

**СИСТЕМА ЗАЩИТЫ
ИНФОРМАЦИИ**

Dallas Lock Linux



Руководство администратора
по обновлению изделия

СОДЕРЖАНИЕ

1	ОПИСАНИЕ И РАБОТА.....	3
2	ОБНОВЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ	5
2.1	Обновление системы защиты	5
2.2	Подготовка к установке	7
2.3	Установка системы защиты	8
2.4	Удаление системы защиты.....	13

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 Linux¹:

- Альт Рабочая Станция 9.0 x64 (версия ядра СЗИ НСД 4.19);
- Альт Рабочая Станция 9.1 x64 (версия ядра СЗИ НСД 5.10);
- Альт Рабочая Станция 9.2 x64 (версия ядра СЗИ НСД 5.10);
- Альт Рабочая Станция 10.0 x64 (версия ядра СЗИ НСД 5.10);
- Альт Рабочая Станция 10.1 x64 (версия ядра СЗИ НСД 5.10);
- Astra Linux Common Edition (Орел) 2.12.x x64 (версия ядра СЗИ НСД 4.19);
- Astra Linux Common Edition (Орел) 2.12.x x64 (версия ядра СЗИ НСД 5.10);
- Debian 10 x64 (версия ядра СЗИ НСД 5.10);
- Debian 11 x64 (версия ядра СЗИ НСД 5.10);
- CentOS 7 x64 (версия ядра СЗИ НСД 3.16);
- Red Hat Enterprise Linux 7 x64 (версия ядра СЗИ НСД 3.16);
- Ubuntu 18.04 x64 (версия ядра СЗИ НСД 4.19);
- Ubuntu 20.04 x64 (версия ядра СЗИ НСД 5.10);
- РЕД ОС 7.1, 7.2 Муром x64 (версия ядра СЗИ НСД 4.19);
- РЕД ОС 7.3 Муром x64 (версия ядра СЗИ НСД 5.10);
- ROSA Enterprise Linux Desktop/Server 7.3 x64 (версия ядра СЗИ НСД 5.10).

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 файловой системы (это касается всех дистрибутивов).

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

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.

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

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

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

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.

Поддерживаемые внешние устройства:

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

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.

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.

Для защищенных ТС СЗИ НСД Dallas Lock Linux предыдущей версией 4550 реализована возможность обновления системы защиты на текущую 3.25.21 с сохранением действующих настроек и экспортом журналов аудита.



Внимание! Перед выполнением процедуры обновления необходимо убедиться в том, что защищаемое ТС находится под управлением поддерживаемой ОС.

Для обновления системы защиты:

1. Скопировать с установочного диска из каталога в домашний каталог пользователя файл «*dllx-
<номер сборки>.run*». Не удаляя предыдущую версию дистрибутива СЗИ НСД Dallas Lock Linux.

2. Проверить является ли файл «*dllx-<номер сборки>.run*» исполняемым, с помощью команды *ls -l*. Если файл не является исполняемым, необходимо ввести команду *chmod a+x dllx-<номер сборки>.run*. С помощью данной команды файл становится исполняемым для его владельца.

3. Запустить файл командой *./dllx-<номер сборки>.run*, в качестве атрибута необходимо указать параметры, представленные в Таблица 1.

Пример:

```
./dllx-<номер сборки>.run -- --upgrade --admin-login=dlladmin --admin-pass=dlladmin --not-export X-XXX-XXXX
```

4. После деинсталляции системы защиты предыдущей версии 4550 ТС уйдет в автоматическую перезагрузку.

После выполнения деинсталляции системы защиты и перезагрузки будет проходить процедура установки новой версии. Установка новой версии происходит в фоновом режиме. Предоставлена возможность авторизации в терминальную сессию для просмотра процедуры обновления на текущую версию 3.25.21, для этого необходимо выполнить команду *tail -f /dllx-setup-*.log*.

По завершению успешного обновления СЗИ, система автоматически уйдет в перезагрузку. В случае возникновения ошибок установки, автоматической перезагрузки происходить не будет. Для определения причины возникновения ошибки обновления необходимо авторизоваться в системе и выполнить команду *tail -f /dllx-setup-*.log*.

