СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux

Руководство администратора по обновлению изделия

СОДЕРЖАНИЕ

1 ОПИСАНИЕ И РАБОТА

Настоящее руководство распространяется на изделие «Система защиты информации от несанкционированного доступа Dallas Lock Linux» (далее по тексту — СЗИ НСД или изделие).

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

СЗИ НСД предназначена для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа (НСД) на ТС, работающих под управлением следующих операционных систем (ОС) семейства Linux[1]:

- Альт Рабочая Станция 8.2 x64 (версия ядра СЗИ НСД 4.9);
- Альт Рабочая Станция 9.0 x64 (версия ядра СЗИ НСД 4.19);
- Astra Linux Common Edition (Орел) 2.12 x64 (версия ядра СЗИ НСД 4.19);
- Debian 8 x64 (версия ядра СЗИ НСД 3.16);
- Debian 9 x64 (версия ядра СЗИ НСД 4.19);
- CentOS 7 x64 (версия ядра СЗИ НСД 3.16);
- Red Hat Enterprise Linux 7 x64 (версия ядра СЗИ НСД 3.16);
- Fedora 30 x64 (версия ядра СЗИ НСД 4.19);
- Ubuntu 16.04 x64 (версия ядра СЗИ НСД 4.19);
- Ubuntu 18.04 x64 (версия ядра СЗИ НСД 4.19);
- РЕД ОС 7.1, 7.2 Муром x64 (версия ядра СЗИ НСД 4.19);
- ROSA Enterprise Linux Desktop/Server x64 (версия ядра СЗИ НСД 3.16);
- ЛотОС 2.1 x64 (версия ядра СЗИ НСД 3.16).

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, ReiserFS.

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

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

Для размещения файлов СЗИ НСД требуется не менее 4,6 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».

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

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.

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

2 ОБНОВЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ

СЗИ НСД представляет собой программный комплекс средств защиты информации в ОС семейства Linux с возможностью подключения аппаратных идентификаторов. Для функционирования СЗИ НСД необходимо произвести установку и настройку программных компонентов системы защиты.

2.1 Обновление системы защиты

Обновление СЗИ НСД Dallas Lock Linux направлено на:

- устранение уязвимостей средства защиты информации;
- добавление функции (функций) безопасности средства защиты информации, направленной (направленных) на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ;
- добавление функции (функций), не влияющей (не влияющих) на функции безопасности СЗИ (например, изменение интерфейса СЗИ).

Информация о появлении обновленной версии СЗИ НСД регистрируется на сайте www.dallaslock.ru с указанием устраненных недостатков и добавленных функциональных возможностей.

Пользователи СЗИ НСД информируются о выпуске обновлений СЗИ НСД Dallas Lock Linux (с указанием устраненных недостатков и добавленных функциональных возможностей) по электронной почте с подтверждением получения информации.

После получения информации о наличии обновлений на СЗИ НСД Dallas Lock Linux необходимо выполнить следующие действия:

1. С сайта компании www.dallaslock.ru скачать архив, который будет содержать обновленный дистрибутив СЗИ НСД.

2. Сохранить указанный архив на жесткий диск ТС, на котором требуется обновить СЗИ НСД.

3. Рассчитать контрольную сумму для дистрибутива по алгоритму ГОСТ Р 34.11-94 с помощью программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (сертификат соответствия ФСТЭК России № 2031 от 03.02.2010) либо по алгоритму MD5 с помощью программы «md5sum» (является встроенной в поддерживаемые операционные системы) или программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Fsum Frontend» (свободно распространяемая программа, входит в комплект поставки на компакт-диске с СЗИ НСД).

4. Сверить полученную контрольную сумму с соответствующими контрольными суммами, хранящимися на сайте компании www.dallaslock.ru. В случае совпадения контрольных сумм производится установка обновлений. В случае несовпадения контрольных сумм рекомендуется обратиться в службу технической поддержки ООО «Конфидент».

