ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ SCAN (ВЕРСИЯ 0.180720)

2018

СОДЕРЖАНИЕ

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 и 1.5:

- 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. 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;
- 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).

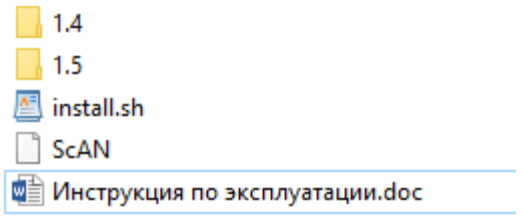

Рисунок 1 – Структура дистрибутива Программы

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

1) (Если программа поставляется на электронном носителе) Выполнить команду монтирования накопителя(носителя) с дистрибутивом от имени суперпользователя:

```
sudo mount /dev/sdX /mnt,
```

где **/dev/sdX** – файл накопителя,

/mnt – директория монтирования.

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

```
sudo sh /mnt/ScAN/install.sh (в случае запуска с носителя)
```

```
sudo sh /«путь к дистрибутиву»/ScAN/install.sh (в случае запуска из иного места)
```

Дождаться завершения установки пакетов.

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

3) Выполнить команду запуска программы от имени суперпользователя:

```
sudo /mnt/ScAN/ScAN (в случае запуска с носителя)
```

```
sudo /«путь к дистрибутиву»/ScAN/ScAN (в случае запуска из иного места)
```

