УТВЕРЖДЕН

ФЛИР.90001-01 31 01-ЛУ

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

ОС ОН «СТРЕЛЕЦ»

Описание применения

ФЛИР.90001-01 31 01

Листов 23

2019

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения операционной системы общего назначения «Стрелец» (ОС ОН «Стрелец») (далее по тексту – ОС) ФЛИР.90001-01.

В документе приводятся назначение ОС, основные характеристики, функциональные возможности, условия применения ОС, приведено описание задачи, сведения о входных и выходных данных.

Документ предназначен для ознакомления с ОС пользователей и системных программистов.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ОС

1.1. Назначение

ОС ОН «Стрелец» предназначена для создания автоматизированных систем в защищенном исполнении, обрабатывающих информацию ограниченного доступа, в том числе содержащую сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно» включительно.

ОС функционирует на отечественных аппаратных платформах и совместима со средствами защиты информации (СЗИ), существующими в ведомственных органах ОС.

ОС может применяться с целью замещения импортных ОС, входящих в состав АС, обрабатывающих информацию ограниченного доступа, а также с целью объединения уже существующих разработок отечественных производителей программного обеспечения.

1.2. Основные характеристики

ОС является операционной системой семейства Debian Linux, функционирующей на аппаратных платформах с процессорной архитектурой x86-64.

Загрузочный модуль ОС ОН «Стрелец», находящийся на компакт-диске ФЛИР.90001-01 «ОС ОН «Стрелец», содержит репозиторий пакетов программ в формате DEB.

Обновления ОС, обеспечивающие устранения уязвимостей, находятся на диске обновлений и представлены в виде репозитория пакетов программ в формате DEB.

1.3. Возможности

Основные возможности ОС:

– установка и функционирование на серверах и АРМ с аппаратной платформой на процессорной архитектуре x86-64;

– работа в режиме liveCD;

– наличие средств интеграции с доменом Windows;

– наличие замкнутой программной среды;

– СЗИ, позволяющие обрабатывать информацию ограниченного доступа;

– поддержка новейшего периферийного оборудования;

– поддержка основных сетевых протоколов;

– наличие средств автоматизации повседневной деятельности (офисные средства, работа с электронной почтой, гипертекстовыми данными, словарями, работа

с графикой, мультимедиа и т.д.).

1.4. Состав ОС

В состав ОС входят:

- средства установки ОС;
- загрузчик;
- набор ядер Linux и модулей ядра с механизмами защиты информации;
- системные компоненты и библиотеки;
- системные компоненты и библиотеки СЗИ;
- средства управления программными пакетами;
- системный менеджер;
- сетевые службы;
- защищенная подсистема печати;
- графическая подсистема (графический сервер, система управления сеансами пользователей и графический менеджер окон);
- средства организации домена;
- программное обеспечение (ПО) работы с мультимедиа;
- средства работы с офисными документами;
- средства виртуализации;
- система управления базами данных (СУБД);
- средства работы с интернетом (браузеры, почтовые клиенты, мессенджеры);
- средства резервного копирования и восстановления.

1.5. Ограничения на область применения

ОС устанавливается и функционирует на серверах и АРМ, основанных на аппаратных платформах с процессорной архитектурой x86-64.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Технические средства

ОС устанавливается и функционирует на серверах и АРМ, основанных на аппаратных платформах с процессорной архитектурой x86-64 (в т. ч. и на отечественных аппаратных платформах), и совместима с СЗИ существующих в ведомственных органах ОС.

Базовыми техническими средствами для функционирования ОС являются технические средства изделия КИ8603 ЦАВМ.461263.152.

