УТВЕРЖДЕН
ПФНА.501410-02 32 01-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА Dallas Lock Linux

Руководство системного программиста (администратора)

ПФНА.501410-02 32 01

Листов 22

2016 г.

Аннотация

Настоящее руководство системного программиста (администратора) распространяются на изделие «Система защиты информации от несанкционированного доступа Dallas Lock Linux» (далее по тексту - изделие).

В состав изделия входит сертифицированное программное обеспечение (ПО) «Система защиты информации от несанкционированного доступа Dallas Lock Linux» (далее по тексту – «СЗИ НСД» или «Dallas Lock Linux»).

Документ предназначается для системных администраторов или других сотрудников организации, осуществляющих установку СЗИ НСД и поддерживающих её в рабочем состоянии.

Документ выполнен в соответствии с ГОСТ 19.503-79 «Руководство системного программиста. Требования к содержанию и оформлению».

Содержание

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

1.1.1. 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).

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

1.2. Программные средства, обеспечивающие выполнение СЗИ НСД

1.1.1. 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:

- 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).

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

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

1.3. Технические средства, обеспечивающие выполнение СЗИ НСД

1.3.1. Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

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

1.1.2. Поддерживаемые внешние устройства:

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

2. СТРУКТУРА СЗИ НСД

2.1. В соответствии с ТУ (ПФНА.501410.002 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 процессов;
  - подсистема контроля гарантированной очистки памяти.
- подсистема контроля внешних систем:
  - подсистема контроля разграничения доступа к блочным и беспроводным устройствам;
  - подсистема контроля печати.
- подсистема анализа:
  - подсистема журналирования;
  - подсистема аудита.
- подсистема самотестирования функционала.

3. УСТАНОВКА И НАСТРОЙКА

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.

После установки СЗИ при обновлении ОС необходимо выбрать ядро, которое было выбрано до установки СЗИ НСД, в противном случае работоспособность СЗИ НСД не гарантируется.

3.1. 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 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.

Подготовка к установке должна осуществляться только из сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).

3.1.1. Подготовка к установке (ОС CentOS 7.0)

Необходимо учитывать, что директория “/usr” не может быть на отдельном от корневого каталога “/” разделе ФС.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия.

1) После начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе, либо смены пользователя в текущем. Установку необходимо проводить только из сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).
2) Если на ТС уже установлена система защиты, её необходимо удалить.
3) Рекомендуется проверить состояние файловой системы ПК при помощи специальной утилиты из состава ОС (например, fsck), и устранить выявленные дефекты.
4) Рекомендуется проверить состояние жестких дисков.
5) Необходимо убедиться, что на жёстком диске имеется необходимое свободное пространство для установки системы защиты (1500 МБ).

6) Рекомендуется перед началом установки убедиться, что блокировка экрана отключена, и выполнить процедуру установки непрерывно, так как процедура установки включает в себя замену PAM-модуля (в случае блокировки экрана станет невозможной авторизация).

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

8) В консоли (терминале) ОС выполнить команды:

   systemctl stop firewalld

   systemctl disable firewalld

9) Изменить режим работы системы принудительного контроля доступа «SElinux». Для этого необходимо отредактировать файл «/etc/selinux/config», в котором необходимо заменить строчку «SELINUX=enforcing» на «SELINUX=permissive».

10) Выполнить команду *setenforce 0*

11) Выполнить команду *getenforce* (убедиться, что команда вернула текущее значение политики – «permissive»).

12) В консоли (терминале) ОС выполнить команды:

   systemctl start cups

   killall packagekitd

13) Скопировать с установочного диска пакет «epel-release-7-5.noarch.rpm» с настройками для подключения репозитория EPEL и выполнить установку *yum localinstall –y epel-release-7-5.noarch.rpm*

14) В консоли (терминале) ОС выполнить команду:

   yum repolist

15) В консоли (терминале) ОС выполнить команду:

   yum -y remove rsyslog

Подготовка к установке (Red Hat Enterprise Linux Server 7.0)

Необходимо учитывать, что директория “/usr” не может быть на отдельном от корневого каталога “/” разделе ФС.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия.

1) После начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе, либо смены пользователя в текущем. Установку необходимо проводить только из

сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).

2) Если на ТС уже установлена система защиты, её необходимо удалить.

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

4) Рекомендуется проверить состояние жестких дисков.