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

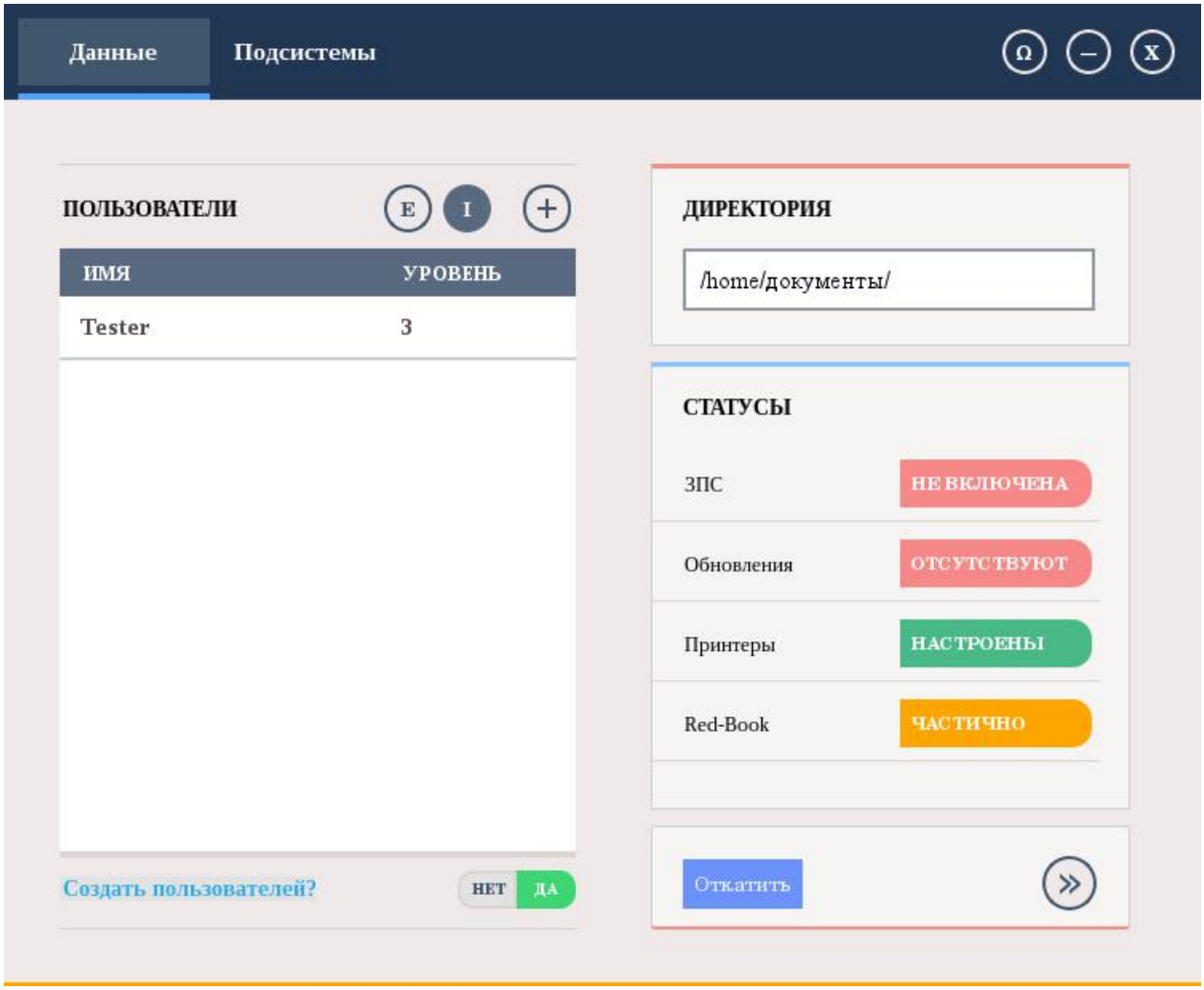

Рисунок 2 – Окно ввода информации

Окно ввода информации содержит инструментарий для:

- заведения новых пользователей и установка им (или уже существующим пользователям) максимального мандатного уровня доступа (mac);
- 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 .

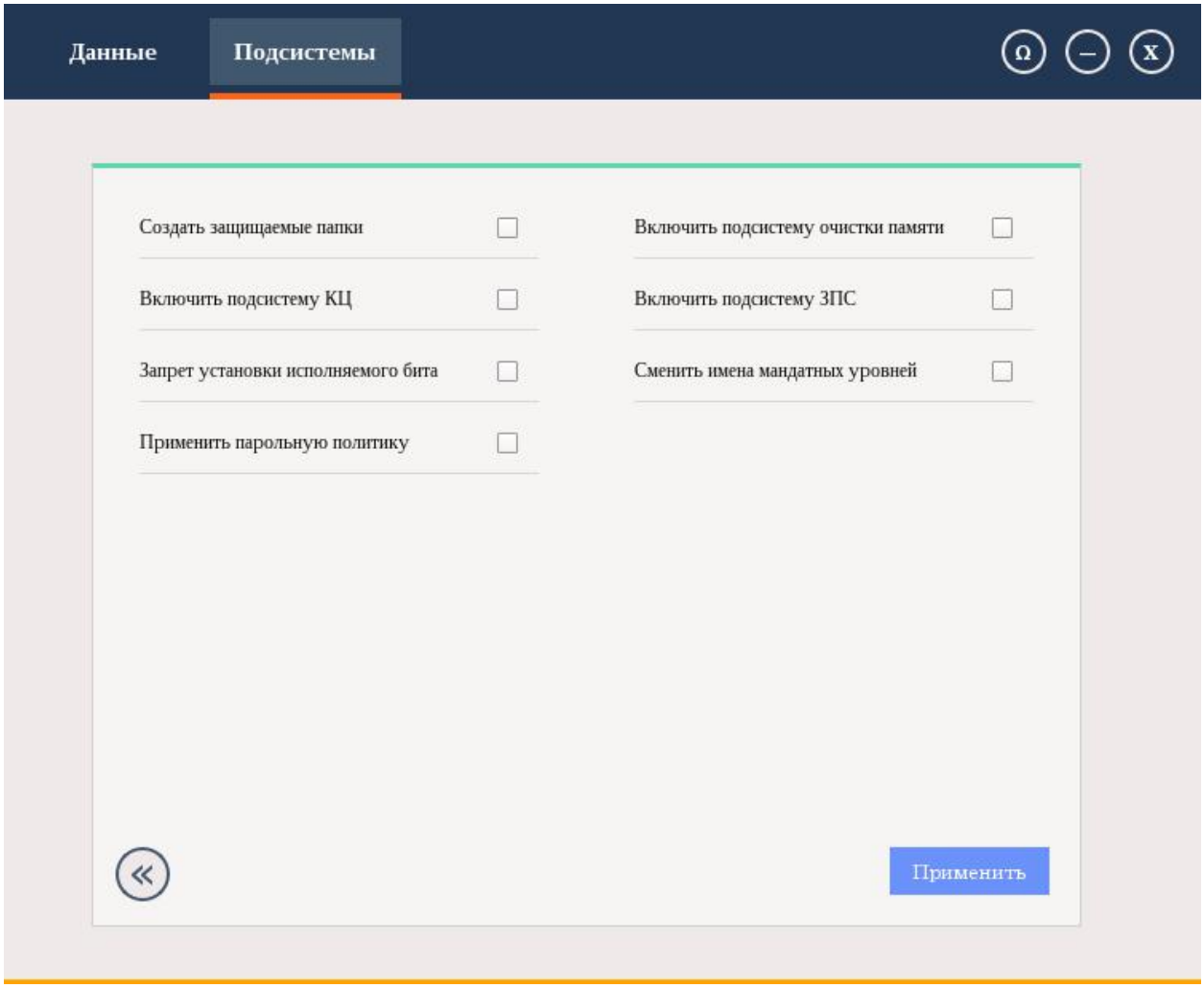

Рисунок 3 – Окно включения механизмов защиты

2.2 Последующие запуски программы

Для последующих запусков программы достаточно выполнить действия, указанные в пункте п. 2.1.3 настоящей инструкции.