Таблица 1

№	Параметр	Описание
1	<i>--upgrade</i>	Запуск обновления ранее установленной системы защиты Dallas Lock Linux, версия сборки 4550. При указании данного атрибута будет осуществлена идентификация и деинсталляция Dallas Lock Linux версии 4550
2	<i>--admin-login=<login></i>	Ввод логина Администратора СЗИ НСД при запуске обновления ранее установленной системы защиты Dallas Lock Linux версии 4550. Обязательный параметр
3	<i>--admin-pass=<password></i>	Ввод пароля Администратора СЗИ НСД при запуске обновления ранее установленной системы защиты Dallas Lock Linux версии 4550. Обязательный параметр
4	<i>--not-export</i>	Команда для отмены экспорта журналов. Журналы ранее установленной версии Dallas Lock Linux не будут экспортированы в процессе обновления системы защиты. Обязательный параметр
5	<i>--export-pdf</i>	Команда экспорта журнала в формат PDF. Журналы ранее установленной версии Dallas Lock Linux будут экспортированы в процессе обновления системы защиты в формате PDF. Обязательный параметр
6	<i>--export-ods</i>	Команда экспорта журнала в формат ODS. Журналы ранее установленной версии Dallas Lock Linux будут экспортированы в процессе обновления системы защиты в формате ODS. Обязательный параметр
7	<i>--export-xml</i>	Команда экспорта журнала в формат XML. Журналы ранее установленной версии Dallas Lock Linux будут экспортированы в процессе обновления системы защиты в формате XML. Обязательный параметр
8	<i>X-XXXX-XXXX</i>	Номер лицензии при запуске обновления системы защиты Dallas Lock Linux. Обязательный параметр



Примечание. Путь к экспортируемым журналам по умолчанию установлен `/dllx/backup/ik2_journals`.

Реализована возможность обновления системы защиты с предыдущей версии 4550 на текущую 3.25.21 с сохранением действующих настроек и экспортом журналов аудита с помощью Единого центра управления Dallas Lock (ЕЦУ Dallas Lock), управление которым осуществляется отдельным приложением «Консоль ЕЦУ».

Для этого в окне «Мастер удаленной установки Dallas Lock Linux» в дополнительные ключи установки необходимо ввести параметры, представленные в Таблица 1. С подробным описанием ЕЦУ Dallas Lock можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock ПФНА.501410.002 ИЗ.

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 суперпользователь (*root*) будет заблокирован до смены пароля средствами СЗИ. В дальнейшем пароль суперпользователя (*root*) можно задать только средствами СЗИ НСД.



Примечание. Рекомендуется до или сразу после установки СЗИ НСД задать пароль для суперпользователя (*root*). В случае нарушения аппаратной целостности и при этом отсутствия пароля суперпользователя (*root*), не будет предоставлена возможность авторизоваться в ОС ни одному зарегистрированному пользователю ОС, в том числе суперпользователю (*root*).

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 корневом каталоге жесткого диска имеется свободное пространство для размещения файлов СЗИ НСД в объеме 9 Гб:
 - 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.



Внимание! 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.

5. Перед началом установки убедиться, что отключена блокировка экрана. Установка системы защиты должна выполняться непрерывно, так как процедура установки включает в себя замену ПАМ-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.



Примечание. При замене AppArmor на SELinux для ОС Ubuntu корректная установка СЗИ НСД Dallas Lock Linux не гарантируется.

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, 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.

Номер лицензии указан на коробке компакт-диска с дистрибутивом Dallas Lock Linux.

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

Таблица 2

Атрибут	Описание
<i>--help</i>	Вывод на экран списка атрибутов с подсказками Пример: <i>./dllx-<номер сборки>.run --help <enter></i>
<i>--info</i>	Печать встроенной информации: заголовков, целевой каталог по умолчанию, встроенный скрипт
<i>--lsm</i>	Данный атрибут не используется в процессе установки СЗИ НСД
<i>--list</i>	Вывод на экран списка файлов в архиве
<i>--check</i>	Проверка целостности архива
<i>--confirm</i>	Спросить перед запуском встроенного скрипта
<i>--quiet</i>	Не печатать ничего кроме сообщений об ошибках
<i>--accept</i>	Принять номер лицензии
<i>--noexec</i>	Не запускать встроенный скрипт
<i>--noexec-cleanup</i>	Не запускать встроенный скрипт очистки
<i>--keep</i>	Не удалять данные о целевой директории после выполнения встроенного скрипта
<i>--noprogess</i>	Не показывать прогресс в процессе декомпрессии

