HWMF Нарушитель, имеющий законный физический доступ к аппаратным средствам ОО (например, технический персонал или законные пользователи), или некоторые условия среды могут вызвать сбой аппаратных средств, в результате которого пользователь (обычный или административный) потеряет сохраненные данные. Такой сбой аппаратных

средств нарушитель может вызвать либо при наличии физического доступа к аппаратным средствам, на которых функционирует ОО, либо выполнением ПО, способного порождать сбои в работе аппаратных средств. Необходимо отметить, что такой сбой аппаратных средств может быть вызван случайно, без злонамеренного действия лиц, имеющих физический доступ к ОО.

TE.COR_FILE Нарушитель (включая, но не ограничиваясь неуполномоченным пользователем ОО) или некоторые условия среды (сбои аппаратных средств) могут преднамеренно или случайно изменить или разрушить важные для безопасности или функционирования ОО файлы, и это не сможет обнаружить административный пользователь. Нарушитель может разрушить такие файлы либо при наличии физического доступа к аппаратным средствам ОО, используя ПО, не входящее в оцениваемую конфигурацию ОО, либо изменив или разрушив файлы на резервном носителе информации. Заметим, что такое искажение может быть случайным, без злонамеренного действия лиц, имеющих законный доступ к носителю информации, где сохраняются такие данные.

3.3 Политика безопасности организации

ОО выполняет следующие политики безопасности организации:

P.AUTHORIZED_USERS К системе могут иметь доступ только пользователи, которым был разрешен доступ к информации в ней.

P.NEED_TO_KNOW Организация должна определить дискреционную политику управления доступом на основе необходимого знания, которая может моделироваться на следующих атрибутах:

- идентификаторе владельца объекта;
- идентификаторе субъекта, делающего попытку доступа;
- неявных и явных правах доступа к

объекту, предоставленных субъекту владельцем объекта.

Примечание: Будучи доступной для моделирования, политика управления доступом организации, основанная на этих трех указанных выше аспектах, обеспечивает возможность отображения политики организации на ОО посредством функций безопасности, которые предоставляет ОО. Например, политика управления доступом, основанная на правилах, зависящих от времени или содержимого, не удовлетворяет вышеупомянутой политике.

P.ACCOUNTABILITY Пользователи системы должны быть подотчетны за свои действия в системе.

3.4 Предположения

Этот подраздел указывает на минимальные физические и процедурные меры, требуемые для поддержания безопасности ОО.

3.4.1 Физические аспекты

A.ASSET Предполагается, что значение сохраняемых активов может стать причиной попыток замаскированных нападений или проникновений с умеренной интенсивностью.

A.LOCATE Вычислительные ресурсы ОО должны располагаться в пределах средств управления доступом, которые предотвращают несанкционированный физический доступ к ним.

A.PROTECT Аппаратное и программное обеспечение ОО, критичное к применению политики безопасности, должно быть защищено от несанкционированной физической модификации, в том числе со стороны потенциально враждебных посторонних лиц.

3.4.2 Аспекты персонала

A.ACCESS Права пользователей для получения доступа и выполнения обработки информации основываются на одной или более ролях, которые им назначает администратор ОО. Эти роли точно отражают производственную функцию, обязанности,

квалификацию и/или компетентность пользователей в рамках предприятия.

A.MANAGE Предполагается наличие (одного или более) компетентных лиц, которые назначаются для управления безопасностью ОО и информации в нем. Эти лица должны иметь личную ответственность за следующие функции:

- создание и сопровождение ролей;
- установление и сопровождение отношений между ролями;
- назначение и аннулирование ролей, назначаемых пользователям. Кроме того, эти лица (в качестве владельцев всех корпоративных данных), наряду с владельцами объекта, должны иметь возможность назначать и отменять права доступа ролей к объектам.

A.OWNER Ограниченному числу пользователей даются права создавать новые объекты данных, и они становятся владельцами этих объектов данных. Организация является владельцем остальной части информации, находящейся под управлением ОО.

A.NO_EVIL_ADMIN Административный персонал системы не является беспечным, небрежным или преднамеренно враждебным и должен применять и соблюдать инструкции, предоставленные документацией администратора.

A.COOP Ожидается, что уполномоченные пользователи обладают необходимым разрешением на доступ, по крайней мере, к части информации, управляемой ОО, и согласованно действуют в благоприятной среде.

A.UTRAIN Пользователи обучены применять функциональные возможности безопасности, предоставляемые системой.

A.UTRUST Пользователям доверено выполнение некоторой задачи или группы задач в безопасной ИТ-среде с применением полного управления своими данными.

3.4.3 Аспекты связности

A.NET_COMP Предполагается, что все сетевые компоненты (такие, как мосты и маршрутизаторы) передают данные правильно, без модификации.

A.PEER Предполагается, что любые другие системы, с которыми общается ОО, находятся под тем же самым административным управлением и работают с теми же самыми ограничениями политики безопасности.

A.CONNECT Все подключения к периферийным устройствам и сетевые подключения, не использующие защищенные протоколы SSH v2 или SSL v3, постоянно находятся в пределах действия средств управления доступом.

4 Цели безопасности

4.1 Цели безопасности для ОО

O.AUTHORIZATION	ФБО должны предоставлять возможность получения доступа к ОО и его ресурсам только уполномоченным пользователям.
O.DISCRETIONARY_ ACCESS	ФБО должен управлять доступом к ресурсам, основанным на идентификаторах пользователей. ФБО должны разрешать уполномоченным пользователям определять, к каким ресурсам какие пользователи могут обращаться.
O.AUDITING	ФБО должны регистрировать действия пользователей, относящиеся к безопасности ОО. ФБО должны предоставлять эту информацию уполномоченным администраторам. Информация в записях о событиях безопасности должна быть достаточно детальной, чтобы помочь администратору ОО в поиске предпринятых попыток нарушения безопасности или потенциально ошибочной конфигурации свойств безопасности ОО, которые оставляли бы ИТ-активы открытыми, для компрометации.
O.RESIDUAL_INFO	ФБО должны предотвращать возможность раскрытия любой информации, содержащейся в защищаемом ресурсе, при его перераспределении.
O.MANAGE	ФБО должны предоставлять все необходимые функции и возможности для поддержки административных пользователей, ответственных за управление безопасностью ОО, и обеспечивать доступ к таким функциональным возможностям только административным пользователям. Эти функции должны давать возможность уполномоченному администратору эффективно управлять ОО и его функциями безопасности.
O.ENFORCEMENT	ФБО должны быть спроектированы и

	реализованы способом, обеспечивающим выполнение политик безопасности организации в целевой среде. Политика безопасности ОО выполняется способом, обеспечивающим выполнение политик безопасности организации в целевой среде, то есть защищает целостность ФБО.
O.COMPROT	ФБО должны быть спроектированы и реализованы способом, который позволяет устанавливать соединение ОО с другим доверенным ИТ-продуктом посредством доверенного канала, который защищает передаваемые по нему пользовательские данные от раскрытия и необнаруженной модификации.

4.2 Цели безопасности для среды ОО

Все требования безопасности, перечисленные в этом подразделе, предназначаются для не-ИТ-среды ОО.

OE.ADMIN	Ответственные за администрирование ОО лица являются компетентными, надежными и способными безопасно управлять ОО и содержащейся в нем информацией.
OE.CREDEN	Ответственные за ОО должны обеспечивать надежное хранение аутентификационных данных пользователей и их защиту от раскрытия неуполномоченными лицами. В особенности: - должны быть установлены процедуры, соответствующие целям системы, для обеспечения безопасного способа генерации администратором паролей пользователей, распределяемых при создании или модификации их учетных записей; должна отсутствовать физическая возможность удаления из системы кем-либо, кроме административных пользователей, носителя

	информации, хранящего аутентификационные данные; пользователи не должны раскрывать свои пароли другим лицам.
OE.INSTALL	Ответственные за ОО должны безопасным способом применять процедуры и инструменты, обеспечивающие установку, поставку, инсталляцию и конфигурирование составляющих систему аппаратных средств, компонентов ПО и встроенного ПО.
OE.PHYSICAL	Ответственные за ОО должны обеспечивать защиту критичных к политике безопасности частей ОО от физических атак, которые могут скомпрометировать цели безопасности ИТ.
OE.INFO_PROTECT	Ответственные за ОО должны устанавливать процедуры и инструменты, обеспечивающие защиту информации соответствующим способом. В особенности: - защита критичных по безопасности файлов (файлов конфигурации и аутентификационных баз данных) с помощью DAC должна всегда устанавливаться правильно; - сетевое и периферийное кабельное оборудование, входящее в систему, должно испытываться для передачи большинства уязвимых данных. Предполагается, что такие физические связи защищаются соответственно от угроз конфиденциальности и целостности передаваемых данных, если для связи с другой доверенной сущностью используется один из безопасных протоколов, предоставляемых ОО; - пользователи должны быть обучены выполнять свои задачи должным образом и заслуживают доверия в части отсутствия намерения неправильного использования ими доступа к информации и

	передачи своих прав лицам, не имеющим таких прав.
OE.MAINTENANCE	Административные пользователи ОО должны иметь возможность вызова любых поставляемых с продуктом средств диагностики в любой намеченный период профилактического обслуживания.
OE.RECOVER	Ответственные за ОО должны обеспечивать процедуры и/или механизмы, удостоверяющие факт восстановления системы без компрометации защиты (то есть, безопасно) после отказа или другого прерывания.
OE.SOFTWARE_IN	Ответственные за ОО должны обеспечивать такую конфигурацию системы, при которой установка в нее нового доверенного ПО разрешается только административному пользователю.
OE.SERIAL_LOGIN	Ответственные за ОО должны реализовать процедуры, обеспечивающие очистку пользователем экрана последовательного устройства системы (например, терминала IBM 3151) перед выходом из нее.
OE.PROTECT	Ответственные за ОО должны обеспечивать процедуры и/или механизмы защиты данных, передаваемых между клиентами, от раскрытия и вмешательства.

5 Требования безопасности

5.1 Функциональные требования безопасности ОО

Большинство ФТБ в данном ЗБ взяты из [LSPP] и [RBACPP] и приспособлены, включая некоторые конкретные расширения ОО.

В режиме DAC все роли, определенные в ФТБ, включены в категорию единственной роли администратора (пользователь «root» с UID(0)).

5.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

1. запуск и завершение выполнения функций аудита;
2. все события, потенциально подвергаемые аудиту, на *базовом* уровне аудита;
3. [перечисленные в столбце «Событие» таблицы 5.1, исключая неуспешную идентификацию пользователя по FIA_UID.2, а также:
4. назначение пользователей, ролей и привилегий ролям;
5. удаление пользователей, ролей и привилегий ролей;
6. создание и удаление ролей].

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

1) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
2) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ЗБ,

[

1. дополнительная информация, определенная в столбце «Детали» таблицы 5.1**;**
2. роль Администратора RBAC, сделавшая возможным вызов каждой функции безопасности;
3. роль, сделавшая возможным вызов каждого действия по управлению доступом к данным пользователя].

Таблица 5.1 – События аудита

Компонент	Событие	Детали (Названия событий)
FAU_GEN.1	Запуск и завершение функций аудита.	События: «старт аудита», «останов аудита» (из *auditd*).
FAU_GEN.2	Нет.	
FAU_SAR.1	Чтение информации из записей аудита.	Системный вызов *open* (на журнал аудита).
FAU_SAR.2	Неудачные попытки чтения информации из записей аудита.	Как в FAU_SAR.1, но при отрицательном результате.
FAU_SAR.3	Нет.	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время работы функции сбора информации аудита.	Событие: «AUDIT_CONFIG_CHANGE»; системные вызовы *open, link, unlink, rename, truncate* (доступ на запись к конфигурационным файлам).
FAU_STG.1	Нет.	
FAU_STG.3	Действия, предпринимаемые вследствие превышения порога заполнения журнала.	Событие: «размер журнала больше максимального» или «нехватка дискового пространства» (генерируется *auditd*); выполнение действий по сигналу тревоги, указанных администратором, таких как смена файла, переключение в однопользовательский режим или останов системы.
FAU_STG.4	Действия, предпринимаемые вследствие отказа памяти аудита.	Событие: «не осталось места» или «ошибка записи события на диск» (генерируется *auditd*); выполнение аварийных действий, указанных

Компонент	Событие	Детали (Названия событий)
		администратором, таких как переключение в однопользовательский режим или останов системы, которые завершают все программы, способные к генерации событий аудита.
FDP_ACC.1	Нет.	
FDP_ACF.1	Все запросы на выполнение действий на объекте, охваченном ПФБ.	Системные вызовы: *chmod*, *chown*, *setxattr*, *removexattr*, *link*, *symlink*, *mknod*, *open*, *rename*, *truncate*, *unlink*, *rmdir*, *mount*, *umount*, *msgctl*, *msgget*, *semget*, *semctl*, *semop*, *semtimedop*, *shmget*, *shmctl*; детали включают идентификацию объекта
FDP_RIP.2 (1)	Нет.	
FDP_RIP.2 (2)	Нет.	
FDP_UCT.1	Нет.	
FDP_UIT.1	Нет.	
FIA_ATD.1	Нет.	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного секрета.	Событие: «аутентификация PAM» (из структуры PAM); детали включают происхождение попытки (приемлемы терминал или IP адрес).
FIA_UAU.2	Все использования опознавательного механизма.	Событие: «аутентификация PAM» (из структуры PAM).
FIA_UAU.7	Нет.	

Компонент	Событие	Детали (Названия событий)
FIA_UID.2	Все использования идентифицирующего механизма пользователя, включая идентификацию, обеспечиваемую во время успешной попытки.	События: «аутентификация PAM» и «ошибка идентификации PAM» (из структуры PAM).
FIA_USB.1	Успех и отказ связывания атрибутов безопасности пользователя с субъектом (например, успех или отказ при создании субъекта).	События: «открытие сессии PAM» (из структуры PAM); Системные вызовы: *fork, vfork* и *clone;* События отказа: «аутентификация PAM» и «ошибка идентификации PAM» (из структуры PAM, состояние отказа).
FMT_MSA.1	Все модификации значений атрибутов безопасности.	Системные вызовы: *chmod, chown, setxattr, msgctl, semctl, shmctl*; Системный вызов *open* на файлы интерфейса SELinux /proc/self/attr/current и /selinux/load.
FMT_MSA.3	Модификации настроек по умолчанию, разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности.	Системные вызовы: *umask, open*; Системный вызов *open* на файлы интерфейса SELinux /proc/self/attr/exec, /proc/self/attr/fscreate, и /selinux/load.
FMT_MTD.1 (1)	Все модификации	Системные вызовы: *open*,

Компонент	Событие	Детали (Названия событий)
	значений данных ФБО.	*rename*, *link*, *unlink*, *truncate* (файлов журналов аудита).
FMT_MTD.1 (2)	Все модификации значений данных ФБО.	Системные вызовы: *open*, *link*, *rename*, *truncate*, *unlink* (конфигурационных файлов аудита); Событие: «изменение конфигурации».
FMT_MTD.1 (3)	Все модификации значений данных ФБО. Требуется включить создание и удаление пользователей.	Текстовые сообщения аудита от «теневых утилит» доверенных программ, детали включают новые значения данных ФБО.
FMT_MTD.1 (4, 5)	Все модификации значений данных ФБО.	Текстовые сообщения аудита от «теневых утилит» доверенных программ; попытки обхода доверенных программ, обнаруженные через контролируемые аудитом системные вызовы: *open*, *rename*, *truncate*, *unlink.*
FMT_MTD.1 (6)	Управление ролями.	Текстовые сообщения аудита от утилит *semodule* и *load_policy*; системных вызовов *open* на файл интерфейса SELinux /selinux/load.
FMT_MTD.3 Безопасные Данные ФБО	Все отклоненные значения данных ФБО.	Текстовые сообщения аудита от PAM, указывающие отклоненные попытки выбора слабого пароля.
FMT_REV.1	Все попытки отмены атрибутов безопасности.	Событие: Текстовые сообщения аудита от «теневых

Компонент	Событие	Детали (Названия событий)
		утилит» доверенных программ; попытки обхода доверенных программ, обнаруженные через контролируемые аудитом системные вызовы: *open, rename, truncate, unlink.*
FMT_REV.1	Все модификации значений данных ФБО.	Системные вызовы: *chmod, chown, setxattr, unlink, truncate, msgctl, removexattr , semctl, shmctl.*
FMT_SMF.1	Нет (охвачено другими функциями управления).	
FMT_SMR.2	Модификации в группе пользователей, которая является частью роли, включая: – Назначение ролям пользователей; – Назначение ролям привилегий; – Создание ролей; – Удаление ролей; – Удаление из ролей привилегий.	Событие: Текстовые сообщения аудита от «теневых утилит» доверенных программ: «добавление членов группы», «удаление членов группы», «назначение администраторов группы», «назначение членов группы» (из доверенных программ в теневом наборе). Текстовые сообщения аудита от инструмента *semanage.* Текстовые сообщения аудита от инструментальных средств *semodule* и *load_policy,* указывающих определения новых заказных ролей или их модификации.
FMT_SMR.2	Каждое использование прав роли. (Дополнительное/детали-зированное)	Результат действий пользователя в контролируемых аудитом системных вызовах и

Компонент	Событие	Детали (Названия событий)
		использовании подвергаемых аудиту доверенных программ. Детали включают имя входа в систему, происхождение которого и имени сеанса аудита может быть определено из связанной записи входа в систему.
FMT_SMR.2	Неудачные попытки использовать роль вследствие налагаемых на роли условий.	Событие: текстовые сообщения аудита от программ *newrole, login, sshd, su.*
FPT_AMT.1	Выполнение тестов основной машины и результаты тестов.	Сообщения событий «amtu- *» (сгенерированных тестовым инструментом AMTU).
FPT_FLS.1	Отказ ФБО.	Событие: текстовые сообщения аудита от программ набора «утилит политик ядра», включая *load_policy, restorecon, fixfiles, newrole*; текстовые сообщения аудита от политики осознанного использования программ libselinux*: login, sshd, su, crond.*
FPT_RCV.1	Факт произошедшего отказа или отказа в обслуживании.	Событие: текстовые сообщения аудита от *init*, указывающие переключение на однопользовательский уровень выполнения.
FPT_RCV.1	Возобновление регулярной эксплуатации.	Событие: текстовые сообщения аудита от *init*, указывающие переключение на многопользовательский

Компонент	Событие	Детали (Названия событий)
		уровень выполнения.
FPT_RCV.1	Тип отказа или отказа в обслуживании.	Событие: текстовые сообщения аудита от программы инициализации переключения на однопользовательский режим через libselinux: *auditd, init, load_policy.*
FPT_RCV.4	Если возможно, невозможность возврата к безопасному состоянию после отказа функции безопасности.	Событие: текстовые сообщения аудита от *init,* указывающее на отказ переключения между уровнями выполнения.
FPT_RCV.4	Если возможно, обнаружение отказа функции безопасности.	Событие: текстовые сообщения аудита от *init,* указывающее переключение на однопользовательский уровень выполнения.
FPT_RVM.1	Нет.	
FPT_SEP.1	Нет.	
FPT_STM.1	Изменения времени.	Событие: системные вызовы: *settimeofday, adjtimex, clock_settime*
FPT_TST.1	Выполнение самотестирования ФБО и результаты тестирования.	Событие: текстовые сообщения аудита от программы *rbac-self-test.*
FTA_LSA.1	Все попытки выбора атрибутов безопасности сеанса.	Событие: текстовые сообщения аудита от роли, которая осознанно использует программы libselinux: *login, sshd, su, crond.*

Компонент	Событие	Детали (Названия событий)
FTA_TSE.1	Все попытки установления сеанса пользователя.	Событие: текстовые сообщения аудита от роли, которая осознанно использует программы libselinux: *login, sshd, su, crond.*
FTP_ITC.1	Установка доверенного канала.	Событие: системный вызов *exec* (программы *stunnel*).

Примечание: В таблице приведены названия событий, связанных с ФТБ. Детали конкретных данных, записываемых при каждом событии, приведены в проектной документации аудита.

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

Примечание: ОО поддерживает «Входной идентификатор», который наследуется каждым новым порожденным процессом. Это позволяет ОО идентифицировать «реального» автора события, независимо от того, изменил ли он реальный и/или эффективный идентификатор и идентификатор пользователя владельца файловой системы, например, используя команды su или выполняя программу setuid или setgid.

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченным административным ролям] возможность читать [всю информацию аудита, включая:

1) дату и время события аудита;
2) идентификатор пользователя, ответственного за событие и, дополнительно, принадлежность к роли, которая дала возможность пользователю успешно выполнить событие;
3) тип операции управления доступом и объект, на котором она выполнялась;
4) результат события (успех или отказ);
5) идентификатор сеанса пользователя или тип терминала]

из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Примечание: ОО конфигурируется так, чтобы ограничить прямой доступ к записям аудита пользователями в роли администратора аудита.

FAU_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.

Примечание: Меры безопасности DAC, RBAC обеспечивают доступ к записям аудита только пользователям в роли администратора аудита.

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны предоставить возможность выполнить *поиск, сортировку и упорядочивание* данных аудита, основанные на [следующих атрибутах:

1) идентификатор пользователя;
2) идентификатор группы (реальный и эффективный);
3) тип события;
4) результат (успех/отказ);
5) имя конкретного удаленного хоста, с которого осуществлен вход в систему;
6) идентификатор пользователя при входе в систему;
7) идентификатор процесса;
8) роль, которая разрешила доступ;
9) дата и время события аудита;
10) имя объекта;
11) тип доступа;
12) любая комбинация вышеупомянутых элементов].

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой

совокупности по следующим атрибутам:

1) *идентификатор объекта, идентификатор пользователя, тип события*;

2) принадлежность пользователя к указанной роли;

3) типы доступа на отдельном объекте;

4) номер системного вызова;

5) имя каталога или файла;

6) идентификатор субъекта (процесса);

7) идентификатор хоста].

Примечание: ОО предоставляет администратору возможность выбирать события для аудита. Администратор может сделать это, редактируя файл конфигурации фильтра демона аудита и затем используя сценарий */etc/rc.d/init.d/auditd* с параметром «reload» для регистрации изменения в конфигурации демона аудита. Демон аудита, в свою очередь, регистрирует ядро новой политики аудита.

Примечание: Система в оцениваемой конфигурации не поддерживает распределенный аудит, поэтому идентификатор хоста для всех записей аудита на конкретном хосте всегда совпадает с именем этого хоста. Система поддерживает различные, определяемые на различных хостах, правила аудита, которые являются эквивалентными фильтрации по идентификатору хоста в нераспределенной среде.

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны к *предотвращению* модификации записей аудита.

Примечание: Это достигается использованием мер безопасности DAC.

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [генерацию сигнала тревоги уполномоченному администратору], если журнал аудита превышает [значение, определенное в файле /etc/auditd.conf, для минимального пространства файловой системы, в которой постоянно находится журнал аудита].

Примечание: Сигналом тревоги, генерируемым ОО, является сообщение системного журнала. Это сообщение генерируется, когда потребности журнала аудита превышают предел, определенный в файле auditd.conf. Этот предел может определяться администратором аудита после редактирования файла auditd.conf с последующей перезагрузкой конфигурации аудита.

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить *предотвращение событий,*

подвергающихся аудиту, исключая предпринимаемые уполномоченным администратором, и [остановить все процессы, которые пытаются генерировать записи аудита] при переполнении журнала аудита.

Примечание: ОО останавливает процессы, которые хотят генерировать вход аудита, когда очередь в ядре, используемая для входов аудита, заполнена. Эта очередь должна непрерывно освобождаться демоном аудита и остановленные процессы должны быть продолжены, когда в очереди появляются пустые входы. Если заполняется сам журнал аудита, то демон аудита не способен освобождать очередь, пока не выполнит действие, которое определил администратор аудита. Возможные действия включают переключение в однопользовательский режим или останов системы, каждое из которых завершит все процессы, способные к генерации событий аудита. Администратор аудита в однопользовательском режиме может скопировать журнал аудита на резервный носитель и сделать освободившееся пространство снова доступным для журнала аудита, затем перезапустить ОО в многопользовательском режиме.

5.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 (1) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом (DAC)] для [процессов как субъектов, действующих от имени пользователей, и объектов файловой системы (обычные файлы, каталоги, символические ссылки, специальные файлы устройств, специальные файлы сокетов домена UNIX, именованные каналы), объектов IPC (SYSV и POSIX очереди сообщений, SYSV семафоры, SYSV сегменты совместно используемой памяти) и всех операций между субъектами и объектами, охваченных политикой DAC].