2.2. Программные средства

2.2.1. Средства установки ОС:

– реализованы в виде загрузочного DVD-диска, обеспечивающего загрузку в режиме Live;

– обеспечивают возможность установки ОС на компьютеры с архитектурой x86_64 с объемом оперативной памяти (ОП) от 2 ГБ и объемом жесткого диска от 16 ГБ;

– поддерживают установку как в режиме BIOS, так и в режиме UEFI;

– поддерживают установку на диски с разбиением MBR и GPT;

– позволяют проводить первоначальные настройки компьютера, необходимые для инсталляции,

– позволяют проводить разбиение жесткого диска;

– позволяют проводить установку даты и времени, конфигурирование сетевых интерфейсов, создание пользовательского аккаунта.

2.2.2. Загрузчик ОС обеспечивает:

– загрузку ОС, установленной на диски с разбиением MBR и GPT;

– возможность загрузки одного из ядер ОС и соответствующих модулей ядра с механизмами защиты информации.

2.2.3. Набор ядер ОС и модулей ядра с механизмами защиты информации:

– предоставляет ядро ОС и соответствующие модули ядра с механизмами защиты информации (управление доступом, замкнутая программная среда, очистка памяти, регистрация событий);

– предоставляет ядро ОС с пониженным временем отклика и соответствующие модули ядра с механизмами защиты информации (управление доступом, замкнутая программная среда, очистка памяти, регистрация событий);

– предоставляет ядро ОС с набором изменений, затрудняющим эксплуатацию уязвимостей в ПО, и соответствующие модули ядра с механизмами защиты

информации (управление доступом, замкнутая программная среда, очистка памяти, регистрация событий);

– предоставляет ядро ОС с пониженным временем отклика и набором изменений, затрудняющим эксплуатацию уязвимостей в ПО, и соответствующие модули ядра с механизмами защиты информации (управление доступом, замкнутая программная среда, очистка памяти, регистрация событий);

– предоставляет ядро ОС, содержащее отладочные символы, и соответствующие модули ядра (размещается на диске обновлений).

2.2.4. Системные компоненты и библиотеки предоставляют стандартный для ОС семейства Debian Linux набор программных средств (ПС) и библиотек, обеспечивающих решение функциональных задач ОС (работа с устройствами, работа с файловыми системами (ФС), управление учетными записями пользователей и прочие).

2.2.5. Системные компоненты и библиотеки СЗИ предоставляют набор ПС и библиотек совместно с ядром ОС и модулями ядра с механизмами защиты информации, обеспечивающих выполнение требований документов:

– «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);

– «Профиль защиты операционных систем типа «А» второго класса защиты» ИТ.ОС.А2.ПЗ (ФСТЭК России, 2017).

Они реализуют следующие функции безопасности:

– идентификация и аутентификация;
– управление доступом;
– регистрация событий безопасности;
– ограничение программной среды;
– изоляция процессов;
– защита памяти;
– контроль целостности;
– обеспечение надежного функционирования;
– фильтрация сетевого потока;
– маркирование документов.

Дополнительно осуществляется совместимость формата передачи мандатных атрибутов в поле опций IP-пакетов при сетевом взаимодействии по протоколам стека TCP/IPv4 с ОС МСВС 3.0, ОС МСВС 5.0 и Astra Linux Special Edition (соответствие ГОСТ Р 58256-2018).

Полный набор функций безопасности представлен в документе ФЛИР.90001-01 97 01 «ОС ОН «Стрелец». Задание по безопасности».

2.2.6. Системный менеджер обеспечивает совместно с компонентами и библиотеками СЗИ запуск служб (сервисов) ОС в соответствующем контексте безопасности (с установленными мандатными и дискреционными атрибутами).

2.2.7. Сетевые службы обеспечивают функционирование сетевых сервисов для создания инфраструктуры автоматизированных (информационных) систем: DNS, DHCP, SSH, FTP, NTP, NFS, SNMP.

2.2.8. Графическая подсистема (графический сервер, система управления сеансами пользователей и графический менеджер окон) обеспечивает совместно с компонентами и библиотеками СЗИ запуск и функционирование графических сессий пользователей ОС в соответствующем контексте безопасности (с установленными мандатными и дискреционными атрибутами).

