УТВЕРЖДЕН
ПФНА.501410.002 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux

Описание применения

ПФНА.501410.002 31

Листов 10

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

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 (ГИС), 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

СЗИ НСД может быть использовано на ТС, работающих под управлением операционных систем семейства Linux[1]:

- Альт Рабочая Станция 8.2, 9.0 x64;
- Astra Linux Common Edition (Орёл) 2.12 x64;
- Debian 8;
- Debian 9;
- CentOS 7 x64;
- Red Hat Enterprise Linux 7 x64;
- Fedora 30 x64;
- Ubuntu 16.04 x64;
- Ubuntu 18.04 x64;
- РЕД ОС 7.1, 7.2 Муром;
- ROSA Enterprise Linux Desktop/Server x64;
- ЛотОС 2.1 x64.

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

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

Директория “/usr” не должна быть на отдельном от корневого каталога “/” разделе файловой системы (ФС) (это касается всех дистрибутивов).

Для размещения файлов СЗИ НСД требуется не менее 4,5 Гб пространства на системном разделе жесткого диска, из них:

- не менее 3 Гб пространства монтируемого раздела «/»;
- не менее 1,5 Гб пространства монтируемого раздела «/tmp»;
- не менее 100 Мб пространства монтируемого раздела «/boot».

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;

[1] При установке СЗИ НСД происходит замена ядра ОС на ядро, включающее программные модули СЗИ НСД.

- «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.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:

- 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 Состава 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 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

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

Изделие включает в себя следующие **функциональные модули**:

- систему защиты информации от несанкционированного доступа;
- средство контроля съемных машинных носителей информации (СКН).

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 ресурсов операционной системы:
  - подсистема контроля процессов;
  - подсистема гарантированной очистки памяти;
- 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.

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.

В рамках **подсистемы идентификации и аутентификации** осуществляется:

- запрос идентификационной информации пользователя при попытках его доступа к ОС и/или СЗИ НСД и проверка подлинности идентификации – аутентификация;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация,

блокирование средств аутентификации (eToken PRO/Java, Рутокен ЭЦП/Lite, электронные ключи Touch Memory, JaCarta ГОСТ/PKI) и принятие мер в случае утраты и (или) компрометации средств аутентификации;

- управление (создание, активация, блокирование и уничтожение) учетными записями пользователей;
- управление группами учетных записей пользователей;
- разделение полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

В рамках **подсистемы контроля сессий** осуществляется:

- блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя или по его запросу;
- ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя.

В рамках **подсистемы разграничения доступа к файлам и каталогам** СЗИ НСД содержит механизмы, реализующие:

- дискреционные правила разграничения доступа;
- контроль доступа, который применим к каждому объекту и каждому субъекту.

В рамках **подсистемы гарантированной очистки остаточной информации** СЗИ НСД предотвращает:

- восстановление удаленных данных, остаточной информации;
- доступ субъекту к остаточной информации при первоначальном назначении или при перераспределении внешней памяти.

В рамках **подсистемы контроля целостности** осуществляется:

- контроль целостности программных компонентов СЗИ;
- контроль целостности аппаратной среды;
- контроль целостности объектов файловой системы.

В рамках **подсистемы контроля процессов** осуществляется:

- идентификация внешних устройств ЭВМ по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

В рамках **подсистемы контроля гарантированной очистки памяти** СЗИ НСД реализует очистку освобождаемых областей оперативной памяти и внешних, подключаемых накопителей.

В рамках **подсистемы контроля и разграничения доступа к блочным и беспроводным устройствам** осуществляется:

- разграничение доступа пользователей и групп к блочным устройствам (сменные накопители информации);
- ограничение доступа к беспроводным устройствам передачи информации.

В рамках **подсистемы контроля печати** осуществляется:

- ограничение доступа к устройствам вывода на печать;
- контроль за переносом информации на твердую копию посредством контроля доступа к принтерам;
- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- регистрация выдачи печатных (графических) документов на «твердую» копию;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В рамках **подсистемы журналирования** осуществляется:

- регистрация событий в журналах информационной безопасности;
- предоставление администратору СЗИ НСД инструментальных средств для работы с такими журналами.

В рамках **подсистемы аудита** осуществляется возможность аудита событий, производимых пользователями над защищаемыми объектами, аудита событий входов (выходов) в информационную систему, в т.ч. сетевых, аудита системных событий, отчуждения информации на накопители или твердую копию.

В рамках **подсистемы самотестирования функционала** выполняется автоматическое тестирование основного функционала системы защиты.

В рамках **подсистемы сигнализации о событиях безопасности** выполняется регистрация и сигнализация о событиях, относящихся к возможным нарушениям безопасности, а также предоставление возможности выборочного ознакомления с информацией о произошедших событиях.

В рамках **подсистемы управления использованием СКН подключения** осуществляется предоставление возможности управления и контроля 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.

В рамках **подсистемы управления питанием** осуществляется обеспечение возможности выключения и перезагрузки ТС средствами СЗИ НСД.

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.

Логином 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.