5. Перед установкой обновлений необходимо удалить установленную ранее версию СЗИ НСД (подробнее — в разделе Удаление системы защиты) и выполнить установку СЗИ, используя в качестве дистрибутива скачанный архив (подробнее — в разделе Установка системы защиты).

6. После установки обновлений необходимо сделать соответствующую отметку в разделе 13 формуляра СЗИ НСД Dallas Lock Linux с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

2.2 Подготовка к установке

При установке СЗИ НСД требуется скачивание пакетов из глобальной сети. Для автономных компьютеров, не подключенных к глобальной сети, необходимо, чтобы в локальной сети был расположен официальный репозиторий соответствующего дистрибутива ОС и были выполнены соответствующие настройки инфраструктуры. Следует обратить внимание, что корректная работа СЗИ НСД гарантируется только с официальными репозиториями, подключение к которым осуществляется сразу после установки ОС.

Примечание. Необходимым условием установки является доступность официального репозитория соответствующего дистрибутива ОС.

Подготовка к установке должна осуществляться только с правами суперпользователя (*root*), обладающего правами администратора на данном ТС.

Внимание! Суперпользователь (root) и пользователи с аналогичными правами обладают привилегиями, с помощью которых могут внести изменения в СЗИ и ее настройки, способные нарушить корректность выполнения функций СЗИ вплоть до неработоспособности СЗИ. Контроль привилегированных пользователей должен осуществляться посредством применения организационных мер защиты.

Внимание! В случае если пароль суперпользователя (*root*) не был задан до установки СЗИ НСД, то после установки СЗИ НСД пароль суперпользователя (*root*) можно будет задать только средствами СЗИ НСД.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия:

1. Убедиться, что на ТС не установлена система защиты. Если система защиты установлена, ее необходимо удалить.

2. Проверить состояние файловой системы ПК при помощи специальной утилиты из состава ОС (например, fsck) и устранить выявленные дефекты.

3. Проверить состояние жестких дисков при помощи специальной утилиты из состава ОС (например, smartctl или hdparm) и устранить выявленные дефекты.

4. Убедиться, что на жестком диске имеется свободное пространство для размещения файлов СЗИ НСД в объеме 4,6 Гб, 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».

5. Перед началом установки убедиться, что отключена блокировка экрана. Установка системы защиты должна выполняться непрерывно, так как процедура установки включает в себя замену PAM-модуля, при блокировке экрана авторизация станет невозможной.

6. Закрыть все запущенные приложения, так как установка системы защиты потребует принудительной перезагрузки.

7. На время установки СЗИ отключить автоматическое обновление ОС.

Внимание! До установки СЗИ НСД необходимо вручную отключить SELinux.

1. Открыть файл */etc/selinux/config* с правами суперпользователя (root).
2. В файле */etc/selinux/config* заменить строку *SELINUX=enforcing* на *SELINUX=disabled*.
3. Выполнить перезагрузку ОС.

До установки СЗИ НСД для Debian, Ubuntu, Astra Linux, Альт Рабочая Станция необходимо в терминале выполнить команду:

apt-get update

До установки СЗИ НСД для CentOS, Red Hat Enterprise Linux, Fedora, РЕД ОС, ROSA Enterprise Linux Desktop/Server необходимо в терминале выполнить команду:

yum repolist ; yum makecache.

2.3 Установка системы защиты

Следует обратить внимание, что после начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе либо смены пользователя в текущем.

Графическая оболочка администрирования устанавливается отдельно от СЗИ НСД. Установку СЗИ НСД и графической консоли необходимо проводить от имени пользователя с правами, аналогичными правам администратора (*root*) на данном ТС.

Во время установки СЗИ НСД устанавливается также программа по созданию сертификатов OpenSSL. Использование программы описано в разделе Управление сертификатами системы защиты.

Внимание! Если во время установки СЗИ НСД Dallas Lock Linux был запущен сервис ssh, то после выполнения установки СЗИ НСД сервис ssh необходимо остановить.

