



ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
SCAN (ВЕРСИЯ 0.101120)

СОДЕРЖАНИЕ

1	ОБЩЕЕ ОПИСАНИЕ	4
1.1	Назначение	4
1.2	Системные требования	5
1.3	Состав и возможности	5
2	ЗАПУСК ПРОГРАММЫ	7
2.1	Первый запуск программы	7
2.2	Последующие запуски программы	11
2.3	Дополнительная информация	12
3	КОНФИГУРИРОВАНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА	13
3.1	Создание защищаемых директорий	13
3.1.1	Редактирование списка пользователей	13
3.1.2	Указание директории для размещения информации разного уровня доступа	15
3.1.3	Дополнительная информация	15
3.2	Раздел Статусов	16
3.2.1	Статус ЗПС	17
3.2.2	Обновление системы	18
3.2.3	Настройка принтеров	21
3.2.4	Astra Linux Red-Book	23
3.2.5	Дополнительная информация	24
3.3	Включение подсистемы контроля целостности	26
3.4	Настойка параметров необходимых для введения в эксплуатацию ОССН	26
3.5	Применение парольной политики	26
3.6	Включение подсистемы очистки памяти	27
3.7	Включение замкнутой программной среды	27
3.8	Запрет монтирования неучтенных носителей	28
3.9	Изменение наименования мандатных уровней	28
3.10	Включение режима запрета установки исполняемого бита	29
3.11	Выключение МКЦ	29
3.12	Отключение маркировки печати	29
3.13	Завершение работы программы	29

3.14	Откат настроек системы.....	30
3.15	Дополнительные функциональные возможности	31
3.16	Дополнительная информация.....	31
3.16.1	Перечень изменяемых параметров.....	31

1 ОБЩЕЕ ОПИСАНИЕ

1.1 Назначение

Данная инструкция описывает правила работы с программным обеспечением ScAN версии 0.180720 (далее – программа). Программа предназначена исключительно для быстрого и удобного конфигурирования автоматизированных рабочих мест (далее – АРМ) на базе операционной системы специального назначения (далее – ОССН) Astra Linux Special Edition версий 1.4, 1.5, 1.6 (на соответствие требованиям, изложенным в руководящем документе Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. до класса 1Б включительно).

Программа выполняет конфигурирование АРМ в соответствии с документами на операционную систему Astra Linux Special Edition версий 1.4, 1.5 и 1.6:

- РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1»;
- РУСБ.10015-01 97 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 2»;
- РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»;
- РУСБ.10015-01 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 2».

А также в соответствии с инструкциями и рекомендациями, представленными на официальном сайте разработчика ОССН (<https://wiki.astralinux.ru>).

ВАЖНО!

Программа разработана на высокоуровневом языке программирования, не является средством защиты информации, не привносит в ОССН какие-либо дополнительные исполняемые модули (в т.ч. модули защиты), утилиты (и т.п.) и не модифицирует/рекомпилирует программный код уже существующих.

Программа осуществляет настройку исключительно штатными средствами и возможностями, доступными для администратора ОССН, задекларированными официальной документацией и дополнительными официальными источниками.

1.2 Системные требования

Программа может запускаться на любом техническом средстве, работающим под управлением ОССН Astra Linux Special Edition версий 1.4, 1.5, 1.6 (для каждой версии ОС предусмотрен отдельный дистрибутив программы). Минимальные системные требования к техническим средствам определяются системными требованиями к ОССН.

1.3 Состав и возможности

- Упрощенное создание пользователей, присвоение или смена им мандатного уровня доступа (mac), экспорт-импорт базы пользователей;
- Создание соответствующей заведенным пользователям и их мандатным уровням (mac) структуры защищенных папок для хранения «грифованных» документов;
- Автоматизированная установка последних обновлений безопасности;
- Упрощенное конфигурирование принтеров для дальнейшей возможности печати «грифованных» документов (ненулевого мандатного уровня);
- Astra Linux Red-Book - автоматизированное применение рекомендованных настроек безопасности конфигурации ПК и ОС (только тех, параметры и методология включения которых однозначно определены разработчиком ОС);
- Запуск механизма очистки освобождаемых областей памяти Файловой системы ОС;

- Инициализация подсистемы контроля целостности ОС;
- Включение/выключение режима замкнутой программной среды;
- Включение режима запрета установки исполняемого бита;
- Смена имен мандатных уровней;
- Смена парольной политики ОС;
- Запрет на монтирование неучтенных носителей;
- Настройка параметров, необходимых для эксплуатации ОС;
- Выключение МКЦ;
- Установка приложения «Управление печатью»;
- Отключение маркировки печати при мандатном разграничении доступа;
- Возможность отката большинства примененных настроек до состояния, предшествующего запуску программы.

2 ЗАПУСК ПРОГРАММЫ

2.1 Первый запуск программы

Структура дистрибутива Программы приведена ниже (см. Рисунок 1).

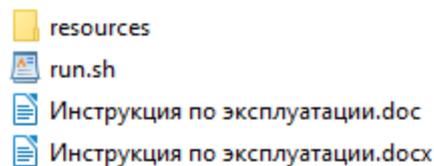


Рисунок 1 – Структура дистрибутива Программы

Для запуска программы необходимо выполнить следующие действия (команды выполняются в терминале ОС).

ВНИМАНИЕ!

Если дистрибутив находится не на физическом носителе необходимо сразу перейти ко второму пункту.

1) Выполнить команду монтирования диска с дистрибутивом от имени суперпользователя:

```
sudo mount /dev/srX /mnt,
```

где **/dev/srX** – файл накопителя,

/mnt – директория монтирования.

2) Выполнить команду запуска инсталляции пакетов (через скрипт run.sh), необходимых для работы программы, от имени суперпользователя:

ВНИМАНИЕ!

Пред запуском убедитесь, что на всех файлах в каталоге с дистрибутивом установлен бит исполнения.

Для версии, находящейся не на физическом носителе:

Для Astra Linux 1.5:

```
sudo sh / (путь до каталога с дистрибутивом) /ScAN15/run.sh
```

Для Astra Linux 1.6:

```
sudo sh / (путь до каталога с дистрибутивом) /ScAN16/run.sh
```

Для версии, расположенной на носителе:

Для Astra Linux 1.5:

```
sudo sh /mnt/ScAN15/run.sh
```

Для Astra Linux 1.6:

```
sudo sh /mnt/ScAN16/run.sh
```

Дождаться завершения установки пакетов.

Удостовериться, что все пакеты установились корректно (если они ранее не присутствовали в системе).

Дождаться запуска программы.

Процесс установки.

3) Выполнить команду запуска программы от имени суперпользователя:

Для версии, находящейся не на физическом носителе:

Для Astra Linux 1.5:

```
sudo / (путь до каталога с дистрибутивом) /ScAN15/  
resources/ScanData/ScAN15
```

Для Astra Linux 1.6:

```
sudo / (путь до каталога с дистрибутивом) /ScAN16/  
resources/ScanData/ScAN16
```

Для версии, расположенной на носителе:

Для Astra Linux 1.5:

```
sudo /mnt/ScAN15/resources/ScanData/ScAN15
```

Для Astra Linux 1.6:

```
sudo /mnt/ScAN16/resources/ScanData/ScAN16
```

При успешном выполнении описанных действий произойдет запуск программы – появится окно ввода информации (см. Рисунок 2).