5) Необходимо убедиться, что на жёстком диске имеется необходимое свободное пространство для установки системы защиты (1500 МБ).

6) Рекомендуется перед началом установки убедиться, что блокировка экрана отключена, и выполнить процедуру установки непрерывно, так как процедура установки включает в себя замену PAM-модуля (в случае блокировки экрана станет невозможной авторизация).

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

8) В консоли (терминале) ОС выполнить команды:

   systemctl stop firewalld

   systemctl disable firewalld

9) Изменить режим работы системы принудительного контроля доступа «SElinux». Для этого необходимо отредактировать файл «/etc/selinux/config», в котором необходимо заменить строчку «SELINUX=enforcing» на «SELINUX=permissive».

10) Выполнить команду *setenforce 0*

11) Выполнить команду *getenforce* (убедиться, что команда вернула текущее значение политики – «permissive»).

12) В консоли (терминале) ОС выполнить команды:

   systemctl start cups

   killall packagekitd

13) Скопировать с установочного диска пакет «epel-release-7-5.noarch.rpm» с настройками для подключения репозитория EPEL и выполнить установку *yum localinstall –y epel-release-7-5.noarch.rpm*

14) В консоли (терминале) ОС выполнить команду:

   yum repolist

15) В консоли (терминале) ОС выполнить команду:

yum -y remove rsyslog

Подготовка к установке (Fedora 20)

Необходимо учитывать, что директория “/usr” не может быть на отдельном от корневого каталога “/” разделе ФС.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия.

1) После начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе, либо смены пользователя в текущем. Установку необходимо проводить только из сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).
2) Если на ТС уже установлена система защиты, её необходимо удалить.
3) Рекомендуется проверить состояние файловой системы ПК при помощи специальной утилиты из состава ОС (например, fsck), и устранить выявленные дефекты.
4) Рекомендуется проверить состояние жестких дисков.
5) Необходимо убедиться, что на жёстком диске имеется необходимое свободное пространство для установки системы защиты (1500 МБ).
6) Рекомендуется перед началом установки убедиться, что блокировка экрана отключена, и выполнить процедуру установки непрерывно, так как процедура установки включает в себя замену PAM-модуля (в случае блокировки экрана станет невозможной авторизация).
7) Закрыть все запущенные приложения, так как установка системы защиты потребует принудительной перезагрузки.
8) В консоли (терминале) ОС выполнить команды:

   systemctl stop firewalld

   systemctl disable firewalld
9) Изменить режим работы системы принудительного контроля доступа «SElinux». Для этого необходимо отредактировать файл «/etc/selinux/config», в котором необходимо заменить строчку «SELINUX=enforcing» на «SELINUX=permissive».
10) Выполнить команду *setenforce 0*
11) Выполнить команду *getenforce* (убедиться, что команда вернула текущее значение политики – «permissive»).

12) В консоли (терминале) ОС выполнить команды:

systemctl start cups

systemctl stop packagekit

Подготовка к установке (OpenSUSE 12.3)

Необходимо учитывать, что директория “/usr” не может быть на отдельном от корневого каталога “/” разделе ФС.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия.

1) После начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе, либо смены пользователя в текущем. Установку необходимо проводить только из сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).
2) Если на ТС уже установлена система защиты, её необходимо удалить.
3) Рекомендуется проверить состояние файловой системы ПК при помощи специальной утилиты из состава ОС (например, fsck), и устранить выявленные дефекты.
4) Рекомендуется проверить состояние жестких дисков.
5) Необходимо убедиться, что на жёстком диске имеется необходимое свободное пространство для установки системы защиты (1500 МБ).
6) Рекомендуется перед началом установки убедиться, что блокировка экрана отключена, и выполнить процедуру установки непрерывно, так как процедура установки включает в себя замену PAM-модуля (в случае блокировки экрана станет невозможной авторизация).
7) Закрыть все запущенные приложения, так как установка системы защиты потребует принудительной перезагрузки.
8) Подключить официальные сетевые репозитории для zypper:

   http://download.opensuse.org/distribution/12.3/repo/oss/

   http://download.opensuse.org/distribution/12.3/repo/non-oss/

   http://download.opensuse.org/update/12.3/

   http://download.opensuse.org/update/12.3-non-oss/

   Подключение выполняется из-под учётной записи «root» командой

   zypper ar <ссылка на репозиторий> <псевдоним репозитория>

(также, можно использовать опцию -c для задания более удобного названия репозитория, иначе название репозитория будет присвоено по соответствующей ему ссылке).