Графическая подсистема включает компоненты графического окружения, предоставляющие пользователю графический рабочий стол, содержащие файловый менеджер, эмулятор терминала, редактор текста, панель задач, средство просмотра изображений, индикаторы раскладки клавиатуры, монитор системных ресурсов (памяти, процессора, жесткого диска, процессов), ПС с открытым исходным кодом для записи, создания и копирования оптических дисков с данными, звуковых оптических дисков и для работы с образами дисков.

2.2.9. Средства организации домена обеспечивают:

– создание совместимой с Active Directory доменной инфраструктуры;

– единое пространство учетных записей пользователей и групп;

– сквозную аутентификацию в сети;

– централизацию хранения информации об окружении пользователей;

– поддержку создания резервных (альтернативных) контроллеров домена;

– включение в домен рабочих мест под управлением ОС семейства Windows.

2.2.10. Средства управления программными пакетами обеспечивают:

– установку и удаление пакетов программ из состава поставляемых на компакт-диске ФЛИР.90001-01;

– обновление пакетов программ, находящихся на диске обновлений;

– установку и удаление дополнительных пакетов программ из подключаемых репозиториев.

2.2.11. Средства разработки включают в себя комплекс ПС, необходимых для создания прикладного и системного ПО:

– компиляторы и интерпретаторы для наиболее популярных языков (C++, Java, PHP, Python);

– интегрированные среды разработки (Qt Creator), отладчики (gdb);

– средства сборки deb пакетов (debhelper).

2.2.12. ПО работы с мультимедиа состоит из:

– средств воспроизведения видеофайлов в наиболее популярных форматах (MPEG-4, AVC, H.265/HEVC (SMPlayer) и т.д.);

– средств создания и воспроизведения аудиофайлов в форматах FLAC, mp3, WAV и т. п. (Audacious Media Player).

2.2.13. Средства работы с офисными документами реализованы на основе офисного пакета (LibreOffice) с открытым исходным кодом, содержащего следующие компоненты:

– текстовый редактор (Writer);

– табличный процессор (Calc);

– программу для подготовки и просмотра презентаций (Impress);

– векторный графический редактор (Draw);

– систему управления базами данных (Base) (СУБД);

– редактор формул (Math).

Основным поддерживаемым форматом файлов является открытый международный формат OpenDocument (ODF) с поддержкой форматов Office Open XML, DOC, XLS, PPT, CDR.

Средства работы с устройствами сканирования изображений обеспечивают поддержку режима пакетного сканирования и графический интерфейс пользователя (SANE, XSane).

ПС для работы с растровой и векторной графикой реализованы на основе ПО с открытым исходным кодом (GIMP).

2.2.14. ПС виртуализации и управления реализованы на основе ПО с открытым исходным кодом (libvirt, qemu/kvm, virt-manager) и обеспечивают функционал, необходимый для создания и управления виртуальной средой.

2.2.15. СУБД реализована на основе свободной объектно-реляционной СУБД и включает ПО, предоставляющее графический интерфейс для работы с базой данных (БД) (PostgreSQL, pgAdmin).

2.2.16. Средства работы с интернетом содержат:

– веб-сервер, обеспечивающий поддержку работы веб-протоколов (Apache);

– прокси-сервер (nginx), обеспечивающий кэширование и сжатие данных;

– почтовый сервер (Exim), почтовый клиент (Mozilla Thunderbird);

– веб-браузеры Mozilla Firefox и Chromium.

2.2.17. Защищенная подсистема печати реализована на основе ПО с открытым исходным кодом и обеспечивает:

– поддержку сетевой печати и управление заданиями печати (CUPS);

– мандатное разграничение доступа при выводе документов на печать;

– управление мандатными атрибутами устройств печати;

– идентификацию и аутентификацию пользователей при попытках вывода документов на печать и управления атрибутами устройств печати;

– маркировку документов при выводе на печать;

– управление параметрами маркировки документов при выводе на печать;

– регистрацию событий безопасности при выводе документов на печать.