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 «Применить» 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 в списке отображаются 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.

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

3) Если необходимо создать пользователей в операционной системе, добавленных в список пользователей, и директории для них, следует активировать переключатель «Создать пользователей» в нижней части таблицы в положение «ДА». **Важно!** Созданным пользователям присваивается по-умолчанию пароль «**SetOwnPa$$w0rd**» (без кавычек). Установить другой пароль пользователям можно впоследствии стандартными средствами операционной системы, например, используя графическую утилиту fly-admin-smc.

4) Если необходимо создать только директории для пользователей из списка (например, в случае необходимости создания директорий для доменных пользователей, доступ для управления которыми программой не предусмотрен), следует активировать переключатель в положение «Нет».

5) Для сохранения (экспортирования) списка пользователей нужно нажать на кнопку , расположенную над таблицей. Файл "database" со списком сохранится в каталоге «resources» в директории, из которой происходил запуск программы.

6) Для открытия ранее сохраненного списка пользователей нужно нажать на кнопку , расположенную над таблицей. Для этого необходимо, чтобы в папке «resources» программы находился файл "database" с ранее экспортируемыми пользователями.

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 4). 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.

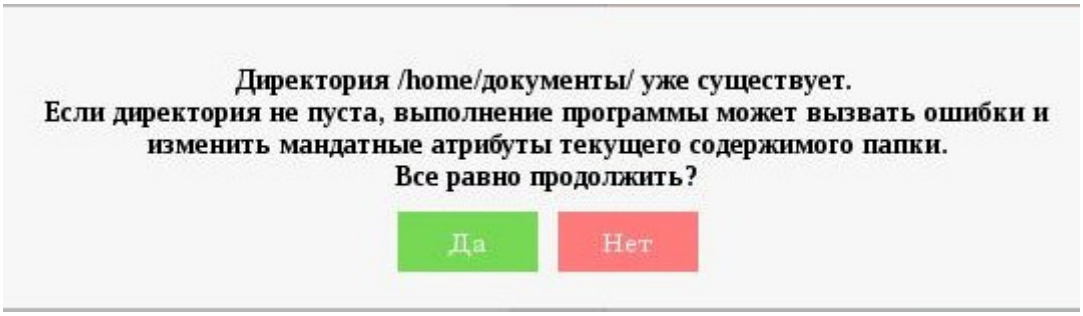

Рисунок 4 – Сообщение о наличии указанной директории

3.2 Раздел Статусов

Раздел статусов (см. Рисунок 5) представляет с 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).

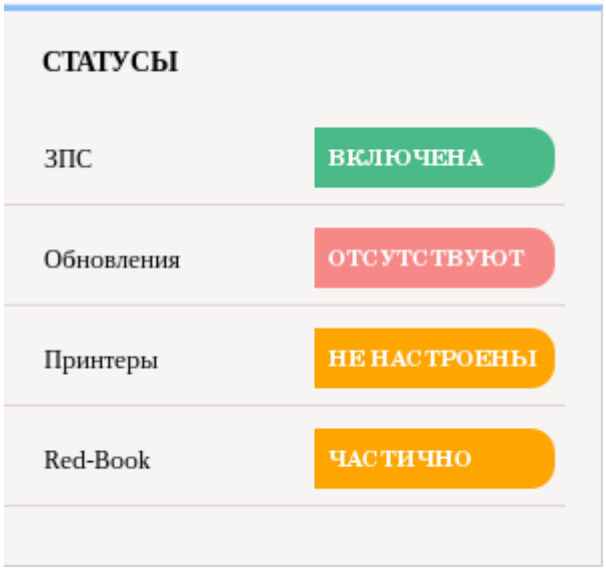

Рисунок 5 – Раздел статусов

Зеленый цвет кнопки означает позитивный статус подсистемы (например, включенная ЗПС, как на Рисунке 5). Оранжевый – неопределенный статус - если подсистема по тем или иным причинам настроена не полностью (например, не настроены все принтеры, не установлены или некорректно установлены все обновления и т.п.). Красный цвет означает негативный статус подсистемы (выключенный режим, отсутствие необходимой настройки настройки и т.п.)

