

УТВЕРЖДЕН
ПФНА.501410.002 31-ЛУ

**СИСТЕМА ЗАЩИТЫ
ИНФОРМАЦИИ**

Dallas Lock Linux



Описание применения

ПФНА.501410.002 31

АННОТАЦИЯ

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Система защиты информации от несанкционированного доступа «Dallas Lock Linux» ПФНА.501410.002 (далее по тексту — изделие).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия (далее по тексту — ПО изделия или СЗИ НСД), условиях применения, описание задачи, перечень входных и выходных данных.

СОДЕРЖАНИЕ

1	НАЗНАЧЕНИЕ	4
2	УСЛОВИЯ ПРИМЕНЕНИЯ	5
3	ОПИСАНИЕ ЗАДАЧИ.....	8
4	ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ.....	16

1 НАЗНАЧЕНИЕ

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), государственных информационных системах, при защите значимых объектов критической информационной инфраструктуры (КИИ).

Изделие предназначено для использования на технических средствах (ТС), таких как персональные компьютеры, портативные компьютеры (ноутбуки), серверы и ТС с поддержкой виртуальных сред.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

Система защиты информации от несанкционированного доступа «Dallas Lock Linux» (СЗИ НСД) может быть использована на ТС, работающих под управлением операционных систем (ОС) семейства Linux¹ (x64):

- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- Альт Рабочая Станция 9.0;
- Альт Рабочая Станция 9.1;
- Альт Рабочая Станция 9.2;
- Альт Рабочая Станция 10.0;
- Альт Рабочая Станция 10.1;
- Альт Сервер 10;
- Astra Linux Common Edition (Опел) 2.12.x;
- Astra Linux 1.7;
- Debian 10;
- Debian 11;
- CentOS 7;
- Red Hat Enterprise Linux 7;
- Ubuntu-desktop 18.04;
- Ubuntu-desktop 20.04;
- РЕД ОС 7.1, 7.2 Муром;
- РЕД ОС 7.3 Муром;
- ROSA Enterprise Linux Desktop/Server 7.3.

СЗИ НСД поддерживает 64-разрядные версии ОС архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).

СЗИ НСД поддерживает следующие типы файловой системы: ext2, ext3, ext4, JFS, ReiserFS.

Директория «/usr» не должна быть на отдельном от корневого каталога «/» разделе ФС (это касается всех дистрибутивов).

Для размещения файлов СЗИ НСД требуется 9 Гб пространства на корневом каталоге жесткого диска:

- в каталоге «/boot» (или «boot/efi») должно быть не менее 300 Мб свободного пространства;
- в каталоге «/dllx» должно быть не менее 530 Мб свободного пространства;
- в каталоге «/dllibscr» должно быть не менее 374 Мб свободного пространства;
- в каталоге «/lib/modules» должно быть не менее 4,2 Гб свободного пространства;
- в каталоге «/tmp» должно быть не менее 3 Гб свободного пространства.

СЗИ НСД успешно устанавливается на АРМ как с UEFI/GPT, так и с BIOS/MBR на автоматически размеченный жесткий диск (разметка жесткого диска по умолчанию при установке ОС). При условии, что для всех каталогов есть необходимое свободное место.

Минимальный объем оперативной памяти, занимаемый компонентами СЗИ НСД, составляет 500 Мб. При высокой интенсивности файловых операций потребление может достигать до 3 Гб.

Для обеспечения интеграции с доменом², изделие поддерживает работу со следующими компонентами:

¹ Модуль «Персональный межсетевой экран» может использоваться на операционных системах семейства Linux с ядром версии 5.6 и выше. Для использования модуля «Персональный межсетевой экран» на операционных системах семейства Linux с ядром версии ниже 5.6 необходимо использовать версию изделия 3.31.58.

² Microsoft Active Directory — служба каталогов корпорации Microsoft для операционных систем семейства Windows Server;

- SSSD 2.6.3 и старше;
- Winbind 4.13.17 и старше;
- Kerberos 5 и старше;
- OpenLDAP 2.6.1 и старше;
- Samba 4 и старше;
- FreeIPA 3 и старше.

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети.

Поддерживаемые внешние устройства:

- USB-накопители, внешние жесткие диски, накопители на оптических дисках;
- принтеры;
- беспроводные устройства.