Для последующих запусков рекомендуем использовать команды:

Для Astra Linux 1.5:

```
sudo /opt/SCAN/resources/ScanData/SCAN15
```

Для Astra Linux 1.6:

```
sudo /opt/SCAN/resources/ScanData/SCAN16
```

Для версии, находящейся не на физическом носителе:

Для Astra Linux 1.5:

```
sudo / (путь до каталога с дистрибутивом) /SCAN15/  
resources/ScanData/SCAN15
```

Для Astra Linux 1.6:

```
sudo / (путь до каталога с дистрибутивом) /SCAN16/  
resources/ScanData/SCAN16
```

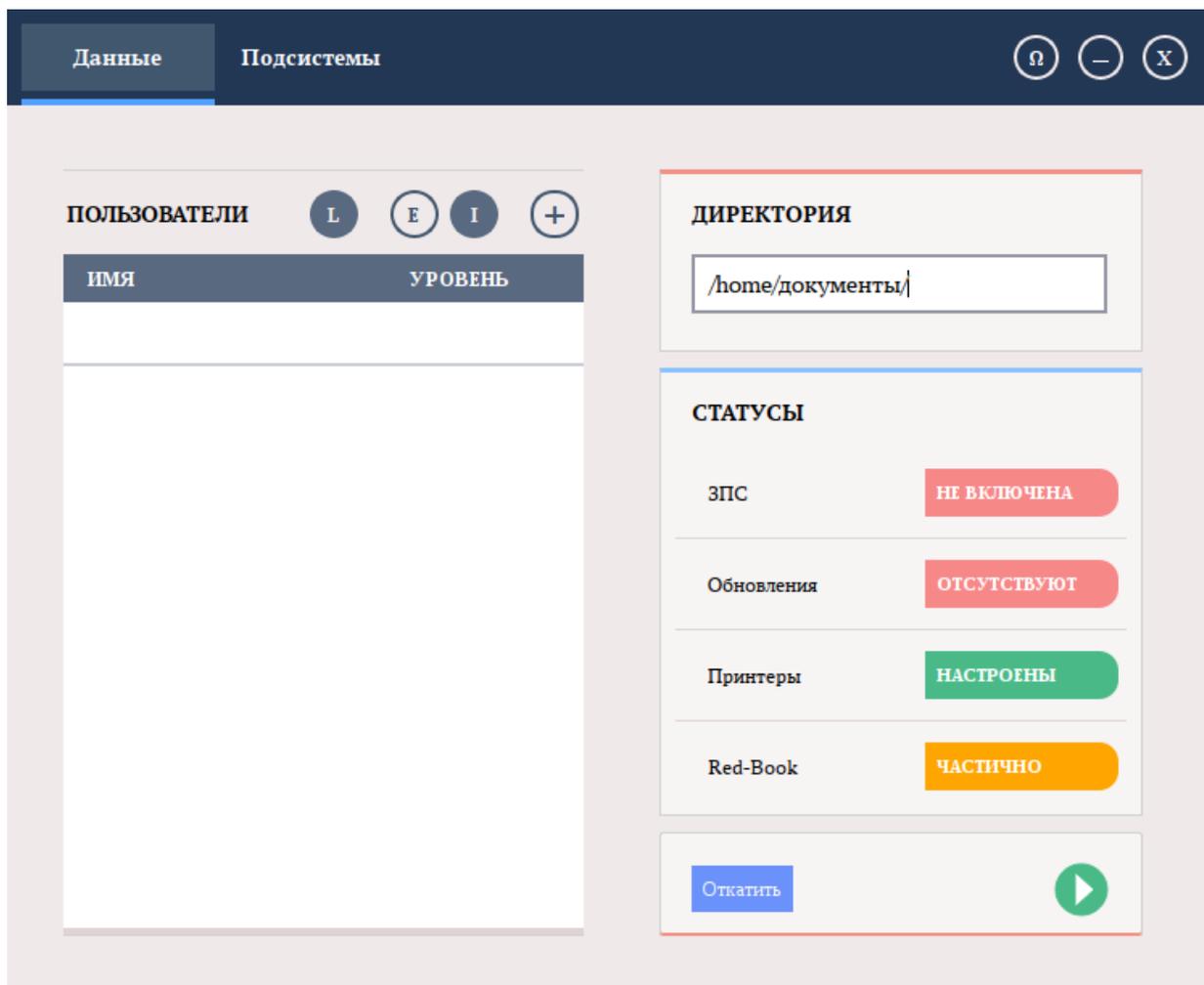


Рисунок 2 – Окно ввода информации

Окно ввода информации содержит инструментарий для:

- создания новых пользователей и установка им (или уже существующим пользователям) максимального мандатного уровня доступа (мас);
- задания пути для директории «документы», в которой будет размещаться древо каталогов различного мандатного уровня доступа для хранения «грифованных» документов;
- статус-переключатель для включения/выключения замкнутой программной среды;
- статус-переключатель для перехода к интерфейсу обновлений безопасности;
- статус-переключатель для перехода к интерфейсу настройки принтеров;
- статус-переключатель для настройки рекомендуемых параметров безопасности ОС Astra Linux Red-Book;

- кнопка отката произведенных программой настроек.

При нажатии на кнопку , расположенную в правом нижнем углу окна ввода информации, либо при клике на вкладку «Подсистемы» в верхней части окна, произойдет переключение на окно включения механизмов защиты (см. Рисунок 3). Оно содержит инструментарий для выбора механизмов защиты и дополнительных опций, которые необходимо применить для конфигурирования АРМ. Обратное переключение осуществляется кнопкой , расположенной в левой нижней части окна включения механизмов защиты, либо кликом на вкладку «Данные» в верхней части окна.

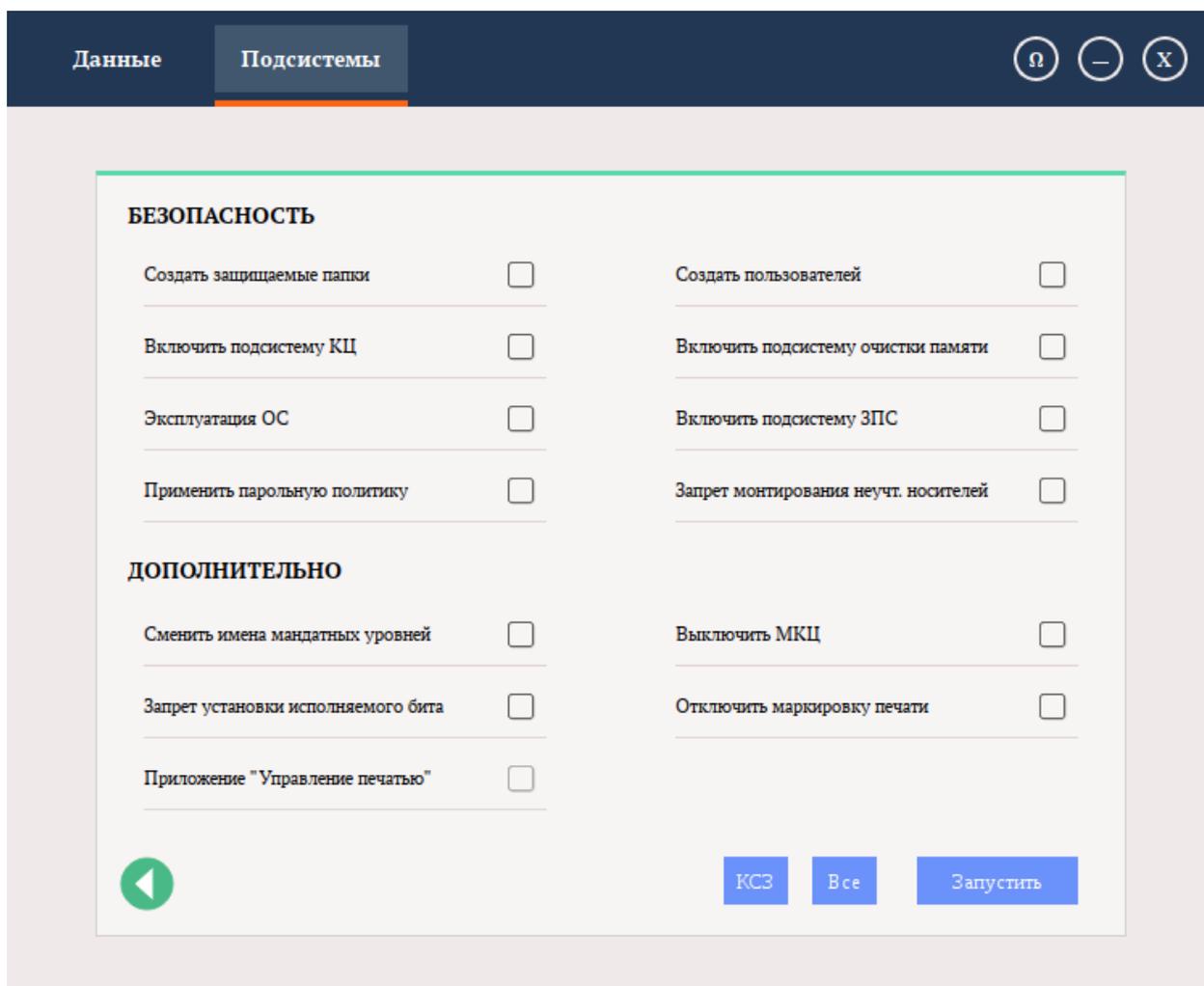


Рисунок 3 – Окно включения механизмов защиты

2.2 Последующие запуски программы

Для последующего запуска программы достаточно выполнить действия, указанные в пункте п. 3) настоящей инструкции.