Для остановки сервиса ssh необходимо выполнить команды:

systemctl stop ssh

systemctl disable ssh

Внимание! Для возможности удаленного управления СЗИ НСД необходимо выполнить дополнительную настройку Firewall Linux, открыв порт 13133.

Для установки СЗИ НСД необходимо выполнить следующие действия:

1. Скопировать с установочного диска из каталога в домашний каталог пользователя файл «*dllx-<номер сборки>.run*».

2. Проверить, является ли файл «*dllx-<номер сборки>.run»* исполняемым, с помощью команды *ls –l.*

Пример:

ls -l <enter>

rw-rw---- отображаются последовательно без пробелов флаги владельца, флаги группы, флаги всех остальных пользователей. В данном примере файл не является исполняемым ни для владельца, ни для группы, ни для всех остальных пользователей.

Если файл не является исполняемым, необходимо ввести команду *chmod a +x dllx-<номер сборки>.run;*

Пример:

chmod a+x dllx-<номер сборки>.run <enter> с помощью этой команды файл становится исполняемым для его владельца.

3. Запустить файл командой *./dllx-<номер сборки>.run*, в качестве атрибута к которой можно указать номер лицензии.

Пример:

./dllx-<номер сборки>.run 0-0000-0000

Примечание. Если не указать номер лицензии при запуске скрипта, он будет запрошен во время процесса установки.

В качестве атрибутов к команде *./dllx-<номер сборки>.run* можно указывать следующие:

Таблица 1

Атрибут	Описание
--help	Вывод на экран списка атрибутов с подсказками **Пример:** *./dllx-<номер сборки>.run --help <enter>*
--info	Печать встроенной информации: заголовок, целевой каталог по умолчанию, встроенный скрипт
--lsm	Данный атрибут не используется в процессе установки СЗИ НСД
--list	Вывод на экран списка файлов в архиве
--check	Проверка целостности архива

Атрибут	Описание
--confirm	Спросить перед запуском встроенного скрипта
--quiet	Не печатать ничего кроме сообщений об ошибках
--accept	Принять номер лицензии
--noexec	Не запускать встроенный скрипт
--keep	Не удалять данные о целевой директории после выполнения встроенного скрипта
--noprogress	Не показывать прогресс в процессе декомпрессии
--nox11	Данный атрибут не используется в процессе установки СЗИ НСД
--nochown	Не давать доступ к распакованным файлам текущему пользователю
--nodiskspace	Не проверять доступное место на диске
--target dir	Извлечь непосредственно в целевую директорию (по абсолютной или относительной ссылке). Этот каталог может быть подвергнут рекурсивной обработке (см. *nochown*)
--tar arg1 [arg2 ...]	Доступ к содержимому архива через команду *tar*. Во встроенный скрипт будут переданы следующие аргументы
--kvers4	Установочному скрипту будет передана инструкция — использовать 4 версию ядра ОС. При этом, вместо стандартной версии ядра ОС, которая устанавливается по умолчанию, будет установлена указанная версия ядра ОС

Для защиты от несанкционированного изменения параметров загрузки на загрузчик установлен пароль.

1. Задание пароля[2] загрузчика во время установки СЗИ НСД.

Чтобы задать пароль загрузчика при установке, необходимо ввести пароль в качестве аргумента команды запуска установочного скрипта:

./dllx-<номер сборки>.run -- --bootpass=<пароль загрузчика> <enter>

или

./dllx-<номер сборки>.run <номер лицензии СЗИ НСД> --bootpass=<пароль загрузчика> <enter>

Если при установке СЗИ НСД не ввести пароль, будет установлен пароль по умолчанию — *dlladmin*[3].

2. Смена пароля[2] загрузчика после установки СЗИ НСД.

Для смены пароля необходимо:

2.1 запустить программу grub-mkpasswd-pbkdf2;

2.2 дважды ввести новый пароль загрузчика. Программа выдаст хэш нового пароля;

2.3 открыть файл /etc/grub.d/00_dllx_password, найти строку *password_pbkdf2* и заменить хэш старого пароля на новый;

2.4 сохранить файл.

