УТВЕРЖДЕН
ПФНА.00002-01 31 01-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА Dallas Lock Linux

Описание применения

ПФНА.00002-01 31 01

Листов 10

2016 г.

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).

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

2. УСЛОВИЯ ПРИМЕНЕНИЯ

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

- Debian 7.8 (systemd) x86/x64 (версия ядра 3.2.65-1 x86_64);
- CentOS 7.0 x86/x64 (версия ядра 3.10.0-123.el7. x86_64);
- Red Hat Enterprise Linux Server 7.0 x86/x64 (версия ядра 3.10.0-123.el7.x86_64);
- Fedora 20 x86/x64 (версия ядра 3.11.10-301.fc20.x86_64);
- openSUSE 12.3 x86/x64 (версия ядра 3.7.10-1.1-desktop).

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

Для размещения файлов СЗИ НСД требуется не менее 1500 МБ пространства на системном разделе жесткого диска.

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.

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;
- «Защита от несанкционированного доступа к информации часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 4 уровню контроля.

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));
- в государственных информационных системах 1 класса защищённости (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в

государственных информационных системах»);

- для обеспечения 1 уровня защищенности персональных данных (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»);
- при создании защищенных информационных 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»).

3. ОПИСАНИЕ ЗАДАЧИ

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

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 памяти;
  - подсистема контроля целостности.
- подсистема контроля ресурсов ОС:
  - подсистема контроля гарантированной очистки памяти;
  - подсистема контроля процессов.
- подсистема контроля внешних систем:
  - подсистема контроля и разграничения доступа к блочным и беспроводным устройствам;
  - подсистема контроля печати.
- подсистема анализа:
  - подсистема журналирования;
  - подсистема аудита объектов файловой системы.

- подсистема автоматического тестирования функционала.

В рамках подсистемы идентификации и аутентификации:

- СЗИ НСД требует от пользователей идентифицировать себя при запросах на доступ и подвергать проверке подлинность идентификации – осуществлять аутентификацию. Осуществляется управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации (eToken PRO Java, Рутокен) и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- осуществляется управление (создание, активация, блокирование и уничтожение) учетными записями пользователей;
- осуществление управление группами учетных записей пользователей;
- осуществляется разделение полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

В рамках подсистемы контроля сессий СЗИ НСД осуществляет блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя или по его запросу.

В рамках подсистемы разграничения доступа к файлам и каталогам:

- СЗИ НСД содержит механизмы, реализующие дискреционные правила разграничения доступа;
- контроль доступа применим к каждому объекту и каждому субъекту.

В рамках подсистемы гарантированной очистки памяти СЗИ НСД предотвращает восстановление удаленных данных, остаточной информации.

В рамках подсистемы контроля гарантированной очистки памяти СЗИ НСД при первоначальном назначении или при перераспределении внешней памяти СЗИ НСД должна предотвращать доступ субъекту к остаточной информации.

В рамках подсистемы контроля целостности СЗИ НСД:

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

В рамках подсистемы контроля гарантированной очистки памяти реализуется очистка освобождаемых областей оперативной памяти и внешних, подключаемых накопителей.

В рамках подсистемы контроля процессов:

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

В рамках подсистемы контроля внешних систем:

- осуществляется разграничение доступа пользователей и групп к блочным устройствам (сменные накопители информации);
- выполняется ограничение доступа к беспроводным устройствам передачи информации, устройствам вывода на печать.

В рамках подсистемы контроля печати:

- СЗИ НСД осуществляет контроль за переносом информации на твердую копию посредством контроля доступа к принтерам;
- осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- осуществляется регистрация выдачи печатных (графических) документов на «твердую» копию;

- осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В рамках подсистем анализа:

- реализуется возможность аудита событий, производимых пользователями над защищаемыми объектами, аудита событий входов (выходов) в информационную систем, в т.ч. сетевых, аудита системных событий, отчуждения информации на накопители или твердую копию;
- осуществляется регистрация событий в журналах информационной безопасности и предоставление администратору СЗИ НСД инструментальных средств для работы с такими журналами.

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

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. 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.

4.2. Выходные данные

Выходными данными являются:

- сообщения СЗИ НСД на действия пользователей;
- журналы событий, создаваемые СЗИ НСД в процессе работы;
- значения контрольных сумм объектов, на которых 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 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.