2.3 Дополнительная информация

2.3.1 Процесс установки.

При запуске инсталляции пакетов (посредством инструмента run.sh), будет выполнена установка необходимых пакетов из дистрибутива программы (см. Рисунок 4).

```
** Установка пакетов интерфейса с диска Astra Linux. Ожидайте... **

** Не удалось обнаружить диск Astra Linux. Пакеты для граф. интерфейса программы будут установлены из собственного дистрибутива **

Установка пакета интерфейса libqt5test5_5.5.1+dfsg-8astra5_amd64.deb :
Успех!
Установка пакета интерфейса libpython3.2_3.2.3-7_amd64.deb :
Успех!
Установка пакета интерфейса python3-sip_4.16.9+dfsg-1astra1_amd64.deb :
Успех!
Установка пакета интерфейса python3-pyqt5_5.5.1+dfsg-3astra1_amd64.deb :
Успех!

** Пакеты интерфейса успешно установлены! **
```

Рисунок 4 – Процесс установки пакетов из дистрибутива программы

Есть возможность установки необходимых пакетов с диска ОССН Astra Linux Special Edition. Для этого необходимо вставить его в дисковод и запустить инструмент установки run.sh (см. Рисунок 5).

```
** Установка пакетов интерфейса с диска Astra Linux. Ожидайте... **

Установка пакета интерфейса libqt5test5_5.5.1+dfsg-8astra5_amd64.deb :
Успех!
Установка пакета интерфейса libpython3.2_3.2.3-7_amd64.deb :
Успех!
Установка пакета интерфейса python3-sip_4.16.9+dfsg-1astra1_amd64.deb :
Успех!
Установка пакета интерфейса python3-pyqt5_5.5.1+dfsg-3astra1_amd64.deb :
Успех!

** Пакеты интерфейса успешно установлены! **
```

Рисунок 5 – Процесс установки пакетов с диска ОССН Astra Linux

3 КОНФИГУРИРОВАНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

3.1 Создание защищаемых директорий

Создание директорий для хранения информации разного уровня доступа происходит для пользователей, указанных в списке пользователей в окне ввода информации. Созданные директории имеют соответствующие мандатные метки (уровни доступа) и атрибуты аудита, установленные согласно требованиям руководящего документа Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г для класса 1Б.

Для создания защищаемых директорий необходимо перейти в окно включения механизмов защиты и установить флажок напротив пункта «Создать защищаемые папки», выполнив перед этим действия согласно п. 3.1.1 и п 3.1.2 текущего руководства, и далее кликнуть кнопку «Запустить» в правой нижней части окна.

3.1.1 Редактирование списка пользователей

Инструментарий для редактирования списка пользователей расположен в левой части окна ввода информации. Список пользователей представлен в виде таблицы, содержащей имена пользователей и их максимальные мандатные уровни доступа (далее – уровень доступа). При запуске программы по нажатию на кнопку  в списке отобразятся локальные пользователи системы и их уровни доступа, если таковые установлены ранее. Привилегированный пользователь, созданный при установке системы (uid 1000), в таблице не отображается.

Редактирование списка пользователей, для которых необходимо создать директории для хранения «грифованных» файлов, происходит следующим образом.

1) Для добавления нового пользователя в список нужно кликнуть кнопку , расположенную над таблицей. В появившейся строчке заполнить поля: имя пользователя и его уровень доступа. Наивысший уровень, который может назначить программа, – 3.

ВНИМАНИЕ!

Поле уровень доступа обязательно к заполнению.

2) Для удаления выделенной строки в таблице нужно кликнуть правой клавишей мыши и выбрать из всплывающего контекстного меню пункт «Удалить строку».

ВНИМАНИЕ!

При удалении пользователя будьте внимательны, обязательно прочитайте дополнительную информацию о контекстном меню таблицы (пункт “Удалить пользователя”), расположенную по ссылке ниже.

3.1.3.1. Контекстное меню таблицы пользователей

3) Если необходимо создать пользователей в операционной системе, добавленных в список пользователей, и директории для них, следует перейти на вкладку «Подсистемы» и установить флажок напротив пункта «Создать пользователей». Далее необходимо нажать на кнопку «Запустить» и дождаться сообщения о завершении операции.

ВАЖНО!

Созданным пользователям присваивается по умолчанию пароль «12345678» (без кавычек). Установить другой пароль пользователям можно впоследствии стандартными средствами операционной системы, например, используя графическую утилиту fly-admin-smc.

4) Для сохранения (экспортирования) списка пользователей нужно нажать на кнопку  , расположенную над таблицей. Файл “database” со списком сохранится в каталоге «/opt/ScAN/ScanData» в директории, из которой происходил запуск программы.

5) Для открытия ранее сохраненного списка пользователей нужно нажать на кнопку  , расположенную над таблицей. Для этого необходимо, чтобы в папке «/opt/ScAN/ScanData» программы находился файл “database” с ранее экспортируемыми пользователями.

3.1.3.2. Создание директорий.

3.1.2 Указание директории для размещения информации разного уровня доступа

Поле для указания директории, в которой будет размещаться древо каталогов различного уровня доступа, находится в правой верхней части окна ввода информации. Для указания директории следует кликнуть левой клавишей мыши по полю и ввести данные. Формат пути должен быть вида /путь/.../путь/. По умолчанию указана директория /home/документы/. Создаваемая папка-дерево (в нашем случае – «документы») должна располагаться в корне директории /home/. Это обусловлено спецификой модели разграничения доступа в ОС и минимизацией рисков вызова ошибки.

Если указанная директория существует, при переходе в окно включения механизмов защиты отобразится соответствующее уведомление (см. Рисунок 6). При нажатии на кнопку «Да» произойдет переход в окно включения механизмов защиты, при нажатии на кнопку «Нет» будет возможность указать новую директорию в окне ввода информации.

ВАЖНО!

Мы настоятельно не рекомендуем создавать древо защищаемых папок в уже существующей директории.

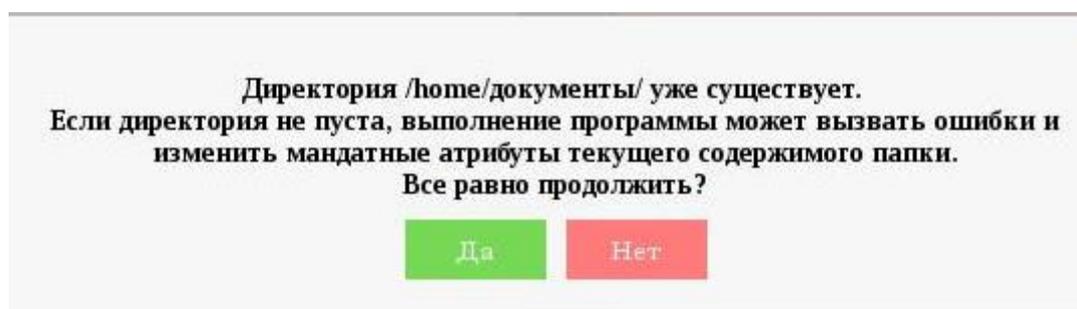


Рисунок 6 – Сообщение о наличии указанной директории

3.1.3 Дополнительная информация

3.1.3.1. Контекстное меню таблицы пользователей

При нажатии правой кнопкой мыши на строку таблицы, активируется контекстное меню, состоящее из трех пунктов (см. Рисунок 7):

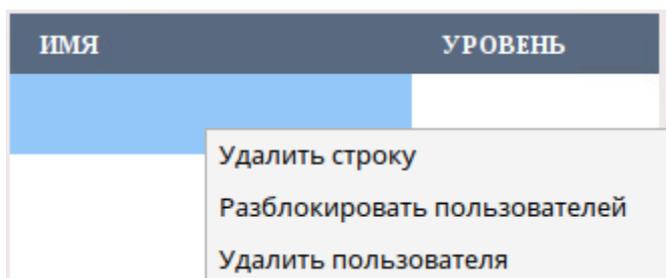


Рисунок 7 – Контекстное меню таблицы пользователей

- Удалить строку;
- Разблокировать пользователя;
- Удалить пользователя (после нажатия появится окно для подтверждения действия удаления).