Изделие соответствует требованиям руководящих документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» — по 5 классу защищенности;
- «Требования к средствам контроля съемных машинных носителей информации» (документ утвержден приказом ФСТЭК России № 87 от 28 июля 2014 г.) — по 4 классу защиты;
- «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ;
- «Требования к межсетевым экранам» (документ утвержден приказом № 9 ФСТЭК России от 9 февраля 2016 г.) — по 4 классу защиты;
- «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты» ИТ.МЭ.В4.ПЗ»;
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (документ утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 4 уровню доверия.

При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.501410.002 ФО), изделие может быть использовано при создании:

- защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- защищенных государственных информационных систем до 1 класса защищенности включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- защищенных информационных систем персональных данных до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- защищенных автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных

FreeIPA — открытый проект для создания централизованной системы по управлению идентификацией пользователей, задания политик доступа и аудита для сетей на базе Linux и Unix;

Samba — программное обеспечение для реализации файлового сервера. Устанавливается на Windows, Linux/FreeBSD.

объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);

- защищенных значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

3 ОПИСАНИЕ ЗАДАЧИ

3.1 Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» ПФНА.501410.002 ТУ (ТУ).

3.2 Изделие включает в себя следующие функциональные модули:

- система защиты информации от несанкционированного доступа;
- средство контроля съемных машинных носителей информации (СКН);
- персональный межсетевой экран (МЭ)

3.3 В соответствии с ТУ СЗИ НСД состоит из программного ядра и следующих подсистем:

- подсистема управления пользователями:
 - подсистема идентификации и аутентификации;
 - подсистема контроля сессий;
- подсистема контроля файловой системы:
 - подсистема разграничения доступа к файлам и каталогам;
 - подсистема гарантированной очистки остаточной информации;
 - подсистема контроля целостности;
- подсистема управления питанием;
- подсистема контроля процессов;
- подсистема анализа:
 - подсистема журналирования;
 - подсистема аудита;
- подсистема самотестирования функционала;
- подсистема контроля внешних систем:
 - подсистема контроля разграничения доступа к блочным и беспроводным устройствам;
 - подсистема контроля печати;
- подсистема сигнализации о событиях безопасности;
- подсистема управления использованием СКН подключения;
- подсистема меж сетевого экранирования;
- подсистема восстановления после сбоев.

3.4 Ядро системы защиты выполняет основные функции СЗИ НСД:

- обеспечение доступа к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
- обеспечение проверки целостности СЗИ НСД, объектов ФС, программно-аппаратной среды;
- осуществление полной проверки правомочности и корректности администрирования СЗИ НСД;
- осуществление управления подсистемами и обеспечение их взаимодействия.

3.5 Система защиты информации от несанкционированного доступа

3.5.1 Подсистема идентификации и аутентификации

- 3.5.1.1 Изделие требует от пользователей идентифицировать себя при запросах на доступ.
- 3.5.1.2 Изделие проверяет подлинность идентификации — осуществляет аутентификацию.
- 3.5.1.3 Изделие располагает данными для проверки идентификации и аутентификации пользователей в информационной системе.
- 3.5.1.4 Изделие препятствует доступу к защищаемым ресурсам неидентифицированными пользователями и пользователями, подлинность идентификации которых при аутентификации не подтвердилась.
- 3.5.1.5 Изделие осуществляет идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия,