Атрибут	Описание
<code>--nox11</code>	Данный атрибут не используется в процессе установки СЗИ НСД
<code>--nochown</code>	Не давать доступ к распакованным файлам текущему пользователю
<code>--chown</code>	Рекурсивно назначить доступ к распакованным файлам текущему пользователю
<code>--nodiskspace</code>	Не проверять доступное место на диске
<code>--target dir</code>	Извлечь непосредственно в целевую директорию (по абсолютной или относительной ссылке). Этот каталог может быть подвергнут рекурсивной обработке (см. <i>nochown</i>)
<code>--tar arg1 [arg2 ...]</code>	Доступ к содержимому архива через команду <i>tar</i> . Во встроенный скрипт будут переданы следующие аргументы
<code>--kvers4</code>	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
<code>--kvers5</code>	Установочному скрипту будет передана инструкция — использовать 5.10 версию ядра ОС. При этом, вместо стандартной версии ядра ОС, которая устанавливается по умолчанию, будет установлена указанная версия ядра ОС
<code>--arm-name=name</code>	Указать под каким именем будет зарегистрирован АРМ в Домене безопасности ЕЦУ
<code>--ucc-addr=address</code>	Указать IP-адрес или сетевое имя компьютера Домена безопасности ЕЦУ
<code>--ucc-key=key</code>	Указать ключ Домена безопасности ЕЦУ
<code>--grub-pass=password</code>	Установить пароль GRUB для суперпользователя. По умолчанию — <i>dlladmin</i>
<code>--just-check</code>	Не устанавливать, а только проверить поддержку хост-системы
<code>--upgrade</code>	Запуск обновления установленной системы защиты Dallas Lock Linux. При указании данного атрибута будет осуществлена идентификация и деинсталляция Dallas Lock Linux, версии сборки 4550. Подробнее — в разделе Обновление системы защиты Error! Reference source not found.
<code>--admin-login=login</code>	Ввод логина Администратора СЗИ НСД при запуске обновления установленной системы защиты Dallas Lock Linux, версия сборки 4550
<code>--admin-login=password</code>	Ввод пароля Администратора СЗИ НСД при запуске обновления установленной системы защиты Dallas Lock Linux, версия сборки 4550
<code>X-XXXX-XXXX</code>	Номер лицензии при запуске инсталляции системы защиты Dallas Lock Linux

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

1. Задание пароля³ 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*⁴.

2. Смена пароля³ загрузчика после установки СЗИ НСД.

Для смены пароля загрузчика GRUB необходимо:

2.1 запустить программу `grub-mkpasswd-pbkdf2`;

³ Необходимо обладать правами суперпользователя (*root*).

⁴ Также будет установлен логин по умолчанию — *dlladmin*.

- 2.2 дважды ввести новый пароль загрузчика. Программа выдаст хэш нового пароля нового пароля: `grub.pbkdf2.sha512.10000...`;
- 2.3 создать для пользователя root dsb-правило **arwxmusl** для каталога `/boot/grub` выполнив следующие команды в консольной оболочке администрирования:
- ```
ishl <enter>
resources <enter>
files <enter>
dsb <enter>
set-rights-user root arwxmusl /boot/grub <enter>
```
- 2.4 открыть файл `/etc/grub.d/40_custom`, и добавить в него логин и сгенерированный новый пароль:
- ```
set-superusers="dlladmin"
password_pbkdf2 root grub.pbkdf2.sha512.10000...
```
- 2.5 сохранить файл;
- 2.6 поскольку файл `/etc/grub.d/40_custom` содержит хэш пароля, то рекомендуется запретить его чтение и изменения всеми, кроме пользователя root, выполнив следующую команду:
- ```
sudo chmod 771 /etc/grub.d/40_custom
```
- 2.7 запустить программу для создания нового конфигурационного файла загрузчика, выполнив следующую команду:
- ```
sudo grub-mkconfig -o /boot/grub/grub.cfg
```
- 2.8 в результате, пароль загрузчика будет заменен на новый.