Помимо добавления сетевых репозиториев, необходимо удалить либо отключить репозиторий установочного диска. Удаление репозитория из списка производится от имени учётной записи «root» командой

zypper rr <ссылка на репозиторий | название репозитория | алиас (псевдоним) | порядковый номер в списке репозиториев>.

Отключение репозитория производится из-под учётной записи «root» командой

zypper mr -d <ссылка на репозиторий | название репозитория | алиас (псевдоним) | порядковый номер в списке репозиториев>

Просмотреть список используемых репозиториев можно командой *zypper lr*.

Команда *zipper lr* должна вывести список подключенных в ОС репозиториев в виде таблицы.

В указанном списке должны отображаться следующие репозитории:

- repo-non-oss;
- repo-oss;
- repo-update;
- repo-update-non-oss.

Указанные репозитории должны иметь статус «Yes» в столбце «Enabled», остальные подключенные репозитории должны иметь статус «No».

9) В консоли (терминале) ОС выполнить команды:

   zypper remove rsyslog

   systemctl stop SuSEfirewall2

   systemctl disable SuSEfirewall2

10) Запустить скрипт prepare.sh

11) В консоли (терминале) ОС выполнить команды:

   systemctl enable auditd

   systemctl enable syslog-ng

12) Выполнить перезагрузку из сеанса суперпользователя («root»).

Подготовка к установке (ОС Debian 7.8 (systemd))

Необходимо учитывать, что директория “/usr” не может быть на отдельном от корневого каталога “/” разделе ФС.

Перед установкой СЗИ НСД необходимо выполнить нижеперечисленные действия.

1) Рекомендуется проверить состояние жестких дисков.
2) Необходимо убедиться, что на жёстком диске имеется необходимое свободное пространство для установки системы защиты (1500 МБ).
3) Закрыть все запущенные приложения, так как установка системы защиты потребует принудительной перезагрузки.
4) Запустить установку с DVD-диска «debian-7.8.0-amd64-DVD-1» ОС в режиме «expert install» в минимальной конфигурации (только базовые утилиты без графического окружения, источник пакетов – только DVD, от предложения подключить сетевые репозитории во время установки необходимо отказаться).
5) Выполнить настройку менеджера пакетов: снять выбор с обновлений безопасности и обновлений выпуска.
6) Осуществить выбор устанавливаемого программного обеспечения: выбрать только стандартные системные утилиты и, при необходимости, SSH server.
7) Удалить пакет «rsyslog»: *apt-get remove rsyslog*.
8) С установочного диска DLL скопировать файлы «sources.list.DVD» и «sources.list.NET» в каталог «/etc/apt/».
9) Выполнить команду

   cp /etc/apt/sources.list.NET /etc/apt/sources.list

10) Выполнить команду

    apt-get update

11) Выполнить команду

    apt-get install auditd syslog-ng libpam-cracklib parted cups rsync attr mc

12) В файле «/etc/apt/sources.list» раскомментировать строку (убрать символ # в начале строки), содержащую слово «backports».
13) Выполнить команду *apt-get update*.
14) Выполнить команду *apt-get -t wheezy-backports install systemd udev libgnutls-deb0-28 tmux*
15) Выполнить команду *apt-get install vlock*.

16) Выполнить команду

cp /etc/apt/sources.list.DVD /etc/apt/sources.list

17) Выполнить команду *apt-cdrom add.*

18) Выполнить команду *apt-get update.*

19) Выполнить команду

apt-get install x-window-system-core gdm3 gnome-screensaver gnome-terminal iceweasel

20) Перезагрузить компьютер командой *reboot.*

21) Выполнить команду

cp /etc/apt/sources.list.NET /etc/apt/sources.list

22) В файле «/etc/apt/sources.list» раскомментировать строку (убрать символ # в начале строки), содержащую слово «backports».