ВАЖНО!

При удалении пользователя **будут удалены** все его данные включая **домашний каталог, файлы на рабочем столе и т.п.** Поэтому настоятельно рекомендуем перед удалением сохранить все необходимые пользовательские данные.

3.1.3.2. Создание директорий.

Если необходимо создать только директории для пользователей из списка (например, в случае необходимости создания директорий для доменных пользователей, управление которыми программой не предусмотрено), следует вписать пользователей в таблицу и не ставить флажок «Создать пользователей».

3.2 Раздел Статусов

Раздел статусов (см. Рисунок 8) представляет собой элемент интерфейса, предназначенный для оперативного мониторинга и управления наиболее востребованными аспектами настройки ОССН. Раздел состоит из списка статус-кнопок. Текст и цвет кнопок отображают текущий статус подсистемы (для более удобного восприятия).

СТАТУСЫ	
ЗПС	ВКЛЮЧЕНА
Обновления	ОТСУТСТВУЮТ
Принтеры	НЕ НАСТРОЕНЫ
Red-Book	ЧАСТИЧНО

Рисунок 8 Раздел статусов

Зеленый цвет кнопки означает позитивный статус подсистемы (например, включенная ЗПС, как на Рисунок 8). Оранжевый – неопределенный статус - если подсистема по тем или иным причинам настроена не полностью (например, не настроены все принтеры, не установлены или некорректно установлены обновления и т.п.). Красный цвет означает негативный статус подсистемы (выключенный режим, отсутствие необходимой настройки и т.п.)

3.2.1 Статус ЗПС

Статус-кнопка ЗПС позволяет отслеживать текущее состояние подсистемы ЗПС и оперативно включать или выключать её, например, для установки дополнительного ПО или отладки работы ОССН в случае сбоев. После нажатия на кнопку подсистема перейдет в противоположенный статус, то есть если на момент нажатия на кнопку подсистема, например, была включена, после нажатия она выключится и наоборот.

Процесс включения-выключения ЗПС занимает некоторое время. В момент выполнения такого процесса, в целях безопасности, окно программы блокируется, выводится сообщение «Ожидайте». После завершения операции появится сообщение о готовности работать дальше.

ВАЖНО!

Перед использование данной функции обязательно прочитайте пункт 3.7.

После включения или выключения ЗПС, для вступления статуса подсистемы в силу, не забудьте перезагрузить ОССН.

3.2.2 Обновление системы

Статус-кнопка «Обновления» позволяет определить, установлены ли последние официальные обновления безопасности для текущей версии ОССН и, в случае необходимости, установить их.

Для установки обновлений вам понадобится оригинальный диск Astra Linux Special Edition и .ISO образ с последними обновлениями безопасности вашей версии ОССН. Образ с обновлениями можно скачать с официального сайта разработчиков из раздела «обновления безопасности» <https://wiki.astralinux.ru> (веб-адрес на момент написания документа).

Для начала установки обновлений необходимо кликнуть на статус-кнопку, после чего появится дополнительное окно обновлений (см. Рисунок 9).

Далее, для подготовки к установке следует:

- 1) Кликнуть на кнопку со значком «+», расположенную справа от строки указания пути к файлу-образу обновлений. Далее в открывшемся окне выбрать необходимый файл-образ обновлений с расширением .ISO, нажать ниже кнопку «Открыть». В случае успеха окно выбора закроется, а путь к файлу-образу отобразится в строке окна обновлений;
- 2) Вставить оригинальный диск Astra Linux Special Edition в привод;
- 3) Кликнуть кнопку запуск, в случае корректного выполнения п. 1) и 2) начнется установка обновлений.