2.2.18. Средства резервного копирования и восстановления данных обеспечивают возможность создания и хранения резервных копий (в т. ч. сетевых) (Bacula).

3. ОПИСАНИЕ ЗАДАЧИ

ОС ОН Стрелец разработана, как ОС семейства Debian Linux, в основе которой лежит набор ядер с интегрированными СЗИ. ОС обеспечивает управление процессами, сетевыми функциями, периферийными устройствами, доступом к ФС и эффективное распределение ресурсов между процессами.

По функциональному назначению процессы, которыми управляет ядро ОС, делятся на:

- системные;
- сервисные;
- прикладные.

Системные процессы являются частью ядра и всегда расположены в ОП. Системные процессы не имеют соответствующих им программ в виде исполняемых файлов и запускаются особым образом при инициализации ядра. Т. к. выполняемые инструкции и данные этих процессов находятся в ядре ОС, они могут вызывать функции и обращаться к данным, недоступным для остальных процессов. Системные процессы имеют привилегированный режим исполнения (режим суперпользователя) и ориентированы на выполнение системно-ориентированных функций.

К системным процессам следует отнести init, хотя он не является частью ядра, и его запуск осуществляется из файла /sbin/init, который является символической ссылкой на исполняемый файл /lib/systemd/systemd. Работа init важна для функционирования всей ОС в целом.

Сервисные процессы запускаются при инициализации ОС (но после инициализации ядра) и обеспечивают работу различных систем и сетевых служб: Samba, FTP, и т.д. Сервисные процессы подобны пользовательским процессам в том, что они работают в непривилегированном режиме – «пользователь». Для выполнения системных функций сервисные процессы используют механизм системных вызовов.

Сервисные процессы не связаны ни с одним интерактивным пользовательским сеансом работы и не могут непосредственно управляться пользователем. Большую часть времени сервисные процессы ожидают, пока тот или иной процесс запросит определенную услугу, например, доступ к файловому архиву или печать документа.

К прикладным процессам относятся процессы, которые запускаются обычным образом – путем загрузки в память соответствующих им программ (исполняемых файлов, выполняющихся в системе). Как правило, это процессы, порожденные в рамках пользовательского интерактивного сеанса работы. Важнейшим пользовательским процессом является основной командный интерпретатор (login shell).

Он запускается сразу же после регистрации пользователя в системе, а завершение работы login shell приводит к отключению от системы. Пользовательские процессы могут выполняться как в интерактивном, так и в последующем в фоновом режиме.

Первый пользовательский процесс, который запускается в ОС и отвечает за взаимодействие пользователя с системой, это login. Все процессы, которые запускает пользователь, являются «дочерними» по отношению к нему. При этом соблюдается принцип наследственности. Т. е. атрибуты привилегий СЗИ наследуются всеми «дочерними» процессами, порожденными от процесса login.

Основная задача, решаемая ОС в процессе своего функционирования – предоставление интерфейса для доступа ПО к ресурсам в соответствии с требованиями РД по обеспечению защиты информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно». Решение основной задачи функционирования ОС включает следующие классы задач:

– отображение исполняемых модулей в адресное пространство процесса и управление исполнением процесса;

– функционирование в многозадачном режиме (исполнение множества процессов);

– распределение между процессами доступных ОС ресурсов;

– управление доступом к оперативной и виртуальной памяти;

– управление доступом к данным на носителях с использованием ФС;

– выполнение по запросу процессов системных операций (выделение и освобождение памяти, операции ввода-вывода на носители и т. д.);

– предоставление стандартизованного доступа программ к периферийным устройствам (устройствам ввода-вывода);

– обеспечение сетевого взаимодействия между процессами посредством поддержки протоколов, соответствующих различным уровням модели взаимодействия открытых систем;

– обеспечение одновременной работы нескольких сессий пользователей;

– предоставление пользовательского интерфейса в текстовом и графическом режиме;

– организация коллективной работы пользователей в сети (организация домена);

– задачи системы защиты информации ОС.