23) Выполнить команду *apt-get update.*

24) Убедиться, что включен демон аудита командой

systemctl status auditd

25) Если выключен, то включить командой *systemctl start auditd,* и включить его загрузку при старте системы командой *systemctl enable auditd*

26) Убедиться что включен демон «syslog» командой

systemctl status syslog-ng

27) Если выключен, то включить командой *systemctl start syslog-ng,* и включить его загрузку при старте системы командой

systemctl enable syslog-ng

28) Убедиться, что включен «демон» печати командой

systemctl status cups

29) Если выключен, то включить командой *systemctl start cups,* и включить его загрузку при старте системы командой *systemctl enable cups*

30) Обратите внимание, что после начала установки СЗИ НСД до перезагрузки ОС отключается возможность авторизации в новом сеансе, либо смены пользователя в текущем. Установку необходимо проводить только из сеанса суперпользователя (обладающего правами администратора («root») на данном ТС).

3.2. Установка системы защиты

Инсталлировать систему защиты на ТС может только пользователь, обладающий правами администратора («root») на данном ТС.

С установочного диска из каталога «DLL» скопировать в домашний каталог пользователя архив «* -local.tar.gz»[1], распаковать, перейти в образовавшийся каталог «local» и запустить установочный скрипт «setup.sh». Если СЗИ НСД устанавливается на ТС, не оснащенное приводом компакт дисков, то можно скопировать с инсталляционного диска на данное ТС необходимые установочные пакеты и установочный скрипт любым удобным способом: через ЛВС, при помощи USB Flash Drive и т.д. Название каталога, в который копируются установочные пакеты и установочный скрипт, должно содержать только латинские символы.

После запуска установочного скрипта, статус установки компонент будет отображаться в консоли (терминале) ОС.

Во время установки СЗИ НСД необходимо ввести действительный номер лицензии продукта (указан в формуляре на изделие). Запрос на ввод номера лицензии будет отображен в системной консоли ОС.

Для ОС Debian 7.8 (systemd) после завершения выполнения установочного скрипта необходимо перейти в каталог, из которого был запущен установочный скрипт setup.sh, а затем командой *dpkg -i isvpd_1.0.0-1_amd64.deb* установить прокси доступа к серверу обновлений.

Для всех поддерживаемых ОС Linux необходимо с установочного диска скопировать dll_sw_cs-1.5.tar.bz2 в отдельный пустой каталог и распаковать командой tar -xjf dll_sw_cs-1.5.tar.bz2 -C <путь к созданному каталогу>. Перейти в каталог, куда был распакован архив и из под учетной записи пользователя root выполнить команды:

./prelink_exclude.sh -f ./cli_files.list

./prelink_exclude.sh -f ./szi_files.list

После выполнения всех вышеуказанных действий по установке необходимо выполнить перезагрузку ТС.

3.1. Удаление

Чтобы осуществить удаление СЗИ НСД, необходимо обладать правами администратора операционной системы («root») на данном ТС.

Перед удалением СЗИ НСД рекомендуется завершить работу всех приложений и сохранить результаты, так как удаление СЗИ НСД потребует перезагрузки ТС.

Во время процедуры удаления модули взаимодействуют с системным

[1] В зависимости от дистрибутива имя архива может отличаться (*-название дистрибутив ОС Linux).

сервисом печати «CUPS», поэтому перед запуском процедуры необходимо проверить статус системного сервиса. Для этого требуется ввести команду systemctl status cups. Значение статуса должно быть «active (running)». В случае иного значения требуется выполнить команду systemctl start cups.

Для отключения механизмов защиты и удаления СЗИ НСД необходимо запустить исполняемый скрипт «uninstaller.sh», который расположен в каталоге дистрибутива СЗИ НСД, который планируется к удалению.

После успешного удаления СЗИ НСД необходимо выполнить перезагрузку ТС.

3.2. Обновление системы защиты

Для ТС, защищенных СЗИ НСД Dallas Lock Linux, возможно обновление до последней сборки Dallas Lock Linux.

Обновление СЗИ НСД Dallas Lock Linux направлено на:

- устранение уязвимостей средства защит информации;

- добавление функции (функций) безопасности средства защиты информации, на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ;

- добавление функции (функций), не влияющих на функции безопасности СЗИ (например, изменение интерфейса СЗИ).

Информация о появление обновленной версии СЗИ НСД отображается на сайте www.dallaslock.ru, с указанием устраненных недостатков и добавленного функционала.

Пользователи СЗИ НСД информируются по электронной почте, с подтверждением получения информации, о выпуске обновлений Dallas Lock Linux, с указанием устраненных недостатков и добавленного функционала.