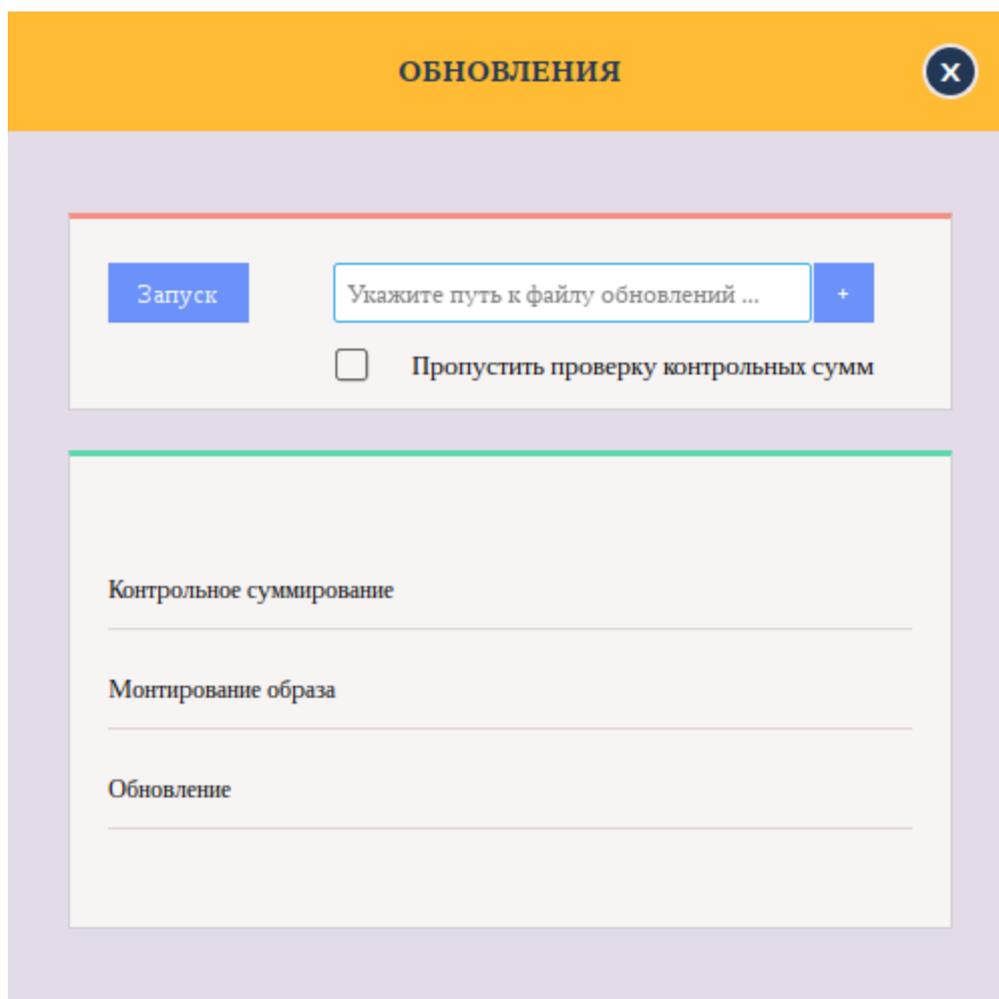
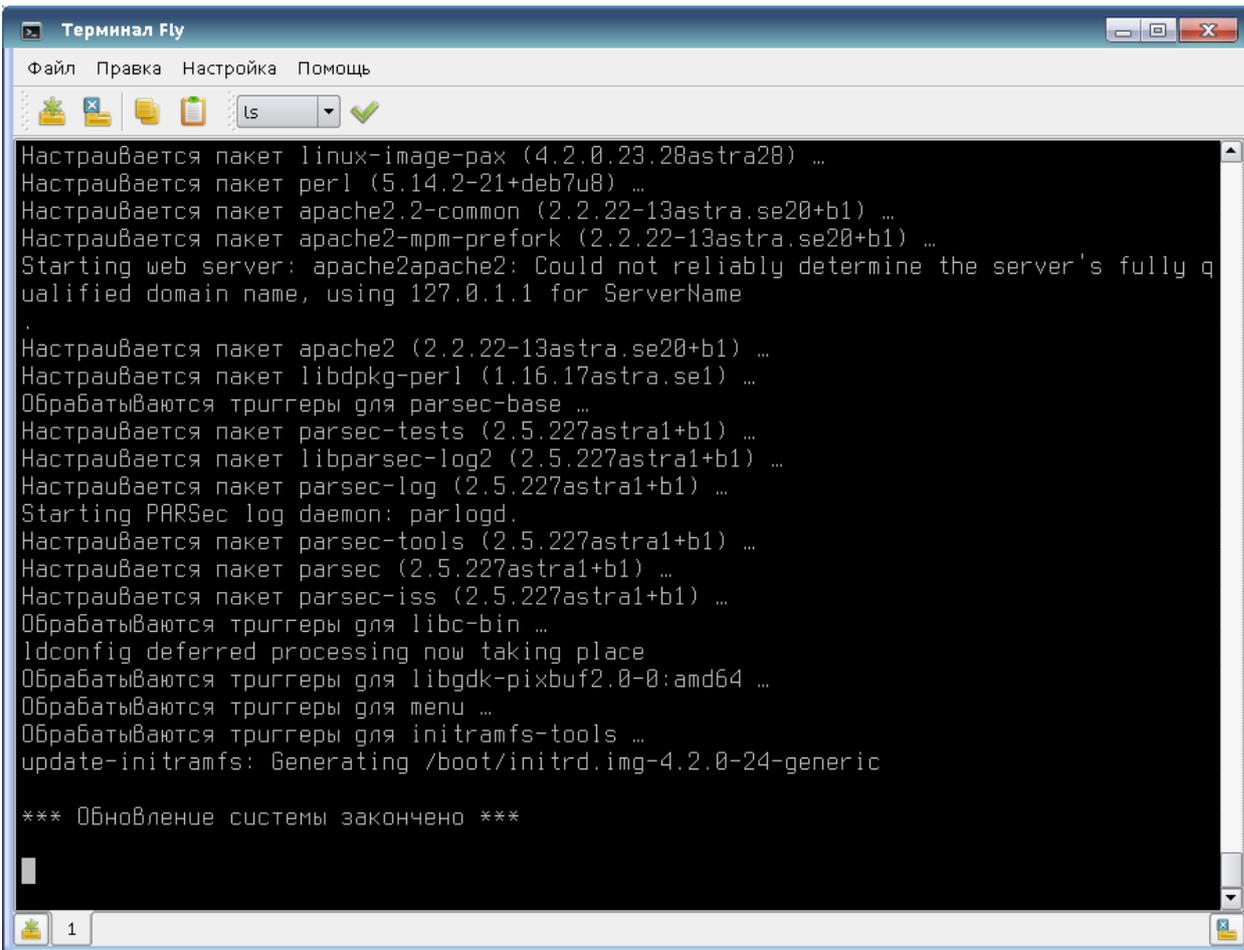


Рисунок 9 – Окно обновлений

В процессе установки программа откроет окно терминала fly-term для мониторинга пользователем корректности процесса установки обновлений. Когда обновление системы будет закончено – терминал выдаст сообщение «Обновление системы закончено» (см. Рисунок 10). Далее можно закрыть окно терминала fly-term или оно будет автоматически закрыто через 30 секунд.



```
Терминал Fly
Файл  Правка  Настройка  Помощь
ls
Настраивается пакет linux-image-pax (4.2.0.23.28astra28) ...
Настраивается пакет perl (5.14.2-21+deb7u8) ...
Настраивается пакет apache2.2-common (2.2.22-13astra.se20+b1) ...
Настраивается пакет apache2-mpm-prefork (2.2.22-13astra.se20+b1) ...
Starting web server: apache2apache2: Could not reliably determine the server's fully q
ualified domain name, using 127.0.1.1 for ServerName
.
Настраивается пакет apache2 (2.2.22-13astra.se20+b1) ...
Настраивается пакет libdpkg-perl (1.16.17astra.se1) ...
Обрабатываются триггеры для parsec-base ...
Настраивается пакет parsec-tests (2.5.227astra1+b1) ...
Настраивается пакет libparsec-log2 (2.5.227astra1+b1) ...
Настраивается пакет parsec-log (2.5.227astra1+b1) ...
Starting PARSec log daemon: parlogd.
Настраивается пакет parsec-tools (2.5.227astra1+b1) ...
Настраивается пакет parsec (2.5.227astra1+b1) ...
Настраивается пакет parsec-iss (2.5.227astra1+b1) ...
Обрабатываются триггеры для libc-bin ...
ldconfig deferred processing now taking place
Обрабатываются триггеры для libgdk-pixbuf2.0-0:amd64 ...
Обрабатываются триггеры для menu ...
Обрабатываются триггеры для initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-4.2.0-24-generic

*** Обновление системы закончено ***
```

Рисунок 10 – Окно терминала обновлений

Далее программа откроет окно терминала fly-term для мониторинга пользователем корректности процесса исправления зависимостей пакетов. Когда исправление будет закончено – терминал выдаст сообщение «Обновление системы закончено» (см. Рисунок 11). Далее можно закрыть окно терминала fly-term или оно будет автоматически закрыто через 30 секунд.