3.1. Задачи СЗИ ОС

Задачи СЗИ ОС включают:

– обеспечение идентификации и аутентификации пользователей;

– реализацию дискреционного принципа контроля доступа процессов (субъектов доступа) к защищаемым объектам (файлам, средствам межпроцессного взаимодействия и т.д.);

– реализацию мандатного принципа контроля доступа процессов (субъектов доступа) к защищаемым объектам (файлам, средствам межпроцессного взаимодействия и т.д.);

– обеспечение изоляции адресных пространств процессов;

– обеспечение взаимодействия между процессами в соответствии с установленными правилами разграничения доступа;

– регистрацию событий безопасности;

– очистку оперативной и внешней памяти;

– контроль целостности;

– создание замкнутой программной среды;

– разграничение доступа и маркировку документов при выводе на печать;

– резервное копирование и восстановление данных;

– контроль и фильтрацию в соответствии с заданными правилами и управление правилами фильтрации входящих и исходящих информационных потоков.

Ниже представлено описание задач. Более подробная информация приведена в ФЛИР.90001-01 34 01 «ОС ОН «Стрелец». Руководство оператора»

3.1.1. Обеспечение идентификации и аутентификации пользователей

Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании стандартного для ОС семейства Linux механизма PAM (Pluggable Authentication Modules – подключаемые модули аутентификации). Данный механизм построен на использовании набора специальных разделяемых библиотек (модулей) для проведения процедуры аутентификации (подтверждение подлинности) пользователей. Каждый модуль реализует собственный механизм аутентификации. Используя определенный набор модулей и порядок их вызова, формируется требуемый сценарий аутентификации, что позволяет изменять процедуру аутентификации. Сценарии аутентификации описываются в соответствующих конфигурационных файлах ОС.

В ОС реализована возможность хранения аутентификационной информации пользователей с использованием хэш-функции.

3.1.2. Реализация дискреционного принципа контроля доступа

Реализация дискреционного принципа контроля доступа основана на правилах разграничения доступа ОС семейства Linux, формируемых в виде идентификаторов

учетных записей пользователей (UID) и групп пользователей (GID), и набора прав доступа к объекту (чтение, запись, исполнение). Дополнительно для реализации дискреционного принципа контроля доступа используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux.

Дополнительно к битовой маске существуют специальные биты: SUID, SGID, Sticky:

– SUID – Set User ID бит смены идентификатора пользователя. Когда пользователь или процесс запускает исполняемый файл с выставленным битом SUID, то порожденный процесс получает UID владельца файла. Таким образом, осуществляется возможность запуска файла с правами другого пользователя;

– SGID – Set Group ID бит смены идентификатора группы аналогично SUID;

– Sticky – определяет владельца объектов в каталоге. Sticky-бит выставляется администратором и означает, что файл из этого каталога может удалить только владелец файла. Владелец каталога может удалить Sticky-бит, но не может выставить его. Примером такого каталога является каталог /tmp.

3.1.3. Реализация мандатного принципа контроля доступа

Реализация мандатного принципа контроля доступа основана на контексте безопасности подсистемы NESS (далее – контекст безопасности), связанном с каждым субъектом доступа в ОС (процессом) и с каждым объектом доступа.

Контекст безопасности включает в себя мандатные атрибуты конфиденциальности (уровень и категории), мандатный уровень целостности, модификаторы управления доступом.

Каждому пользователю в системе соответствует множество допустимых контекстов безопасности. После аутентификации в системе, в процессе авторизации, указывает контекст, который будет действовать в порожденной сессии.

В ОС реализована поддержка двухфакторной идентификации и аутентификации пользователей (субъектов доступа) с использованием электронного идентификатора Guardant ID.