Также реализован механизм проверки наличия более новых версий СЗИ с использованием консольной оболочки администрирования путем ввода управляющих команд. Для проверки наличия обновления необходимо выполнить следующие действия:

1. выполнить команду *ishl <enter>;*
2. далее войти в раздел управляющих команд «information», выполнив команду *information <enter>;*
3. в разделе «information» выполнить команду *show-version <enter>*. Будет выполнена проверка номера текущей версии и полученного номера актуальной версии СЗИ НСД.

   В случае если доступен сервер обновлений и доступна новая версия СЗИ НСД будет получен ответ вида:

Installed 1.0.0.0 (Release version)

Available 2.0.0.0 (New version)

где 1.0.0.0. и 2.0.0.0 – переменные значения, обозначающие номер версии.

В случае если установленная версия является актуальной, вторая строка (*Available 2.0.0.0 (New version)*) отображаться не будет.

Для проведения обновления 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, с помощью СЗИ НСД. Сверить полученную контрольную сумму с 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»;
4. перед установкой обновлений необходимо удалить установленную ранее версию СЗИ НСД (более подробно см. п. 3.3 «Удаление системы защиты» данного руководства) и выполнить установку СЗИ, используя в качестве дистрибутива скаченный архив (более подробно см. п.3.2 «Установка системы защиты» данного руководства);
5. после установки обновлений необходимо сделать соответствующую отметку в разделе 12 формуляра СЗИ НСД Dallas Lock Linux с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

3.3. Вход в защищенную ОС

Вход в защищенную ОС не отличается от процедуры входа в незащищенную ОС.

Для осуществления входа без использования графической оболочки ОС необходимо ввести логин пользователя.

После корректного ввода логина должно отобразиться предложение ввести пароль пользователя.

Следует обратить внимание, что в случае входа в ОС без использования графической оболочки при вводе пароля символы пароля отображаться

на экране не будут, так же не будут отображаться звездочки или иные символы.

После корректного ввода логина и пароля должна отобразиться строка приветствия.

Более подробная информация содержится в документации к используемой операционной системе.

Следует обратить внимание, что для осуществления входа при помощи графической оболочки ОС, в политике безопасности СЗИ НСД необходимо указать значение максимального допустимого количества сессий пользователей равным или большим 2 (по умолчанию установлено значение «10») или равным 0 (отключение ограничения на максимальное допустимое количество сессий).

3.4. Консольная оболочка администрирования

Управление СЗИ НСД осуществляется посредством консольной оболочки администратора СЗИ НСД путем ввода управляющих команд. Для запуска консольной оболочки необходимо выполнить команду *ishl*.

Для работы в консольной оболочке необходимо в ней авторизоваться.

При первом входе в оболочку администрирования необходимо использовать пароль «dlladmin» администратора СЗИ НСД. По умолчанию вход осуществляется под именем «dlladmin» (учетная запись администратора СЗИ НСД).

Команда запуска *ishl* имеет ряд параметров, которые можно использовать, чтобы изменить параметры подключения, используемые по умолчанию. Список атрибутов приведен в таблице 1.

Таблица 1

№	Команда	Описание
1	-r, --rootca	Путь к корневому сертификату. **Пример:** *ishl –r <путь_к_корневому_ сертификату>*
2	-u, --cert	Путь к пользовательскому сертификату. **Пример:** *ishl –r <путь_к_пользовательскому_сертификату>*
3	-l, --login	Имя пользователя, под учетной запись которого будет производиться вход: *ishl -l <логин_администратора_безопасности>* После успешной авторизации строка приглашения ввода команд будет иметь следующий вид: 127.0.0.1/szi#