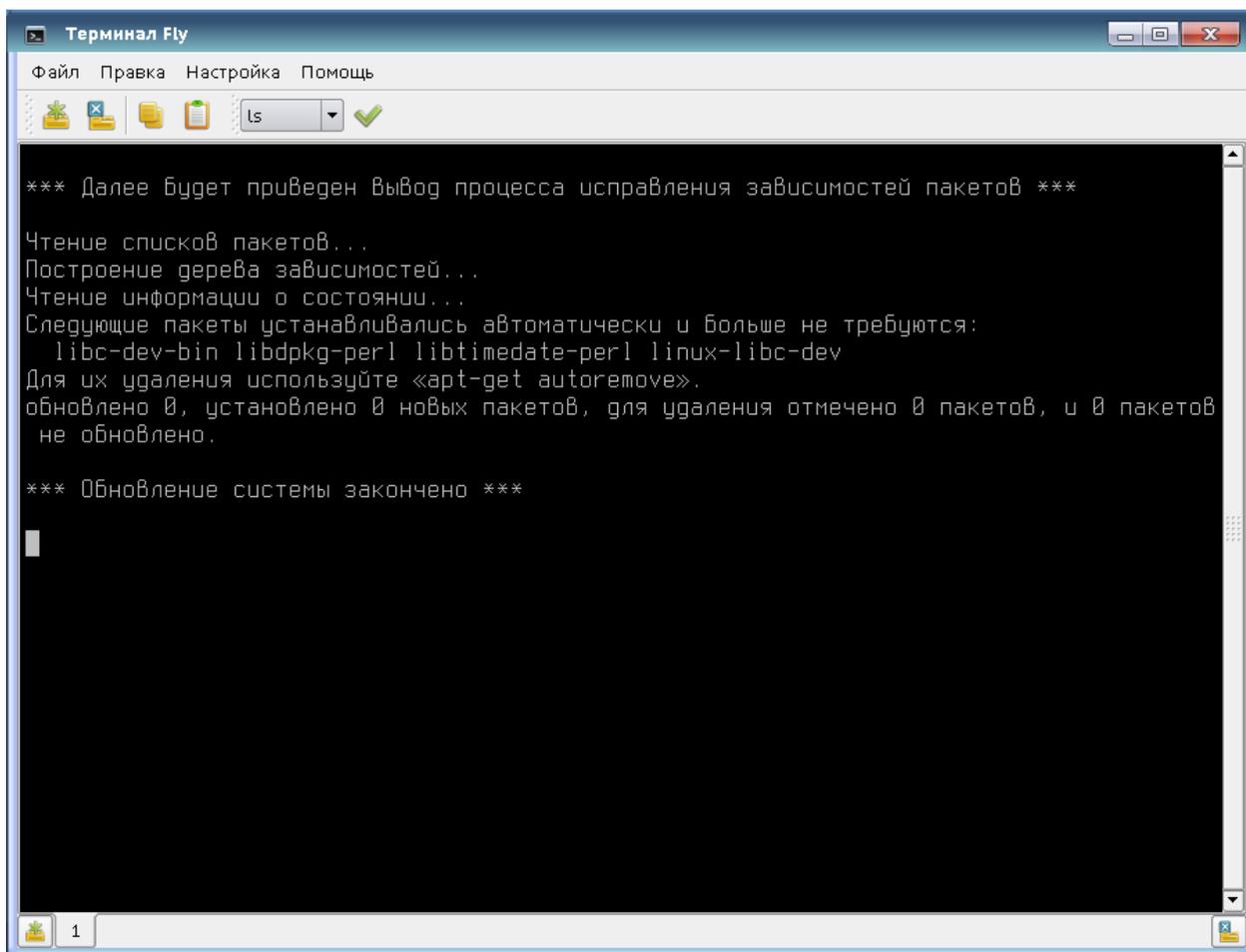


Рисунок 11 – Окно терминала исправления зависимостей

3.2.5.1 Обновление системы.

3.2.3 Настройка принтеров

Кнопка-статус «Принтеры» предназначена для подготовки принтеров/МФУ (далее по пункту – устройства) к возможности печати документов с ненулевым мандатным уровнем.

ВАЖНО!

На данный момент настройка возможна только для устройств, непосредственно подключенных к настраиваемому АРМ. До проведения настройки, принтер должен быть установлен в ОССН и работать в штатном режиме.

Для начала настройки необходимо кликнуть на кнопку-статус «Принтеры». Откроется окно настройки (см. Рисунок 12). Окно состоит из кнопки «Настроить», строки выбора устройства для настройки (на случай, если их подключено более одного) и полей ввода минимально и максимально возможных уровней задания для устройства.

В строке выбора устройства указано наименование и модель устройства, которое будет сконфигурировано по нажатию кнопки «Настроить». Если необходимо выбрать другое устройство - кликните в любую точку строки выбора устройства, после чего ниже строки появится список устройств, которые возможно сконфигурировать, далее выберите нужное устройство одинарным кликом.

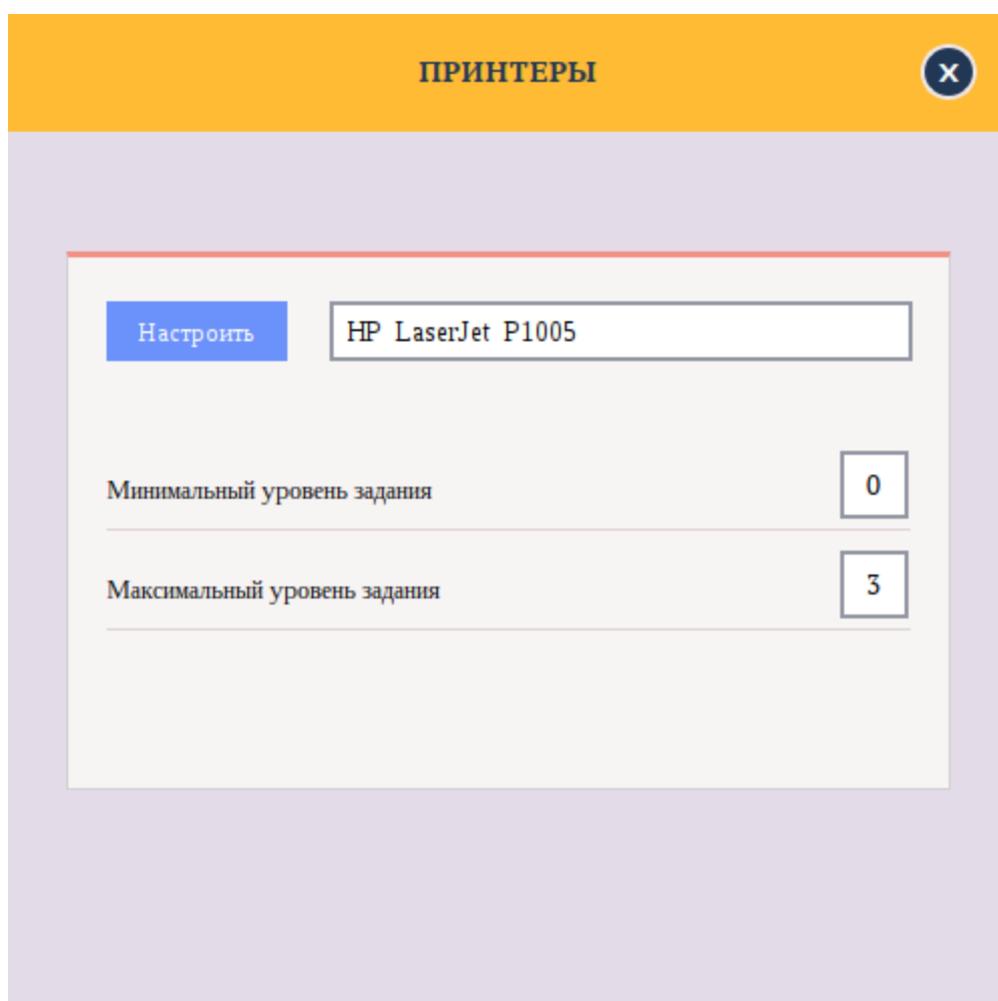


Рисунок 12 – Окно настройки принтеров

Следующим этапом укажите минимальный и максимальный доступный уровень задания печати для устройства, если вас не устраивают значения, установленные в программе по умолчанию. При этом максимальный уровень задания не может быть ниже минимального. Если говорить простыми словами – минимальный и максимальный уровни заданий печати – это диапазон мандатных уровней документов, в пределах

которого у пользователей будет возможность этот документ распечатать на устройстве. Более подробно про уровни задания печати устройств и печать документов с ненулевым мандатным уровнем вы можете ознакомиться в официальной документации ОССН.

По завершении выбора устройства и указания уровней печати кликните на кнопку «Настроить». Программа приступит к настройке и по окончании каждого этапа выдаст статус-иконку успешности настройки: зеленая – успешно, красная – неуспешно (возникла ошибка, конфликт и т.п.). В случае успеха всех 3-х этапов окно настройки можно закрыть, устройства настроены.

3.2.4 Astra Linux Red-Book

Astra Linux Red-Book (далее – Red-Book) представляет собой набор настроек и исправлений, направленных на общее повышение уровня безопасности компьютера с ОССН, выходящего за рамки требований Руководящих документов РФ по защите информации от НСД.

Полный перечень действий для реализации Red-Book приведен на сайте разработчиков ОССН <https://wiki.astralinux.ru/> (на момент написания документа).

ВАЖНО!

Реализация Red-Book в программе не предусматривает настройку всех пунктов из полного перечня разработчика ОССН. Осуществляется настройка тех пунктов, которые возможно осуществить только после установки ОССН и параметры настроек которых четко определены разработчиком.

Для запуска настройки необходимо кликнуть на статус-кнопку Red-Book. После выполнения необходимых операций конфигурирования системы статус-кнопка изменит свой цвет в зависимости от результата выполненной операции.

3.2.5.2 Перечень параметров конфигурации.

3.2.5 Дополнительная информация

3.2.5.1 Обновление системы.