3.2.1 Статус ЗПС

Статус-кнопка ЗПС позволяет мониторить 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 программа выдаст сообщение о готовности работать дальше.

Важно! 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 6).

Далее, для подготовки к установке следует:

1) Кликнуть на кнопку со значком «+», прикрепленную 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» (либо дважды кликнуть по нему). 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.

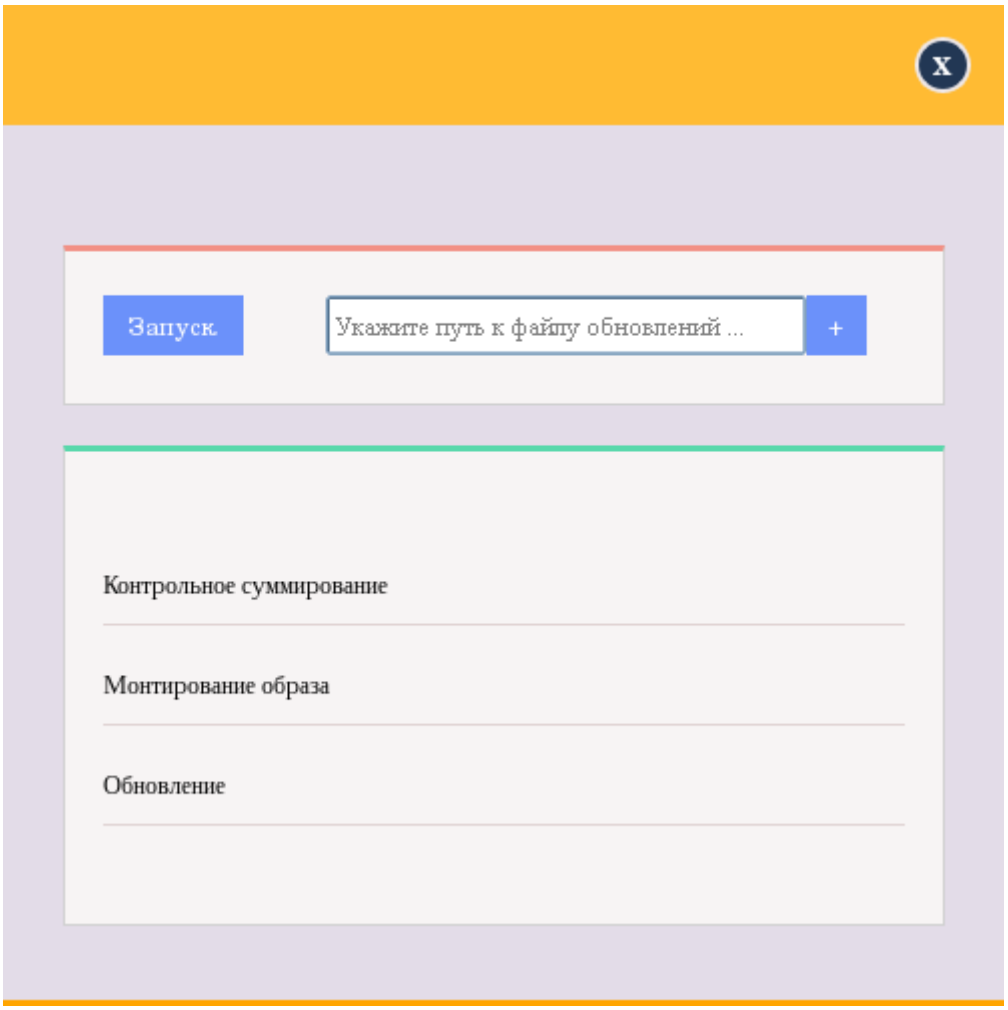

Рисунок 6 – Окно обновлений

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 7). Далее можно закрыть окно терминала fly-term и окно обновлений программы.