		Важно! Необходимо изменить пароль администратора СЗИ НСД. Для этого администратор СЗИ НСД должен последовательно выполнить следующие команды в консольной оболочке администратора: *user-management <enter>* *user-update <enter>* *login <логин_пользователя> <enter>* *password <пароль><enter>* *execute <enter>*
4	-a, --address	Подключение при помощи консольной оболочки администратора СЗИ НСД к удаленной рабочей станции, защищенной СЗИ НСД Dallas Lock Linux. **Пример:** *ishl* -a *<ip_адрес_рабочей_станции>* *-l <логин_администратора_безопасности>* ввести пароль учетной записи администратора СЗИ НСД удалённой рабочей станции. После успешной авторизации строка приглашения ввода команд будет иметь следующий вид: *<ip_адрес_рабочей_станции>/szi#*
5	-p, -port	Ввод номера порта. *ishl –p <порт_сервера>*
6	-v, --version	Отображение версии консольной оболочки СЗИ НСД **Пример:** *ishl -v* *Command line interface for Information Security System for GNU/Linux ishl 0.0.3*
7	-f, --cmd	При запуске консольной оболочки СЗИ НСД возможно указать файл списком команд для удобства применения типовых настроек. **Пример:** *ishl -f <путь и имя_файла>*
8	-h, --help	Вывести справку по использованию параметров консольной оболочки СЗИ НСД. **Пример:** *ishl -h* Результат выполнения команды:

		Command line interface for Information Security System for GNU/Linux *Usage : ishl [OPTION...]* *-r, --rootca Path to the root certificate* *-u, --cert Path to the user certificate* *-l, --login Login to connect to the server* *-a, --address Server's address to connect to* *-p, --port Server's port to connect to* *-v, --version Display version and exit* *-f, --cmd Command file* *-h, --help Display this help and exit*

Система меню консольной оболочки имеет многоуровневую структуру. Список команд доступных на текущем уровне можно получить при помощи команды *list*, для перехода на уровень выше следует использовать команду *exit*.

4. ПРОВЕРКА СИСТЕМЫ ЗАЩИТЫ

4.1. Проверка работоспособности средствами системы защиты

Данная функция позволяет выполнить автоматическое тестирование основного функционала системы защиты (создание/удаление пользователя, проверки параметров доступа к ресурсам и пр.).

Для перехода в подсистему автоматического тестирования функционала необходимо в консольном приложении управления средством защиты информации необходимо команду – *self-testing*, а затем использовать команды, приведенные в следующей таблице:

Таблица 2

№	команды	Описание
1	*auth-test*	Проверка функционирования подсистемы идентификации и аутентификации. **Описание теста.** Тест включает в себя попытку пройти аутентификацию в системе под несуществующим именем пользователя - *auth_test_login*. **Ожидаемый результат.** Сообщение в CLI об удачном / неудачном выполнении команды. Соответствующие записи в системе аудита в журнале Entries: - запись о попытке аутентификации; - запись о результате теста системы самотестирования
2	*dac-test*	Проверка функционирования подсистемы управления доступом. **Описание теста.** Тест включает в себя следующие проверки и действия: - создание тестовой группы (*auth_test_group*) и пользователя (*auth_test_login*); - создание тестового файла (*/home/auth_test_login/dac_test_file.txt*); - назначение прав «только чтение» на тестовый файл для тестового пользователя; - попытка произвести запись в тестовый файл от имени тестового пользователя; - удаление тестового файла, тестовых пользователя

		и группы. **Ожидаемый результат.** Сообщение в CLI об удачном / неудачном выполнении команды. Соответствующие записи в системе аудита в журналах Entries, Users, Resources: - запись о создании группы и пользователя; - запись о назначении прав на тестовый файл; - запись о попытке изменения файла со стороны пользователя; - запись о результате теста системы самотестирования.
3	*mem-test*	Проверка подсистемы контроля гарантированной зачистки информации. **Описание теста.** Тест включает в себя проверку очистки остаточной информации из памяти ОС. Для этого используется специализированный тестовой модуль ядра, проверяющий затирание данных в памяти. **Ожидаемый результат.** Сообщение в CLI об удачном / неудачном выполнении команды. Соответствующие записи в системе аудита в журнале Entries о результатах теста системы самотестирования
4	*sw-integrity-test*	Проверка подсистемы контроля целостности программной части СЗИ. **Описание теста.** Тест включает в себя следующие проверки и действия: - изменение одного из подконтрольных файлов; - запуск службы проверки контроля целостности; - проверка факта восстановления измененного в тесте файла. **Ожидаемый результат**. Сообщение в CLI об удачном/неудачном выполнении команды. Соответствующие записи в системе аудита в журналах Entries, Resources: - запись об изменении подконтрольного файла со стороны пользователя; - запись о результате теста системы самотестирования

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

В процессе установки, настройки и проверки СЗИ НСД системному программисту выводятся сообщения об удачно или неудачно выполненных операциях.