FDP_ACC.1 (2) Политика управления доступом, основанного на ролях

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях (RBAC)] для [процессов как субъектов, действующих от имени пользователей, и объектов файловой системы (обычные файлы, каталоги, символические ссылки, специальные файлы устройств, специальные файлы сокетов домена UNIX, именованные каналы), объектов IPC (SYSV и POSIX очереди сообщений, SYSV семафоры, SYSV сегменты совместно используемой памяти) и всех операций между субъектами и объектами, охваченных политикой RBAC].

FDP_ACF.1 (1) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на: [

1) Идентификаторе пользователя владельца файловой системы и членстве в группе(ах), связанных с субъектом;
2) Следующих атрибутах управления доступом, связанных с объектом:

Объекты файловой системы:

- биты разрешений;
- POSIX ACL (ACL могут использоваться для предоставления или запрета доступа с детализацией до конкретного

пользователя или группы, применяя элементы ACL для управления доступом. Эти элементы включают стандартные биты разрешений Unix. POSIX ACL могут использоваться для объектов файловой системы ext3).

Права доступа для объектов файловой системы:

- читать;
- писать;
- выполнять (обычные файлы);
- искать (каталоги);

Объекты IPC:

- биты разрешений.

Права доступа для объектов IPC:

- читать;
- писать].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [

Объекты файловой системы ext3:

Субъект должен иметь разрешение на поиск каждого элемента имени пути к объекту и на требуемый доступ к нему. Субъект обретает конкретный тип доступа к объекту указанием в соответствующей графе ACL объекта разрешающих значений. Разрешения на доступ предоставляются в следующих графах ACL объекта:

- ACL_USER_OBJ или ACL_OTHER;
- ACL_USER, ACL_GROUP_OBJ или ACL_GROUP, и связующие права предоставляется также графой ACL_MASK, при ее

наличии;

- ACL_GROUP_OBJ, при отсутствии графы ACL_MASK.

Объекты других файловых систем:

Субъект должен иметь разрешение на поиск для каждого элемента имени пути к объекту и на требуемый доступ к нему. Субъект имеет конкретный тип доступа к объекту если:

- субъект имеет идентификатор пользователя владельца объекта файловой системы, и для «владельца» определен требуемый тип доступа, представленный в битах разрешений;
- субъект не имеет идентификатора пользователя владельца объекта файловой системы, но идентификатор группы владельца файловой системы равен идентификатору группы объекта файловой системы, и для данной группы определен требуемый тип доступа, представленный в битах разрешений;
- субъект не имеет ни идентификатора пользователя владельца объекта файловой системы, ни идентификатора группы владельца файловой системы, равного идентификатору группы объекта файловой системы, и для «всех

остальных» определен требуемый тип доступа, представленный в битах разрешений.

Объекты IPC:

Разрешения на доступ определяются битами разрешений объекта IPC. Процесс, создающий объект, определяет создателя, владельца и группу, основанные на идентификаторе пользователя текущего процесса. Доступ процесса к объекту IPC разрешается, если:

- эффективный идентификатор пользователя текущего процесса равен идентификатору пользователя создателя или владельца объекта IPC, и для «владельца» определен требуемый тип доступа, представленный в битах разрешений;
- эффективный идентификатор пользователя текущего процесса не равен идентификатору пользователя создателя или владельца объекта IPC, и эффективный идентификатор группы текущего процесса равен идентификатору группы объекта IPC, и для данной группы определен требуемый тип доступа, представленный в битах разрешений;
- для «всех остальных»

пользователей, которые не удовлетворяют ни одному из первых двух условий, определен требуемый тип доступа, представленный в битах разрешений].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [

Объекты Файловой системы:

Процесс с эффективным идентификатором пользователя, равным 0, известен как процесс пользователя «root». Таким процессам вообще разрешаются все типы доступа. Но если процесс пользователя «root» запрашивает разрешение «выполнять» для программы как объекта файловой системы, то данный тип доступа предоставляется ему только, если разрешение «выполнять» предоставляется, по крайней мере, одному из пользователей.

Объекты IPC:

Процесс с эффективным идентификатором пользователя, равным 0, известен как процесс пользователя «root». Таким процессам вообще разрешаются все типы доступа].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах: [

К объектам файловой системы, смонтированным только на «чтение», доступ на «запись» всегда запрещен, исключая специальные файлы устройств.

К файлу, отмеченному как

«неизменяемый», доступ на «запись» всегда запрещен].

FDP_ACF.1 (2) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом, основанным на ролях] к объектам, основываясь на [

атрибутах пользователя:

1) идентификатор пользователя;
2) роли, разрешенные пользователю,

атрибутах субъекта:

1) идентификатор субъекта;
2) роли, которые может применять субъект,

атрибутах объекта:

1) идентификатор объекта;
2) операции, разрешенные на объектах для различных ролей].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [субъект, выполняющий операцию на объекте, назначается на роль, набор привилегий которой включает операцию на объекте].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [пользователь, связанный с субъектом, обладает ролью, которая разрешает операцию доступа к объекту].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах: [пользователь, связанный с субъектом, не обладает ролью, которая разрешает операцию доступа к объекту].

FDP_RIP.2 (1) Защита остаточной информации объекта

FDP_RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при *распределении ресурса* для всех объектов.

FDP_RIP.2 (2) Защита остаточной информации субъекта

FDP_RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего

информационного содержания ресурсов при *распределении ресурса* для всех субъектов.

FDP_UCT.1 Базовая конфиденциальность обмена данными

FDP_UCT.1.1 ФБО должны осуществлять [**дискреционную политику управления доступом, политику управления доступом, основанным на ролях**], предоставляющую возможность ***отправления и получения*** данных пользователя способом, защищенным от несанкционированного раскрытия.

Примечание: Конфиденциальность данных во время передачи обеспечивается при использовании одного из защищенных протоколов ssh или ssl. Пользовательские процессы, кроме того, связаны политикой дискреционного управления доступом с данными, которые они в состоянии передать.

FDP_UIT.1 Целостность передаваемых данных

FDP_UIT.1.1 ФБО должны осуществлять [**дискреционную политику управления доступом, политику управления доступом, основаннымо на ролях**], предоставляющую возможность ***отправления и получения*** данных пользователя способом, защищенным от следующих ошибок: ***вставки и модификации***.

FDP_UIT.1.2 ФБО должны быть способны определить после получения данных пользователя, произошли ли следующие ошибки: ***вставка или модификация***.

Примечание: Целостность данных во время передачи обеспечивается при использовании одного из защищенных протоколов ssh или ssl. Пользовательские процессы, кроме того, связаны политикой дискреционного управления доступом относительно данных, которые они в состоянии передать.

5.1.3 Идентификация и аутентификация (FIA)

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности: [

1) идентификатор пользователя;
2) членство в группах;
3) аутентификационные данные;
4) допуски пользователей;
5) список относящихся к безопасности ролей;
6) **никакие другие атрибуты**].

Примечание: «Аутентификационные данные» включают все данные, необходимые для успешного аутентификации пользователя или изменения аутентификационного маркера. Они состоят из пароля пользователя, срока действия пароля, устаревших сведений из ранее использованных паролей и информации о блокированных или с истекшим сроком действия учетных записях.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что секреты отвечают [следующему:

1) вероятность успеха случайной попытки использования аутентификационного механизма меньше 0,0000001;
2) вероятность успеха для множественных случайных попыток использования аутентификационного механизма во время минутного периода меньше 0,000001; и
3) любая обратная связь при попытках использования механизма аутентификации не должна приводить к превышению уровня вероятности, приведенного в метриках п.п. а), б)].

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Примечание: Недоверенные процессы, выполняющиеся от имени обычного пользователя, могут использовать сетевые функции для импорта и экспорта данных, к которым они имеют доступ. Поэтому

такой процесс может экспортировать пользовательские данные без аутентификации или даже без знания идентификатора пользователя, получающего такие данные. Предполагается, что это не является нарушением политики безопасности относительно идентификации, аутентификации и дискреционного управления доступом, так как известно, что дискреционное управление доступом не может управлять потоком информации. Примером такой экспортной функции является пользовательский процесс, запускающий сервер сети на непривилегированный порт. Кроме того, доступ к этому процессу ограничивается политикой безопасности ОО.

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять пользователю только [скрытую обратную связь] во время выполнения аутентификации.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать следующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя: [

1) идентификатор пользователя, который связан с событиями аудита;
2) идентификатор(ы) пользователя, который используется для обеспечения политики дискреционного управления доступом;
3) членство в группе(ах), которое используется для обеспечения политики дискреционного управления доступом;
4) текущая роль пользователя (из списка ролей, с которыми пользователю разрешено работать)].

FIA_USB.1.2 ФБО должны обеспечивать следующие правила начальной ассоциации атрибутов безопасности пользователя с субъектами, действующими от имени пользователя: [

1) при успешной идентификации и аутентификации в графе пользователя должны быть определены идентификатор пользователя для входа в систему, реальный идентификатор

пользователя, идентификатор пользователя владельца файловой системы и эффективный идентификатор пользователя;

2) при успешной идентификации и аутентификации в графе пользователя должны быть определены через атрибут членства в группе реальный идентификатор группы, идентификатор группы владельца файловой системы и эффективный идентификатор группы;

3) роль, связанная с субъектом, должна быть одной из уполномоченных ролей, назначенных пользователю].

FIA_USB.1.3 ФБО должны обеспечивать следующие правила, определяющие изменения в атрибутах безопасности пользователя, связанных с субъектами, действующими от имени пользователя: [

1) эффективный идентификатор пользователя и идентификатор пользователя владельца файловой системы могут быть изменены при помощи команды setuid, установкой бита «выполнять». В этом случае программа выполняется с эффективным идентификатором пользователя владельца программы и идентификатором пользователя владельца объекта файловой системы - программы. Затем оцениваются права доступа, используя идентификатор пользователя владельца объекта файловой системы - программы. Реальный идентификатор пользователя и идентификатор пользователя для входа в систему остаются неизменными.

2) эффективный идентификатор пользователя, идентификатор пользователя владельца файловой системы и реальный идентификатор

пользователя могут быть изменены командой su. В этом случае эффективный идентификатор пользователя, идентификатор пользователя владельца файловой системы и реальный идентификатор пользователя изменяются на идентификатор, определяемый пользователем в команде su (если аутентификация прошла успешно). Идентификатор пользователя для входа в систему остается неизменным.

3) идентификатор группы владельца файловой системы и эффективный идентификатор группы пользователя могут быть изменены при помощи команды setuid, установкой бита «выполнять». В этом случае программа выполняется с идентификатором группы владельца объекта файловой системы - программы и эффективным идентификатором группы владельца программы. Затем оцениваются права доступа, используя идентификатор группы владельца объекта файловой системы - программы
4) роли могут быть изменены выполнением доверенных программ, для которых политика SELinux определяет переход роли, например, программа newrole (при успешной аутентификации);
5) привилегированные субъекты могут изменять их собственные атрибуты безопасности].

Примечание: Привилегированные исполнители, для которых политика SELinux определяет домен или переход роли, имеют имя, заканчивающееся на «_exec_t», например, *newrole_exec_t*.

5.1.4 Управление безопасностью (FMT)

FMT_MSA.1(1) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], чтобы ограничить возможность *модификации* атрибутов безопасности [атрибутов управления доступом, связанных с поименованным объектом] только

[пользователями в административных ролях, позволяющих модификацию атрибутов управления доступом, и владельцами объектов].

FMT_MSA.1(2) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], чтобы ограничить возможность *модификации* атрибутов безопасности [атрибутов управления доступом, связанных с IPC объектом], только [первоначальным создателем объекта].

FMT_MSA.1(4) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях], чтобы ограничить возможность *модификации, удаления и создания экземпляров* атрибутов безопасности [полномочий ролей пользователей], только [перечнем административных ролей управления доступом, основанного на ролях].

FMT_MSA.1(5) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях], чтобы ограничить возможность *создания* атрибутов безопасности [перечня активных ролей, заданных по умолчанию], только [перечнем административных ролей управления доступом, основанного на ролях].

FMT_MSA.1(6) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях], чтобы ограничить возможность *модификации* атрибутов безопасности [состава перечня активных ролей сеанса пользователя], только [владельцем сеанса].

FMT_MSA.1(7) Управление атрибутами безопасности объекта

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях], чтобы ограничить возможность *модификации* атрибутов безопасности [атрибутов безопасности объекта], только [владельцами объектов и

перечнем административных ролей управления доступом, основанного на ролях].

FMT_MSA.3 (1) Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], чтобы обеспечить *ограничительные* значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2 ФБО должны предоставить возможность [пользователям в административной роли и владельцу объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

FMT_MSA.3 (2) Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику управления доступом, основанного на ролях], чтобы обеспечить *определяемые административным пользователем* значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2 ФБО должны предоставить возможность [перечню административных ролей управления доступом, основанного на ролях] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

FMT_MTD.1 (1) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность *удаления, очистки,* [создания] следующих данных [журнала аудита] только [уполномоченными администраторами].

Примечание: Данное требование реализуется использованием особенностей дискреционного управления доступом ОО для защиты файлов, содержащих журнал аудита.

FMT_MTD.1 (2) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность *модификации,* [просмотра] следующих данных [набора событий аудита] только [уполномоченными администраторами].

Примечание: Данное требование реализуется использованием особенностей дискреционного управления доступом ОО для защиты конфигурационных файлов аудита.

FMT_MTD.1 (3) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность *модификации,* [инициализации] следующих данных [атрибутов безопасности пользователей, кроме аутентификационных данных] только [пользователями в должным образом уполномоченной административной роли].

FMT_MTD.1 (4) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность [инициализации] следующих данных [аутентификационных данных] только [пользователями в должным образом уполномоченной административной роли].

FMT_MTD.1 (5) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность *модификации* следующих данных [аутентификационных данных] только: [

1) пользователями в должным образом уполномоченной административной роли;
2) пользователями, которым разрешается изменять их собственные аутентификационные данные].

FMT_MTD.1 (6) Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность *модификации,* [создания] следующих данных [список данных ФБО:

1) определения и атрибуты ролей;
2) иерархии ролей (назначением одной или более ролей на другие роли);
3) ограничения между отношениями ролей]

только: [перечнем административных ролей управления доступом, основанного на ролях].

FMT_MTD.3 Безопасные данные ФБО

FMT_MTD.3.1 ФБО должны обеспечить присвоение данным ФБО только безопасных значений.

Примечание: ОО реализует механизм проверки качества пароля, который предотвращает выбор слабых паролей пользователями.

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны ограничить возможность отмены атрибутов

безопасности, ассоциированных с *пользователями*, в пределах ОДФ только [перечнем административных ролей].

FMT_REV.1.2 ФБО должны реализовать правила: [

1) немедленная отмена разрешений, от которых зависит безопасность;
2) отмена/модификация уполномоченным администратором атрибутов безопасности пользователя, таких как идентификатор, имя, группа, пароль или имя командного процессора, которые должны быть задействованы при следующих входах пользователя в систему].

Примечание: Подобно другим операционным системам типа UNIX, ОО также не обеспечивает «немедленную отмену» для атрибутов безопасности пользователя. Для достижения этого системный администратор должен проверить, активен ли в системе пользователь, атрибуты безопасности которого были изменены. Если да, то системный администратор должен «вынудить» пользователя выйти из системы, как обозначено в Прикладном примечании CAPP.

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны ограничить возможность отмены атрибутов безопасности, ассоциированных с *объектами*, в пределах ОДФ только [пользователями, уполномоченными дискреционной и основанной на ролях политиками управления доступом изменять атрибуты безопасности].

Примечание: Политики определяют права владельцев объектов и административных ролей, уполномоченных отменять атрибуты безопасности. Отмена разрешается, только если ее разрешают все применяемые политики.

FMT_REV.1.2 ФБО должны реализовать правила: [

1) права доступа, ассоциированные с объектом, должны быть приведены в действие только после проверки доступа;
2) права доступа к объектам файловой системы и IPC проверяются при их открытии. Отмена прав доступа к объектам файловой системы вступает в силу при следующей попытке пользователя, права которого отменены, открыть объект].

Примечание: Подобно другим операционным системам типа UNIX, ОО реализует отсроченную отмену как обозначено в Прикладном примечании CAPP. Требование от [RBACPP] об отмене следующего «доступа к объекту» и требование [LSPP] на «всю последующую эксплуатацию» интерпретируется на момент следующего обращение к проверке доступа.

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1.1 ФБО должны включать в себя следующие функции управления безопасностью: [

1) администрирование атрибутов безопасности объекта;
2) администрирование атрибутов пользователя;
3) администрирование аутентификационных данных;
4) администрирование событий аудита].

Примечание: Данное функциональное требование безопасности отсутствует в [CAPP], но было добавлено в ЗБ, поскольку включено в ОК (интерпретация 65) и определена зависимость от этого нового компонента ФТБ FMT_MSA.1 и FMT_MTD.1.

FMT_SMR.2 Ограничения на роли безопасности

FMT_SMR.2.1 ФБО должны поддерживать следующие роли: [

1) перечень административных ролей управления доступом, основанного на ролях;
2) пользователи, уполномоченные политикой дискреционного управления доступом на изменение атрибутов безопасности;
3) пользователи, уполномоченные модифицировать свои собственные аутентификационные данные;
4) пользователи, не уполномоченные модифицировать свои собственные аутентификационные данные].

FMT_SMR.2.2 ФБО должны быть способны ассоциировать пользователей с ролями.

FMT_SMR.2.3 ФБО должны обеспечить выполнение [следующих условий для:

1) владельцев объектов – возможность изменять атрибуты безопасности только для объектов, которыми они владеют (за исключением меток

чувствительности);

2) перечня административных ролей управления доступом, основанного на ролях – возможность изменять атрибуты безопасности для всех объектов под управлением ОО (так как они автоматически наследуют привилегии всех владельцев объектов)].

Примечание: Ролевая модель, поддерживаемая ОО в режиме DAC, очень проста: административным пользователем является «root» (распространяемый на всех членов всех групп, которые могут переключаться на «root» посредством команды su). Все другие пользователи системы имеют роль пользователя.

5.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование базовой абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ *по запросу уполномоченного администратора* для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

FPT_FLS.1 Сбой с сохранением безопасного состояния

FPT_FLS.1.1 ФБО должны сохранить безопасное состояние при следующих типах сбоев [когда отключены, испорчены или недоступны:
вся база данных RBAC, содержащая данные о привилегиях, назначенных ролям, пользователях, уполномоченных на роли, ограничениях и отношениях ролей или некоторые конкретные таблицы, содержащие подмножества этих данных].

FPT_RCV.1 Ручное восстановление

FPT_RCV.1.1 После сбоя или прерывания обслуживания ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возвращения ОО к безопасному состоянию.

FPT_RCV.4 Восстановление функции

FPT_RCV.4.1 ФБО должны обеспечить следующее свойство для [

1) ФБ, которая проверяет, назначена ли некоторой роли указанная привилегия, но не подключена база данных, содержащая данные о привилегии, или недоступна конкретная таблица данных;
2) ФБ, которая проверяет, назначена ли конкретному пользователю указанная роль, но не подключена база данных, содержащая информацию о членстве в роли, или недоступна конкретная таблица данных.]

ФБ либо нормально заканчивает работу, либо для предусмотренных сценариев сбоев, восстанавливается к устойчивому и безопасному состоянию

FPT_RVM.1 Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие

ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Примечание: ОО обеспечивает это требование, используя особенности разделения адресов, характерные для устройств управления памятью, и защиту, предполагаемую центральным процессором с несколькими состояниями. Хотя ОО работает на различных платформах, все они имеют устройство управления памятью, позволяющее разделять адресное пространство между доверенными и недоверенными субъектами. Все платформы поддерживают центральный процессор со многими состояниями, где определение адресного пространства, прямой доступ к внешнему устройству и конфигурация центрального процессора могут быть ограничены для состояния, зарезервированного для определенной части ФБО (ядра). ОО обеспечивает правильное использование этих особенностей, чтобы запретить любому недоверенному субъекту неразрешенное вмешательство и подделку в ФБО.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны предоставить надежные метки времени для собственного использования.

Примечание: ОО использует аппаратный таймер для обеспечения собственных меток времени. Этот аппаратный таймер защищен от вмешательства со стороны недоверенных субъектов. Начальное значение таймера может быть установлено системным администратором, который может также запустить программу, использующую внешний доверенный источник времени, чтобы установить начальное значение аппаратного таймера.

FPT_TST.1 Самотестирование ФБО

FPT_TST.1.1 ФБО должны выполнить набор программ самотестирования *по запросу уполномоченного пользователя* для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО.

FPT_TST.1.3 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО.

5.1.6 Доступ ОО (FTA)

FTA_LSA.1 Ограничение области выбираемых атрибутов

FTA_LSA.1.1 ФБО должны ограничить область атрибутов безопасности сеанса [перечень активных ролей для пользователя], основываясь на [перечне активных ролей для пользователя].

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на [заданном по умолчанию пустом перечне активных ролей для пользователя].

Примечание: Система не разрешает определять для пользователей пустой перечень ролей. Администраторы не могут определять пользователей, не назначая им, по крайней мере, одну роль, и не могут удалять определение роли, если в системе существуют пользователи, назначенные на эту роль. Невозможно установить сеанс с пустым перечнем ролей, поэтому это ФТБ выполняется неявно.

FTP_ITC.1 Доверенный канал передачи между ФБО

FTP_ITC.1.1 ФБО должны предоставлять канал связи между собой и удаленным доверенным продуктом ИТ, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.

FTP_ITC.1.2 ФБО должны позволить ***ФБО или удаленному доверенному продукту ИТ*** инициировать связь через доверенный канал.

FTP_ITC.1.3 ФБО должны инициировать связь через доверенный канал для выполнения [соединений с использованием протоколов SSH v2 или SSL v3, предлагаемых в качестве сервисов ОО].

5.1.7 Стойкость функции

Требуемой минимальной стойкостью функции является СФБ-средняя.

Примечание: Функцией безопасности, использующей перестановочный или вероятностный механизм, в ОО является функция аутентификации, основанная на паролях.

5.2 Требования доверия к безопасности ОО

Целевым оценочным уровнем доверия для ОО является ОУД2.

5.3 Требования доверия к безопасности для ИТ-среды

Функциональные требования безопасности для ИТ-среды не применимы, потому что все функции безопасности полностью реализованы ОО без какой-либо поддержки со стороны ИТ-среды.

5.4 Требования доверия к безопасности для не-ИТ-среды

Все цели безопасности для среды ОО относятся к его физической защите или процедурам, которые должны соблюдаться уполномоченными администраторами.

6 Краткая спецификация ОО

6.1 Обзор компонентов, определяющих безопасность

6.1.1 Введение

Этот раздел описывает широкое подмножество функций МСВСфера 5.2 Desktop, обеспечивающих основную безопасность клиента ОО в защищенной среде и являющихся предметом оценки. Эти функции обеспечивают основную безопасность клиента в рамках защищенной среды. Они позволяют проводить идентификацию и аутентификация пользователей, контроль доступа к файлам и объектам IPC, аудит критичных событий безопасности и безопасную связь с другими доверенными системами. ОО защищает функции безопасности от неправомочного вмешательства и обхода и позволяет управлять ими только уполномоченным администраторам. Обычным пользователям разрешено управлять правами доступа только к файловой системе и объектам IPC, владельцами которых они являются, и изменять свой собственный пароль в соответствии с правилами, предоставленными ОО. Эти функции необходимы как основа для функций и механизмов безопасности прикладного уровня и могут использоваться для построения конкретных политик безопасности приложения.

ОО можно управлять в режиме ПЗКД (CAPP). В нем ОО обеспечивает функции безопасности, очень похожие на те, которые оценивались в версии ОО Red Hat Enterprise Linux Version 4.

6.1.2 Сервисы ядра

Ядро МСВСфера 5.2 Desktop включает основное ядро и некоторые модули ядра. Основное ядро включает поддержку для управления инициализацией системы, памятью, файлами, вводом/выводом, процессами и сервисами связи между процессами (IPC). Модули ядра являются динамически загружаемыми модулями, которые ядро загружает по требованию, и они выполняются с привилегиями ядра.

Драйверы устройства могут быть реализованы как модули ядра.

Ядро МСВСфера 5.2 Desktop реализует менеджер виртуальной памяти (VMM), который распределяет большое, непрерывное адресное пространство каждому процессу, выполняющемуся в системе. Это адресное пространство распространяется через физическую память и пространство страниц на устройстве внешней памяти.