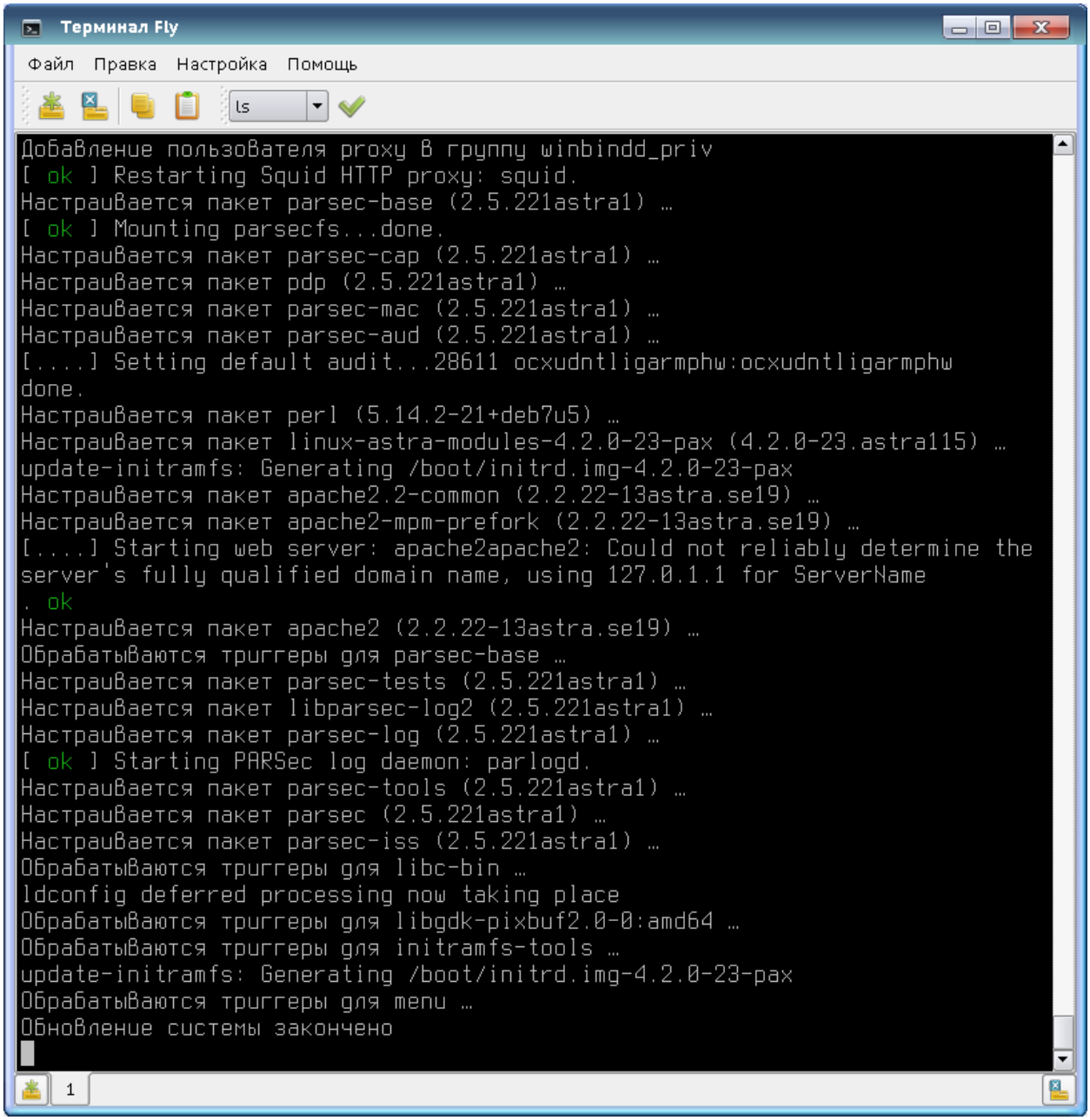

Рисунок 7 – Окно терминала обновлений

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 8). Окно состоит и 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 стоки появится список устройств, которые возможно сконфигурировать, далее выберите нужное устройство одинарным кликом.