Все решения о предоставлении доступа субъекту принимаются диспетчером доступа на основании контекста безопасности субъекта, контекста безопасности объекта и типа доступа, который субъект хочет осуществить к объекту.

3.1.4. Обеспечение изоляции адресных пространств процессов

Ядро ОС с помощью механизмов защиты страниц памяти и трансляции виртуального адреса в физический гарантирует изоляцию собственных адресных пространств процессов. При этом процесс не может несанкционированным образом

получить доступ к адресному пространству других процессов, в т. ч. и ядра ОС.

3.1.5. Обеспечение взаимодействия между процессами в соответствии с установленными правилами разграничения доступа

Обеспечение взаимодействия между процессами в соответствии с установленными правилами разграничения доступа осуществляется с использованием механизмов, реализующих дискреционный и мандатный принцип контроля доступа.

3.1.6. Регистрация событий безопасности

В ядре ОС реализована подсистема протоколирования, которая осуществляет регистрацию событий безопасности с использованием службы auditd.

3.1.7. Очистка оперативной и внешней памяти

В ядре ОС семейства Linux с целью предотвращения утечки данных реализовано обнуление выделяемого пользователю сегмента памяти. Таким образом, очистка ОП осуществляется при ее перераспределении.

Для очистки внешней памяти в ОС реализован механизм, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа данного механизма снижает скорость выполнения операций удаления и усечения размера файла. Данные любых удаляемых/урезаемых файлов в пределах заданной ФС предварительно очищаются предопределенной или псевдослучайной маскирующей последовательностью. Механизм является настраиваемым для разделов с ФС Ext2/Ext3/Ext4. Опции монтирования разделов с включенным механизмом очистки совместимы с опциями монтирования в ОС МСВС и Astra Linux Special Edition.

3.1.8. Контроль целостности

Решение задачи контроля целостности среды исполнения ОС обеспечивают:

- средства регламентного контроля целостности – afick;
- средство подсчета контрольных сумм файлов и носителей – gostsum.

Каждое из указанных средств нацелено на решение конкретных задач обеспечения контроля целостности.

Для решения задачи контроля целостности предназначена библиотека gost-engine-openssl-1.1, в которой для вычисления контрольных сумм реализованы функции хэширования с длиной хэш-кода 256 бит и с длиной хэш-кода 512 бит. Названная библиотека используется в средствах подсчета контрольных сумм файлов и носителей и средствах регламентного контроля целостности, модулях аутентификации.

3.1.9. Создание замкнутой программной среды

Для решения задачи создания замкнутой программной среды используются

модули ядра Integrity Measurement Architecture (IMA) и Extended Verification Module (EVM) с реализованной поддержкой функциями хеширования, формирования и проверки цифровой подписи.

Модуль IMA предоставляет возможность внедрения контрольной суммы или цифровой подписи в расширенные атрибуты файлов. При обращении к файлу проводится проверка корректности подписи и в случае несоответствия доступ к такому файлу запрещается. При этом модуль IMA контролирует только содержание файла, сохранность самой подписи в расширенных атрибутах файла не производится, выполнение этой функции возложено на модуль EVM.

Модуль EVM используется для контроля за целостностью мета данных файлов, в т. ч. цифровых подписей. После подписывания файлов с помощью IMA проводится подпись расширенных атрибутов и в случае их изменения или сопутствия подписи доступ к такому файлу будет запрещен.

3.1.10. Разграничение доступа и маркировка документов при выводе на печать

Разграничение доступа и маркировка документов при выводе на печать осуществляется защищенной подсистемой печати, реализованной на основе сервера печати CUPS. Мандатные атрибуты конфиденциальности автоматически связываются с заданием для печати на основе мандатных атрибутов конфиденциальности, получаемых с сетевого соединения или из мандатного контекста пользователя. Вывод на печать документов, не содержащих атрибутов маркировки субъектами доступа, работающими в ненулевом мандатном контексте, невозможен.