Файл-образ обновлений можно расположить по пути «/opt/ScAN/ScanData», тогда при нажатии на статус-кнопку «Обновление», будет автоматически сгенерирован путь до файла обновлений.

Контрольные суммы образов обновлений должны находиться в файле “hash”, расположенном по пути «/opt/ScAN/ScanData». Формат файла “hash” представлен на Рисунок 13. Проверку соответствия контрольной суммы необходимо произвести, выполнив команду: `gostsum -d ../путь/20191029SE16.iso` или скопировать из раздела «Обновления безопасности» <https://wiki.astralinux.ru> (веб-адрес на момент написания документа). Затем полученный хэш необходимо поместить в файл “hash”, в строку, начинающуюся с “updateISO=” в соответствии с используемой версией ОССН т.е. 1.6, 1.5 или 1.4.

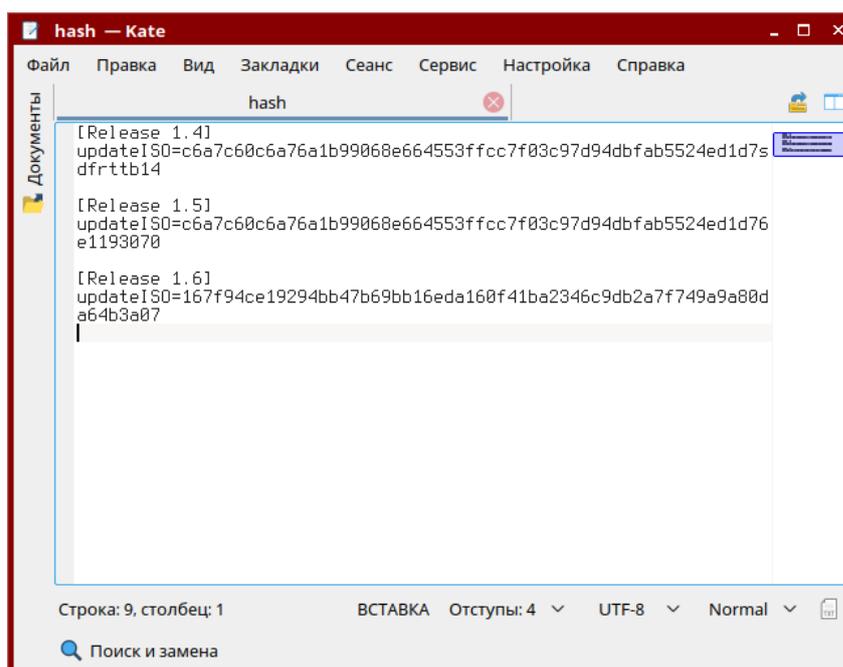


Рисунок 13 – Файл “hash”

Существует возможность пропустить проверку контрольных сумм. Для этого необходимо установить соответствующий флажок в окне «Обновления».

3.2.5.2 Перечень параметров конфигурации

Для Astra Linux 1.5:

- 1) Установка доступных обновлений ОССН: выполняется отдельно от Red-Book, см. п. Обновление системы;
- 2) Настройка загрузчика на загрузку ядра GENERIC, скрытие меню загрузчика;
- 3) Отключение доступа к консоли пользователям;
- 4) Включение блокировки установки бита исполнения: выполняется отдельно от Red-Book, см. п.Включение режима запрета установки исполняемого бита;
- 5) Включение блокировки макросов в VLC;
- 6) Включение механизма контроля подписи в ELF файлах: выполняется отдельно от Red-Book, см. п.Статус ЗПС или п.Включение замкнутой программной среды;
- 7) Включение гарантированного удаления файлов и папок: выполняется отдельно от Red-Book, см. п.Включение подсистемы очистки памяти;
- 8) Включение системных ограничений Ulimits;
- 9) Применение парольной политики, способствующей использованию «взломостойких» паролей: выполняется отдельно от Red-Book, см. п.Применение парольной политики;
- 10) Установка пакета quota для дальнейшей настройки дисковых квот;

ВАЖНО!

Сама программа квоты не настраивает, только устанавливает необходимый пакет.

- 11) Настройка параметров ядра sysctl.conf;
- 12) Блокировка исполнения модулей python с расширенным функционалом;

3.3 Включение подсистемы контроля целостности

Для включения подсистемы контроля целостности необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Включить подсистему КЦ».

3.4 Настойка параметров необходимых для введения в эксплуатацию ОССН.

Для выполнения требований, указанных в документации на операционную систему Astra Linux Special Edition, необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Эксплуатация ОС».

Перечень изменяемых параметров.

3.5 Применение парольной политики

Применение парольной политики – установление требований к паролям пользователей. Для редактирования требований к паролям пользователей нужно кликнуть на кнопку  в верхней правой части окна. Откроется окно настроек (см. Рисунок 14). В правой части окна настроек представлены необходимые параметры:

- минимальная длина пароля;
- минимальное количество строчных литер;
- минимальное количество заглавных литер;
- минимальное количество цифр;
- максимальный срок действия пароля;
- минимальный срок действия паролей;
- дни предупреждений о смене пароля.

Для редактирования параметров следует кликнуть левой клавишей мыши по полю напротив соответствующего параметра и ввести значение. После завершения редактирования параметров парольной политики нужно кликнуть левой кнопкой мыши по кнопке «Сохранить», расположенной в нижней части окна настроек.

Для применения парольной политики необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Применить парольную политику».

The screenshot shows a configuration window with a dark blue header containing a minus sign and an 'X' icon. The main content area is light gray and contains several form fields:

- Наименования мандатных уровней** (Mandatory level names):
 - Уровень 0:
 - Уровень 1:
 - Уровень 2:
 - Уровень 3:
- Имя привилегированного пользователя** (Privileged user name):
 - Имя:
- Парольная политика** (Password policy):
 - Минимальная длина пароля:
 - Минимальное кол-во строчных литер:
 - Минимальное кол-во заглавных литер:
 - Минимальное кол-во цифр:
 - Максимальный срок действия пароля (дн):
 - Минимальный срок действия пароля (дн):
 - Дни предупреждений о смене пароля:

At the bottom center, there is a blue button labeled "Сохранить" (Save).

Рисунок 14 – Опции по умолчанию

3.6 Включение подсистемы очистки памяти

Включение подсистемы очистки памяти – затирание памяти согласно требованиям из руководящего документа Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г.

Для включения подсистемы очистки памяти необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Включить подсистему очистки памяти».

3.7 Включение замкнутой программной среды

Включение замкнутой программной среды – включение в штатном режиме функционирования замкнутой программной среды, то есть загрузка на исполнение исполняемых файлов и разделяемых библиотек с

неверной электронной цифровой подписью, а также без электронной цифровой подписи запрещается.

Для включения замкнутой программной среды нужно перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Включить подсистему ЗПС».

ВАЖНО!

После включения ЗПС, для вступления статуса подсистемы в силу, необходимо перезагрузить ОССН.

ВНИМАНИЕ!

Перед запуском ЗПС установите все необходимые программы и убедитесь, что они имеют электронно-цифровую подпись для полноценного функционирования.

3.8 Запрет монтирования неучтенных носителей

Для включения запрета монтирования неучтенных носителей (по требованиям руководящего документа Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г.), необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Запрет монтирования неучт. носителей».

3.9 Изменение наименования мандатных уровней

Для переименования мандатных уровней (уровней доступа) нужно кликнуть на кнопку  в верхней правой части окна. В левой части окна настроек необходимо проверить наименования уровней доступа, которые будут присвоены системе. Для редактирования наименований следует кликнуть на поле напротив соответствующего уровня и ввести новые данные. После этого кликнуть левой кнопкой мыши по кнопке «Сохранить», расположенной в нижней части окна настроек.

Далее необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Сменить имена мандатных уровней».

3.10 Включение режима запрета установки исполняемого бита

Включение режима запрета установки исполняемого бита – включение режима, обеспечивающего предотвращение несанкционированного создания пользователями или непреднамеренного создания администратором исполняемых сценариев для командной оболочки.