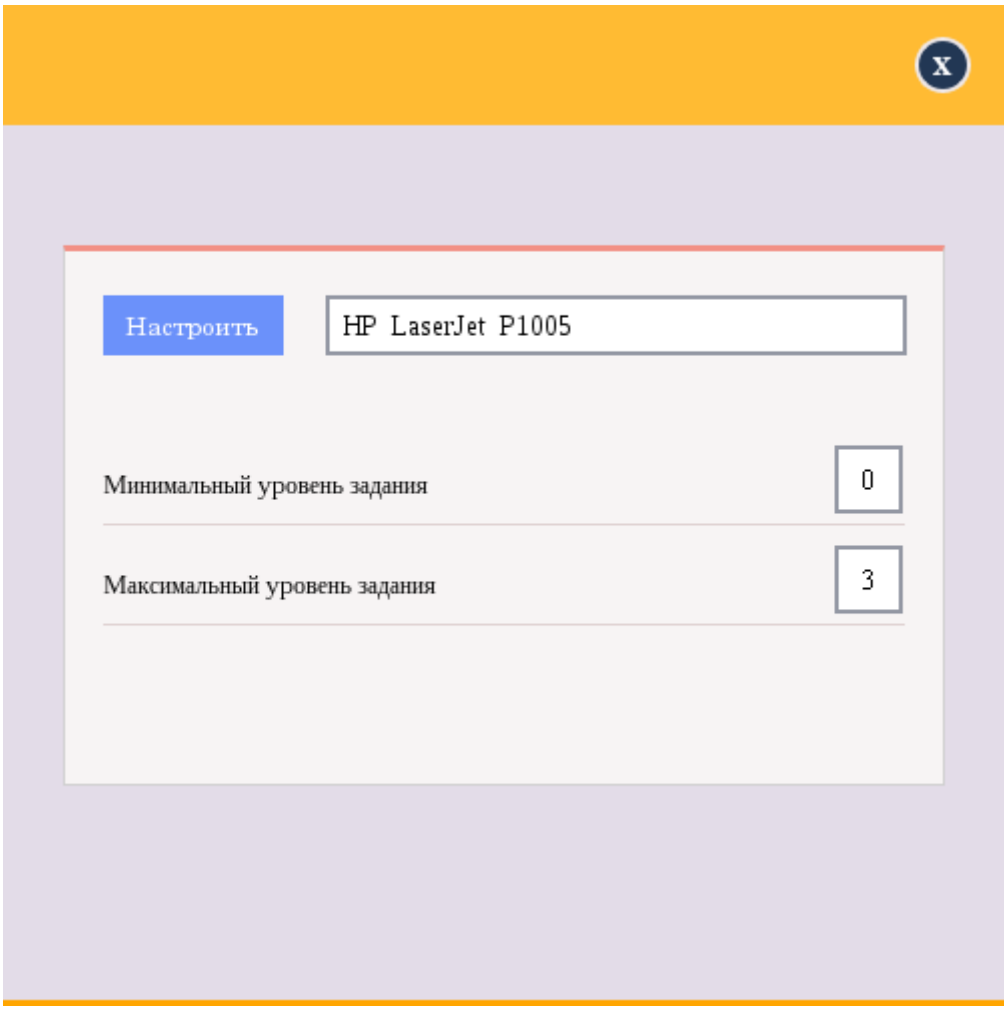

Рисунок 8 – Окно настройки принтеров

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.

Далее приведен перечень настроек, которые конфигурирует программа:

1) Установка доступных обновлений ОССН: выполняется отдельно от Red-Book, см. п. 3.2.2;
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. 3.7;
5) Включение блокировки макросов в VLC;
6) Включение механизма контроля подписи в ELF файлах: выполняется отдельно от Red-Book, см. п.3.2.1 или п.3.8;

7) Включение гарантированного удаления файлов и папок: выполняется отдельно от Red-Book, см. п.3.6;
8) Включение системных ограничений Ulimits;
9) Применение парольной политики, способствующей использованию «взломостойких» паролей: выполняется отдельно от Red-Book, см. п.3.4;
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;

Для запуска настройки необходимо кликнуть на статус-кнопку Red-Book. По окончании статус-кнопка изменит свой цвет и надпись в зависимости от успешности выполнения настроек.

3.3 Включение подсистемы контроля целостности

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

3.4 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). 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 данные. 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 и установить флажок напротив пункта «Применить парольную политику».