Компонент управления процессами включает программное обеспечение, которое является ответственным за создание, планирование и завершение процесса и

нитей процессов. Управление процессами позволяет множеству процессов одновременно существовать в компьютере и совместно использовать процессор(ы) компьютера. Процесс определяется как программа на стадии выполнения, то есть он состоит из программы и состояния выполнения программы. Управление процессами также предоставляет сервисы, типа связи между процессами и уведомления о событиях (IPC). Основные инструменты ядра:

- не именованные каналы;
- сигналы;
- семафоры SYSV;
- совместно используемая память SYSV;
- очереди сообщений SYSV;
- очереди сообщений POSIX;
- сокеты домена Интернет;
- сокеты домена UNIX.

Программное обеспечение работы с файлами и вводом/выводом обеспечивает доступ к файлам и устройствам. Виртуальная файловая система (VFS) МСВСфера 5.2 Desktop обеспечивает непротиворечивое представление множества физических реализаций файловой системы.

В подразделе 2.4.1 данного документа приведен перечень файловых систем, включенных в оцененную конфигурацию.

Ext3 и ISO-9660 представляют файловые системы на физических носителях (диск (ext3), CD-ROM (ISO-9660)), и файловая система tmpfs обеспечивает непостоянное хранение файлов в оперативной памяти системы.

Другие поддерживаемые файловые системы не представляют и не обеспечивают физические файловые системы хранения данных, но используются как интерфейс для конфигурации и контроля ядра, предоставляются ядром только в работающей системе.

6.1.3 Неядерные сервисы ФБО

Неядерные сервисы ФБО:

- сервисы идентификации и аутентификации;
- сервисы уровня сетевого приложения;
- команды конфигурирования и управления, требующие привилегий root.

Эти сервисы поддерживают функции безопасности, реализованные в ядре, и используют интерфейс ядра с этой целью, но они не выполняются в

привилегированном режиме. Эти функции включены в ФБО, поскольку они требуются для сервисов безопасности ОО (сервисы идентификации и аутентификации). В то же время другие сервисы, реализованные, как инструментальные средства или команды, пользуются функциями ядра, поэтому их использование ограничено административными пользователями, а попытки их использования обычными пользователями запрещаются ядром.

6.1.4 Сетевые сервисы

ОО способен предоставлять следующие типы сервисов:

- локальные сервисы для пользователя, в текущее время вошедшего с локального компьютерного пульта;
- локальные сервисы для предыдущих пользователей через отложенные работы;
- локальные сервисы для пользователей, которые обратились к локальному хосту через сеть, используя протоколы типа ftp или ssh;
- сетевые сервисы для клиентов или на локальном хосте, или на удаленных хостах.

Сетевые сервисы предоставляются клиентам через архитектуру клиент-сервер. Архитектура клиент-сервер ссылается на раздел программного обеспечения, который предоставляет обслуживание клиента в части выдачи запросов, и сервера в части выполнения запросов клиента (обычно на различных компьютерах). Протокол обслуживания действует как интерфейс между клиентом и сервером.

Первичными протоколами низкого уровня являются: межсетевой протокол (IP), протокол управления передачей (TCP) и протокол пользовательских дейтаграмм (UDP). IP не видим пользователю, но процессы не-ФБО могут общаться с другими хостами в сетевой системе, используя надежный поток байтов (TCP) или ненадежных дейтаграмм (UDP) соответственно. Сетевые сервисы верхнего уровня основаны на TCP или UDP. Основанные на TCP протоколы прикладных программ, поддерживающие пользовательскую аутентификацию и выполняющиеся на привилегированных портах:

- безопасная оболочка (SSH v2)
- сервисы передачи файлов (FTP).

Кроме того, ОО поддерживает Протокол уровня безопасного сокета (SSL v3), который может использоваться для надежного туннелирования протоколов с более высоким уровнем. Этот сервис предоставляется доверенным процессом, который может использоваться приложениями для туннелирования протоколов, базируемых

на TCP, используя отдельный порт. Туннель фактически обеспечивает аутентификацию, основанную на сертификате, с серверной стороны туннеля и защиту конфиденциальности и целостности информации, передаваемой по сетевым соединениям.

6.1.5 Краткий обзор политики безопасности

ОО является единственной системой МСВСфера 5.2 Desktop, функционирующей на одной машине. Несколько таких систем могут быть связаны через локальную сеть и обмениваться информацией, используя сетевые сервисы. Но следует иметь в виду следующие утверждения, которые полагают, что:

- Имеется ядро МСВСфера 5.2 Desktop, функционирующее на каждом главном компьютере в сетевой системе;
- Идентификация и аутентификация (I&A) выполняются локально на каждом главном компьютере. Каждый пользователь обязан входить в систему с правильной комбинацией пароля и идентификатора пользователя в локальной системе и также на любом удаленном компьютере, где пользователь может ввести команды в программную оболочку (используя ssh) или использовать программу передачи файлов. Идентификатор пользователя и пароль для одного человека-пользователя может быть различным на разных хостах. Идентификатор пользователя и пароль на одной хост системе не известен другим хост системам в сети, и поэтому идентификатор пользователя является соответствующим только тому хосту, где он был определен.
- Дискреционное управление доступом (DAC), управление доступом на основе ролей выполняется в локальном масштабе каждым из главных компьютеров и основывается на идентификаторе пользователя, членстве в группах, ролях и атрибутах объектов на этом хосте. Каждый процесс имеет идентификатор (пользователь, от имени которого он работает) и принадлежит одной или более группам и работает с ролью. Все названные объекты имеют пользователя-владельца, группу-владельца и атрибут DAC, который является рядом битов разрешения. Кроме того, объекты файловой системы имеют расширенные разрешения, также известные как списки управления доступом (ACL). Механизм ACL представляет собой существенное расширение вне традиционных систем UNIX и

разрешает управление доступом, основанное на списках пользователей и/или групп, которым могут быть индивидуально предоставлены или отменены конкретные разрешения.

- Повторное использование объекта выполняется в локальном масштабе, безотносительно к другим хостам.
- Обработка прерывания выполняется в локальном масштабе, безотносительно к другим хостам.
- Привилегии основываются на идентификаторе и роли пользователя.

6.1.6 Структура ФБО

ФБО является частью системы, которая отвечает за определение политики безопасности системы. ФБО МСВСфера 5.2 Desktop состоит из двух главных компонентов: программного обеспечения ядра и доверенных процессов. Все эти компоненты должны работать правильно в системе, которая должна быть доверенной. Эти функции поддерживаются механизмами используемого оборудования для защиты ФБО от вмешательства недоверенных процессов.

МСВСфера 5.2 функционирует на аппаратных платформах, поддерживающих два состояния процессора, когда в режиме ядра или состоянии супервизора программное обеспечение выполняет операции с конкретными привилегиями на используемом оборудовании платформы, и в режиме пользователя или состоянии задачи программное обеспечение выполняется без этих привилегий. МСВСфера 5.2 Desktop также предоставляет два типа защиты памяти: сегментацию и защиту страниц. Свойства защиты памяти изолируют критические части ядра от пользовательских процессов и обеспечивают недоступность сегментов, используемых одним процессом, для других процессов. Архитектура с двумя состояниями и реализациями защиты памяти формирует основу параметра для изоляции процесса и защиты ФБО.

Доверенные процессы включают программы типа административных программ Linux, сценариев, оболочек и стандартных утилит Linux, которые выполняются с административными привилегиями как следствие того, что были вызваны пользователем с административными привилегиями. Программное обеспечение ФБО, не входящее в ядро, также включает демонов, которые предоставляют системные сервисы типа программ работы с сетями, а также setuid и setgid, которые могут выполняться недоверенными пользователями.

6.1.7 Интерфейсы ФБО

Каждый подпункт здесь объединяет классы интерфейсов в операционной системе МСВСфера 5.2 Desktop и характеризует их в терминах границы ФБО. Граница ФБО включает некоторые интерфейсы, например, команды, реализуемые привилегированными процессами, которые являются подобными по стилю другим интерфейсам, не являющимися частью границы ФБО и таким образом не являющимися доверенными. Некоторые интерфейсы являются частью границы ФБО только, когда используются в привилегированной среде, например, процесс административного пользователя, но не когда используются в непривилегированной среде, как процесс обычного пользователя. Все классы интерфейсов описаны в деталях в следующем подпункте, а механизмы - еще дальше, поэтому обеспечиваются неявные ссылки вперед.

Интерфейсы пользователя

Типичным интерфейсом, предоставленным пользователю, является интерпретатор команд или оболочка. Пользователь набирает команды в интерпретаторе, и, в свою очередь, интерпретатор вызывает программы. Программы выполняют команды аппаратных средств и вызывают ядро, чтобы выполнить сервисы типа доступа к файлу или ввода/вывода на терминал пользователя. Программа может также вызвать другие программы или запросы сервисов, используя механизм IPC. Перед использованием интерпретатора команд пользователь должен войти в систему. Интерпретатор команд или оболочка так же, как и другие программы, работающие от имени пользователя, имеют следующие интерфейсы:

- Команды центрального процессора, которые используют процесс выполнения вычислений в регистрах процессора и областях памяти процесса. Команды центрального процессора интерпретируются аппаратными средствами, которые являются частью ОО. Поэтому команды центрального процессора являются интерфейсом ФБО.
- Системные вызовы (например, open, fork), через которые процесс запрашивает сервисы у ядра. Они вызываются с использованием специальной команды центрального процессора. Системные вызовы являются первичным путем запроса сервисов ОО для программы, работающей от имени пользователя, включая сервисы безопасности. Поэтому системные вызовы, связанные с функциями безопасности, являются частью интерфейса ФБО.

- Доверенные процессы (например, passwd) выполняют сервисы верхнего уровня и непосредственно вызываются системным вызовом exec, который указывает соответствующую программу, являющуюся частью ФБО, и заменяет ею содержимое текущего процесса; существует ограниченное число таких процессов, выполняющих функции безопасности, и поэтому они являются частью интерфейса ФБО.
- Демоны, которые принимают запросы, сохраненные в файлах или переданные через механизмы IPC, создаются через использование непосредственно вызываемых процессов (одни доверенные, другие недоверенные). Некоторые демоны выполняют функции безопасности, и поэтому они являются частью интерфейса ФБО.
- Сетевые сервисы (ssh, ftp, stunnel, использующий ssl, IPsec). Интерфейс сетевых сервисов работает на многих разных уровнях абстракции. На самом высоком уровне одного хоста интерфейс сетевых сервисов предоставляет пользователям средство для запроса виртуального оконечного подключения на другом хосте в системе. На более низком уровне он позволяет одному хосту в сетевой системе запросить конкретный сервис у другого хоста в системе от имени пользователя. Примеры требуемых сервисов включают удаленный вход в систему ОО и получение оболочки или передачи целых файлов. На самом низком уровне он позволяет субъекту на одном хосте в системе запросить подключение (TCP) или передачу данных (UDP) к слушающему субъекту на другой системе. Сетевые сервисы обычно состоят из клиента на запрашивающей стороне и сервера (обычно демона), выполняющегося на стороне сервера. Аутентификация (если таковая требуется сервисом) и контроль доступа используют специализированные интерфейсы для функций на стороне сервера, которые поэтому являются частью интерфейса ФБО. Отметим, что для ОО только IPsec, ssh, stunnel и ftp отмечаются как ФБО, потому что они используют привилегированные порты. Ssh и ftp требуют идентификации и аутентификации пользователя, а ssh и stunnel обеспечивают защиту целостности и конфиденциальности.

Примечание: Пользователи могут запустить программы, используя непривилегированные порты, но эти программы работают с эффективным идентификатором и идентификатором владельца файловой системы вызывающего пользователя и поэтому ограничены политикой безопасности ОО. Эти пользовательские программы, использующие непривилегированные порты, не являются частью ФБО.

Эксплуатационный и административный интерфейс

Первоначально административные интерфейсы к МСВСфера 5.2 Desktop представляют собой те же интерфейсы, что и для обычных пользователей; административные пользователи входят в систему со стандартным, недоверенным идентификатором и паролем, и после принятия идентификатора root используют стандартные команды Linux, чтобы выполнять административные задачи. Прямой вход в систему от имени root разрешается только с системной консоли (прямой вход в систему с системной консоли разрешен, чтобы избежать конкретного нападения, вызывающего отказ в обслуживании). Часть административной базы данных (которая является набором всех файлов конфигурации, относящихся к безопасности), которая используется для конфигурирования и управления ФБО, отмечается как часть интерфейса ФБО. Файлы в административной базе данных защищены механизмами управления доступом ОО. Поэтому очень важно установить такие права и контекст безопасности для доступа к файлам административной базы данных, чтобы запретить пользователям в неадминистративных ролях изменять эти файлы и, при необходимости, иметь к ним доступ только на чтение. Отметим, что каждый сервер в системе имеет свою собственную административную базу данных, и если синхронизация между этими базами данных ФБО требуется политикой безопасности организации, она должна быть сделана вручную в системной среде. ОО не предоставляет какую-либо функцию для синхронизации баз данных ФБО в различных системах. В ОО административные задачи назначаются определенным ролям, позволяющим более тонкую градацию административной модели, основанной на ролях пользователя.

Безопасные и небезопасные состояния

Безопасное состояние для МСВСфера 5.2 Desktop определяется по мере ввода хоста в многопользовательский режим с административными базами данных, конфигурированными с требуемыми правами доступа. В этом состоянии хост воспринимает попытки входа в систему пользователей и обслуживает сетевые запросы через сетевую систему. Полагают, что если эти средства недоступны, хост находится в небезопасном состоянии. Хотя он может быть работоспособным в ограниченном смысле и доступным уполномоченному пользователю для выполнения ремонта, сопровождения и диагностического обслуживания системы, ФБО находятся

не в полной эксплуатации и не обязательно защищают все системные ресурсы согласно политике безопасности.

6.2 Описание функций, осуществляющих безопасность

6.2.1 Введение

Этот подраздел описывает, как компоненты ОО, связанные с безопасностью, обеспечивают выполнение требований безопасности, идентифицированных в разделе 5.

Высокоуровневое описание предоставляется для каждой группы функций, обеспечивающих безопасность; приводятся общие особенности или сервисы и устанавливается, как функциональные возможности, определенные группой функций, обеспечивающих безопасность, предоставляются идентифицированными в этом подразделе компонентами, осуществляющими безопасность. Группы функций, обеспечивающих безопасность, следуют из описания, приведенного в разделе 2. Это:

- идентификация и аутентификация;
- аудит;
- дискреционное управление доступом;
- повторное использование объекта;
- управление безопасностью;
- безопасная связь;
- защита ОО.

Функции безопасности ОО описаны достаточно детально, чтобы дать общее понятие об этих функциях, и как они работают. Более детализированное описание этих функций и отображение ФБО на подсистемы ОО предоставляется в проекте высокого уровня. Ссылки на компоненты ОО, данные курсивом, могут прослеживаться вручную к страницам или источникам для дальнейшей информации. Отметим также, что некоторые команды инициируют доверенные процессы или являются локальным фасадом к доверенному процессу (например, ftp и ftpd демон, ssh и sshd демон). В этих случаях делается общая ссылка на команду.

6.2.2 Идентификация и аутентификация (IA)

Идентификация и аутентификация пользователя в МСВСфера 5.2 Desktop включают все формы интерактивного входа в систему (например, используя протоколы ssh или ftp) так же, как и изменения идентификатора через команду su. Они все полагаются на явную аутентификационную информацию, предоставляемую

пользователем в интерактивном режиме. Идентификация и аутентификация пользователей выполняются с терминала, где еще не вошел ни один пользователь, или когда пользователь, который уже вошел в систему, запускает сервис, который требует дополнительной аутентификации. Все такие сервисы используют общий механизм аутентификации, описанный в этом пункте. Они все используют административную базу данных. Административная база данных управляется административными пользователями, но обычным пользователям разрешено изменять свой собственный пароль, используя команду passwd. Этот пункт также описывает аутентификационный процесс для тех сетевых сервисов, которые требуют аутентификации.

Linux использует набор библиотек, называемых «Подключаемыми модулями аутентификации» (PAM), которые позволяют административному пользователю выбирать, как должны аутентифицировать пользователей приложения, использующие PAM. В оцениваемую конфигурацию включены следующие модули PAM, реализующие функции безопасности:

- pam_unix.so (основной для аутентификации, основанной на пароле, конфигурируется для использования MD5),
- pam_loginuid.so (устанавливает постоянный, подвергаемый аудиту идентификатор пользователя для входа в систему, и обеспечивает безопасное поведение, отказывая во входе в систему, в случае, если идентификатор неверен, а система аудита не функционирует),
- pam_wheel.so (ограничивает использование команды su членами важной группы);
- pam_tally2.so (ограничивает число последовательных неудачных попыток аутентификации);
- pam_nologin.so (проверяет /etc/nologin);
- pam_securetty.so (ограничивает доступ пользователя «root» конкретными терминалами);
- pam_passwdqc.so (дополнительная проверка пароля);
- pam_selinux.so (устанавливает значения по умолчанию для контекста безопасности сеанса. Когда приложение открывает сеанс, используя pam_selinux.so, вызываемая оболочка будет выполняться в контексте безопасности, заданном по умолчанию. Модуль изменяет контекст безопасности управляемого терминала, чтобы он соответствовал одному из пользователей);

- pam_namespace.so (устанавливает личное пространство имен с многоинстанционными каталогами при установлении сеанса. Многоинстанционные каталоги необходимы для достижения большего информационного разделения для каталогов общего использования, типа /tmp и /var/tmp, и предоставить пользователям записываемые домашние каталоги после перехода роли, типа.)

Кроме того, может использоваться модуль pam_rootok.so для отмены необходимости повторного ввода пароля административным пользователем с эффективным идентификатором пользователя «root».

Администрирование идентификационных и аутентификационных данных пользователя (IA.1)

Каждый клиент сопровождает свой собственный набор пользователей с их паролями и атрибутами. Хотя один и тот же человек-пользователь может иметь учетные записи на различных клиентах, связанных сетью, эти учетные записи и их параметры не синхронизированы на различных клиентах. В результате, тот же самый пользователь может иметь различные имена пользователя, различные идентификаторы пользователя, различные пароли и различные атрибуты на различных машинах в сетевом окружении. Существующий механизм для их синхронизации в пределах всей сетевой системы не является предметом данной оценки.

Каждая машина в сети обеспечивает сопровождение своей собственной административной базы данных, производя все административные изменения на локальной машине. Системное администрирование должно обеспечивать конфигурирование всех машин в сети в соответствии с требованиями, определенными в этом ЗБ. Пользователям разрешается изменять свои пароли при использовании команды passwd, которая реализуется программой setuid, обладающей идентификатором пользователя 0. Эта конфигурация позволяет процессу, выполняющему программу passwd, читать и изменять содержание файла /etc/shadow для ввода пароля пользователя, который обычно должен быть недоступным непривилегированному пользовательскому процессу (IA1.1). Пользователи также вынуждены изменять свои пароли во время входа в систему, если срок действия пароля истек (IA1.2).

Файл /etc/passwd содержит имя пользователя, идентификатор пользователя, индикатор правильности пароля пользователя, идентификатор основной группы пользователя и некоторую другую, не относящуюся к безопасности информацию

(IA1.3). Зашифрованный пароль самого пользователя сохраняется не в этом файле, а в файле/etc/shadow, который может быть защищен от доступа на чтение для обычных пользователей. Это предотвращает словарное нападение на пароли в файле passwd, как, например, описано в статье Кена Томсона и Боба Морриса «Безопасность пароля – история болезни». Файл /etc/shadow содержит зашифрованный алгоритмом MD5 пароль, идентификатор пользователя, время последнего изменения пароля и некоторую другую информацию, которая не является подчиненной функциям безопасности, как определено в этом ЗБ (IA1.4).

Для полного списка атрибутов пользователя см. описание функции SM.

Уполномоченный администратор может определять следующие ограничения на процесс входа в систему (определенные в /etc/login.defs для использования инструментальными средствами управления; в конфигурации PAM и доверенных базах данных /etc/shadow и /etc/security/opasswd для использования самим процессом аутентификации):

- Максимальное число дней, которое пароль может использоваться.
- Минимальное число дней, разрешенных между изменениями пароля.
- Минимальная приемлемая длина пароля (определенная в параметре для pam_passwdqc.so).
- Число дней, которое дается для предупреждения перед истечением срока действия пароля.
- Число последовательных неудачных попыток входа в систему.
- Число старых, но недавних паролей, совпадения с которыми будут отвергнуты при изменении пароля пользователем (хронология пароля)

Это позволяет уполномоченному администратору определять ограничения на аутентификационные данные, такие как минимальная длина пароля, проверяя пароль по элементам словаря, а также максимальное время существования пароля, число разрешенных неудачных попыток входа в систему до блокировки учетной записи (IA1.5). Эти ограничения сохраняются в файле /etc/login.defs, /etc/shadow и в конфигурации PAM. Уполномоченный администратор может использовать эти параметры для определения такой политики пароля, чтобы пароли удовлетворяли требованиям, определенным в FIA_SOS.1. Время последних успешных попыток входа в систему записывается в /var/log/lastlog (IA1.6).

В оцениваемой конфигурации вышеупомянутый параметр должен быть установлен в соответствии со следующими ограничениями:

- Максимальное время существования пароля: меньше или равно 60 дням
- Минимальное время жизни пароля: 1 день
- Минимальная длина пароля: 8 символов
- Число дней, которые даются для предупреждения об истечении срока действия пароля: 7 дней
- Число последовательных неудачных попыток входа в систему: 5
- Максимальное число попыток изменять пароль: 3
- Длина хронологии пароля: 7 (IA1.7)

Общий аутентификационный механизм (IA.2)

МСВСфера 5.2 включает общий аутентификационный механизм, который является подпрограммой, используемой для всех видов деятельности, которые создают сеанс пользователя, включая все интерактивные действия по входу в систему, пакетные задания и аутентификацию для команды su (IA2.1).

Общий механизм включает следующие проверки и операции:

- Проверить аутентификацию пароля;
- Проверить истечение времени действия пароля;
- Проверить, нужно ли отказать в доступе вследствие слишком многих последовательных отказов в аутентификации;
- Получить пользовательские характеристики безопасности (например, идентификатор пользователя и группы);

Общий механизм I&A идентифицирует пользователя, основываясь на предоставляемом имени пользователя, получает атрибуты безопасности этого пользователя и выполняет аутентификацию по паролю пользователя.

Эта функция вносит вклад в удовлетворение требований безопасности FIA_UAU.2 и FIA_UID.2.

Интерактивный вход в систему и связанные с ним механизмы (IA.3)

Команды ssh и ftp, так же как и команда su, используются для изменения идентификаторов пользователя (реального, владельца файловой системы и эффективного), которые в оцениваемой конфигурации используют тот же самый опознавательный механизм (IA3.1). Это относится и к правильной защите ввода пароля пользователя для удаленной системы (например, предоставление только закрытой обратной связи). Если удаленная система также является оцениваемой версией ОО, она обеспечивается функцией безопасности ОО.

Эта функция вносит вклад в удовлетворение требований безопасности FIA_UAU.2, FIA_UID.2 и FIA_UAU.7.

Изменение идентификатора пользователя (IA.4)

Пользователи могут изменять свой идентификатор (то есть, переключаться на другой идентификатор), используя команды su (IA4.1). Когда происходит переключение, то идентификатор пользователя (реальный, владельца файловой системы и эффективный) и идентификатор группы (реальный, владельца файловой системы и эффективный) изменяются на значения, которые определены пользователем в команде (после успешной аутентификации в качестве этого пользователя) (IA4.2). Первичное использование команды su в пределах МСВСфера 5.2 Desktop должно позволить соответственно уполномоченным лицам иметь возможность получать идентификатор «root» для выполнения административных действий. В данной системе возможность входить под идентификатором «root» ограничивается только определенными терминалами (IA4.3). Кроме того, использование команды su для переключения на «root» ограничивается пользователями, принадлежащими руководящей группе (IA4.4). Пользователи, которые не имеют доступа к терминалу, где разрешен вход в систему для «root», и не являющиеся членами руководящей группы, не будут в состоянии переключать свои идентификаторы пользователя (реальный, владельца файловой системы и эффективный) на «root», даже если бы они знали аутентификационную информацию для «root». Отметим, что когда пользователь выполняет программу, которая только устанавливает биты setuid, эффективный идентификатор и идентификатор пользователя владельца файловой системы изменяются на тот, что имеет владелец файла, содержащего программу, в то время как реальный идентификатор пользователя остается идентификатором вызывающей программы (IA4.5). Входное имя не изменяется ни командой su, ни выполнением программы, которая устанавливает биты setuid или setgid (IA4.6).

Команда su вызывает общий аутенификационный механизм, чтобы подтвердить предоставляемую аутентификацию.

Пользователь может изменить свою текущую активную роль, используя команду newrole -r (IA.4.7). Команда требует пользователя аутентифицировать себя и позволяет изменять его роль на одну из назначенных ему ролей после успешной аутентификации (IA.4.8).