- длиной не менее шести буквенно-цифровых символов.
- 3.5.1.6 В изделии осуществляется управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
 - 3.5.1.7 В изделии осуществляется управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации (eToken PRO/Java, 72K, eToken Pro/SC, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite, Рутокен ЭЦП PKI, JaCarta ГОСТ, JaCarta PKI, JaCarta PKI/Flash, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta LT, JaCarta PRO, ESMART Token, ESMART Token ГОСТ, ESMART 64K, электронные ключи Touch Memory) и принятие мер в случае утраты и (или) компрометации средств аутентификации.
 - 3.5.1.8 В изделии осуществляется возможность хранения на аппаратном идентификаторе (защита пин-кодом) и считывания из аппаратного идентификатора авторизационных данных пользователей (не распространяется на электронные ключи Touch Memory).
 - 3.5.1.9 В изделии осуществляется защита обратной связи при вводе аутентификационной информации посредством замены вводимых знаков специальными символами, не позволяющими однозначно определить вводимые знаки.
 - 3.5.1.10 В изделии осуществляется управление (создание, активация, блокирование и уничтожение) учетными записями пользователей, в том числе регистрация новых и уже имеющихся доменных учетных записей пользователей системы.
 - 3.5.1.11 В изделии осуществляется разделение полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
 - 3.5.1.12 В изделии осуществляется назначение необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
 - 3.5.1.13 В изделии должен быть реализован ролевой механизм разграничения доступа к администрированию СЗИ НСД.
 - 3.5.1.14 В изделии осуществляется ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
 - 3.5.1.15 В изделии осуществляется разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты.
 - 3.5.1.16 В изделии реализована возможность авторизации доменных (LDAP) пользователей.
 - 3.5.1.17 В изделии реализована возможность добавления доменных учетных записей в локальные группы.
 - 3.5.1.18 В изделии гарантирована корректная аутентификация при нескольких подключенных аппаратных идентификаторах во время аутентификации.
 - 3.5.1.19 В изделии обеспечена работоспособность команд управления аппаратной идентификацией при удаленном подключении администратора информационной безопасности к автоматизированному рабочему месту.
- 3.5.2 Подсистема контроля сессий**
- 3.5.2.1 В изделии возможно блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.
 - 3.5.2.2 В изделии есть возможность ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя.
 - 3.5.2.3 В изделии реализована возможность задавать расписание работы пользователей.
- 3.5.3 Подсистема разграничения доступа к файлам и каталогам**
- 3.5.3.1 Изделие может контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).
 - 3.5.3.2 Для каждой пары (субъект — объект) в информационной системе задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу информационной системы (объекту).
 - 3.5.3.3 Изделие содержит механизм, реализующий дискреционные правила разграничения
-

доступа.

- 3.5.3.4 Контроль доступа может быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).
- 3.5.3.5 Механизм, реализующий дискреционный принцип контроля доступа, предусматривает возможности санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей информационной системы и списка защищаемых объектов.
- 3.5.3.6 В изделии предусмотрены средства управления, ограничивающие распространение прав на доступ.
- 3.5.3.7 В изделии реализовано осуществление контроля доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа (дискреционный принцип разграничения прав доступа).

3.5.4 Подсистема гарантированной очистки остаточной информации

- 3.5.4.1 Изделие предотвращает доступ субъекту к остаточной информации при первоначальном назначении или при перераспределении внешней памяти.
- 3.5.4.2 В изделии осуществляется очистка (обнуление, обезличивание) освобождаемых областей памяти внешних накопителей и объектов ФС.

3.5.5 Подсистема контроля целостности

- 3.5.5.1 В изделии предусмотрены средства периодического контроля целостности программной и информационной части СЗИ НСД.
- 3.5.5.2 В изделии осуществляется контроль целостности программного обеспечения, включая программное обеспечение СЗИ НСД.
- 3.5.5.3 В изделии обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
 - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ НСД;
 - целостность программной среды проверяется с периодичностью в 10 минут и по команде администратора по рассчитанным контрольным суммам.
- 3.5.5.4 В изделии должен осуществляться контроль состава технических средств, программного обеспечения и средств защиты информации.

3.5.6 Подсистема управления питанием

- 3.5.6.1 В изделии реализована возможность выключения и перезагрузки ТС средствами СЗИ НСД.

3.5.7 Подсистема контроля процессов

- 3.5.7.1 В изделии осуществляется идентификация внешних устройств ТС по логическим именам.
- 3.5.7.2 В изделии осуществляется идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

3.5.8 Подсистема журналирования

- 3.5.8.1 В изделии осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.
- 3.5.8.2 В изделии осуществляется регистрация выдачи печатных (графических) документов на «твердую» копию.
- 3.5.8.3 В изделии осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.
- 3.5.8.4 В изделии осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.
- 3.5.8.5 В изделии осуществляется регистрация следующих событий:
 - использование идентификационного и аутентификационного механизма;
 - запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
 - создание и уничтожение объекта;

– действия по изменению правил разграничения доступа.

3.5.8.6 Изделие регистрирует события безопасности, связанные с выполнением средством контроля съемных машинных носителей информации функций безопасности, и записывать информацию аудита безопасности.

3.5.9 Подсистема аудита

3.5.9.1 В изделии осуществляется регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: внешним устройствам ТС, программам, томам, каталогам, файлам, записям, полям записей.

3.5.9.2 В изделии реализована возможность определения типов событий безопасности, подлежащих регистрации, и сроков их хранения.

3.5.9.3 В изделии реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.

3.5.9.4 В изделии осуществляется сбор, запись и хранение информации о событиях безопасности в течение установленного настройками СЗИ НСД времени хранения.

3.5.9.5 В изделии реализован экспорт журналов аудита в форматы, используемые для анализа и печати данных (PDF, ODS, XML).