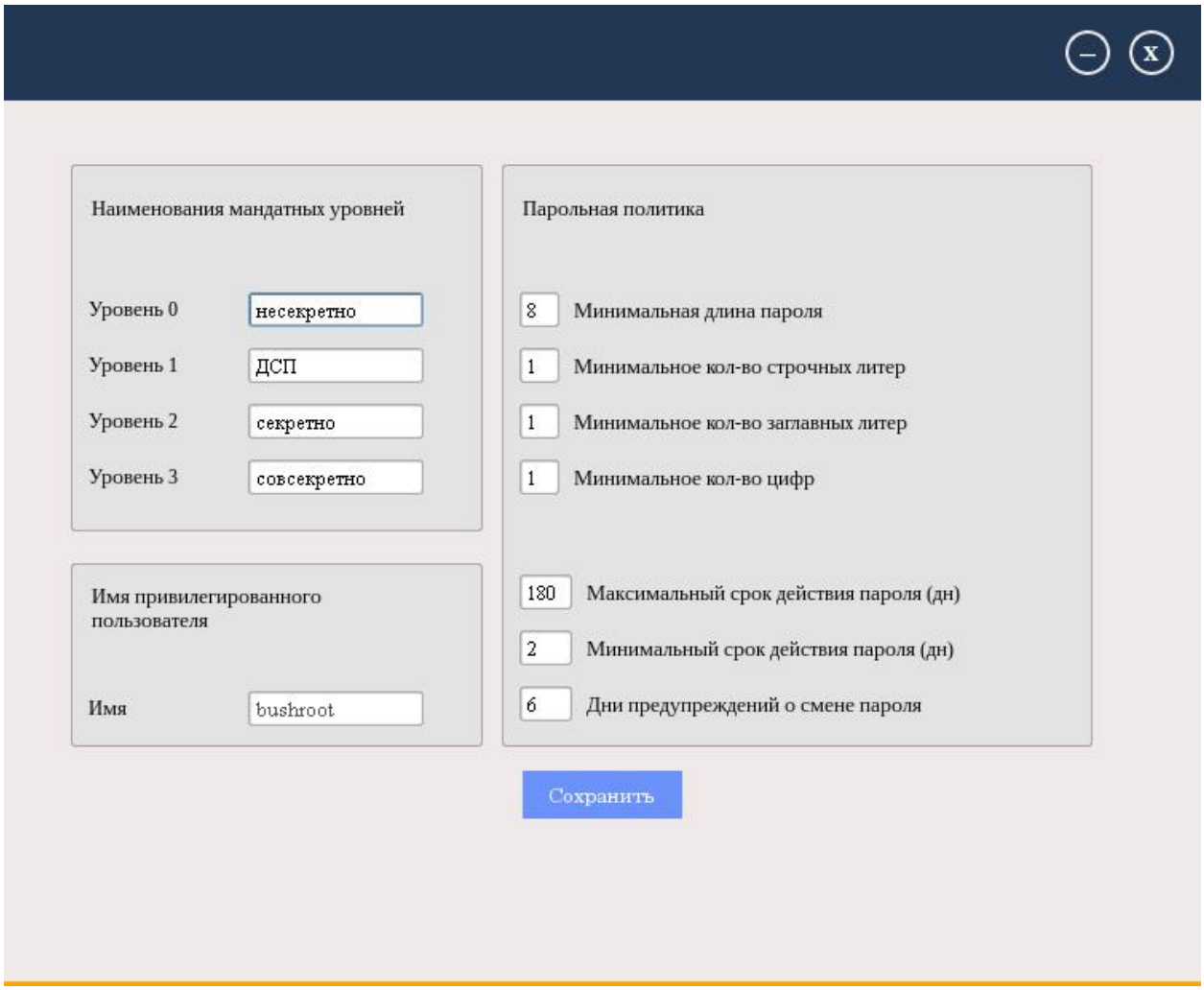

Рисунок 9 – Опции по умолчанию

3.5 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 новое

значение. После этого кликнуть левой кнопкой мыши по кнопке «Сохранить», расположенной в нижней части окна настроек.

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 и установить флажок напротив пункта «Включить подсистему очистки памяти».

3.7 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 и установить флажок напротив пункта «Запрет установки исполняемого бита».

3.8 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 и установить флажок напротив пункта «Включить подсистему ЗПС».

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

3.9 Завершение работы программы

После определения конфигурационных настроек (см. подразделы 3.1, 3.2, 3.4, 3.5, 3.6, 33.7, Ошибка: источник перекрёстной ссылки не найден) нужно кликнуть на кнопку «Применить», расположенную в нижней части окна включения механизмов защиты. После этого отобразится окно статуса выполнения программы (см. Рисунок 10). 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.