Примечание. Для смены логина необходимо в файле /etc/grub.d/00_dllx_password найти строку *set superusers="dlladmin"* и заменить *dlladmin* на новый логин.

Информацию о ходе процесса установки можно увидеть в файле install.log, который создается при установке DLL в папке, в которой находится установочный файл install.sh.

После выполнения всех вышеуказанных действий необходимо выполнить перезагрузку ТС.

[2] Необходимо обладать правами суперпользователя (*root*).
[3] Также будет установлен логин по умолчанию — *dlladmin*.

Внимание! В случае возникновения ошибки «Could not connect to session bus», не позволяющей зайти в систему, используя графическую оболочку, после установки СЗИ НСД Dallas Lock Linux на ОС Альт 8.2, необходимо выполнить вход через терминал от имени пользователя root или учетной записи, имеющей право повышать привилегии до root, и повысить ей привилегии до root, после чего выполнить команду *apt-get remove ConsoleKit2 ConsoleKit2-x11.*

2.3.1 Установка графической оболочки администрирования

Установка графической оболочки администрирования в операционных системах на базе Linux

С установочного диска необходимо скопировать в домашний каталог пользователя файл *«dllx-<номер сборки>-gui.run»* и запустить его, выполнив команду *./dllx-<номер сборки>-gui.run*.

Пример:

./dllx-<номер сборки>-gui.run <enter>

Установка графической консоли не требует перезагрузки ТС.

Установка графической оболочки администрирования в операционных системах на базе Windows

Для установки графической оболочки администрирования в ОС на базе Windows необходимо запустить файл *«win_gui_<номер сборки>.exe»*.

Примечание. Графическая оболочка администрирования СЗИ НСД в ОС на базе Windows поддерживает 64-битные версии ОС Windows:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server).

После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге инсталляции предоставляется возможность отмены инсталляции с возвратом сделанных изменений с помощью кнопки «Отмена». Выполнение следующего шага инсталляции выполняется с помощью кнопки «Далее».

2.4 Удаление системы защиты

Для удаления СЗИ НСД необходимо обладать правами администратора операционной системы (*root*) на данном ТС.

Для отключения механизмов защиты и удаления СЗИ НСД необходимо запустить исполняемый файл uninstall.sh, который расположен в директории */dllx/uninstall*, в качестве атрибутов указав логин и пароль учетной записи администратора СЗИ НСД *dlladmin* (по умолчанию пароль администратора СЗИ НСД — *dlladmin*).

Пример:

sh /dllx/uninstall/uninstall.sh dlladmin dlladmin <enter>

Примечание. В случаях, когда к СЗИ НСД невозможно подключиться, используя учетные данные администратора СЗИ НСД, необходимо передать в качестве атрибута скрипту uninstall.sh ключ *--force*. Затем нужно подтвердить принудительное удаление СЗИ НСД, ответив на соответствующий запрос. Логин и пароль для аутентификации использовать при вызове скрипта uninstall.sh не нужно.

2.4.1 Удаление системы защиты с помощью консольной оболочки администрирования

Удалить СЗИ НСД также можно с помощью управляющих команд консольной оболочки администрирования. Для этого необходимо выполнить следующие шаги:

1. Выполнить команду *ishl* и авторизоваться в консольной оболочке администрирования.

2. Выполнить команду *services*, после выполнения команды система перейдет в раздел *svc*.

3. В разделе *svc* выполнить ввод команды *uninstall* с атрибутами *--login* и *--password* (в качестве атрибутов указывается логин и пароль того пользователя, под которым была выполнена авторизация в консольной оболочке администрирования).

4. Завершить процедуру удаления с помощью команды *execute.*

Пример:

services <enter>

uninstall <enter>

login dlladmin <enter>

password dlladmin <enter>

execute <enter>

После успешного удаления СЗИ НСД необходимо выполнить перезагрузку ТС.

2.4.2 Удаление графической оболочки администрирования

Чтобы удалить графическую оболочку СЗИ НСД, необходимо запустить скрипт */dllx/uninstall/uninstall_gui.sh*.