Пользователь может изменять свой текущий активный допуск, используя команду newrole –l с применением несетевых терминалов (например,

последовательной консоли) или запуская неинтерактивные процессы, которые не взаимодействуют с терминалом (IA.4.9). Команда требует от пользователя аутентифицировать себя, и позволяет изменять на новый его уровень допуска и комбинацию категорий из набора назначенных ему после успешной аутентификации (IA.4.10)

Эта функция вносит вклад в удовлетворение требования безопасности FIA_USB.1.

Обработка входа в систему (IA.5)

В процессе входа в систему идентификаторы пользователя (входной, реальный, владельца файловой системы и эффективный) устанавливаются в идентификатор, под которым пользователь вошел (IA5.1). С помощью команды su изменяются идентификатор пользователя (реальный, владельца файловой системы и эффективный) и идентификатор группы (реальный, владельца файловой системы и эффективный), но входное имя остается неизменным (IA.5.2).

Эта функция вносит вклад в удовлетворение требования безопасности FIA_USB.1.

Доступ к ОО (IA.6)

При инициализации интерактивного сеанса пользователя посредством login, ftp или sshd, или при выполнении задачи от имени пользователя через crond, система ограничивает перечень активных ролей для пользователя набором разрешенных для него ролей (IA.6.1). Система всегда реализует для пользователя наличие непустого набора разрешенных ролей (IA.6.2).

Эта функция вносит вклад в удовлетворение требований безопасности FTA_LSA.1 и FTA_TSE.1.

6.2.3 Аудит (AU)

Облегченная структура аудита (LAF) разработана как согласованная с CAPP(ПЗКД) система аудита для Linux. LAF построена на вершине systrace, которая является механизмом реализации политики безопасности системного вызова, сначала разработанным для BSD, и затем перенесенный в Linux. Подсистема позволяет из набора всех событий, для которых возможен аудит, конфигурировать события, которые фактически должны подвергаться аудиту. Эти события конфигурируются в конкретном файле конфигурации, из которого затем извлекаются ядром для построения своей собственной внутренней структуры событий, подвергаемых аудиту.

Конфигурация аудита (AU.1)

Системный администратор, используя простые правила фильтрации, может определять события, подвергаемые аудиту, из всех возможных событий, которые LAF способна учитывать, используя правила, определенные в файле конфигурации аудита /etc/audit.rules (AU1.1). Это позволяет гибко определять события, которые подвергаются аудиту, и условия, при которых они подвергаются аудиту. Системный администратор также в состоянии определять ряд идентификаторов пользователя, для которых аудит активируется (AU1.2), или, наоборот, ряд идентификаторов пользователя, которые не подвергаются аудиту (AU1.3). Изменения в конфигурации аудита вступают в силу, когда демон аудита уведомляется о них (AU1.4). Это уведомление может быть выполнено только административным пользователем (использование сценария /etc/rc.d/init.d/auditd с параметром «перезагрузка») (AU1.5).

Системный администратор может выбирать файлы, которые подвергаются аудиту, добавляя их к списку наблюдений, который загружается в ядро, используя инструмент auditctl всякий раз, когда система аудита запускается или повторно инициализируется. Список позволяет администратору выбирать произвольное значение тэга аудита для каждого файла, который сохраняется как доступный для поиска атрибут в журнале регистрации аудита (AU1.6). Интерфейс ядра для конфигурирования этих свойств аудита применим только для использования пользователями «root» (AU1.7).

Эта функция вносит вклад в удовлетворение требований безопасности FAU_SEL.1 и FMT_MTD.1 (2).

Обработка аудита (AU.2)

Аудит предоставляется для каждого процесса. Процесс может разрешить или отменить для себя аудит, подключая или отделяя себя к/от подсистеме(ы) аудита, если он выполняется с привилегиями «root» (AU2.1). Атрибут подключения к подсистеме аудита наследуется всеми процессами, которые отпочковываются от процесса, предоставляющего аудит событий, сгенерированных также и дочерними процессами (AU2.2).

Ядро подвергает аудиту системные вызовы в соответствии с правилами, определенными в файле конфигурации аудита audit.rules. Кроме того, доверенные процессы могут генерировать записи аудита и посылать их ядру (AU2.3). Входное имя связывается с событиями аудита, обеспечивая связь событий с идентификатором, который использует пользователь для входа в ОО (AU2.4).

События, которые подвергаются аудиту, отправляются ядром демону аудита, который пишет записи аудита в журнал аудита. С этой целью используется

внутренний механизм постановки в очередь. Если пространство файловой системы не имеет достаточного места, чтобы хранить новые записи аудита, для остановки записи ОО переключается в однопользовательский режим или останавливается, в зависимости от конфигурации демона аудита (AU2.5). Это предупреждает потерю записей аудита вследствие нехватки ресурса, и администратор может копировать журнал аудита на свободное дисковое пространство и очищать его для новых журналов регистрации аудита.

Демон аудита добавляет записи аудита к файлу, имя которого определено в файле конфигурации аудита (AU2.6).

Файл конфигурации аудита может использоваться для выполнения указанных администратором действий уведомления, когда свободное пространство на диске достигнет указанного администратором порога (AU2.7). Это используется, чтобы сообщить системному администратору, что он должен резервировать текущий журнал аудита и сделать доступным пространство для дополнительных записей аудита. В случае если системный администратор не выполняет этого вовремя и доступное дисковое пространство исчерпывается, демон аудита может конфигурироваться для переключения в однопользовательский режим или остановки системы в целом (AU2.8). В этом случае системный администратор должен зарезервировать и очистить журнал аудита в однопользовательском режиме и затем перезагрузить ОО в безопасном многопользовательском режиме.

Доступ обычным пользователям к данным аудита запрещен функцией дискреционного управления доступом ОО, которая используется для предоставления доступа к журналу аудита и файлам конфигурации аудита только системному администратору.

Эта функция вносит вклад в удовлетворение требований безопасности FAU_SAR.2, FAU_STG.1, FAU_STG.3, FAU_STG.4 и FMT_MTD.1 (1).

Формат записи аудита (AU.3)

Запись аудита состоит из одной или более строк текста, содержащего отмеченные поля в формате «ключевое слово = значение». Во всех строках записей аудита содержится следующая информация:

- Тип: указывает источник события типа SYSCALL, FS_WATCH, USER или LOGIN
- Штамп времени: Дата и время, когда запись аудита была сгенерирована
- Идентификатор аудита: уникальный числовой идентификатор события

- Входное имя («auid»), идентификатор пользователя, аутентифицированного системой (независимо, изменил ли пользователь впоследствии свой реальный и/или эффективный идентификатор),
- Эффективный идентификатор пользователя: эффективный идентификатор пользователя процесса в момент времени генерации события аудита
- Успех или отказ (соответственно). (AU3.1)

За этой информацией следуют конкретные данные о событии. В некоторых случаях, типа записей событий syscall, включающих объекты файловой системы, для единственного события будут сгенерированы множество текстовых строк; все они имеют тот же самый штамп времени и идентификатор аудита, что позволяет легко связать их с одним событием.

Примечание: Хотя ОО различает эффективный идентификатор пользователя и идентификатор пользователя владельца файловой системы, они оба идентичны во всех состояниях ОО.

Конкретные данные о событии всегда будут содержать результат запроса, который вызвал событие, успешен или нет (AU3.4).

ОО сопровождает «Входное имя», которое устанавливается, когда пользователь выполняет свой первоначальный вход в систему с терминала или через сетевое подключение (AU3.5). Это входное имя поддерживается для действий этого пользователя, пока он не закончит сеанс. Это входное имя остается неизменным, когда пользователь выполняет переключение идентификатора пользователя (реального и/или эффективного и владельца файловой системы) командой su или посредством вызова программы, которая устанавливает биты suid (AU3.6). Оно позволяет прослеживать все действия реального пользователя.

Эта функция вносит вклад в удовлетворение требований безопасности FAU_GEN.1 и FAU_GEN.2.

Последующая обработка аудита (AU.4)

ОО предоставляет инструментальные средства для чтения административных файлов в кодировке ASCII, которые могут использоваться для последующей обработки данных аудита. Эти инструментальные средства включают:

- less читает данные аудита в кодировке ASCII (AU4.1);
- ausearch позволяет выборочное извлечение записей из журнала аудита, используя определенные критерии выбора (AU4.2).

По умолчанию записи аудита приводятся в хронологическом порядке. Для использования различного порядка сортировки вместе с ausearch может использоваться утилита sort (AU.4.3).

Эта функция вносит вклад в удовлетворение требований безопасности FAU_SAR.1 и FAU_SAR.3.

6.2.4 Дискреционное управление доступом (DAC)

Этот пункт выделяет общую политику DAC в МСВСфера 5.2 Desktop, как она реализована для ресурсов, доступ к которым управляется битами разрешения и POSIX ACL; преимущественно они являются объектами в файловой системе. Во всех случаях политика основана на идентификаторе пользователя (и в некоторых случаях на членстве в группах, связанном с идентификатором пользователя). Чтобы позволить осуществление политики DAC, все пользователи должны быть идентифицированы, а их идентификаторы аутентифицированы. Детали конкретной политики DAC, относящиеся к каждому типу ресурса, приведены в подпунктах «Дискреционное управление доступом: Объекты файловой системы» и «Дискреционное управление доступом: Объекты IPC».

Примечание: Сигналы не являются предметом дискреционного управления доступом, как описано в этом пункте ЗБ. Правила, по которым процессу разрешается посылать сигнал другому процессу, не отмечены как относящиеся к безопасности и поэтому не упоминаются в этом ЗБ.

Общая политика DAC (DA.1)

Общая поддерживаемая политика состоит в том, что субъектам (то есть, процессам) доступ разрешается только конкретными политиками, определяемыми классом. Следовательно, возможность размножать разрешения на доступ ограничена субъектами, имеющими это разрешение, установленное политиками, определяемыми классом.

Наконец, субъект с идентификатором пользователя владельца файловой системы равным 0 свободен от всех ограничений и может выполнять любое желаемое действие (DA1.1).

DAC предоставляет механизм, который позволяет пользователям определять и управлять доступом к объектам, которыми они владеют (DA1.2). Атрибуты DAC назначаются на объекты во время их создания и остаются в силе, пока объект не будет уничтожен или атрибуты объекта не будут изменены (DA1.3). Существуют характерные атрибуты DAC для каждого типа объекта МСВСфера 5.2 Desktop . DAC реализуется битами разрешений и, когда это определено, ACL. Субъект, идентификатор пользователя владельца файловой системы которого соответствует

идентификатору владельца файла, может изменять атрибуты файла, основные разрешения и расширенные разрешения (за исключением файловых систем, открытых только для чтения) (DA1.4). Изменения в файловой группе ограничиваются владельцем и пользователем «root» (DA1.5).

Новый идентификатор владельца файловой группы должен быть или текущим идентификатором владельца группы файловой системы, или одним из идентификаторов группы в наборе совпадающих групп (DA1.6). Кроме того, субъект, идентификатор пользователя владельца файловой системы которого равен 0, может делать любые изменения в атрибутах файла, основных разрешениях, расширенных разрешениях и пользователе владельце файла (см. DA1.1). Биты разрешений являются стандартным механизмом DAC UNIX и используются на всех поименованных объектах файловой системы МСВСфера 5.2 Desktop (DA1.7). Для указания разрешения доступа на чтение, запись и выполнение для владельца объекта, группы объекта и всех других пользователей (то есть, «всех остальных») используются индивидуальные биты. Расширенный механизм разрешений поддерживается только для объектов файловой системы ext3 и предоставляет более тонкую, чем биты разрешений, степень детализации (DA1.8).

Доступ для записи вообще не предоставляют для файлов файловой системы, установленной только для чтения (DA1.9). Доступ для записи также отвергается для файлов, которые имеют атрибут «неизменяемый» (DA1.10).

Эта функция вносит вклад в удовлетворение требований безопасности FDP_ACC.1 (1) и FDP_ACF.1 (1).

Биты разрешений (DA.2)

МСВСфера 5.2 поддерживает стандартные биты разрешений UNIX для обеспечения единой формы DAC для объектов всех поддерживаемых файловых систем (см подраздел 2.4.1). Есть три набора из трех битов, которые определяют доступ для трех категорий пользователей: пользователя-владельца, пользователей в группе владельца и других пользователей. Три бита в каждом наборе указывают разрешения на доступ, предоставленные каждой пользовательской категории: один бит для чтения (r), один для записи (w) и один для выполнения (x). Отметим, что доступ на запись к файловым системам, установленным только для чтения (например, CD-ROM), всегда отвергается. Отметим также, что доступ к конкретным объектам в файловой системе /proc, может быть ограничен только пользователем «root», независимо от установки битов разрешения. Кроме того, файловые системы не обязательно поддерживают для файлов и каталогов индивидуально конфигурируемые

атрибуты владения и прав, разрешения могут быть предопределены на основе общих свойств для файловых систем или неявных свойств объекта.)

Доступ каждого субъекта к объекту определен некоторой комбинацией этих битов:

- символами rwx читать/писать/выполнять
- символами r-x читать/выполнять
- символами r-- читать
- символами --- пустой указатель (DA2.1).

Когда процесс пытается обратиться к объекту, защищенному только битами разрешения, доступ определяется следующим образом:

- Пользователи с идентификатором пользователя владельца файловой системы равным 0 способны читать и писать все файлы, игнорируя биты разрешения. Пользователи с идентификатором пользователя владельца файловой системы равным 0 также способны выполнять любой файл, если он для кого-то выполняем.
- Если идентификатор пользователя владельца файловой системы равен идентификатору пользователя владельца объекта, и биты разрешений пользователя владельца позволяют требуемый тип доступа, доступ предоставляется или отвергается без дальнейших проверок.
- Если идентификатор группы файловой системы или каких-нибудь дополнительных групп процесса равен идентификатору группы владельца объекта, и биты разрешения группы владельца позволяют требуемый тип доступа, доступ предоставляется или отвергается без дальнейших проверок.
- Если пользователь, от имени которого запущен процесс, не является ни владельцем объекта, ни членом соответствующей группы владельца объекта, и биты разрешения для «всех остальных» разрешают требуемый тип доступа, то доступ субъекту предоставляется.
- Если не удовлетворяется ни одно из условий, приведенных выше, и идентификатор пользователя, от имени которого запущен процесс, не является «root», то попытка доступа отвергается (DA2.2).

Каждый процесс имеет наследуемый атрибут «umask», который используется, для определения значений по умолчанию разрешений на доступ для новых объектов. Он соответствует битовой маске пользователь/группа/«всех остальные», читать/писать/выполнять, и определяет биты доступа, которые будут удалены для

новых объектов. Например, установка umask в значение «002» обеспечивает владельцам и группе, но не «всем остальным», запись в такие новые объекты. (DA2.3)

Эта функция вносит вклад в удовлетворение требований безопасности FAU_SAR.2, FDP_ACC.1 (1), FIA_USB.1 и FDP_ACF.1 (1).

Списки управления доступом, поддерживаемые МСВСфера 5.2 Desktop (DA.3)

Существуют следующие типы тэгов:

- ACL_GROUP определяет элемент ACL, в котором права доступа для процессов, идентификатор группы владельца файловой системы или любые дополнительные идентификаторы группы соответствуют идентификатору в спецификаторе элемента ACL;
- ACL_GROUP_OBJ определяет элемент ACL, в котором права доступа для процессов, идентификатор группы владельца файловой системы или любые дополнительные идентификаторы группы соответствуют идентификатору группы владельца файла;
- ACL_MASK определяет элемент ACL, в котором указаны максимальные дискреционные права доступа процесса в классе группы файла.
- ACL_OTHER определяет элемент ACL, в котором указаны права доступа для процессов, атрибуты которых не соответствуют любому другому элементу в ACL
- ACL_USER определяет элемент ACL, в котором указаны права доступа для процессов, чей идентификатор пользователя владельца файловой системы соответствует спецификатору элемента ACL
- ACL_USER_OBJ определяет элемент ACL, в котором указаны права доступа для процессов, чей идентификатор пользователя владельца файловой системы соответствует идентификатору пользователя владельца файла (DA3.2).

Спецификатор ACL

Спецификатор требуется для элементов ACL типа ACL_GROUP и ACL_USER и содержит или пользовательский идентификатор, или идентификатор группы, для которого должны применяться права доступа, определенные в элементе (DA3.3).

Разрешения ACL

Разрешения, которые могут быть определены в элементе ACL: читать, писать и выполнять/искать (DA3.4).

Отношение с битами разрешений файла

ACL содержит ровно один элемент для каждого из типов тэгов ACL_USER_OBJ, ACL_GROUP_OBJ и ACL_OTHER (называемых «требуемыми элементами ACL») (DA3.5). ACL может иметь от нуля до определенного максимального числа элементов типа ACL_GROUP и ACL_USER (DA3.6). ACL, который имеет только три требуемых элемента ACL, называется «минимальным ACL». ACL с одним или более элементами ACL типа ACL_GROUP или ACL_USER называют «расширенным ACL». Стандартные биты разрешений файла UNIX, как описывается в предыдущем пункте, представлены элементами в минимальном ACL. Биты разрешений владельца представлены элементом типа ACL_USER_OBJ, элемент типа ACL_GROUP_OBJ представляет биты разрешений группы файла и элемент типа ACL_OTHER представляет биты разрешений процессов, выполняющихся с идентификатором пользователя владельца файловой системы и идентификатором группы владельца файловой системы или дополнительным идентификатором группы, отличными от определенных в элементах ACL_USER_OBJ и ACL_GROUP_OBJ (DA3.7).

ACL_MASK

Если ACL содержит элемент типа ACL_GROUP или ACL_USER, то ровно один элемент типа ACL_MASK требуется в ACL. Иначе элемент типа ACL_MASK является дополнительным (DA3.8).

ACL, заданные по умолчанию

ACL, заданный по умолчанию, является дополнительным ACL, который может быть связан с каталогом. Этот заданный по умолчанию ACL не имеет влияния на доступ к этому каталогу. Вместо этого заданный по умолчанию ACL используется для инициализации ACL любого файла, который создан в этом каталоге. Если новый созданный файл является каталогом, он наследует заданный по умолчанию ACL его каталога предыдущего уровня (DA3.9). Когда объект создается в каталоге и ACL не определяется с функцией создания объекта, новый объект наследует заданный по умолчанию ACL каталога предыдущего уровня в качестве своего начального ACL.

Алгоритм проверки оценки дискреционного доступа

Когда процесс пытается сослаться на объект, защищенный ACL, он делает это через системный вызов (например, open, exec).

Если объект был предоставлен, доступ ACL определяется согласно нижеследующему алгоритму:

АЛГОРИТМ ПРОВЕРКИ ДИСКРЕЦИОННОГО ДОСТУПА

Процесс может запросить доступ типа читать, писать или выполнять/искать к объекту файловой системы, защищенному ACL. Алгоритм проверки дискреционного доступа определяет, будет ли предоставляться доступ к объекту согласно политике DAC.

1. Доступ на запись к файлу в файловой системе, доступной только на чтение, будет всегда отвергаться для объектов файловой системы, кроме специальных файлов устройств.

2. Доступ на запись к файлу с атрибутом «неизменяемый» будет всегда отвергаться.

3. Если идентификатор пользователя файловой системы, от имени которого запущен процесс, соответствует идентификатору пользователя владельца объекта, **тогда,**

если элемент ACL_USER_OBJ содержит требуемые разрешения, доступ предоставляется,

иначе доступ отвергается

4. **Иначе, если** идентификатор пользователя файловой системы, от имени которого запущен процесс, соответствует спецификатору любого элемента типа ACL_USER, **тогда,**

если соответствующие элементы ACL_USER и ACL_MASK содержат требуемые разрешения, доступ предоставляется,

иначе доступ отвергается.

5. **Иначе, если** идентификатор группы файловой системы или любой из дополнительных идентификаторов группы, от имени которой запущен процесс, соответствуют спецификатору из элемента типа ACL_GROUP_OBJ или спецификатору любого элемента типа ACL_GROUP, **тогда,**

если элемент ACL_MASK и любые соответствующие элементы ACL_GROUP_OBJ или ACL_GROUP содержат все требуемые разрешения, доступ предоставляется,

иначе доступ отвергается.

6. **Иначе, если** элемент ACL_OTHER содержит требуемые разрешения, доступ предоставляется.

7. **Иначе** доступ отвергается. (DA3.10)

Эта функция вносит вклад в удовлетворение требований безопасности FDP_ACC.1 (1), FIA_USB.1 и FDP_ACF.1 (1)

Отмена DAC на объектах файловой системы

Проверки доступа к объектам файловой системы выполняются, когда объект первоначально открыт, и не проверяются при каждом последующем доступе. Изменения в управлении доступом (то есть, отмена) вступают в силу при следующей попытке открыть объект (DA3.11).

В случаях, когда административный пользователь решает, что требуется немедленная отмена доступа к объекту файловой системы, он может перезагрузить компьютер, приводя к закрытию объекта и вызывая открытие объекта после перезагрузки системы.

DAC: Каталог

В случае каталогов бит разрешения «выполнять» определяет возможность упоминать каталог как часть имени пути к файлу. Процесс должен иметь доступ на поиск (выполнение) каталога, чтобы пройти через него при детальном разборе имени пути (DA3.12). Каталоги не могут записываться непосредственно, но только через создание, переименование и удаление (отсоединение) объектов в них. Операции записи рассматриваются в целях политики DAC (DA3.13).

DAC: Специальный файл сокета домена UNIX

Файлы сокетов домена UNIX с точки зрения управления доступом обрабатываются в МСВСфера 5.2 Desktop как файлы файловой системы, за исключением того, что использование системных вызовов связывания или соединения требует, чтобы вызывающий процесс имел доступ на запись к файлу сокета (DA3.14).

Сокеты домена UNIX существуют в пространстве имен файловой системы, файлы сокетов могут иметь и основные биты режима, и расширенные элементы ACL (DA3.15).

Сокеты домена UNIX состоят из специального файла сокета (управляемого файловой системой) и соответствующей структуры сокета (управляемой IPC). ОО управляет доступом к сокету, основываясь на правах вызывающего процесса на специальный файл сокета (DA3.16).

DAC: Именованные каналы

Именованные каналы с точки зрения управления доступом обрабатываются аналогично любому другому файлу в файловой системе МСВСфера 5.2 Desktop. Поэтому могут использоваться биты разрешений и расширенные разрешения (DA3.17). По этой причине именованные каналы перечислены как объекты файловой системы (хотя они используются для связи между процессами). Отметим, что

именованные каналы следуют правилам для объектов IPC, если не используются ACL (которые, вероятно, являются нормальным случаем их использования).

DAC: Специальный файл устройства

Система управления доступом, описанная для объектов файловой системы, используется для защиты специальных файлов символьного и блочного устройства (DA3.18). Большинство специальных файлов устройств конфигурируются так, чтобы разрешить доступ на чтение и запись пользователю «root» и доступ на чтение привилегированным группам. Все файлы устройств, за исключением оконечных, псевдооконечных и нескольких случаев специальных устройств (например, /dev/null и /dev/tty), конфигурируются недоступными для обычных пользователей (DA3.19). Режим доступа к файлам устройств, определяющих терминалы (tty), устанавливаются во время входа пользователя в систему на чтение/запись, а при его выходе из системы права на доступ сбрасываются, чтобы разрешить доступ только для «root» (DA3.20).

Эта функция вносит вклад в удовлетворение требований безопасности FDP_ACC.1 (1) FDP_ACF.1 (1), FMT_MSA.1 (1, 2), FMT_SMF.1, FMT_MSA.3 (1), FIA_USB.1 и FPT_SEP.1.

Дискреционное управление доступом: Объекты IPC (DA.4)

DAC: Совместно используемая память SYSV

Для объектов сегментов совместно используемой памяти (далее SMS) выполняются проверки доступа, когда SMS первоначально присоединяется, и не проверяются при каждом последующем доступе. Изменения в управлении доступом (то есть, отмена) эффективны со следующей попытки присоединения к SMS (DA4.1).

В случаях, когда административный пользователь решает, что требуется немедленная отмена доступа к SMS, он может перезагрузить компьютер, разрушая, таким образом, SMS и весь доступ к ним.

Если процесс просит удаление SMS, он не удаляется, пока последний процесс, который присоединен к SMS, не отделится (что эквивалентно окончанию последнего процесса, присоединенного к SMS) (DA4.2).

Управление доступом по умолчанию на вновь созданном SMS определяется в соответствии с эффективным идентификатором пользователя и эффективным идентификатором группы процесса, который создал SMS, и конкретными разрешениями, которые требует процесс, создающий SMS (DA4.3).