3.1.11. Резервное копирование и восстановление данных

Для решения задачи обеспечения надежного резервного копирования и восстановления данных в ОС реализованы следующие средства:

– утилита работы с архивами tar, которая предоставляет возможность сохранения расширенных атрибутов файлов;

– утилита rsync, которая предоставляет возможности для локального и удаленного резервного копирования или синхронизации файлов и каталогов с минимальными затратами трафика;

– комплекс программ Bacula, предназначенный для решения различных задач резервного копирования и восстановления данных.

3.1.12. Контроль и фильтрация в соответствии с заданными правилами и управление правилами фильтрации входящих и исходящих информационных потоков

Для решения данной задачи в ОС используется фильтр сетевых пакетов, который осуществляет обработку пакетов, проходящих через сетевой интерфейс. При

анализе входного пакета фильтр принимает решение о том, какое действие следует произвести для этого пакета: выбросить пакет, принять или выполнить другое действие.

Функции фильтра реализуются модулем ядра netfilter. Интерфейсом для управления правилами, по которым этот модуль обрабатывает пакеты, служит утилита iptables для IPv4 и утилита ip6tables для IPv6. Для расширения функциональных возможностей iptables используются подключаемые модули.

3.1.13. Защита от выполнения машинного кода из сегмента данных адресного пространства процесса

В состав ОС входят ядра, к которым применен набор изменений PaX, ограничивающий права доступа к страницам памяти и предотвращающий выполнение произвольного кода посредством контроля доступа (чтение, запись, исполнение и их комбинации) к сегментам памяти в адресном пространстве процесса на основе использования аппаратной реализации в процессоре неисполняемого бита.

3.1.14. Разграничение доступа к внешним устройствам

Для решения данной задачи используется подсистема systemd, которая разрешает доступ пользователей к подключаемым устройствам на основе UDEV-правил работы с устройствами, содержащими в т. ч. и контекст безопасности зарегистрированного в системе внешнего устройства.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

Входными данными для ОС при решении функциональных задач являются запросы на обработку прерываний, которые могут быть инициированы субъектом (процессом), периферийным устройством (таймер, сетевой адаптер и прочие), которые распределяются ядром ОС по специализированным программам, в зависимости от источника происхождения. Например, нажатие клавиши на клавиатуре порождает в ядре процесс обработки прерывания с периферийного устройства.

С точки решения задач защиты информации в ОС входными данными являются:

– виды доступа субъектов (процессов ОС) к защищаемым именованным объектам доступа – файлам (программам и библиотекам, конфигурационным файлам со служебной информацией, файлам пользователей), каталогам, специальным файлам (устройствам, ссылкам, именованным каналам и прочим), а также средствам межпроцессного взаимодействия (сокетам, семафорам, сегментам разделяемой памяти);

– дискреционные атрибуты и контекст безопасности объекта подсистемы NESS, к которому осуществляется доступ;

– дискреционные атрибуты и контекст безопасности субъекта подсистемы NESS, осуществляющего доступ к объекту.

4.2. Выходные данные

Выходными данными для ОС при решении функциональных задач являются результаты выполнения программ, выведенные на экран, или данные, записанные в файлы или переданные другим процессам через средства межпроцессного взаимодействия в т. ч. по сети.

С точки решения задач защиты информации выходными данными является результат использования субъектом доступа защищаемого объекта: вход пользователя в систему, запуск программы, открытие файла для редактирования, создание сокетов и т. п.

5. ПОРЯДОК ОБНОВЛЕНИЯ ОС

В целях реализации функций безопасности по управлению обновлениями функций СЗИ для ОС и по модернизации функциональных возможностей ОС предусмотрен выпуск плановых обновлений (новых версий) и выпуск обновлений безопасности.