Для смены пароля загрузчика GRUB2 необходимо:



Примечание. Для систем с UEFI файл конфигурации GRUB2 располагается по адресу `/boot/efi/EFI/<имя системы>/grub.cfg`. Следовательно, создание нового конфигурационного файла загрузчика будет выглядеть следующим образом: `grub2-mkconfig -O /boot/efi/EFI/<имя системы>/grub.cfg`. Также стоит учесть, что и dsb-правило для пользователя root следует создавать для каталога `/boot/efi/EFI/<имя системы>`.

- 2.9 запустить программу `grub2-setpassword`;
- 2.10 дважды ввести новый пароль загрузчика. Программа выдаст хэш нового пароля загрузчика GRUB в файле `/boot/grub2/user.cfg`, который можно посмотреть с помощью команды `cat`:
- ```
cat /boot/grub2/user.cfg
```
- 2.11 создать для пользователя root dsb-правило **arwxmusl** для каталога `/boot/grub2` выполнив следующие команды в консольной оболочке администрирования:
- ```
ishl <enter>
resources <enter>
files <enter>
dsb <enter>
set-rights-user root arwxmusl /boot/grub2 <enter>
```
- 2.12 открыть файл `/etc/grub.d/40_custom`, и добавить в него логин и сгенерированный новый пароль:
- ```
set-superusers="dlladmin"
password_pbkdf2 root grub.pbkdf2.sha512.10000...
```
- 2.13 сохранить файл;
- 2.14 поскольку файл `/etc/grub.d/40_custom` содержит хэш пароля, то рекомендуется запретить его чтение и изменения всеми, кроме пользователя root, выполнив следующую команду:
- ```
sudo chmod 771 /etc/grub.d/40_custom
```
- 2.15 запустить создание нового конфигурационного файла загрузчика, выполнив следующую команду:
- ```
grub2-mkconfig -o /boot/grub2/grub.cfg
```
- 2.16 в результате, пароль загрузчика будет заменен на новый.

**Внимание!** После завершения процедуры смены пароля загрузчика рекомендуется удалить dsb-правило для каталога `/boot/grub` (или `/boot/grub2`).



**Пример:**

```
ishl <enter>
resources <enter>
files <enter>
rm-rights-user root /boot/grub <enter>
```



**Примечание.** Для смены логина необходимо в строке `set superusers="dlladmin"` 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 ТС уйдет в автоматическую перезагрузку. Для отмены автоматической перезагрузки ТС после успешной установки необходимо перед запуском файла `./dllx-<номер сборки>.run`, в качестве атрибута указать `--no-reboot`.



**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-gui-<номер сборки>.run`» и запустить его, выполнив команду `./dllx-gui-<номер сборки>.run`.

**Пример:**

```
./dllx-gui-<номер сборки>.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 «`dllx-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);



- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

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 *dllx-remove.sh*, который расположен в директории */dllx/remove*, в качестве атрибутов указав логин и пароль учетной записи администратора СЗИ НСД *dlladmin* (по умолчанию пароль администратора СЗИ НСД — *dlladmin*).

### Пример:

```
/dllx/remove/dllx-remove.sh dlladmin dlladmin<enter>
```



**Примечание.** В случаях, когда к СЗИ НСД невозможно подключиться, используя учетные данные администратора СЗИ НСД, необходимо запустить исполняемый файл *run-dllx-remove.sh*.

### Пример:

```
/dllx/remove/run-dllx-remove.sh <enter>
```

Логин и пароль для аутентификации использовать при вызове скрипта *run-dllx-remove.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 встроенных сервисов *services*.
3. В разделе *services* выполнить ввод команды *uninstall*, затем последовательно ввести *login* и *password* (требуется указать логин и пароль Администратора СЗИ НСД Dallas Lock Linux).

### Пример:

```
services <enter>
uninstall <enter>
login <login> <enter>
password <password> <enter>
execute <enter>
```




**Примечание.** Для отслеживания процесса удаления СЗИ НСД по лог-файлу в режиме реального времени, необходимо выполнить команду *tail -f /dllx-remove-<дата>-<время>.log*.

### 2.4.2 Удаление графической оболочки администрирования

Чтобы удалить графическую оболочку СЗИ НСД, необходимо запустить исполняемый файл *uninstall.sh*, который расположен в директории */dllx-gui/bin*.

### Пример:

```
/dllx-gui/bin/uninstall.sh <enter>
```

Также процесс инсталляции графической оболочки СЗИ НСД можно запустить из информационного окна «О программе», вызвав его из списка дополнительных функций кнопки главного меню  (см. Рисунок 1).

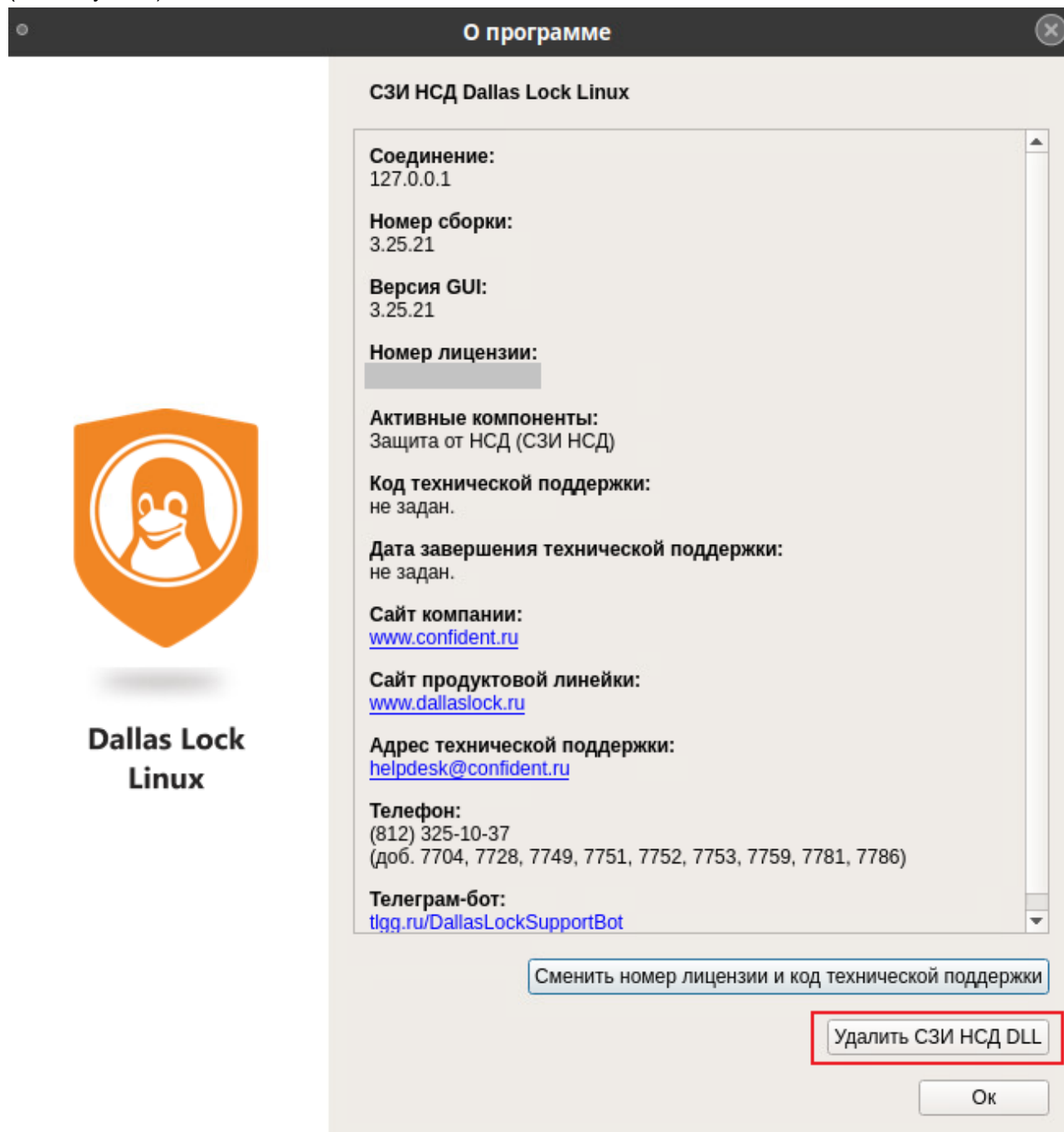


Рисунок 1. Кнопка «Удалить СЗИ НСД DLL»