- Пользователь-владелец и пользователь-создатель вновь созданного SMS будут иметь эффективный идентификатор пользователя, создающего процесса (DA4.4).

- Группа-владелец и группа-создатель вновь созданного SMS будут иметь эффективный идентификатор группы, создающего процесса (DA4.5).
- Процесс-создатель должен определить начальные разрешения на доступ к SMS или они устанавливаются в нуль, и объект недоступен, пока владелец не установит их (DA4.6).
- SMS не имеют ACL, как описано выше, они имеют только биты разрешений (DA4.7).

Разрешения на доступ могут быть изменены любым процессом с эффективным идентификатором пользователя, равным идентификатору пользователя-владельца или идентификатору пользователя-создателя SMS (DA4.8). Разрешения на доступ могут также быть изменены любым процессом с эффективным идентификатором пользователя 0, также известным как выполняющимся с идентификатором «root» (DA4.9).

DAC: Очереди сообщений POSIX и SYSV

Для очередей сообщений проверки доступа выполняются при каждом запросе на доступ (например, послать или получить сообщение в очереди) (DA4.10). Изменения в управлении доступом (то есть, отмена) эффективны для следующего запроса на доступ (DA4.11). Таким образом, изменение затрагивает все будущие операции посылки и получения, за исключением случая, когда процесс уже сделал запрос к очереди сообщений и ждет ее доступности (например, процесс ждет получения сообщения), тогда изменение в управлении доступом неэффективно для этого процесса до следующего запроса (DA4.12). Если процесс запрашивает удаление очереди сообщения, она не удаляется, пока последний процесс, который ждет очереди сообщения, не получит свои сообщения (что эквивалентно, окончанию последнего процесса, ждущего сообщения в очереди) (DA4.13). Однако, как только очередь сообщения отмечается как удаленная, она не может быть восстановлена, и дополнительные процессы не могут выполнять с ней операции передачи сообщений (DA4.14). Заданное по умолчанию управление доступом на вновь создаваемых очередях сообщений определяется в соответствии с эффективным идентификатором пользователя и эффективным идентификатором группы процесса, который создает очередь сообщений, и конкретными разрешениями, которые требует процесс, создающий очередь сообщений.

- Пользователь-владелец и пользователь-создатель вновь созданной очереди сообщений будут иметь эффективный идентификатор пользователя, создающего процесс.
- Группа-владелец и группа-создатель вновь созданной очереди сообщений будут иметь эффективный идентификатор группы, создающей процесс.
- Начальные разрешения на доступ к очереди сообщений должны быть определены создающим процессом или они устанавливаются в нуль, и объект недоступен, пока владелец не установит их.
- Очереди сообщений не используют ACL, как описано выше, они имеют только биты разрешений. (DA4.15).

Разрешения на доступ могут быть изменены любым процессом с эффективным идентификатором пользователя, равным идентификатору пользователя-владельца или идентификатору пользователя-создателя очереди сообщений. Разрешения на доступ могут быть также изменены любым процессом с эффективным идентификатором пользователя 0 (DA4.16).

DAC: Семафоры SYSV

Для семафоров проверка доступа выполняется при каждом запросе на доступ (например, блокировать или разблокировать семафор) (DA4.17). Изменения в управлении доступом (то есть, отмена) эффективны при следующем запросе на доступ (DA4.18). Таким образом, изменение затрагивает всю будущую эксплуатацию семафора, за исключением случая, когда процесс уже сделал запрос семафора и ждет его доступности, тогда изменение доступа неэффективно для этого процесса до следующего запроса (DA4.19).

В случаях, когда уполномоченный администратор решает, что требуется немедленная отмена доступа к семафору, он может перезагрузить компьютер, таким образом разрушая семафор и любые процессы, ждущие его. Этот метод описывается в Руководстве оцениваемой конфигурации. Чтобы отменить всякий доступ к некоторому семафору, достаточно перезагрузить хост, где присутствуют семафоры, так как семафор существует только в пределах отдельного хоста в сети.

Если процесс запрашивает удаление семафора, он не удаляется, пока последний процесс, который ждет семафора, не получит его блокировку (что эквивалентно окончанию последнего процесса, ждущего семафор) (DA4.20). Однако

если семафор был отмечен как удаленный, он не может быть восстановлен, и дополнительные процессы не могут выполнять операции с семафором (DA4.21).

Заданное по умолчанию управление доступом на вновь созданных семафорах определяется в соответствии с эффективным идентификатором пользователя и эффективным идентификатором группы процесса, который создал семафор, и конкретными разрешениями, которые требует процесс, создающий семафор (DA4.22).

- Пользователь-владелец и пользователь-создатель вновь созданного семафора будут иметь эффективный идентификатор пользователя, создающего процесса.
- Группа-владелец и группа-создатель недавно созданного семафора будут иметь эффективный идентификатор группы, создающего процесса.
- Начальные разрешения на доступ к семафору должны быть определены создающим процессом или они устанавливаются в нуль, и объект недоступен, пока владелец не установит их.
- Семафоры не имеют ACL, как описано выше, они имеют только биты разрешений (DA4.23).

Разрешения на доступ могут быть изменены любым процессом с эффективным идентификатором пользователя, равным идентификатору пользователя-владельца или идентификатора пользователя-создателя семафора (DA4.24). Разрешения на доступ могут также быть изменены любым процессом с эффективным идентификатором пользователя 0 (DA4.25).

Эта функция вносит вклад в удовлетворение требований безопасности FDP_ACC.1 (1), FDP_ACF.1 (1), FMT_MSA.1 (1, 2), FMT_SMF.1, FIA_USB.1, и FMT_MSA.3 (1).

6.2.5 Повторное использование объекта (OR)

Повторное использование объекта представляет собой механизм защиты от возможного чтения информации, оставшейся от действий предыдущего субъекта, путем ее очистки. Явная инициализация является соответствующей для большинства абстракций, управляемых ФБО, где ресурс реализован некоторой внутренней структурой данных ФБО, содержание которой невидимо вне ФБО: очереди, датаграммы, каналы и устройства. Эти ресурсы полностью инициализируются при создании и не имеют сохранившегося информационного содержания.

Явная очистка используется в МСВСфера 5.2 Desktop только для элементов каталога, потому что они доступны двумя способами: через интерфейсы ФБО как для

управления каталогами, так и для чтения файлов. Поскольку это отражается на внутренней структуре ресурса, она должна быть явно очищена при выходе для предотвращения раскрытия внутреннего содержимого ресурса. Управление памятью используется вместе с явной инициализацией для повторного использования объекта на файлах и процессах. Эта методика следит за тем, как используется память, и может ли она быть безопасно сделана доступной субъекту. Следующие подпункты подробно описывают, как повторное использование объекта обрабатывается для различных типов объектов и областей данных, и как удовлетворяются требования, определенные в FDP_RIP.2.

Повторное использование объекта: Объекты файловой системы (OR.1)

Ко всем объектам файловой системы (FSO), доступным для обычных пользователей, обращается общий механизм распределения памяти на диске и общий механизм чтения и записи данных страничной памяти на диск. Он включает Журналируемую файловую систему (ext3). Повторное использование объекта неприменимо для файловой системы CD-ROM (ISO 9660), потому что данная файловая система может использоваться только для чтения и, таким образом, в ней нет возможности для пользователя читать остаточные данные, оставленные предыдущим пользователем. Файловые системы на других носителях информации (ленты, дискеты) являются неприменимыми из-за предупреждений в Руководстве оцениваемой конфигурации о недопустимости монтирования файловых систем на этих устройствах.

Отметим, что ext3 и ISO 9660 являются единственными файловыми системами, поддерживаемыми на диске. Все другие файловые системы не имеют постоянную внешнюю память, и поэтому повторное использование объекта дискового пространства для них не является проблемой.

Повторное использование объекта в файловой системе tmpfs обрабатывается функциями повторного использования объектов управления памятью. Распределяя новое пространство для файла, ОО использует функции управления памятью, которые очищают память прежде, чем она распределяется.

Повторное использование объекта для объектов файловой системы devpts обрабатывается уровнем VFS. Файловые системы procfs, sysfs, selinuxfs, binfmt_misc, и rootfs обеспечивают только очень ограниченные представления специфических внутриядерных структур данных, и не могут использоваться на устройствах с произвольным доступом. Повторное использование объекта обрабатывается внутри ядра при выделении и освобождении структур данных.

Для этого анализа термин FSO относится не только к названным объектам файловой системы (файлы, каталоги, специальные файлы устройств, именованные каналы, и сокеты домена UNIX), но также и к другим абстракциям, которые используют память файловой системы (символические связи и неименованные каналы). Все они, кроме неименованных каналов, имеют элемент каталога, который содержит последнюю часть имени пути и узел, который управляет правами доступа и указывает на дисковые блоки, используемые FSO.

Вообще, объекты файловой системы создаются без содержимого. Каталоги и символические ссылки являются исключениями, и некоторое их содержимое определяется во время создания (OR1.1).

Эта функция вносит вклад в удовлетворение требования безопасности FDP_RIP.2.

Повторное использование объекта: Объекты IPC (OR.2)

Совместно используемая память МСВСфера 5.2 Desktop, очереди сообщения и семафоры инициализируются нулями при создании. Эти объекты имеют конечный размер (сегмент совместно используемой памяти колеблется от одного байта до значения, определенного в /proc/sys/kernel/shmmax, семафор представляет собой один бит), и таким образом отсутствует способ увеличить объект сверх его начального размера (OR2.1).

Обработка не выполняется при обращении к объектам, или когда объекты освобождаются и возвращаются назад в пул.

Эта функция вносит вклад в удовлетворение требования безопасности FDP_RIP.2 (1).

Повторное использование объекта: Объекты памяти (OR.3)

Контекст нового процесса полностью инициализирован от родительского процесса, когда выдается системный вызов fork. Все видимые аспекты программного контекста процесса полностью инициализируются. Все структуры данных ядра, связанные с новым процессом, копируются из родительского процесса, затем изменяются, чтобы описать новый процесс, и полностью инициализируются (OR3.1).

Ядро Linux обнуляет каждую страницу памяти перед распределением ее процессу. Она принадлежит памяти в сегменте данных программы и памяти в сегментах совместно используемой памяти (OR3.2). Когда процесс просит больше памяти от ядра, память явно очищается прежде, чем процесс может получить доступ к ней (OR3.3). Она не включает память, которая была буферизирована библиотечными подпрограммами, используемыми процессом. Но эта память уже

была распределена процессу ядром (очищенная в этот раз для повторного использования объекта). Отметим, что процесс управления и буферизации внутренней памяти не является субъектом этого ЗБ. Когда ядро выполняет переключение контекста с одной нити на другую, оно сохраняет Универсальные регистры предыдущей нити (регистры общего назначения) и восстанавливает регистры общего назначения новой нити, полностью записывая поверх любых остаточных данных, оставленных в регистрах предыдущей нитью (OR3.4). Регистры с плавающей запятой (FPR) сохраняются, только если процесс использовал их. Акт доступа к FPR заставляет ядро впоследствии сохранять и восстанавливать все FPR для процесса, записывая, таким образом, поверх любых остаточных данных в этих регистрах (OR3.5).

Процессы создаются со всеми атрибутами, взятыми от родителя. Процесс наследует память (текст и сегменты данных), регистры и описатели файла от своего родительского процесса (OR3.6). Когда процесс выполняет новую программу, текстовый сегмент заменяется полностью.

Эта функция вносит вклад в удовлетворение требований безопасности FDP_RIP.2 (1, 2).

6.2.6 Управление безопасностью (SM)

Этот раздел описывает функции для управления атрибутами безопасности, которые существуют в МСВСфера 5.2 Desktop .

В дополнение к конкретным утилитам, упомянутым в этом разделе, администраторы могут использовать редактор rnano для изменения файлов конфигурации и сценариев, если с системой не поставляется разработанная конкретно для этого доверенная программа.

Роли (SM.1)

ОО сопровождает иерархический перечень ролей с некоторыми административными ролями и двумя ролями пользователей как определено в подпункте 6.2.5 данного документа (SM1.1).

В оцениваемой конфигурации в перечень административных входят пользователи, которым разрешено использовать утилиту newrole для переключения на административную роль. Каждый административный пользователь имеет уникальный персональный идентификатор для входа в систему. Это помогает обеспечивать правильное и подконтрольное использование привилегий. Идентификатор пользователя «root» не может использоваться для прямого входа в систему, за исключением входа с системной консоли.

Используя модель управления доступом на основе ролей SELinux, каждому пользователю может быть разрешен перечень ролей, и каждая роль разрешается для ряда типов реализации (TE) доменов. Отношения доминирования ролей для установления иерархии могут быть дополнительно определены в конфигурации. Назначение разрешений прежде всего подчиняются конфигурации TE. Этот подход объединяет легкость управления, обеспечиваемую моделью RBAC с многоуровневой защитой, обеспечиваемой моделью TE.

SELinux модель RBAC сопровождает атрибут роли в контексте безопасности каждого процесса. Для объектов атрибут роли обычно устанавливается в общую роль object_r и не используется.

SELinux сопровождает атрибут идентификатора пользователя в контексте безопасности, который является независимым от атрибутов идентификатора пользователя Linux. Конфигурация политики ограничивает возможность изменять идентификатор пользователя SELinux некоторыми доменами TE. Эти домены связаны с некоторыми программами, типа login, crond, и sshd, которые были изменены для вызова функций из libselinux, чтобы установить идентификатор пользователя SELinux соответственно. Следовательно, сеансы пользовательского входа в систему и задания cron первоначально связаны с соответствующим идентификатором пользователя SELinux, но последующие изменения в идентификаторе пользователя Linux не отражаются в идентификаторе пользователя SELinux. В некоторых случаях это желательно для предотвращения нарушений безопасности и обеспечения подконтрольности пользователя.

Административные пользователи

Пользователи, которым разрешается использовать команду *newrole* для переключения на административные роли, могут выполнять административные действия. Пользователи, которые не имеют привилегии использовать *newrole* для переключения на административную роль, не могут выполнять административные действия. Пользователи, которые являются не членами руководящей группы, не могут также войти как «root», даже если они знают его пароль (SM1.2).

Обычные пользователи

Обычные пользователи не могут выполнять действия, которые требуют административных привилегий. Они могут выполнять только программу setuid root, если они имеют к ней доступ (SM1.3). В оцениваемой конфигурации это ограничивается программами, в которых у пользователей есть необходимость, типа программы passwd, позволяющей пользователю изменять свой собственный пароль.

Отметим, что использование passwd для изменения собственного пароля может быть запрещено ролью пользователя.

Эта функция вносит вклад в удовлетворение требования безопасности FMT_SMR.2.

Конфигурация управления доступом и администрирование (SM.2)

Управление доступом к объектам определено битами разрешений или ACL (для тех объектов, с которыми связываются ACL). Биты разрешений на доступ, заданные по умолчанию, определены в системных файлах конфигурации, которые определяют значение битов управления доступом для объектов, создаваемых без явного определения битов разрешений. Административный пользователь может определять и изменять эти значения по умолчанию. Разрешения могут быть изменены владельцем объекта и административным пользователем (SM2.1). Когда объект создан, создатель является владельцем объекта (SM2.2). Монопольное владение объектом может быть переназначено (SM2.3). В случае объектов IPC, создатель будет всегда иметь то же самое право, что и владелец, даже когда монопольное владение было переназначено (SM2.4).

Эта функция вносит вклад в удовлетворение требований безопасности FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 и FMT_REV.1 (2).

Администрирование пользователя, группы и аутентификационных данных (SM.3)

Создание новых Пользователей

Административный пользователь может создать нового пользователя и назначить ему уникальный идентификатор пользователя. Начальный пароль должен быть определен с использованием команды passwd. Новый пользователь будет заблокирован, пока начальный пароль не будет установлен (SM3.1). Атрибуты, которые могут быть установлены для каждого пользователя, среди прочих (полный список может быть найден в описании команды useradd и в описании содержания файлов /etc/passwd и /etc/groups):

- Административный статус пользователя;
- Список групп, к которым пользователь принадлежит;
- Домашний каталог для этого пользователя.

Эти атрибуты сохраняются в файле /etc/passwd и /etc/groups (для списка всех групп, к которым пользователь принадлежит). (SM3.2)

Модификация атрибутов пользователя

Атрибуты пользователя могут быть изменены административным пользователем. Модификации атрибутов пользователя требуют модификации административной базы данных, которая их содержит, включая пользовательские роли (главным образом, /etc/passwd) (SM3.3).

Управление аутентификационными данными

Административный пользователь имеет возможность определять правила и ограничения для паролей, которые обычно подтверждают подлинность пользователей. Доступные параметры:

- Число дней (с 1 января 1970), прошедших со дня последнего изменения пароля;
- Число дней, оставшихся до возможного изменения пароля (0 указывает, что пароль может быть изменен в любое время);
- Число дней, по прошествии которых пароль должен быть изменен (99999 указывает, что пользователь может сохранять свой пароль неизменным много, много лет);
- Число дней, за которое нужно предупредить пользователя об истечении срока действия пароля (7 для полной недели);
- Число дней после истечения срока действия пароля, когда его учетная запись еще остается не заблокированной (SM3.4).

Всем пользователям, кроме имеющих роль «пользователя», также разрешено изменять свой собственный пароль, используя команду passwd. При задании пароля применяются ограничения, определенные административным пользователем (SM3.5).

Этот список атрибутов удовлетворяет требованию FIA_ATD.1. Кроме того, эта функция вносит вклад в удовлетворение требований безопасности FIA_SOS.1, FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1 и FMT_REV.1 (1).

Управление конфигурацией аудита (SM.4)

ОО позволяет конфигурировать события, которые подвергаются аудиту. Эти события определяются в конкретном файле конфигурации, и затем используется сценарий /etc/rc.d/init.d/auditd с параметром «перезагрузка», чтобы уведомить подсистему аудита о модификациях в правилах, определяющих события, которые подвергаются аудиту. Использование команды auditd и сценария /etc/rc.d/init.d/auditd ограничено и доступно только административным пользователям. Кроме того, ОО позволяет административному пользователю запускать или останавливать подсистему аудита, также используя сценарий /etc/rc.d/init.d/auditd для запуска (с

параметром «start») или останова (с параметром «stop») подсистемы аудита (SM4.1). Административный пользователь может определять события, которые подвергаются аудиту, в форме ряда правил, используя простые выражения фильтра (SM4.2).

Эта функция вносит вклад в удовлетворение требований безопасности FAU_GEN.1 и FAU_SEL.1, а также FMT_MTD.1 (1) и FMT_MTD.1 (2).

Надежные метки времени (SM.5)

ОО сопровождает надежные часы, используемые для генерации меток времени, требуемых непосредственно для ОО и приложений. Подсистеме аудита необходим такой надежный источник времени для полей даты и времени в заголовке каждой записи аудита. Часы используют таймеры, предоставляемые аппаратными средствами и подпрограммами прерывания, которые обновляют значение часов, поддерживаемых ОО.

Начальное значение для этих часов может быть предоставлено часами аппаратных средств, которые являются частью аппаратных средств ОО, доверенным внешним источником времени (например, через протокол ntp) или системным администратором в роли sysadm, устанавливающим начальное значение. Аппаратные источники времени, которые не находятся в аппаратных средствах ОО, но связаны с ними как вспомогательные аппаратные средства, являются частью среды ОО. Только системному администратору в роли sysadm разрешается перезаписывать значения часов, поддерживаемых ОО (например, исправлять значение в случае, если оно отклонялось в течение длительного времени из-за некоторой погрешности таймера аппаратных средств, используемого ОО) (SM5.1).

Эта функция вносит вклад в удовлетворение требования безопасности FPT_STM.1.

6.2.7 Защита ФБО (TP)

Во время эксплуатации ПО и данные ядра защищены механизмами защиты памяти аппаратных средств, описанными в проекте высокого уровня и руководствах для используемого оборудования. Компоненты администрирования памяти и процессов ядра обеспечивают отсутствие возможности доступа пользовательского процесса к памяти ядра или памяти, принадлежащей другим процессам (TP1.1).

ПО и данные ФБО, не принадлежащие ядру, защищены DAC и механизмами изоляции процессов. В оцениваемой конфигурации, типы реализованных правил обеспечивают защиту файлов, являющихся частью базы данных ФБО, а так же файлов и каталогов, содержащих внутренние данные ФБО (например, очереди

пакетного задания) от несанкционированной модификации и чтения. Типы реализованных правил разрешают доступ к этим файлам только ролям, которым разрешен доступ к этим типам (TP1.2). Кроме того управление доступом DAC может быть определено для дополнительной защиты.

ФБО и аппаратные средства и компоненты встроенного программного обеспечения должны быть физически защищены от несанкционированного доступа. Системное ядро является посредником для всего доступа к самим механизмам аппаратных средств, кроме функций программной визуализации команд центрального процессора и оперативной памяти, определенных ядром для непосредственного доступа к ним пользовательских процессов. Соответственно защищен образ начальной загрузки оцениваемого ОО для каждого хоста в сетевой системе.

Обеспечение вызова ФБО (TP.1)

Защищенные ресурсы всей системы управляются ФБО. Поскольку все структуры данных ФБО защищены, этими ресурсами можно непосредственно управлять только через определенные интерфейсы ФБО. Это удовлетворяет условию, что ФБО должны «всегда вызываться» для управления защищаемыми ресурсами (TP1.3). Управлять ресурсами с помощью ПО ядра можно только в привилегированном режиме центрального процессора (TP1.4). Процессы выполняются в непривилегированном режиме центрального процессора и могут вызывать функции ядра только в исключительных случаях или в результате прерывания (TP1.5). Аппаратные средства и ПО ядра обеспечивают поддержку этих событий и ограничивают вход в ядро только в определенных точках и с определенными параметрами. Только ПО ядра способно управлять всеми управляемыми ядром защищенными ресурсами.

Доверенные процессы, реализующие ресурсы, управляются вне ядра. Доверенные процессы и данные, определяющие ресурсы, защищаются, как описано выше, в зависимости от типа интерфейса. Для непосредственно вызываемых доверенных процессов механизм вызова программы всегда обеспечивает начало работы доверенного процесса в определенной точке защищенной среды (TP1.6). Другие интерфейсы доверенных процессов запускаются во время инициализации системы и используют для получения запросов хорошо определенный протокол или механизмы файловой системы (TP1.7). Некоторые системные вызовы или параметры системных вызовов зарезервированы для доверенных процессов. Когда вызываются

проверки ядра, то вызываемый процесс выполняется с эффективным идентификатором пользователя 0 (TP1.8).

ОО включает структуру SELinux, и получает управление через обработчики прерываний LSM в ядре. С этими обработчиками прерываний SELinux получает управление каждый раз, когда создается поименованный объект или процесс (как субъект) и каждый раз, когда субъект хочет получить доступ к поименованному объекту. SELinux прикрепляет атрибуты безопасности к каждому процессу и каждому названному объекту и использует правила определенные в файле политики, чтобы определить начальные значение по умолчанию этих атрибутов, а так же оценить, может ли быть предоставлен субъекту доступ к объекту. Эти правила оцениваются в дополнение к правилам дискреционного управления доступом, реализованным другими подсистемами ядра (например, подсистемой реализации файловой системы).

В оцениваемой конфигурации существует набор правил политики SELinux. В режиме ПЗКД (CAPP) правила политики реализуют политику DAC с некоторыми дополнительными ограничениями, лежащими вне области оценки данного ЗБ.

Эта функция вносит вклад в удовлетворение требования безопасности FPT_RVM.1.

Ядро (TP.2)

ПО МСВСфера 5.2 Desktop состоит из привилегированного ядра и разнообразных компонентов, не входящих в состав ядра (доверенные процессы). Ядро работает от имени всех процессов (субъектов). Ядро выполняется в привилегированном режиме центрального процессора и имеет доступ ко всей памяти системы. Всё ПО ядра, включая расширения и процессы ядра, выполняется с привилегиями ядра, но только определенные подсистемы в ядре являются частью ФБО. Вход в ядро осуществляется при некотором событии, которое вызывается контекстным переключателем типа системного вызова, прерывания ввода/вывода или исключительного условия программы.

При входе, ядро определяет функцию, которая будет выполнена, выполняет ее и, когда заканчивает, выполняет другой контекстный переключатель для возврата к обработке пользователя (в конечном счете, от имени различных субъектов) (TP2.1).

Ядро совместно используется всеми процессами и управляет системными глобальными общедоступными ресурсами. Оно представляет основной программный интерфейс для МСВСфера 5.2 Desktop в форме системных вызовов.

Поскольку ядро совместно используется всеми процессами, любой процесс, выполняющийся «в ядре» (то есть, выполняющийся в привилегированном состоянии

аппаратных средств в результате контекстного переключения), способен непосредственно ссылаться на структуры данных, обеспечивающих совместно используемые ресурсы.