5.1. Плановое обновление (новая версия ОС)

Плановое обновление (новая версия ОС) предназначена для решения следующего комплекса задач:

– реализация новых функциональных возможностей программных средств (компонент) из состава ОС;

– обеспечение поддержки современного оборудования;

– устранение ошибок в функционировании программного обеспечения из состава ОС и повышение уровня защищенности;

– повышение удобства управления компонентами ОС.

Получение новой версии ОС осуществляется установленным порядком при заключении соответствующего договора. В качестве способа оповещения потребителей (лицензиатов) о порядке получения новой версии ОС используется размещение соответствующей информации на сайте разработчика http://vniins.ru.

Дополнительно оповещение потребителей (лицензиатов) может осуществляться с использованием контактной информации, указанной в заключенных лицензионных договорах.

Проверка потребителями подлинности новой версии ОС (входной контроль) осуществляется посредством подсчета контрольных сумм оптических дисков. Значения контрольных сумм и порядок их вычисления определены в ФЛИР.90001-01 30 01 «ОС ОН «Стрелец». Формуляр».

Дополнительная неизменность файлов, входящих в состав новой версии ОС, осуществляется средствами создания замкнутой программной среды в соответствии с описанием, приведенным в ФЛИР.90001-01 34 01.

5.2. Обновление безопасности ОС

В случае выявления в ПО из состава ОС уязвимости, которая может быть использована в настроенной в соответствии с требованиями эксплуатационной документации и/или ограничениями эксплуатации ОС для НСД к информации в обход установленных правил разграничения доступа, разработчик ОС описывает

организационно-технические мероприятия, предотвращающие использование выявленной уязвимости на объектах эксплуатации.

В случае организационно-технических мероприятий, предотвращающих использование выявленной уязвимости ОС на объектах эксплуатации, уязвимости не могут быть определены, разработчик выпускает обновление безопасности.

Источником оповещения о наличие уязвимостей и предотвращающих их использование на объектах эксплуатации организационно-технические мероприятия или обновлениях безопасности является официальный сайт разработчика ОС. На сайте в соответствующем разделе размещаются обновления безопасности в одном из следующих видов:

– руководство (инструкция) по проведению при эксплуатации ОС обязательных организационно-технических мероприятиях;

– файлы программ с руководством (инструкцией) по их установке и настройке, сопровождаемые сведениями о контрольных суммах для всех файлов обновления безопасности;

– пакетов программ (набора пакетов программ) с руководством (инструкцией) по их установке и настройке, сопровождаемые сведениями о контрольных суммах для всех файлов обновления безопасности;

– руководство (инструкция) по настройке и эксплуатации ОС с установленными обновлениями безопасности.

Потребители (лицензиаты) оповещаются о наличии обновления безопасности и порядке его получения посредством размещения соответствующих сведений информации на сайте разработчика.

Дополнительно оповещение потребителей (лицензиатов) о наличии обновлений безопасности может осуществляться с использованием контактной информации, указанной в заключенных лицензионных договорах.

Проверка потребителями подлинности обновлений безопасности осуществляется с помощью контрольных сумм, рассчитанных с использованием программы подсчета контрольных сумм gost12sum.

Дополнительная подлинность файлов, входящих в состав обновления безопасности ОС, осуществляется средствами создания замкнутой программной среды в соответствии с описанием, приведенным в ФЛИР.90001-01 34 01.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	-	автоматизированное рабочее место
АС	-	автоматизированная система
БД	-	база данных
МСВС	-	мобильная система Вооруженных Сил
ОН	-	общее назначение
ОП	-	оперативная память
ОС	-	операционная система
ПО	-	программное обеспечение
ПС	-	программное средство
РД	-	руководящий документ
СЗИ	-	средства защиты информации
СУБД	-	система управления базами данных
ФС	-	файловая система

Лист регистрации изменений									
	Номера листов (страниц)				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводительного докум. и дата*	*Подп.*	*Дата*
Изм.	*изме-ненных*	*заме-ненных*	*новых*	*аннули-рованных*					