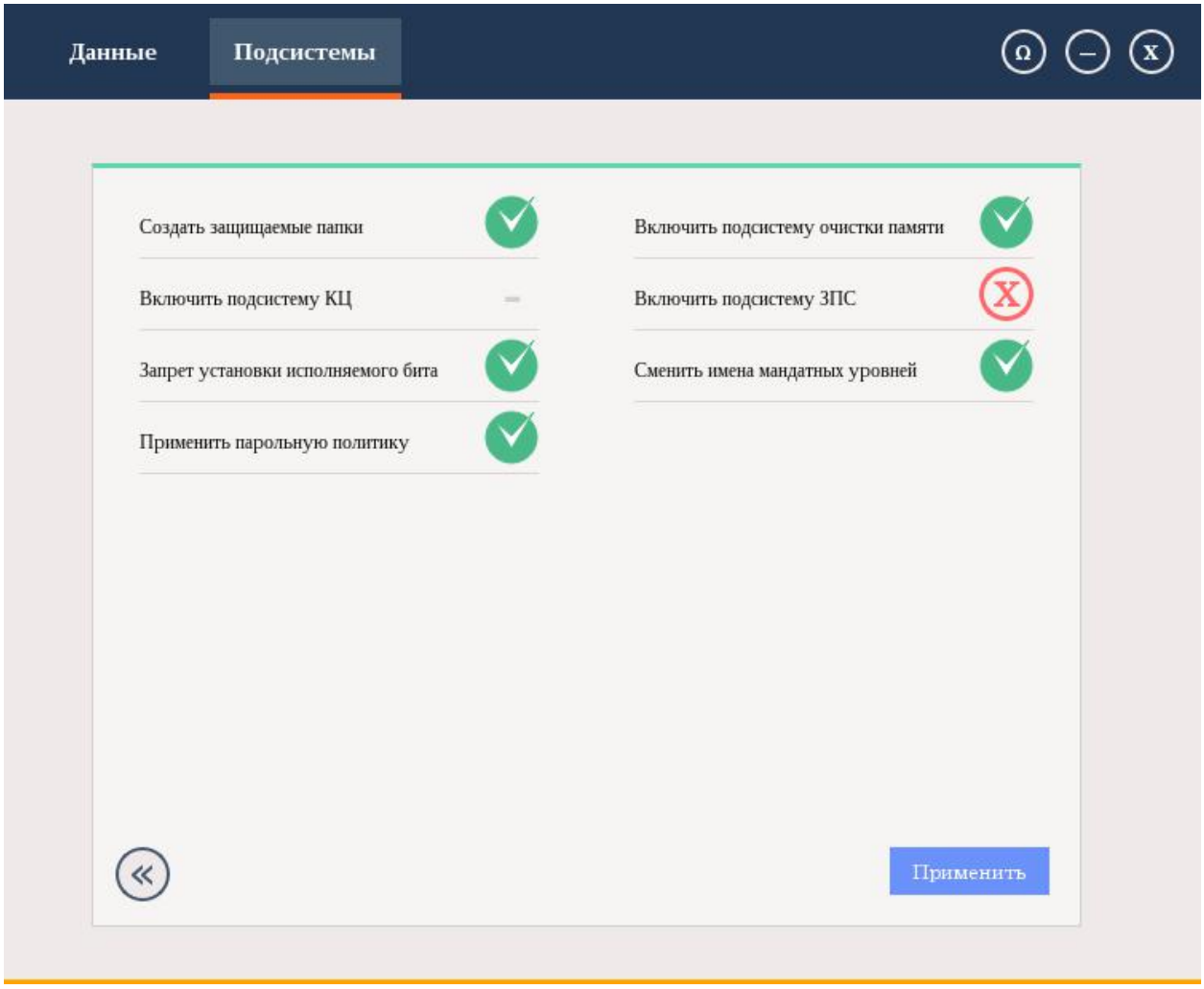

Рисунок 10 – Окно статуса выполнения программы

3.10 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 необходим кликнуть на кнопку «Откатить», расположенную в правой нижней части окна ввода информации. При успешном выполнении процедуры отобразится соответствующее информационное окно (см. Рисунок).

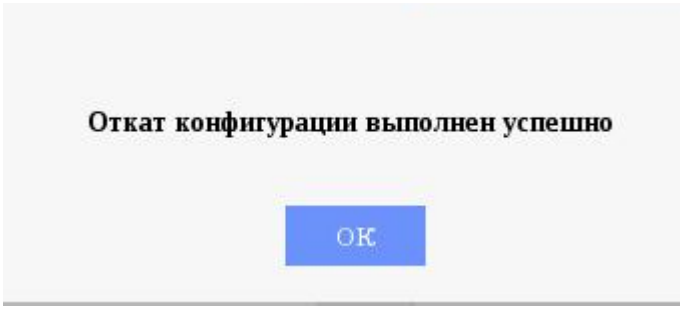

Рисунок 11 – Информационное сообщение

ДЛЯ ЗАМЕТОК

г. Екатеринбург,
ул. Июльская, 41
+7 (343) 374-24-64
www.irsural.ru