Главными компонентами ядра являются: управление памятью, управление процессами, файловая система, интерфейс системного вызова и драйверы устройств.

Эта функция вносит вклад в удовлетворение требования безопасности FPT_SEP.1.

Модули ядра (ТР.3)

МСВСфера 5.2 поддерживает динамически загружаемые модули ядра, которые загружаются автоматически, по требованию. Модули ядра являются фактически частью ядра, но не резидентными, а загружаемыми как часть ядра, при необходимости (ТР3.1). Всякий раз, когда программе необходимо использовать свойство ядра, которое доступно только в качестве загружаемого модуля, и если он еще не загружен, то ядро должно позаботиться об этой ситуации и сделать все как можно лучше (ТР3.2). При этом происходит следующее:

- Ядро отмечает, что требуется свойство, которое реализуется нерезидентным модулем ядра.
- Ядро использует программу modprobe, чтобы загрузить модуль с соответствующим символическим описанием.
- modprobe просматривает свою внутреннюю адресную таблицу «псевдонимов» с целью нахождения соответствия имени. Эта таблица может реконфигурироваться и расширяться при наличии строк в /etc/modprobe.conf.
- затем modprobe загружает модули, в котором, по его мнению, нуждается ядро. Каждый модуль должен конфигурироваться согласно строкам «параметры» в /etc/modprobe.conf.
- modprobe завершает работу и сообщает ядру, что запрос успешен (или не успешен ...)
- Ядро использует вновь загруженный модуль, реализующий требуемое свойство так же, как если бы он был сконфигурирован в ядре, как резидентная часть (ТР3.3).

В ОО нерезидентные модули ядра не должны автоматически удаляться из ядра, когда они не используются некоторое время. Удаление их из ядра должно быть сделано явно.

Конкретным видом модуля ядра является SELinux, который реализован как модуль ядра структуры LSM (Модуль Безопасности Linux). Эта структура обеспечивает большое количество обработчиков прерываний в ядре Linux, где LSM может прерывать функции ядра и выполнять дополнительные проверки или определять и управлять контекстом безопасности задачи или объекта. В отличие от других загружаемых модулей безопасности, SELinux уже собран в ядре. SELinux, в качестве части ОО, использует обработчики прерываний для реализации политик управления доступом и на основе ролей, определяемых использованием файла политик, который собирается отдельно и затем загружается во время начальной загрузки системы.

ОО обеспечивает выполнение каждого процесса в «домене безопасности», и каждый защищенный ресурс имеет связанный с ним «тип». Правила политики определяют действия, которые домен может выполнять на типе. Доменами определяются и роли, которые может выполнять пользователь.

Эта функция вносит вклад в удовлетворение требования безопасности FPT_SEP.1.

Доверенные процессы (TP.4)

Доверенными в МСВСфера 5.2 Desktop являются процессы, выполняющиеся в непривилегированном режиме, но с привилегиями «root».

Доверенный процесс отличает от других пользовательских процессов способность затрагивать политику безопасности. Некоторые доверенные процессы реализуют политики безопасности непосредственно (например, идентификация и аутентификация), но многие являются доверенными просто потому, что они работают в среде, которая предоставляет возможность доступа к данным ФБО (например, программы, выполняемые административными пользователями или во время инициализации системы).

Доверенные процессы имеют в своем распоряжении для использования все интерфейсы ядра, но ограничены в использовании предоставляемых ядром механизмов для связи и совместного использования данных, типа файлов для хранения данных и каналов, сокетов и сигналов для связи.

Главные функции, реализованные доверенными процессами, включают вход пользователя в систему, идентификацию и аутентификацию, пакетную обработку, некоторые сетевые операции, системную инициализацию и системное администрирование. Ядро должно проверить каждый системный вызов, который требует привилегий «root», если процесс, который выдал запрос, имеет эти

привилегии (TP4.1). В противном случае ядро должно отказаться выполнять системный вызов. Ядро также должно проверить каждый доступ к объекту, защищенному любым механизмом DAC, если процесс будет иметь требуемые права для предпринятого типа доступа.

Любая программа, выполняемая с привилегиями «root», способна выполнять действия доверенного процесса. Поэтому важно, чтобы управляющий системой МСВСфера 5.2 Desktop, строго управлял этими программами и запрещал их изменения или выполнение с привилегиями «root» из недоверенных источников (TP4.2). Доверенные процессы не являются частью ядра и собственно ФБО (за исключением тех процессов, которые выполняют инициализацию системы и идентификацию и аутентификацию).

Доверенные процессы обеспечивают содействие в управлении безопасностью, идентификации и аутентификации.

Для идентификации и аутентификации они вносят вклад в удовлетворение функциональных требований безопасности FIA_UAU.2, FIA_UAU.7 и FIA_UID.2.

Эта функция также вносит свой вклад в FPT_SEP.1.

Базы данных ФБО (TP.5)

Таблица 6.4 определяет первичные базы данных ФБО, используемые в МСВСфера 5.2 Desktop , и их назначение. Они перечисляются или как индивидуальные файлы (именем пути), или совокупностями файлов. За исключением баз данных, перечисленных с атрибутом пользователя (который указывает, что пользователь может читать, но не писать в файл), все эти базы данных будут доступны только для административных пользователей. Ни одна из этих баз данных не должна подвергаться изменению каким-либо пользователем, кроме административного.

Эти базы данных являются частью файловой системы, и поэтому для их защиты от несанкционированного доступа должны использоваться механизмы защиты файловой системы ОО. Данная задача выполняется лицами, ответственными за установку и управление системой, чтобы обеспечить во время ее эксплуатации использование особенностей управления доступом ОО для защиты этих баз данных.

Каждая система хоста в ОО сопровождает свою собственную базу данных ФБО. Синхронизация этих баз данных не выполняется в оцениваемой конфигурации. Если такая синхронизация требуется организацией, то ответственность за ее выполнение вручную или с помощью некоторой автоматизации несет административный пользователь ОО.

Таблица 6.4 – Административные базы данных. Эта таблица содержит и другие административные файлы, используемые для конфигурации ФБО.

База данных	**Назначение**
/etc/aide.conf	файл конфигурации для утилиты AIDE
/etc/audit/auditd.conf	установки конфигурации для эксплуатации подсистемы аудита (типа местоположения журнала аудита и пороговых значений дискового пространства)
/etc/audit/audit.rules	определяет фильтры для генерации записи события, подвергаемого аудиту
/etc/cron.d/*	содержит программы, планирующиеся посредством демона cron
/etc/cron. {еженедельно, ежечасно, ежедневно, ежемесячно}/*	содержит программы, которые планируются демоном cron по еженедельному, ежечасному, ежедневному или ежемесячному календарному плану
/etc/cron.allow	файл, содержащий пользователей, которым разрешено использовать crontab
/etc/cron.deny	файл, содержащий пользователей, которым не разрешено использовать crontab. Оцененнивается только, если /etc/cron.allow не существует. Если существует пустой файл /etc/cron.deny и не существует /etc/cron.allow, то всем пользователям разрешено использовать crontab.
/etc/crontab	команды, которые планируются демоном cron
/etc/group	сохраненные имена групп, дополнительные идентификаторы групп и члены группы для всех системных групп.
/etc/gshadow	сохраненные пароли групп и информация администратора групп
/etc/hosts	содержит имена хостов и их адреса в сети. Этот файл используется, чтобы определить соответствие имени хоста его IP-адресу в отсутствии сервера доменных имен

База данных	Назначение
/etc/inittab	описывает процесс, запускаемый программой init на различных уровнях выполнения
/etc/ld.so.conf	файл, содержащий список каталогов, разделенных символами двоеточия, пробела, табуляции, перевода строки или запятой, в которых следует искать библиотеки времени выполнения для связывания с пользователем
/etc/localtime	определяет информацию локального часового пояса, используемую для ввода и отображения даты/времени
/etc/login.defs	определяет различные параметры конфигурации для процесса входа в систему
/etc/modprobe.conf	файл конфигурации для modprobe, которая автоматически загружает или выгружает модули, принимая во внимание их зависимости.
/etc/netlabel.rules	этот файл содержит правила для подсистемы Netlabel. Каждая строка содержит только параметры команды netlabel.
/etc/pam.d/*	этот каталог содержит конфигурацию PAM. В нем есть одна конфигурация для каждого приложения, которое выполняет идентификацию и аутентификацию. Каждый файл конфигурации содержит модули PAM, которые должны использоваться для этой процедуры.
/etc/passwd	сохраненные имена пользователей, идентификаторы пользователей, первичный идентификатор группы, реальное имя пользователя, домашний каталог, командный процессор для всех системных пользователей.
/etc/racoon/racoon.conf	файл конфигурации для демона IKE, включая определения ассоциации безопасности и политику безопасности

База данных	Назначение
/etc/rc.d/init.d/*	сценарии запуска системы
etc/rc.d/init.d/auditd	сценарий запуска для системы аудита
/etc/securetty	содержит имена устройств tty, с которых «root» разрешается входить в систему
/etc/security/opasswd	содержит хронологию пароля для проверки повторного использования старых паролей
/etc/security/rbac-self-test.conf	файл конфигурации для утилиты самотестирования RBAC
/etc/selinux/config	определяет активную политику
/etc/selinux/semanage.conf	конфигурация для инструмента semanage
/etc/shadow	определяет пароли пользователей в односторонней зашифрованной форме плюс дополнительные характеристики
/etc/ssh/sshd_config	содержит параметр ssh конфигурации для ssh сервера
/etc/stunnel/stunnel.conf	файл конфигурации для сервиса stunnel (местоположение конфигурируемо)
/etc/stunnel/stunnel.pem	файл с сертификатом и закрытым ключом для сервиса stunnel (местоположение конфигурируемо)
/etc/sysconfig/*	каталог, содержащий несколько файлов конфигурации для сетевых сервисов
/etc/sysctl.conf	определяет параметры ядра
/etc/vsftpd/ftpusers	содержит пользователей, которым не разрешен удаленный доступ к системе с использованием протокола FTP (только сервер)
/etc/xinetd.conf	главный файл конфигурации для xinetd
/etc/xinetd.d/*	вспомогательные файлы конфигурации для xinetd, читаются из xinetd.conf
/var/lib/aide/aide.db.gz	база данных программного контрольного суммирования информации для утилиты AIDE
/var/lib/aide/aide.db.new.gz	база данных программного контрольного суммирования информации для утилиты AIDE

База данных	Назначение
/var/log/lastlog	сохраненное время и дата последней успешной попытки входа в систему для каждого пользователя.
/var/log/tallylog	сохраненное число неудачных попыток входа в систему для каждого пользователя.
/var/spool/cron/root	файл crontab для пользователя root

Эти таблицы не являются функциями, но они являются частью управления ФБО, и также вносят свой вклад в функциональные требования безопасности сопровождения системы FMT_MSA.3 и FMT_MTD.1 (3-6), FMT_MTD.3, FMT_SMR.2, и FMT_SMF.1.

Внутренние механизмы защиты ОО (TP.6)

Всё ПО ядра имеет доступ ко всей памяти и способно выполнять все команды. Однако ПО ядра управляет только памятью, содержащей структуры данных ядра. Параметры копируются в и из памяти процесса (то есть, доступной вне ядра) явными внутренними механизмами, и эти интерфейсы только обращаются к памяти, принадлежащей процессу, который вызвал ядро (например, системным вызовом). Функции, реализованные в доверенных процессах, более строго изолированы, чем ядро. Поскольку нет явного совместного использования данных, как это есть в адресном пространстве ядра, все связи и взаимодействия между доверенными процессами происходят явно, через файлы и подобные механизмы.

Такой подход поддерживает архитектуру, в которой конкретные функции ФБО реализуются четкими группами процессов.

Эта функция вносит вклад в удовлетворение требования безопасности FPT_SEP.1.

Тестирование механизмов защиты ОО (TP.7)

ОО предоставляет инструмент для системного администратора, который позволяет ему проверять правильность функционирования базовой абстрактной машины. Этот инструмент выполняет тесты

- оперативной памяти (чтобы проверить отказы в аппаратных средствах памяти) (TP7.1)
- процессора (чтобы проверить функции управления объединения и разделения памяти между пользовательским и привилегированным режимом) (TP7.2)

- устройств ввода-вывода (чтобы проверить правильное функционирование некоторых устройств ввода-вывода, включая жесткие диски и встроенное ПО, используемое при доступе к дискам) (TP7.3)

Инструмент генерирует отчет о выполненных тестах и результатах, которые были получены. Отчет генерируется в доступном для чтения человеком формате и может быть сохранен в файле или направлен на принтер (TP7.4).

Эта функция вносит вклад в удовлетворение требования безопасности FPT_AMT.1.

Тестирование механизмов ФБО (TP.8)

ОО обеспечивает инструмент системного администратора rbac-self-test, который позволяет ему выполнять самотестирование системы, чтобы продемонстрировать правильное функционирование ФБО. Этот инструмент выполняет тестирование:

- целостности данных ФБО, включая политику SELinux (TP.8.1);
- целостности сохраненного выполняемого кода ФБО (TP.8.2);

Инструмент обеспечивает отчет о выполненных тестах и результатах проверки. Отчет генерируется в удобном для чтения человеком формате и может сохраняться в файле или направлен на принтер (TP8.4).

Эта функция вносит вклад в удовлетворение требования безопасности FPT_TST.1.

Состояние отказа безопасности (TP.9)

Система обеспечивает поддержку однопользовательского режима. Операция при включенной политике SELinux терпит отказ, если некоторая операция libselinux, которая требует доступа к информации политики или роли, прерывается (TP.9.1). Система может конфигурироваться на автоматический ввод однопользовательского режима, если утилита самотестирования обнаруживает отказ безопасности (TP.9.2).

В однопользовательском режиме все интерактивные сеансы пользователя заканчиваются и все системные демоны, которые могли выполнять задачи от имени пользователя (crond), становятся недоступными (TP.9.3).

Уполномоченный системный администратор может использовать системную консоль для взаимодействия с системой для восстановления нормального многопользовательского режима (TP.9.4).

Эта функция вносит вклад в удовлетворение требований безопасности FPT_FLS.1, FPT_RCV.1, FPT_RCV.4, и FPT_RVM.1.

6.3 Поддержка функций, не являющихся частью ФБО

6.3.1 Пользовательские Процессы

ФБО МСВСфера 5.2 Desktop прежде всего существует для поддержки работы пользовательских процессов. Пользователь или не-ФБО процесс не имеет специальных привилегии или атрибутов безопасности. Пользовательский процесс изолируется от вмешательства других пользовательских процессов прежде всего через механизмы защиты состояния выполнения центрального процессора и адресации и способом, которым они используются ядром, а также через средства защиты интерфейсов ФБО для манипуляций на процессах и файлах. Пользовательские процессы по определению не являются доверенными и поэтому не вносят свой вклад в любую функцию безопасности. ФБО обеспечивают инкапсуляцию пользовательских процессов таким способом, что они отделены от ФБО и от процессов (доверенных и недоверенных), выполняющихся с различными атрибутами, и должны быть в состоянии общаться с ними, используя только определенные интерфейсы ФБО. Поэтому пользовательские процессы не вносят свой вклад в какую-либо функцию безопасности ОО.

6.4 Меры Доверия

Следующая таблица предоставляет краткий обзор того, как меры доверия ОУД2, , выполняются МСВСфера 5.2 Desktop .

Таблица 6.2 – Отображение требований доверия к мерам доверия

Компонент доверия	**Описание мер доверия**
ACM_CAP.2	Разработчик предоставляет документацию УК, включающую в себя список конфигурации с описанием элементов конфигурации, входящих в ОО, и описание метода, используемого для уникальной идентификации элементов конфигурации. Документация УК подтверждает, что разработчик использует систему УК, уникально идентифицирующую все элементы конфигурации. Доказательство того, что ОО маркирован должным образом, обеспечивается в процессе проведения тестирования.
ADO_DEL.1	Разработчик предоставляет свидетельство

Компонент доверияОписание мер доверия
по процедурам поставки, включающее описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.
ADO_IGS.1Разработчик предоставляет свидетельство по процедурам безопасной установки, генерации и запуска, содержащее описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.
ADV_FSP.1Разработчик предоставляет функциональную спецификацию, содержащую неформальное описание ФБО и их внешних интерфейсов, а также описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках. Функциональная спецификация является внутренне непротиворечивой и полностью представляет ФБО.
ADV_HLD.1Разработчик предоставляет проект верхнего уровня, содержащий неформальное и внутренне непротиворечивое описание структуры ФБО в терминах подсистем с указанием функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО, а также идентифицирующий все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами и идентифицирующий все интерфейсы для подсистем ФБО, с указанием, какие из интерфейсов подсистем ФБО являются видимыми извне.
ADV_RCR.1Разработчик представляет свидетельство анализа соответствия между всеми смежными парами имеющихся представлений ФБО, демонстрирующее, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в

Компонент доверияОписание мер доверия
менее абстрактном представлении ФБО.
AGD_ADM.1Разработчик предоставляет согласованное со всей другой документацией, представленной для оценки, руководство администратора, которое содержит: – описание функций администрирования и интерфейсов, доступных администратору ОО; – описание безопасных способов управления ОО; – описание предупреждений относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации; – описание всех предположений о поведении субъектов доступа, которые связаны с безопасной эксплуатацией ОО; – описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения; – описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО; – описание всех требований безопасности к среде ИТ, которые относятся к администратору.
AGD_USR.1Разработчик не предоставляет руководство пользователя ввиду отсутствия у пользователей специфических функций, связанных с ОО.
ATE_COV.1Разработчик предоставляет свидетельство покрытия тестами самостоятельным документом или разделом в тестовой документации. Свидетельство покрытия тестами показывает соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.
ATE_FUN.1Разработчик провел тестирование ФБО, задокументировал результаты и представляет тестовую документацию, которая состоит из планов и

Компонент доверияОписание мер доверия
описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования. Планы тестирования идентифицируют проверяемые функции безопасности и содержат изложение целей тестирования. Описания процедур тестирования идентифицируют тесты, которые необходимо выполнить, и включают в себя сценарии для тестирования каждой функции безопасности. Эти сценарии учитывают любое влияние последовательности выполнения тестов на результаты других тестов. Ожидаемые результаты тестирования показывают прогнозируемые выходные данные успешного выполнения тестов. Результаты выполнения тестов разработчиком демонстрируют, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.
ATE_IND.2Разработчик предоставляет ОО, пригодный для тестирования, а также набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.
AVA_SOF.1Разработчик предоставляет свидетельство анализа стойкости функции безопасности, в котором приведены результаты анализа стойкости функции безопасности ОО для механизма аутентификации субъектов доступа, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.
AVA_VLA.1Разработчик предоставляет свидетельство анализа уязвимостей, в котором задокументирован выполненный анализ поставляемых материалов ОО по поиску явных путей, которыми пользователь может нарушить ПБО, а также задокументировано местоположение явных уязвимостей. Документация показывает для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

6.5 Функции безопасности ОО, требующие оценки стойкости

ОО имеет функцию безопасности для идентификации и аутентификации (IA), основанную на пароле, которая реализует вероятностный или перестановочный механизм. Оцениваемый механизм, стойкость функции которого анализируется, является парольным механизмом для аутентификации пользователей. Для этой функции требуется SOF-средняя стойкость.

7 Утверждение о соответствии ПЗ

7.1 Ссылка на ПЗ

Для данного ЗБ не утверждается соответствие ПЗ.

8 Обоснование

Раздел обоснования предоставляет дополнительную информацию и демонстрирует, что цели безопасности и функции безопасности, определенные в предыдущих разделах, непротиворечивы и достаточны, чтобы противостоять угрозам, определенным в разделе 2.

8.1 Обоснование целей безопасности

Следующие таблицы предоставляют отображение целей безопасности на среду, определяемую угрозами, политиками и предположениями, иллюстрируя, что каждая цель безопасности охватывает, по крайней мере, одну угрозу, предположение или политику, и что каждая угроза, предположение или политика охвачена, по крайней мере, одной целью безопасности.

8.1.1 Охват целей безопасности

Таблица 8.1 – Отображение целей для ОО на угрозы и политики

ЦельУгроза / Политика
O.AUTHORIZATIONT.UAUSER, P.AUTHORIZED_USERS
O.DISCRETIONARY_ACCESST.ACCESS, P.NEED_TO_KNOW
O.RESIDUAL_INFOP.NEED_TO_KNOW, T.ACCESS
O.MANAGEP.AUTHORIZED_USERS, P.NEED_TO_KNOW, T.UAUSER, T.OPERATE
O.ENFORCEMENTP.AUTHORIZED_USERS, P.NEED_TO_KNOW
O.AUDITINGP.ACCOUNTABILITY
O.COMPROTT.COMPROT, P.NEED_TO_KNOW
O.DUTYT.ROLEDEV
O.HIERARCHICALT.ROLEDEV
O.ROLET.ROLEDEV, P.ACCESS

Таблица 8.2 – Отображение целей для среды на угрозы, предположения и политики

Цель среды	**Угроза / Предположение / Политика**
OE.ADMIN	A.MANAGE, A.NO_EVIL_ADMIN
OE.CREDEN	A.COOP
OE.INSTALL	TE.COR_FILE, A.MANAGE, A.NO_EVIL_ADMIN,

	A.PEER, A.NET_COMP
OE.PHYSICAL	A.LOCATE, A.PROTECT, A.CONNECT
OE.INFO_PROTECT	TE.COR_FILE, A.PROTECT, A.UTRAIN, A.UTRUST, A.ASSET, A.ACCESS, A.OWNER, A.CLEARANCE, A.SENSITIVITY
OE.MAINTENANCE	TE.HWMF
OE.RECOVER	A.MANAGE, TE.HWMF, TE.COR_FILE
OE.SOFTWARE_IN	P.NEED_TO_KNOW
OE.SERIAL_LOGIN	A.CONNECT
OE.PROTECT	TE.COR_FILE, A.NET_COMP, A.CONNECT

Таблица 8.3–Отображение угроз на цели

УгрозаЦель
T.UAUSERO.AUTHORIZATION, O.MANAGE
T.ACCESSO.DISCRETIONARY_ACCESS, O.RESIDUAL_INFO
T.COMPROTO.COMPROT
T.OPERATEO.MANAGE
T.ROLEDEVO.DUTY, O.ROLE, O.HIERARCHICAL
TE.HWMFOE.MAINTENANCE, OE.RECOVER
TE.COR_FILEOE.PROTECT, OE.INSTALL, OE.INFO_PROTECT, OE.RECOVER

Таблица 8.4–Отображение предположений на цели

Предположение	**Цель**
A.ASSET	OE.INFO_PROTECT
A.LOCATE	OE.PHYSICAL
A.PROTECT	OE.INFO_PROTECT, OE.PHYSICAL
A.ACCESS	OE.INFO_PROTECT

A.MANAGE	OE.ADMIN, OE.INSTALL, OE.RECOVER
A.OWNER	OE.INFO_PROTECT
A.NO_EVIL_ADMIN	OE.ADMIN, OE.INSTALL
A.COOP	OE.CREDEN
A.UTRAIN	OE.INFO_PROTECT
A.UTRUST	OE.INFO_PROTECT
A.CLEARANCE	OE.INFO_PROTECT
A.SENSITIVITY	OE.INFO_PROTECT
A.NET_COMP	OE.PROTECT, OE.INSTALL
A.PEER	OE.INSTALL
A.CONNECT	OE.SERIAL_LOGIN, OE.PROTECT, OE.PHYSICAL

Таблица 8.5–Отображения политик на цели

Политика	**Цель**
P.ACCESS	O.ROLE
P.AUTHORIZED_USERS	O.AUTHORIZATION, O.MANAGE, O.ENFORCEMENT
P.NEED_TO_KNOW	O.DISCRETIONARY_ACCESS, O.MANAGE, O.ENFORCEMENT, O.RESIDUAL_INFO, O.COMPROT, OE.SOFTWARE_IN
P.ACCOUNTABILITY	O.AUDITING

8.1.2 Достаточность целей безопасности

Угроза T.UAUSER – подмены уполномоченного пользователя нарушителем достаточно уменьшена целью O.AUTHORIZATION, требующей надлежащую регистрацию пользователей, получающих доступ к ОО. Цель O.MANAGE предоставляет возможность добавлять новых пользователей или изменять атрибуты пользователей только уполномоченным администраторам (которые, как предполагается, заслуживают доверия). Вместе эти цели обеспечивают отсутствие возможности для неуполномоченного пользователя выдавать себя за уполномоченного.