3.5.10 Подсистема самотестирования функционала

3.5.10.1 В изделии осуществляется:

- проверка реализации правил разграничения доступа;
- тестирование идентификации и аутентификации пользователей;
- проверка регистрации событий в соответствии с пунктом 3.5.8 настоящего документа, средств защиты регистрационной информации;
- проверка работы механизмов, осуществляющих контроль за целостностью СЗИ НСД;
- самотестирование компонентов программного ядра.

3.5.11 Подсистема контроля и разграничения доступа к беспроводным устройствам

3.5.11.1 В изделии реализована возможность задавать ограничение на использование технологий беспроводного доступа.

3.5.12 Подсистема контроля печати

3.5.12.1 В изделии возможно управление доступом к устройствам печати.

3.5.12.2 В изделии осуществляется контроль за переносом информации на твердую копию посредством контроля доступа к принтерам.

3.5.13 Подсистема сигнализации о событиях безопасности

3.5.13.1 В изделии выполняется регистрация и сигнализация о событиях, относящихся к возможным нарушениям безопасности, а также предоставление возможности выборочного ознакомления с информацией о произошедших событиях.

3.5.14 Средство контроля съемных машинных носителей информации

3.5.15.1 В изделии осуществляется управление и контроль за использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации.

3.5.15.2 Изделие контролирует использование интерфейсов ввода (вывода) информации (в т. ч. на съемные машинные носители информации).

3.5.15.3 Изделие обеспечивает контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

3.5.15.4 В изделии осуществляется разграничение доступа к управлению СКН и режиму выполнения функций безопасности (контроля накопителей) на основе ролей учетных записей пользователей.

3.5.15.5 В изделии осуществляется идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных накопителей информации.

3.5.15.6 В изделии осуществляется регламентация и контроль использования в информационной системе мобильных технических средств.

3.5.15.7 Изделие содержит механизмы генерации временных меток, и (или) должна происходить синхронизация системного времени в информационной системе.

3.5.15 Персональный межсетевой экран

3.5.16.1 Изделие осуществляет фильтрацию по отправителю информации, получателю информации, сетевому трафику и всем операциям перемещения контролируемой МЭ информации сетевого трафика к узлам информационной системы и от них.

3.5.16.2 Изделие обеспечивает распространение фильтрации на все операции перемещения через МЭ информации к узлам информационной системы и от них.

3.5.16.3 Изделие осуществляет фильтрацию, основанную на следующих атрибутах безопасности субъектов:

- сетевой адрес узла отправителя;
- сетевой адрес узла получателя.

3.5.16.4 Изделие осуществляет фильтрацию, основанную на следующих типах информации:

- сетевой протокол, который используется для взаимодействия;
- транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии);
- разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код;
- разрешенные (запрещенные) протоколы прикладного уровня;
- разрешенное (запрещенное) прикладное ПО.

3.5.16.5 Изделие предоставляет возможность разрешать или запрещать информационный поток, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации.

3.5.16.6 Изделие осуществляет фильтрацию пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика.

3.5.16.7 Изделие осуществляет проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию.

3.5.16.8 Изделие осуществляет проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором МЭ установлены разрешительные или запретительные атрибуты безопасности.

3.5.16.9 Изделие осуществляет фильтрацию SSL/TLS трафика.

3.5.16.10 Изделие осуществляет автоматическое блокирование источника информации при кратном срабатывании правила МЭ.

3.5.16.11 Изделие разрешает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации.

3.5.16.12 Изделие запрещает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации.

3.5.16.13 В изделии реализована регистрация и учет выполнения проверок информации сетевого трафика.

3.5.16.14 Изделие генерирует записи аудита для событий, потенциально подвергаемых аудиту.

3.5.16.15 Для администратора МЭ и аудитора реализована возможность читать информацию из записей аудита доступную в соответствии с их полномочиями.

3.5.16.16 Изделие предоставляет записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

3.5.16.17 В изделии реализована регистрация в каждой записи аудита следующей информации об атрибутах безопасности:

- дата и время;
- идентификатор события (ID);

- идентификатор объекта;
- информация (детализация);
- результат;
- тип события;
- адрес источника;
- порт источника;
- адрес назначения;
- порт назначения;
- описание события;
- пользователь.

Основываясь на данных атрибутах, изделие предоставляет возможность поиска и сортировки данных аудита.