Для включения подсистемы очистки памяти необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Запрет установки исполняемого бита».

ВАЖНО!

До применения данного запрета убедитесь, что на все необходимые исполняемые файлы установлен бит исполнения, и все необходимые программы были установлены.

3.11 Выключение МКЦ

Для выключения подсистемы МКЦ необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Выключить МКЦ».

3.12 Отключение маркировки печати

Для удобства пользователя есть возможность отключить маркировку печати при мандатном разграничении доступа, предоставляемую по умолчанию в ОССН.

Для отключения маркировки необходимо перейти в окно включения механизмов защиты (вкладка «Подсистемы») и установить флажок напротив пункта «Отключить маркировку печати».

3.13 Завершение работы программы

После определения конфигурационных настроек (см. подразделы 3.1, 3.2, 3.5, 3.6, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12) нужно кликнуть на кнопку «Запустить», расположенную в нижней части окна включения механизмов защиты (вкладка «Подсистемы»). После этого отобразится окно статуса выполнения программы (см. Рисунок 15). В данном окне отображаются

результаты выполнения программы и активации подсистем. Успешно исполненные задачи помечаются значком . Задания, в процессе выполнения которых произошли ошибки – значком . Задания, не отмеченные пользователем для исполнения, помечаются прочерком.

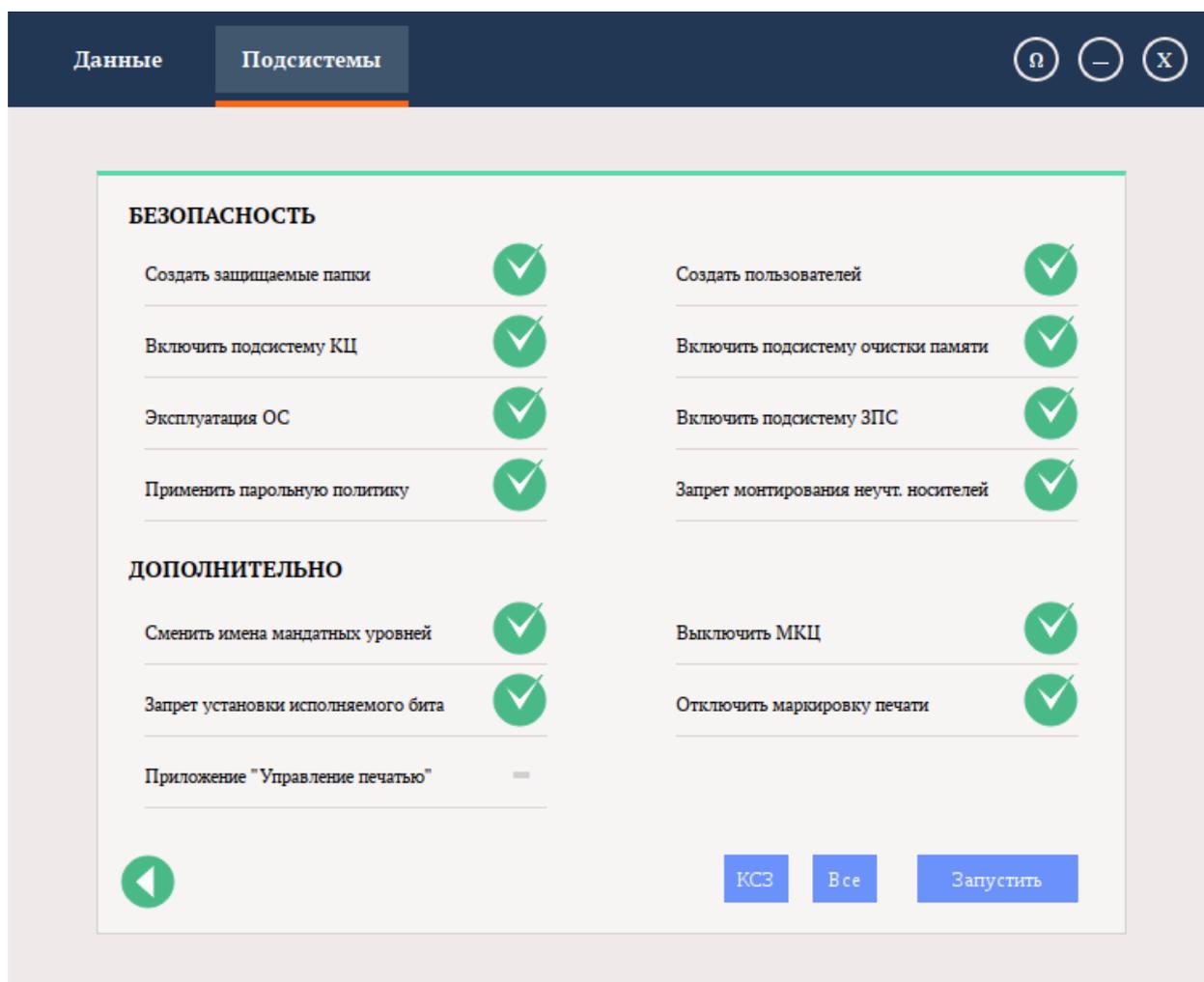


Рисунок 15 – Окно статуса выполнения программы

3.14 Откат настроек системы

В процессе запуска программы и перед выполнением необходимых задач, для любых конфигурационных файлов ОССН, в которые непосредственно вносятся изменения, создаются резервные копии-экземпляры.

Откат настроек системы – замена текущих экземпляров конфигурационных файлов ОССН резервными копиями, созданными до внесения изменений программой.

Для отката настроек необходимо кликнуть на кнопку «Откатить», расположенную в правой нижней части окна ввода информации (вкладка «Данные»). При успешном выполнении процедуры отобразится соответствующее информационное окно (см. Рисунок 16).

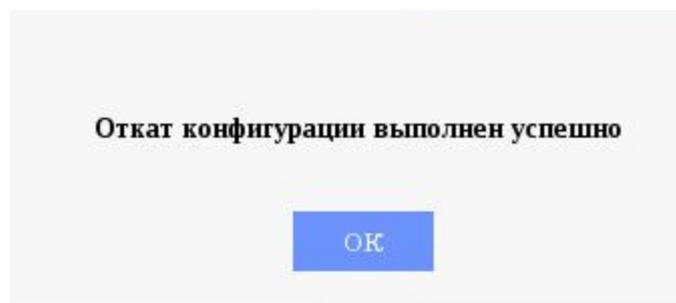


Рисунок 16 – Информационное сообщение

3.15 Дополнительные функциональные возможности

На вкладке «Подсистемы» расположены две кнопки, представленные на Рисунок 17. Нажатие на кнопку «КСЗ» позволяет выбрать минимальный необходимый набор для включения комплекса средств защиты ОССН. Нажатие на кнопку «Все» позволяет выбрать все возможные механизмы защиты.

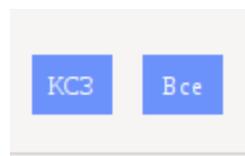


Рисунок 17 – Дополнительные возможности

3.16 Дополнительная информация

3.16.1 Перечень изменяемых параметров.

Список необходимых изменений:

- 1) Настройка механизма замкнутой программной среды для работы в штатном режиме выполняется отдельно, см. п.3.2.1 или п.3.7;
- 2) Запрет пользователям доступ к библиотеке libpcprofile.so;
- 3) Запрет использование неучтенных носителей информации выполняется отдельно, см. п.3.8;
- 4) Запрет запуск средств создания символических ссылок пользователям, не обладающим привилегиями администратора;

- 5) Выключение службы grm для поддержки мыши в консольном режиме;
- 6) Блокировка возможности удаленного входа в ОССН для предотвращения подбора пароля суперпользователя;
- 7) Настройка парольной политики выполняется отдельно, см. п.3.5;
- 8) Настройка политики учетной записи по количеству неуспешных попыток входа в систему и периода блокировки пользователя при превышении допустимого значения.
- 9) Установка параметра «Блокировка экрана» на значение 15 минут.