Угроза T.ACCESS – доступа уполномоченного пользователя ОО к информационным ресурсам без разрешения ответственного за ресурс пользователя нейтрализуется целью O.DISCRETIONARY_ACCESS, требующей управления доступа к ресурсам и способности уполномоченных пользователей определять доступ к своим ресурсам. Она предоставляет возможность доступа пользователя к ресурсу, только если требуемый тип доступа был предоставлен пользователем, ответственным за управление правами доступа к ресурсу. Кроме того, O.RESIDUAL_INFO обеспечивает отсутствие возможности для уполномоченного пользователя получить доступ к информации, содержавшейся в ресурсе, который освобождается системой для повторного использования.

Угроза T.COMPROT пользовательским данным, подвергающая их необнаруживаемой компрометацией или изменениям, нейтрализуется целью O.COMPROT, требующей возможности установления доверенного канала между ФБО ОО и ФБО другого доверенного продукта ИТ, который защищает пользовательские данные, передаваемые по этому каналу, от раскрытия и необнаруживаемой модификации.

Угроза T.OPERATE, подвергающая компрометации активы ИТ вследствие неподходящего администрирования и эксплуатации ОО, нейтрализуется целью O.MANAGE, обеспечивающей наличие функций и средств, необходимых для поддержки деятельности административных пользователей, ответственных за управление безопасностью ОО.

Угроза T.ROLEDEV – разработки и назначения ролей пользователя путем, который подрывает безопасность, нейтрализуется целями O.DUTY, которая обеспечивает возможность «разделение обязанностей», O.HIERARCHICAL, которая поддерживает определения ролей в терминах других ролей, и O.ROLE, которая ограничивает доступ и операции на ресурсах и объектах членами уполномоченных ролей, которые разрешают эти операции.

Угроза TE.HWMF – потери данных вследствие сбоя аппаратных средств смягчается целью для среды OE.MAINTENANCE, требующей вызова диагностических инструментальных средств во время сопровождения профилактических периодов. Кроме того, OE.RECOVER требует наличия организационных процедур, способных восстанавливать критичные данные и перезапускать эксплуатацию в безопасном режиме в случае такого сбоя аппаратных средств.

Угроза TE.COR_FILE – необнаруженной потери целостности файлов ОО, обеспечивающих или относящихся к безопасности, уменьшается целями для среды: OE.INSTALL, требующей процедуры для безопасного распределения, инсталляции и конфигурации систем, таким образом обеспечивая безопасное начальное состояние системы с требуемой защитой таких файлов; OE.PROTECT, требующей защиты передаваемых данных в сети, к которой подключен ОО; и OE.INFO_PROTECT, требующей процедур для соответствующего определения прав доступа, чтобы защитить эти файлы, когда система запущена и функционирует.

Цель для среды OE.RECOVER определяет безопасное восстановление системы, которое включает проверку целостности соответствующих обеспечивающих или относящихся к безопасности файлов как часть процедур восстановления.

Предположение A.LOCATE о физической защите обрабатываемых ресурсов ОО покрывается целью для среды OE.PHYSICAL, требующей его физической защиты.

Предположение A.PROTECT о физической защите всего аппаратного и программного обеспечения, а также сетевых и периферийных кабелей охватывается целями для среды: OE.INFO_PROTECT, требующей аттестации сетевых и периферийных кабелей; и OE.PHYSICAL, требующей физической защиты.

Примечание: Физическая защита сетевых компонентов и кабелей требуется предположением A.PROTECT, которое может показаться избыточным для A.CONNECT. Но предположение A.CONNECT также обращается к защите от пассивного перехвата, который может быть сделан без наличия физического доступа к компоненту аппаратных средств.

Предположение A.MANAGE о компетентных администраторах покрывается целями для среды: OE.ADMIN, требующей компетентных и заслуживающих доверия администраторов; и OE.INSTALL, требующей процедур для безопасного распространения, инсталляции и конфигурации систем так же, как и OE.RECOVER, требующей от администратора выполнения всех требуемых действий для приведения ОО в безопасное состояние после отказа или выключения системы.

Предположение A.NO_EVIL_ADMIN об администраторах, которые не являются нерадивыми, преднамеренно небрежными или враждебными, покрывается целями для среды: OE.ADMIN, требующей компетентных и заслуживающих доверия администраторов; и OE.INSTALL, требующей процедур для безопасного распространения, инсталляции и конфигурации систем.

Предположение A.COOP об уполномоченных пользователях, действующих в манере сотрудничества, покрывается целью для среды OE.CREDEN, требующей безопасного хранения и неразглашения опознавательного мандата.

Предположение A.NET_COMP о сетевых компонентах, не изменяющих передаваемые данные, покрывается целью для среды OE.PROTECT, требующей процедур и/или механизмов, обеспечивающих безопасную передачу данных между системами так же, как и OE.INSTALL, требующей надлежащей инсталляции и конфигурации всех частей сетевой системы, включая также компоненты, которые не являются частью ОО.

Предположение A.PEER о том же самом административном управлении и ограничениях политики безопасности для систем, с которыми взаимодействует ОО, покрывается целью для среды OE.INSTALL, требующей процедур для безопасного распространения, инсталляции и конфигурации сетевой системы.

Предположение A.CONNECT об управляемом доступе к периферийным устройствам и защищенных внутренних путях связи покрывается целями для среды: OE.SERIAL_LOGIN для защиты подключаемых последовательных устройств входа в систему, OE.PROTECT для защиты данных, передаваемых между серверами/рабочими станциями, и OE.PHYSICAL, требующей физической защиты.

Предположение A.UTRAIN об обученных пользователях покрывается целью для среды OE.INFO_PROTECT, которая требует, чтобы пользователи были обучены защищать принадлежащие им данные.

Предположение A.UTRUST о пользователе, которому доверяется защита данных, покрывается целью для среды OE.INFO_PROTECT, которая требует, чтобы пользователям было доверено адекватное использование механизмов защиты ОО для защиты своих данных.

Предположение A.ASSET о значении хранимых активов, достойных настойчивых атак с умеренным потенциалом нападения, покрывается целью OE.INFO_PROTECT, которая требует должной конфигурации механизмов защиты.

Предположение A.ACCESS о ролях, которые точно отражают функцию, обязанности, квалификацию или компетентность работы пользователя в рамках предприятия, охвачено целью OE.INFO_PROTECT, которая требует обучения администраторов, чтобы выполнять должным образом задачи конфигурации.

Предположение A.OWNER, ограничивающее права пользователей по созданию и управлению новым объектом данных, охвачено целью OE.INFO_PROTECT, которая требует обучения пользователей для выполнения этих задач должным образом и не передавать эту информацию кому-либо без права на доступ к ней.

Предположение A.CLEARANCE о процедурах по предоставлению санкционирования для доступа к конкретным уровням безопасности охвачено целью OE.INFO_PROTECT, которая требует правильной установки защиты DAC и обучения пользователей для выполнения этих задач должным образом.

Предположение A.SENSITIVITY о процедурах по установлению уровня безопасности всей импортируемой или экспортируемой информации системы, включая уровень безопасности периферийных устройств, охвачен целью OE.INFO_PROTECT, которая требует правильной установки защиты DAC и обучения пользователей для выполнения этих задач должным образом.

Политика P.AUTHORIZED_USERS, требующая регистрации пользователей для доступа к системе, покрывается целью O.AUTHORIZATION и поддерживается целями: O.MANAGE, позволяющей управлять этими функциями, и O.ENFORCEMENT, определяющей правильное обращение к функциям.

Политика P.NEED_TO_KNOW, ограничивающая доступ и модификацию информации уполномоченными пользователями, которые имеют „потребность знать” эту информацию, покрывается целями: O.DISCRETIONARY_ACCESS, требующей соответствующую функцию контроля доступа, которая позволяет определять права доступа вниз до степени детализации индивидуального пользователя, и O.COMPROT, которая защищает пользовательские данные во время передачи к другому доверенному продукту ИТ. Это поддерживается целями: O.RESIDUAL_INFO, обеспечивающей отсутствие возможности получения такой информации при повторном использовании ресурсов, и OE.SOFTWARE_IN, предотвращающей установку нового программного обеспечения, которое могло бы затронуть функциональные возможности контроля доступа, пользователями, за исключением административных. Цель O.MANAGE позволяет административным и обычным пользователям (для файлов, которыми они владеют) управлять этими функциями, O.ENFORCEMENT определяет правильный вызов и работу функции.

Политика P.ACCOUNTABILITY, предоставляющая средство поддержки учета работы пользователей, реализуется целью O.AUDITING, предоставляющей ОО с такими функциональными возможностями.

Политика P.ACCESS прав доступа к конкретным объектам определяется целью O.ROLE, обеспечивающей управление доступом на основе ролей.

8.2 Обоснование требований безопасности

Этот подраздел демонстрирует обоснование внутренней согласованности и завершенности функциональных требований безопасности, определенных в этом ЗБ.

8.2.1 Внутренняя согласованность требований

Этот пункт описывает взаимную поддержку и внутреннюю согласованность компонентов, отобранных для этого ЗБ. Эти свойства обсуждаются и для функциональных компонентов, и для компонентов доверия. Функциональные компоненты были отобраны из компонентов, определенных в части 2 ОК. Функциональный компонентный FMT_SMF.1 (Спецификация функций управления) был добавлен в соответствии с принятой интерпретацией ОК. Использование уточнения компонентов было достигнуто в соответствии с рекомендациями ОК.

В данном ЗБ использовалось множество представлений идентичных или иерархически-связанных компонентов для ясного изложения требуемых функциональных возможностей.

Для внутренней согласованности требований обеспечивается следующее обоснование.

Аудит

FAU_GEN.1 определяет события, для которых требуется возможность аудита в ОО. Эти события относятся к другим функциональным требованиям безопасности, показывающим, какие события способствуют тому, чтобы сделать пользователей подотчетными за свои действия. FAU_GEN.2 требует, чтобы события были связаны с идентификатором пользователя, вызвавшего эти события. Конечно, это может быть сделано, только если пользователь известен (этого может не быть при неудавшихся попытках входа в систему).

FAU_SAR.1 определяет, что уполномоченные администраторы в состоянии оценить записи аудита, в то время как FAU_SAR.2 требует, чтобы никакие другие пользователи не могли читать записи аудита (так как они могут содержать чувствительную информацию). Принимая во внимание, что может быть собрано очень большое количество записей аудита, FAU_SAR.3 требует, чтобы ОО обладал способностью искать и выбирать записи аудита, которые удовлетворяют определенным атрибутам.

Во избежание постоянной генерации всех возможных записей аудита (которая привела бы к недопустимым накладным расходам для работы системы и могла бы

легко заполнить доступное дисковое пространство), ОО требует в FAU_SEL.1 возможность ограничивать события, которые подвергаются аудиту, основываясь на ряде определенных атрибутов.

Требование FAU_STG.1 определяет записи аудита, которые должны быть защищены от неправомочного удаления и модификации, чтобы обеспечить их законченность и корректность. Требование FAU_STG.3 указывает аспект обнаружения системой нехватки дискового пространства, которое может использоваться для хранения журнала аудита. В этом случае администратору сообщается о потенциальной проблеме, и он может принять необходимые меры во избежание критической ситуации. FAU_STG.4 указывает на проблему отсутствия возможности ОО делать записи аудита далее (например, вследствие нехватки некоторых ресурсов). В этом случае ОО также должен предотвращать возможность неправильного использования пользователем такой ситуации для обхода аудита критичных действий. Иначе пользователь мог бы преднамеренно создать такую ситуацию для обхода аудита критичного действия, выполняемого им, когда ОО не в состоянии подвергать аудиту критичные события. FMT_MTD.1 направлено на управление аудитом как для журнала аудита, так и для событий аудита.

Дискреционное управление доступом

FDP_ACC.1 требует наличия политики дискреционного управления доступом для объектов файловой системы и объектов связи между процессами. Правила этой политики описаны в FDP_ACF.1. Управление правами доступа определено в FMT_MSA.1 и FMT_REV.1. Чтобы быть эффективным, механизм дискреционного управления доступом требует идентификации и аутентификации пользователя должным образом (как требуется FIA_UID.2 и FIA_UAU.2), надлежащего связывания субъектов с пользователями (как требуется FIA_USB.1), посредничества ссылки (как требуется FPT_RVM.1) и разделения домена (как требуется FPT_SEP.1). Также поддерживается политика, соответствующая требованию защиты остаточной информации (FDP_RIP.2), которое запрещает доступ пользователей к остающейся на распределяемых объектах информации, к которой они не допущены.

Идентификация и аутентификация

Как указано выше, идентификация и аутентификация требуются для использования дискреционного управления доступом, основанного на идентификаторах индивидуальных пользователей. FIA_UAU.2 и FIA_UID.2 требуют, чтобы пользователи были аутентифицированы прежде, чем они смогут выполнить любое действие на ОО. FIA_SOS.1 определяет минимальную стойкость механизма,

используемого для аутентификации (пароли), и FIA_UAU.7 определяет некоторый уровень защиты от простой имитации в среде ОО. При выполнении процессов ОО, действующих от имени пользователя, FIA_USB.1 определяет действие этих процессов в пределах, определенных для действий пользователя (если они не доверены для выполнения работ за пределами прав пользователя). FMT_MTD.3 обеспечивает безопасные значения для выбора пароля.

FTA_LSA.1 и FTA_TSE.1 выражают необходимость обеспечения ОО соответствующих меры безопасности на месте установления сеансов, инициированных пользователями.

Повторное использование объекта

Как указано выше, повторное использование объекта (как требуется FDP_RIP.2 (1, 2) поддерживается функцией, которая запрещает свободный доступ к остаточной информации, оставшейся на объектах, когда они перераспределяются другому субъекту или объекту. Так эта функция поддерживает смысл политики дискреционного управления доступом.

Управление безопасностью

Функции представлены для нескольких функций управления, как определено в FMT_SMF.1.

Первая функция управляет правами доступа, как определено в FMT_MSA.1 и FMT_REV.1 (2). Кроме того, новым объектам требуется иметь права доступа, заданные по умолчанию, которые требуются в FMT_MSA.3.

Вторая функция управляет пользователями, как определено в FMT_MTD.1 (3) и FMT_REV.1 (1). Так как для аутентификации используются пароли, управление этими аутентификационными данными требуется также в FMT_MTD.1 (4) и FMT_MTD.1 (5). Управление подсистемой аудита выражено в соответствии с требованиями для управления журналом аудита (FMT_MTD.1 (1)) и управления событиями аудита (FMT_MTD.1 (2)). Управление журналом аудита поддерживается в соответствии с требованиями для просмотра аудита (FAU_SAR.1, FAU_SAR.2 и FAU_SAR.3), а так же требованиями для защиты журнала аудита (FAU_STG.1, FAU_STG.3 и FAU_STG.4). Управление событиями аудита поддерживается способностью выбирать события, которые подвергаются аудиту (FAU_SEL.1). Кроме того, ОО поддерживает роли, которые выражены в FMT_SMR.2 и FMT_MTD.1 (6).

Управление безопасностью также включает управление надежными метками времени. Такие метки времени являются необходимыми для точности информации о времени в записях аудита. Меткам времени указываются компонентом FPT_STM.1.

Защита ФБО

ОО должен обеспечивать работу пользователей в границах, определенных политикой управления доступом. Чтобы выполнить это, ФБО должны проверять весь доступ пользователей к защищенным объектам (как требуется в FPT_RVM.1) и поддерживать домен для своего собственного функционирования, который защищает их от вывода и вмешательства любым субъектом, который не является частью ФБО. Это выражается требованием FPT_SEP.1.

Конфигурацией ФБО предполагается, что базы данных охвачены FMT_MSA.3, FMT_MTD.1 (3–6), FMT_SMR.2, FMT_SMF.1, и FMT_MTD.3.

ОО также должен предоставлять инструмент, который позволяет администратору проверять целостность используемого оборудования и правильной эксплуатации ФБО. Такая способность указывается в FPT_AMT.1 и FPT_TST.1.

ОО должен вводить безопасное состояние при отказе критических функции безопасности, и разрешать администратору выполнять ремонт и повторно вводить режим нормального функционирования. Это выражается требованиями безопасности FPT_FLS.1, FPT_RCV.1, FPT_RCV.4, и FPT_RVM.1.

Следующая таблица показывает, как функциональные требования безопасности отображаются на цели, определенные для ОО.

Таблица 8.6 – Отображение целей в функциональных требованиях безопасности

Цель	**Функциональное требование безопасности**
O.AUTHORIZATION	Определение атрибутов пользователя (FIA_ATD.1) Верификация секретов (FIA_SOS.1) Аутентификация до любых действий пользователя (FIA_UAU.2) Аутентификация с защищенной обратной связью (FIA_UAU.7) Идентификация до любых действий пользователя (FIA_UID.2) Связывание пользователь-субъект (FIA_USB.1) Управление данными ФБО (FMT_MTD.1) Безопасные данные ФБО (FMT_MTD.3) Ограничение области выбираемых атрибутов (FTA_LSA.1) Открытие сеанса с ОО (FTA_TSE.1)
O.DISCRETIONARY_ACCESS	Ограниченное управление доступом

Цель	Функциональное требование безопасности
	(FDP_ACC.1(1)) Управление доступом, основанное на атрибутах безопасности (FDP_ACF.1(1)) Определение атрибутов пользователя (FIA_ATD.1) Связывание пользователь-субъект (FIA_USB.1) Управление атрибутами безопасности (FMT_MSA.1(1, 2)) Инициализация статических атрибутов (FMT_MSA.3(1)) Отмена (FMT_REV.1)
O.RESIDUAL_INFO	Полная защита остаточной информации (FDP_RIP.2 (1)) Полная защита остаточной информации (FDP_RIP.2 (2)) (Примечание 1)
O.MANAGE	Управление атрибутами безопасности (FMT_MSA.1 (1 - 7)) Инициализация статических атрибутов (FMT_MSA.3 (1 - 3)) Управление данными ФБО (FMT_MTD.1 (1 - 6)) Отмена (FMT_REV.1 (1,2)) Управление атрибутами безопасности (FMT_MSA.1 (1 - 7)) Спецификация функций управления (FMT_SMF.1) Ограничения на роли безопасности (FMT_SMR.2) Ручное восстановление (FPT_RCV.1) Восстановление функции (FPT_RCV.4)
O.ENFORCEMENT	Невозможность обхода ПБО (FPT_RVM.1) Отделение домена ФБО (FPT_SEP.1) Тестирование абстрактной машины (FPT_AMT.1) Сбой с сохранением безопасного состояния (FPT_FLS.1) Тестирование ФБО (FPT_TST.1)

Цель	Функциональное требование безопасности
O.AUDITING	Генерация данных аудита (FAU_GEN.1) Ассоциация идентификатора пользователя (FAU_GEN.2) Просмотр аудита (FAU_SAR.1) Ограниченный просмотр аудита (FAU_SAR.2) Выборочный просмотр аудита (FAU_SAR.3) Избирательный аудит (FAU_SEL.1) Защищенное хранение журнала аудита (FAU_STG.1) Действия в случае возможной потери данных аудита (FAU_STG.3) Предотвращение потери данных аудита (FAU_STG.4) Управление данными ФБО (FMT_MTD.1 (1, 2)) Надежные метки времени (FPT_STM.1) Ограничения на роли безопасности (FMT_SMR.2)
O.COMPROT	Базовая конфиденциальность обмена данными (FDP_UCT.1) Целостность передаваемых данных (FDP_UIT.1) Доверенный канал передачи данных между ФБО (FTP_ITC.1)
O.DUTY	Ограничения на роли безопасности (FMT_SMR.2)
O.HIERARCHICAL	Управление данными ФБО (FMT_MTD.1)
O.ROLE	Ограничения на роли безопасности (FMT_SMR.2) Ограниченное управление доступом (FDP_ACC.1 (2)) Управление доступом, основанное на атрибутах безопасности (FDP_ACF.1 (2)) Определение атрибутов пользователя (FIA_ATD.1) Связывание пользователь-субъект (FIA_USB.1) Управление атрибутами безопасности (FMT_MSA.1 (4 - 7)) Инициализация статических атрибутов (FMT_MSA.3 (3))

Цель	Функциональное требование безопасности
	Отмена (FMT_REV.1)

O.AUTHORIZATION ФБО должны предоставлять доступ к ОО и его ресурсам только уполномоченным пользователям. Пользователи, уполномоченные на доступ к ОО, должны использовать процесс идентификации и аутентификации (FIA_UID.2, FIA_UAU.2). Аутентификационные данные, предоставляющие санкционированный доступ к ОО, защищаются (FIA_ATD.1, FIA_UAU.7, FMT_MTD.1 (4-5). Стойкость аутентификационного механизма должна быть достаточной для отсутствия возможности у неуполномоченных пользователей легко выдавать себя за уполномоченного пользователя (FIA_SOS.1). Надлежащие разрешения для субъектов, действующих от имени пользователей, также определяются (FIA_USB.1). Ограничения на установление пользовательских сеансов должны быть определены и реализованы (FTA_LSA.1, FTA_TSE.1).

O.DISCRETIONARY_ACCESS ФБО должны управлять доступом к ресурсам, основываясь на идентификаторе пользователей. ФБО должны разрешать уполномоченным пользователям определять, к каким ресурсам и какие пользователи могут иметь доступ. Дискреционное управление доступом должно иметь область управления, определенную (FDP_ACC.1 (1)). Правила политики DAC должны быть определены (FDP_ACF.1 (1)). Атрибуты безопасности субъектов, используемые для обеспечения политики DAC, должны быть определены (FIA_ATD.1, FIA_USB.1). Уполномоченные пользователи должны иметь возможность управлять доступом к объектам (FMT_MSA.1 (1, 2)) и отменять этот доступ (FMT_REV.1 (2)). Защита поименованных объектов должна быть непрерывной, начиная с момента создания объекта (FMT_MSA.3 (1)).

O.AUDITING События, которые подвергаются аудиту, должны быть определены (FAU_GEN.1) и должны быть связаны с идентификатором пользователя, который вызвал событие (FAU_GEN.2). Административный пользователь должен иметь возможность читать записи аудита (FAU_SAR.1), но другие пользователи не должны иметь эту возможность (FAU_SAR.2). Административный пользователь должен иметь возможность поиска событий в журнале аудита, используя определенные критерии (FAU_SAR.3), и также должен иметь возможность определять события, которые подвергаются аудиту, и условия, при которых они подвергаются аудиту (FAU_SEL.1). Всем записям аудита необходимо предоставить надежную метку времени (FPT_STM.1). Подсистема аудита должна обеспечивать

отсутствие возможности удаления или изменения записей аудита (FAU_STG.1), или их потери из-за нехватки ресурсов (FAU_STG.3 и FAU_STG.4). Административный пользователь должен иметь возможность управлять журналом аудита (FMT_MTD.1 (1)) и событиями аудита (FMT_MTD.1 (2)). Реализация разделения ролей (FMT_SMR.2) обеспечивает возможность надежного отображения данных аудита на действия, относящиеся к безопасности.

O.RESIDUAL_INFORMATION ФБО не должны допускать раскрытия любой информации, содержавшейся в защищенном ресурсе, после его освобождения.

Остаточная информация, связанная с определенными объектами в ОО, должна быть очищена до повторного использования этого объекта (FDP_RIP.2 (1)) и прежде, чем ресурс будет отдан субъекту (FDP_RIP.2 (2)).

O.MANAGE ФБО должны предоставлять все функции и средства, необходимые для поддержки административных пользователей, ответственных за управление безопасностью ОО.

Должны быть определены аспекты управления (FMT_SMF.1). ФБО должны предусматривать наличие административного пользователя для управления ОО (FMT_SMR.2). Административный пользователь должен иметь возможность управлять подсистемой аудита (FMT_MTD.1 (1,2)), учетными записями пользователя (FMT_MTD.1 (3,4), FMT_REV.1 (1)) и атрибутами объекта (FMT_MSA.1). Кроме того, должны быть определены значения по умолчанию для управления доступом (FMT_MSA.3). Должен быть определен механизм для обмена маркированными данными между системами (FPT_TDC.1).

O.ENFORCEMENT ФБО должны быть разработаны и реализованы способом, поддерживающим политики безопасности организации в целевой среде.

ФБО должны формировать и реализовывать решения ПБО (FPT_RVM.1). Они должны быть защищены от вмешательства, которое препятствовало бы им выполнять свои функции (FPT_SEP.1). В дальнейшем, корректность этой цели выполняется через требования доверия, определенные в этом ЗБ. ФБО должны предоставлять администратору инструментальные средства, которые позволяют проверять целостность используемого оборудования (FPT_AMT.1), утилиту самотестирования (FPT_TST.1) и поддержку, перехода в безопасный режим при критических ошибках (FPT_FLS.1).