3.5.16.18В изделии реализована регистрация и учет следующих событий:

- запуск и завершение выполнения функций аудита;
- результаты выполнения проверок информации сетевого трафика;
- запись нового значения любой изменяемой политики/параметра.

3.5.16.19В изделии реализована возможность идентификации/аутентификации каждого пользователя до разрешения любого действия, выполняемого при посредничестве МЭ от имени этого пользователя.

3.5.16.20В изделии реализована поддержка определенных ролей по управлению МЭ.

3.5.16.21Для администратора МЭ реализована возможность управлять режимом выполнения функций безопасности МЭ.

3.5.16.22Для администратора МЭ реализована возможность управлять данными МЭ, используемыми функциями безопасности МЭ.

3.5.16.23Для администратора МЭ реализована возможность управлять атрибутами безопасности.

3.5.16.24В изделии реализована возможность ведения для каждого типа мест расположения узла с установленным МЭ отдельных профилей проверок.

3.5.16.25В изделии реализована возможность изменения значений по умолчанию, модификации, удаления, добавления следующих данных для администраторов безопасности:

- содержимое правил МЭ;
- содержимое профилей проверок.

3.5.16.26В изделии реализована возможность модификации содержимого таблиц состояния соединений для администраторов безопасности.

3.5.16.27В изделии реализована возможность модификации перечня используемых политик МЭ для администраторов безопасности.

3.5.16.28В изделии реализована возможность очистки содержимого журналов аудита МЭ для администраторов безопасности.

3.5.16.29Для администратора МЭ реализована возможность изменения области значений профилей проверок.

3.5.16.30В изделии реализована возможность присвоения профилям проверок допустимых значений, таких как:

- профиль проверок для использования внутри информационной системы;
- профиль проверок для использования за пределами информационной системы и других допустимых профилей проверок.

3.5.16.31Для администратора МЭ реализована возможность изменения области значений информации состояния соединения.

3.5.16.32В изделии реализована возможность присвоения информации состояния соединения допустимых значений, таких как:

- установление соединения;
- использование соединения;

- завершение соединения.
- 3.5.16.33В изделии реализована возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения.
- 3.5.16.34Для администратора МЭ реализована возможность назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для прикладного программного обеспечения (приложений) с целью последующего осуществления фильтрации.
- 3.5.16.35Для администратора МЭ реализована возможность модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления МЭ фильтрации.
- 3.5.16.36В изделии реализована возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования.
- 3.5.16.37В изделии реализована возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ).
- 3.5.16.38В изделии реализована возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с МЭ средств защиты информации других видов.
- 3.5.16.39В изделии предоставлена пользователям возможность верифицировать целостность данных.
- 3.5.16.40В изделии реализована поддержка правил интерпретации данных, получаемых от взаимодействующих с МЭ средств защиты информации других видов.
- 3.5.16.41В изделии реализована возможность осуществлять выдачу предупреждающих сообщений пользователю МЭ при обнаружении возможного нарушения безопасности.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные данные

Входными данными являются:

- файлы конфигураций модулей системы, используемые при установке;
- уникальные для каждого пользователя логин, пароль и серийный номер аппаратного идентификатора;
- сертификаты X.509 для авторизации и верификации компонентов и узлов СЗИ НСД;
- формализованные правила политик безопасности, реализуемые с помощью механизмов СЗИ НСД и преобразованные в значения атрибутов и полномочий;
- команды управления СЗИ НСД;
- сетевой трафик (для МЭ);
- установленные соединения (для МЭ).

Логин может служить набор любых символов (длиной от 1 до 16), введенных с клавиатуры. Паролем может служить набор любых символов (длиной от 6 до 16), введенных с клавиатуры.

Минимальная длина и состав символов пароля регулируются соответствующими параметрами безопасности в СЗИ НСД.

Выходные данные

Выходными данными являются:

- сообщения СЗИ НСД на действия пользователей;
- журналы событий, создаваемые СЗИ НСД в процессе работы;
- значения контрольных сумм объектов, на которые установлен контроль целостности;
- резервные копии программных компонентов СЗИ НСД;
- файлы конфигураций модулей системы;
- изменения в конфигурационных файлах ОС;
- данные отчетов в результате автоматического тестирования функционала;
- резервные копии объектов, создаваемые при назначении администратором информационной безопасности контроля целостности на объекты ФС.

В журналах событий отслеживаются и соответственно отображаются такие данные, как дата, время, имя пользователя, имя объекта, тип операции, результат попытки доступа, характер ошибки и прочее.