Эта цель определяет глобальную поддержку других целей безопасности для ОО, защищая части ОО, которые реализуют политики, и обеспечивает осуществление политик.

O.COMPROT ФБО должны иметь возможность устанавливать доверенный канал между собой и ФБО другого доверенного продукта ИТ (FTP_ITC.1), защищая передаваемые пользовательские данные от раскрытия (FDP_UCT.1) и необнаруженной модификации (FDP_UIT.1).

O.DUTY ОО должен обеспечивать возможность реализации «разделения обязанностей», что поддерживается разделением ролей (FMT_SMR.2).

O.HIERARCHICAL ОО должен обеспечивать возможность определения иерархических ролей, как это требуется (FMT_MTD.1).

O.ROLE ОО должен препятствовать пользователям получать доступ и выполнять операции на своих ресурсах/объектах, если им не предоставлен такой доступ владельцем ресурса/объекта, или они не были назначены на роль (уполномоченным администратором), которая разрешает эту операцию (FMT_SMR.2).

Управление доступом на основе ролей должно иметь определенную область управления (FDP_ACC.1 (2)). Должны быть определены правила политики RBAC (FDP_ACF.1 (2)). И атрибуты безопасности объектов и субъектов, используемых для реализации политики RBAC (FIA_ATD.1, FIA_USB.1). Уполномоченные пользователи должны иметь возможность управлять доступом к объектам (FMT_MSA.1 (4 - 7)) и отменять этот доступ (FMT_REV.1 (2)). Защита названных объектов должна быть непрерывной, начиная с их создания (FMT_MSA.3 (3)).

Никакие функции безопасности для не-ИТ среды не были добавлены, так как процедуры, которые должны быть реализованы, могут быть (и вероятно будут) различными для каждого места, где функционирует оцениваемая версия МСВСфера 5.2 Desktop . Поэтому никакие конкретные функциональные требования безопасности и функции безопасности для не-ИТ среды не были определены в этом ЗБ. Индивидуальные места, на которых функционирует МСВСфера 5.2 Desktop должны подтвердить достаточность установленных на месте процедур и физических мер безопасности для охвата целей безопасности для среды ОО, определенных в этом ЗБ.

Были добавлены требования безопасности для среды ИТ для определения поддержки, требуемой ОО от основного процессора. Также как для каждой операционной системы, в которой выполняется недоверенное ПО, должен существовать некоторый механизм разделения, чтобы помешать недоверенному ПО вмешиваться в доверенное ПО и данные ФБО. В случае данного ОО, процессор должен предоставлять такой механизм разделения, чтобы области памяти так же, как и привилегии аппаратных средств, требуемые для устройств прямого доступа, или функции управления памятью были защищены от прямого доступа недоверенного

ПО. Это определяется политикой управления доступом, названной „политикой управления доступом к памяти”, которую основной процессор должен поддерживать. Эта политика выражается использованием FDP_ACC.1 и FDP_ACF.1 так же, как и FDP_MSA.3 из части 2 ОК.

8.2.2 Охват требований безопасности

Следующая таблица демонстрирует, что каждое функциональное требование безопасности обращается по крайней мере к одной цели.

Таблица 8.7 - Отображение функциональных требований безопасности на цели

ФТБЦели
FAU_GEN.1O.AUDITING
FAU_GEN.1O.AUDITING
FAU_SAR.1O.AUDITING
FAU_SAR.2O.AUDITING
FAU_SEL.1O.AUDITING
FAU_STG.1O.AUDITING
FAU_STG.3O.AUDITING
FAU_STG.4O.AUDITING
FDP_ACC.1(1)O.DISCRETIONARY_ACCESS
FDP_ACF.1(1)O.DISCRETIONARY_ACCESS
FDP_ACC.1(2)O.ROLE
FDP_ACF.1(2)O.ROLE
FDP_RIP.2 (1)O.RESIDUAL_INFO
FDP_RIP.2 (2)O.RESIDUAL_INFO
FDP_UCT.1O.COMPROT
FDP_UIT.1O.COMPROT
FIA_ATD.1O.AUTHORIZATION, O.DISCRETIONARY_ACCESS

8.2.3 Анализ зависимостей требований безопасности

Следующая таблица демонстрирует зависимости между различными функциональными требованиями безопасности, если они устанавливаются в данном ЗБ.

Таблица 8.9 - Зависимости между функциональными требованиями безопасности

Установление зависимости Функциональные требования безопасности

Зависимости

FAU_GEN.1 FPT_STM.1 Надежные метки времени Да Да FAU_GEN.2 FAU_GEN.1 Генерация данных аудита

FIA_UID.1 Выбор момента идентификацииFAU_SAR.1 FAU_GEN.1 Генерация данных аудита ДаFAU_SAR.2 FAU_SAR.1 Просмотр аудита ДаFAU_SAR.3 FAU_SAR.1 Просмотр аудита Да ДаFAU_SEL.1 FAU_GEN.1 Генерация данных аудита

FMT_MTD.1 Управление данными ФБО FAU_STG.1 FAU_GEN.1 Генерация данных аудита ДаFAU_STG.3 FAU_STG.1 Защищенное хранение журнала аудита ДаFAU_STG.4 FAU_STG.1 Защищенное хранение журнала аудита ДаFDP_ACC.1 (1) FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности Да ДаFDP_ACF.1 (1) FDP_ACC.1 Ограниченное управление доступом Управление доступом, основанное на атрибутах безопасности Да ДаFDP_ACF.1 (2) FDP_ACC.1 Ограниченное управление доступом

FMT_MSA.3 Инициализация статических атрибутов FDP_ETC.1 FDP_IFC.1 Ограниченное управление информационными потоками ДаFDP_ETC.2 FDP_IFC.1 Ограниченное управление информационными потоками ДаFDP_IFC.1 FDP_IFF.1 Простые атрибуты безопасности ДаFDP_IFF.2 FDP_IFC.1 Ограниченное управление информационными потоками Да ДаFDP_ITC.1 [FDP_ACC.1 Ограниченное управление доступом или

FMT_MSA.3 Инициализация статических атрибутов ДаFDP_ITC.2 [FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками]

[FTP_ITC.1 Доверенный канал передачи данных между ФБО или

FTP_TRP.1 Доверенный маршрут]

FPT_TDC.1 Базовая согласованность данных ФБО между ФБОFDP_RIP.2 (1) Нет зависимости. ДаFDP_RIP.2 (2) Нет зависимости Да Да (FTP_ITC. 1 и FDP_ACC.1)FDP_UCT.1 [FTP_ITC.1 Доверенный канал передачи данных между ФБО, или

FTP_TRP.1 Доверенный маршрут]

[FDP_ACC.1 Ограниченное управление доступом, или

FDP_IFC.1 Ограниченное управление информационными потоками]FDP_UIT.1

FDP_UIT.1 [FDP_ACC.1 Ограниченное управление доступом, или

FDP_IFC.1 Ограниченное управление информационными потоками]

[FTP_TRP.1 Доверенный маршрут]FIA_ATD.1 Нет зависимости ДаFIA_SOS.1 Нет зависимости ДаFIA_UAU.2 FIA_UID.1 Выбор момента идентификации ДаFIA_UAU.7 FIA_UAU.1 Выбор момента аутентификации ДаFIA_UID.2 Не зависимости ДаFIA_USB.1 FIA_ATD.1 Определение атрибутов пользователя Да ДаFMT_MSA.1 [FDP_ACC.1 Ограниченное управление доступом]

FMT_SMR.1 Роли безопасности

FMT_SMF.1 Спецификация функций управления ДаFMT_MSA.3 FMT_MSA.1 Управление атрибутами безопасности

FMT_SMR.1 Роли безопасности

FMT_SMF.1 1 Спецификация функций управленияFMT_MTD.1 (1) FMT_SMR.1 Роли безопасности ДаFMT_MTD.1 (2) FMT_SMR.1 Роли безопасности ДаFMT_MTD.1 (3) FMT_SMR.1 Роли безопасности ДаFMT_MTD.1 (4) FMT_SMR.1 Роли безопасности ДаFMT_MTD.1 (5) FMT_SMR.1 Роли безопасности ДаFMT_MTD.1 (6) FMT_SMR.1 Роли безопасности Да ДаFMT_MTD.3 ADV_SPM.1

FMT_MTD.1 Управление данными ФБОFMT_REV.1 (1) FMT_SMR.1 Роли безопасности ДаFMT_REV.1 (2) FMT_SMR.1 Роли безопасности ДаFMT_SMF.1 Нет зависимости ДаFMT_SMR.2 FIA_UID.1 Выбор момента идентификации ДаFPT_AMT.1 Нет зависимости ДаFPT_FLS.1 ADV_SPM.1 Да ДаFPT_RCV.1 AGD_ADM.1

ADV_SPM.1FPT_RCV.4 ADV_SPM.1 ДаFPT_RVM.1 Нет зависимости ДаFPT_SEP.1 Нет зависимости ДаFPT_STM.1 Нет зависимости ДаFPT_TDC.1 Нет зависимости ДаFPT_TST.1 FPT_AMT.1 Тестирование абстрактной машины ДаFTA_LSA.1 Нет зависимости ДаFTA_TSE.1 Нет зависимости ДаFTP_ITC.1 Нет зависимости Да

Замечания Зависимости от FIA_UID.1 удовлетворяются включением FIA_UID.2, которое является иерархическим к FIA_UID.1 Зависимости от FMT_SMR.1 удовлетворяются включением FMT_SMR.2, который является иерархическим к FMT_SMR.1.

Зависимости от FDP_IFF. удовлетворяются включением FDP_IFF.2, которое является иерархическим к FDP_IFF.1. Зависимости FMT_MSA.1 и FMT_MSA.3 от FMT_SMF.1 вводятся интерпретацией ОК и рассматриваются здесь.

Множество итераций FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1 и FMT_REV.1 включены в эту таблицу, поскольку множество реализаций одного ФТБ может в некоторых случаях привести к необходимости множества реализаций зависимых ФТБ.

Эта таблица показывает отсутствие неудовлетворенных зависимостей между ФТБ. Между ФТБ также нет неудовлетворенных зависимостей, так как пакет требований доверия основан на оценочном уровне доверия ОУД2, для которого отсутствуют неудовлетворенные зависимости.

8.2.4 Стойкость функции

В ЗБ заявлена средняя стойкость функций безопасности. Это утверждение относится к компоненту FIA_SOS.1, посредством которого устанавливается вероятность случайного подбора пароля 1:1000000. ФТБ, в свою очередь, совместимо с целями безопасности. Заявление средней стойкости функции также совместимо с предположениями о невраждебном пользовательском сообществе и о физической защите, которая не дает возможности получения физического доступа к ОО квалифицированным, враждебным нарушителям.

8.2.5 Оценочный уровень доверия

В данном ЗБ заявлен оценочный уровень доверия ОУД2, который предполагает соответствие управляемой среде, где нарушители имеют лишь низкий потенциал нападения.

8.3 Обоснование краткой спецификации ОО

8.3.1 Обоснование функций безопасности

Следующая таблица демонстрирует функционирование и взаимодействие функций безопасности ИТ, определенных в краткой спецификации ОО, при выполнении всех, удовлетворяющих им ФТБ к ОО.

Таблица 8.9–Отображение функциональных требований безопасности на функции безопасности

Функциональные требования безопасности	**Функции безопасности (Краткая спецификация ОО)**
FAU_GEN.1	События аудита вообще определяются в пояснении **AU** как события, сгенерированные ОО. Системный администратор имеет возможность определить события, подвергаемые аудиту, которые описаны в **SM**.
FAU_GEN.2	Понятие Входного имени, которое сохраняется для пользователя после его начального входа в систему, объясняется в **AU**. Оно позволяет прослеживать события, связанные с пользователем, даже если пользователь изменяет свой идентификатор (реальный и/или эффективный и владельца файловой системы, например, командой su или выполнением программы suid).
FAU_SAR.1	Способность уполномоченного администратора читать журнал аудита и преобразовывать записи аудита в доступный для чтения человеком формат поясняется в **AU**.
FAU_SAR.2	Способность ограничивать доступ к журналу аудита уполномоченными пользователями указывается в **AU** и реализуется посредством **DA**.
FAU_SAR.3	Способность уполномоченного администратора искать в журнале аудита события, соответствующие определенным критериям поиска, выражается в **AU**.
FAU_SEL.1	Способность уполномоченного администратора определять события, которые подвергаются аудиту, используя предикаты и логические выражения, описывается в **AU** и **SM**.

Функциональные требования безопасности	Функции безопасности (Краткая спецификация ОО)
FAU_STG.1	Использование политики дискреционного управления доступом к ОО для защиты журнала и файлов конфигурации аудита от доступа кого-либо еще, кроме уполномоченного администратора, определяется в **AU**.
FAU_STG.3	Способность генерировать сообщение системного журнала, когда дисковое пространство для аудита уменьшается ниже предела, определенного в файле конфигурации аудита, описывается в **AU**.
FAU_STG.4	Способность останавливать процессы, пытающиеся генерировать записи аудита в случае, если трасса аудита заполнена, описывается в **AU**.
FDP_ACC.1 (1)	Политика дискреционного управления доступом основывается на определении в **DA** битов разрешения для субъектов и объектов, поскольку есть объекты файловой системы и объекты IPC.
FDP_ACF.1 (1)	Дискреционное управление доступом реализовано, как описано выше, посредством **DA**. Там подробно описаны индивидуальные механизмы для управления доступом в зависимости от типа объекта.
FDP_ACC.1 (2)	Политика управления доступом, основанного на ролях**,** реализуется определением **RA** субъектов и объектов, охваченных этой политикой.
FDP_ACF.1 (2)	Управление доступом, основанного на ролях**,** реализуется, как описано выше, посредством **RA**. Там подробно описаны индивидуальные механизмы для управления доступом в зависимости от типа объекта.
FDP_RIP.2 (1)	Защита остаточной информации объекта реализована функциями безопасности для повторного использования объекта **(OR)** на объектах файловой системы, объектах IPC, объектах системных очередей и разных других объектах.
FDP_RIP.2 (2)	Повторное использование объекта, выполняемое перед переназначением объекта другому субъекту, описывается

Функциональные требования безопасности	Функции безопасности (Краткая спецификация ОО)
	в **OR**.
FDP_UCT.1	Описание защиты конфиденциальности пользовательских данных, используя протокол SSH v2 или SSL v3, описывается в **SC**.
FDP_UIT.1	Описание защиты пользовательских данных от неправомочных модификаций и вставок, используя протокол SSH v2 или SSL v3, описывается в **SC**.
FIA_ATD.1	Атрибуты безопасности, принадлежащие индивидуальным пользователям, реализуются в **IA** посредством администрирования I&A данных пользователя. Управление атрибутами пользователя описывается в **SM**.
FIA_SOS.1	Функция passwd в **IA** способна реализовывать требуемую верификацию секретов. Для усиления стойкости паролей, выбранных пользователем, могут использоваться команды сопровождения системы, переопределяющие используемые параметры. Администрирование паролей, включая возможный параметр усиления стойкости паролей, объясняется в **SM**.
FIA_UAU.2	Аутентификация каждого пользователя перед любым действием реализуется **IA** (общий аутентификационный и интерактивный механизм входа в систему и связанные механизмы). Аутентификация инициализируется доверенным процессом, описанным в **TP**.
FIA_UAU.7	Механизмы входа в систему **IA** обеспечивают только закрытую обратную связь во время аутентификации. Аутентификационная обратная связь управляется доверенным процессом, описанным в **TP**.
FIA_UID.2	Идентификация каждого пользователя перед любым действием реализуется вместе с аутентификацией в **IA** (см. выше). Идентификация инициализируется доверенным процессом, описанным в **TP**.
FIA_USB.1	Требуемое связывание между субъектами и

Функциональные требования безопасности	Функции безопасности (Краткая спецификация ОО)
	пользователями реализуется функциональными возможностями su и обработкой входа в систему **IA**. Там также описывается процесс выхода из системы, который разрывает связывание между субъектами и пользователями. Реализация связывания между субъектами и пользователями охватывается **DA** и **RA.**
FMT_MSA.1	Управление атрибутами безопасности объекта реализуется конфигурацией контроля доступа и функции управления **SM**, объекты описываются в **DA** (объекты файловой системы и объекты IPC) и **RA.**
FMT_MSA.3	Ограничительные значения по умолчанию для атрибутов безопасности определяются для объектов во время их создания. Значения по умолчанию могут быть определены административным пользователем для всех типов объектов и обычным пользователем для объектов файловой системы, созданных под его управлением (см. выше, то есть, **SM** и **DA** и **RA**). Некоторые значения по умолчанию определяются в базах данных ФБО, как определено в **TP.**
FMT_MTD.1 (1)	Защита и управление журналом аудита описываются в **AU** так же, как и в **SM**. Там же описаны инструментальные средства, доступные для преобразования данных аудита в удобочитаемый для человека формат, а так же инструмент поиска данных в журнале аудита.
FMT_MTD.1 (2)	Путь, которым уполномоченный администратор может выбирать события, подвергаемые аудиту, определен в **AU** и **SM.**
FMT_MTD.1 (3)	Пользовательские атрибуты безопасности защищаются, как требуется администрированием идентификационных и аутентификационных данных пользователя в **IA,** и во время создания новых пользователей в **SM.** Пользовательские атрибуты сохраняются в базах данных

Функциональные требования безопасности	Функции безопасности (Краткая спецификация ОО)
	ФБО, описанных в **TP**.
FMT_MTD.1 (4)	Инициализация аутентификационных данных ограничена административным пользователем во время создания новых пользователей в **SM.** Аутентификационные данные (в зашифрованной форме) и атрибуты сохраняются в базах данных ФБО, описанных в **TP**. Пользователям разрешается изменять свои собственные аутентификационные данные в пределах, определенных административным пользователем. Это описано в **SM.**
FMT_MTD.1 (5)	Инициализация аутентификационных данных ограничена административным пользователем во время создания новых пользователей в **SM**.
FMT_MTD.1 (6)	Управление ролями ограничено административным пользователем в **SM**.
FMT_REV.1 (1)	Отмена пользовательских атрибутов безопасности, как требуется в FMT_REV.1, реализуется пользовательскими функциями управления **SM** и подкрепляется **DA** и **RA**.
FMT_REV.1 (2)	Отмена атрибутов безопасности объекта реализуется конфигурацией управления доступом и функцией управления **SM** и подкрепляется **DA** и **RA.**
FMT_SMF.1	Управление функциями безопасности указывается в следующих функциях безопасности: управление атрибутами безопасности объекта: **DA** (объекты файловой системы и объекты IPC). Кроме того, следующие функции управления определены: Управление журналом аудита: **AU** и **SM.** Управление событиями аудита: **AU** и **SM.** Управление атрибутами пользователя: **SM** Управление аутентификацией: **SM** и **IA**. Кроме того, большинство функций управления использует базы данных ФБО **(TP)**, чтобы хранить

Функциональные требования безопасности	Функции безопасности (Краткая спецификация ОО)
	конфигурации управления.
FMT_SMR.2	Требуемые роли в рамках безопасного управления поддерживаются функциями **SM** и **RA**.
FPT_AMT.1	Способность уполномоченного администратора проверять функционирование основной абстрактной машины описана в **TP**.
FPT_FLS.1	Работа ОО в безопасном состоянии в случае отказа охвачена функцией **SM**
FPT_RCV.1	Восстановление из безопасного состояния в случае отказа охвачено функцией **SM.**
FPT_RCV.4	Восстановление из безопасного состояния в случае отказа охвачено функцией **SM.**
FPT_RVM.1	Вызов ФБО обеспечивается функциональными возможностями **TP**, предполагающими, что функции осуществления ПБО всегда вызываются до того, как разрешается действие функций в ОДФ.
FPT_SEP.1	Требуемое разделение домена для ФБО реализуется собственно функциональными возможностями ядра, модулями ядра и доверенными процессами, как описано в **TP**, механизмом дискреционного управления доступом, описанным в **DA,** и внутренними механизмами защиты ОО, описанными в **TP**.
FPT_STM.1	Функция для генерации надежных меток времени определена в **SM**.
FPT_TST.1	Способность уполномоченного администратора проверять функции ФБО описана в **TP**.
FTA_LSA.1	Ограничения на инициализацию сеансов пользователя охвачены функцией **IA**.
FTA_TSE.1	Ограничения на инициализацию сеансов пользователя охвачены функцией **IA**.
FTP_ITC.1	Функция для установления доверенного канал между ОО и другим доверенным ИТ продукт, используя протокол SSH v2, или SSL v3, описана в **SC.**

Управление доступом определяется политиками дискреционного управления доступом, управления доступом, основанным на ролях (FDP_ACC.1 (1,2) и FDP_ACF.1 (1,2)). Домен безопасности ограничивает доступ к объектам, связанным с безопасностью, уполномоченными пользователями, как заявлено в FPT_SEP.1. Для МСВСфера 5.2 Desktop различают два типа объектов с некоторыми различиями в политиках. Все зависимости от аспектов управления были удовлетворены. Управление этими двумя типами объектов отличается лишь немного, и эти различия объясняются в FMT_MSA.1 и FMT_REV.1. Аудит событий выполняется так, чтобы была возможность поддержать учет работы пользователей. К генерации записей аудита, включая входное имя пользователя, обращаются FAU_GEN.1 и FAU_GEN.2. К доступности журнала аудита обращаются FAU_STG.1, FAU_STG.3 и FAU_STG.4. Журнал аудита должен быть защищен от несанкционированного доступа, как описано в FAU_SAR.2. Просмотр журнала аудита администратором обсуждается в FAU_SAR.1 и FAU_SAR.3. Управление и журналом аудита, и событиями аудита описано в FMT_MTD.1 и FAU_SEL.1.

Повторное использование объекта является полезным требованием, чтобы запретить нежелательный доступ к информации через ресурсы, которые не были готовы к повторному использованию. Так как ОО поддерживает управление доступом, повторное использование объекта имеет смысл. К этому обращаются в FDP_RIP.2.

Безопасная связь используется для защиты данных в пути между ОО и доверенным ИТ-продуктом от раскрытия и необнаруженных несанкционированных модификаций, как описано в FDP_UCT.1 и FDP_UIT.1. Должен быть доверенный канал между ОО и другим доверенным ИТ, как определено в FTP_ITC.1.

Идентификация и аутентификация обрабатываются в FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FTA_LSA.1 и FTA_TSE.1 довольно обычным способом. FIA_USB описывает способ, которым могут быть изменены идентификаторы пользователя и группы (эффективный, владельца файловой системы).

В разделе управления, требования для управления атрибутами пользователя, аутентификационными данными и конфигурацией аудита были разделены в этом ЗБ. Так как они четко разделены, то не противоречат друг другу.

Отмена пользовательских атрибутов описана отдельно от отмены атрибутов объекта в двух итерациях FMT_REV.1. Это имеет смысл, так как отмена обрабатывается по-разному.

FMT_SMF.1 был включен из-за принятых интерпретаций ОК и охватывает различные аспекты управления, к которым обращаются подробно в представлениях FMT_MSA.1 и FMT_MTD.1.

ОО поддерживает роли, как выражено в FMT_SMR.2.

FPT_RVM.1 требует отсутствия возможности обхода функций безопасности. Кроме того, FPT_SEP.1 определяет для недоверенных программ отсутствие возможности вмешиваться и изменять работу ФБО в противоречии с политикой безопасности ОО. Отказы критических функций безопасности приводят к безопасному состоянию (FPT_FLS.1) и методу восстановлении после него (FPT_RCV.1/4). Поэтому FPT_AMT.1, FPT_RVM.1 и FPT_SEP.1 являются взаимно поддерживающими требованиями, определяющими достаточную самозащиту ФБО.

В качестве вывода из этой демонстрации можно констатировать, что ФТБ не противоречат и взаимно поддерживают друг друга.

8.3.2 Обоснование мер доверия

Краткая спецификация ОО в подразделе 6.4 включает подтверждение того, что каждое требование доверия к безопасности ОО реализуется соответствующими мерами доверия.

8.3.3 Стойкость функции

Механизм пароля, используемый для аутентификации, является единственным механизмом в ФБО, который реализуется перестановочным или вероятностным методом, подвергаемым анализу стойкости функции при оценке этого ОО. Для основанного на пароле аутентификационного механизма функции безопасности IA.1 минимальная заявленная стойкость является СФБ-средней. Это соответствует СФБ в связанном ФТБ FIA_SOS.1. Данное утверждение совместимо с целью безопасности O.AUTHORIZATION и описанием в подразделе 3.2, которое говорит, что ОО должен защитить от небрежных угроз или случайных попыток нарушить безопасность системы. Высококвалифицированный и хорошо оснащенный нарушитель явно исключен из сценария угроз, описанного в подразделе 3.2.