

**СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ИНТЕГРИРОВАННОГО
КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ «РАВЕЛИН»**

Руководство системного программиста

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

ЦРПА.2.00397.01.00 32

Листов 43

АННОТАЦИЯ

В настоящем руководстве системного программиста специального программного обеспечения интегрированного комплекса технических средств охраны «Равелин» (далее по тексту — СПО ИК ТСО «Равелин») приведены общие сведения о программе, структуре программы, настройке программы, проверке программы, графическом пользовательском интерфейсе и сообщения системному программисту.

Сокращения, принятые в настоящем руководстве системного программиста:

АПИ	— аппаратно-программный интерфейс;
АРМ	— автоматизированное рабочее место;
АРМ-АБИ	— АРМ администратора безопасности информации;
ВК	— видеокамеры;
ЗМНИ	— защищенный машинный носитель информации;
ИК ТСО	— интегрированный комплекс технических средств охраны;
ЛВС	— локальная вычислительная сеть;
ЛУП	— локальный пункт управления;
МО РФ	— Министерство обороны Российской Федерации;
НТПВ	— неохлаждаемый тепловизор внешнего исполнения;
ОПО	— общее программное обеспечение;
ОС	— операционная система;
ПК	— персональный компьютер;
СВТ	— средства вычислительной техники;
СКУД	— система контроля и управления доступом;
СОН	— система охранного наблюдения;
СПО	— специальное программное обеспечение;
ССКУ	— система сетевого компьютерного управления;
ТО	— техническое обслуживание;
УКУ	— устройство контроля и управления;
ЦПУ	— центральный пункт управления.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ И ЕЕ СТРУКТУРЕ.....	4
2 УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СПО ИК ТСО «РАВЕЛИН»	8
3 ПРОВЕРКА ПРОГРАММЫ	39
4 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ.....	40
5 СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ	41
ПРИЛОЖЕНИЕ А	42

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ И ЕЕ СТРУКТУРЕ

1.1 Назначение программы

Специальное программное обеспечение интегрированного комплекса технических средств охраны «Равелин» (далее — СПО ИК ТСО «Равелин») состоит из компонентов, обеспечивающих:

- непрерывный контроль обстановки, складывающейся на объектах охраны и прилегающих к ним территориях;
- своевременное обнаружение фактов (попыток) несанкционированного проникновения на объект охраны, а также проноса провоза запрещенных предметов и веществ;
- видеофиксацию в режиме реального времени и запись в видеоархив несанкционированного проникновения на объект нарушителя, а также анализ складывающейся обстановки и формирование условий для принятия своевременного решения по прекращению развития нерегламентированной ситуации путем применения средств предупреждения и воздействия и (или) других технических средств ИК ТСО «Равелин»;
- сбор, обработку и представление информации от технических средств и систем ИК ТСО «Равелин», установленных на (в) охраняемых зонах.

1.2 Структура программы

В состав СПО ИК ТСО «Равелин» входят компоненты согласно таблице 1.

Таблица 1 — состав компонентов СПО ИК ТСО «Равелин»

Наименование	Обозначение
СПО системы сетевого компьютерного управления ССКУ	ЦРПА.2.00330.01.00
СПО СКУД. Контроль доступа	ЦРПА.2.00341.01.00
СПО СКУД. Автоматизированная система биоидентификации	ЦРПА.2.00342.01.00
СПО СКУД. Автомобильная досмотровая система	ЦРПА.2.00343.01.00
СПО СКУД. Железнодорожная досмотровая система	ЦРПА.2.00344.01.00
СПО системы охранного наблюдения СОН	ЦРПА.2.00345.01.00
СПО модулей сопряжения	ЦРПА.2.00331.01.00

Далее приведено описание функционала компонентов СПО ИК ТСО «Равелин».

1.2.1 СПО системы сетевого компьютерного управления ССКУ

СПО ССКУ из состава комплекта СПО ИК ТСО «Равелин» обеспечивает:

- контроль за обстановкой на территории охраняемого объекта, прилегающих территориях, во внутренних помещениях зданий и сооружений;
- представление информации на АРМ дежурных сил охраны в двух видах;
- схематичное масштабируемое изображение объекта, используемого операторами АРМ;
- диагностику и управление всеми техническими средствами и системами охраны, установленными на охраняемом объекте;
- разграничение прав пользователей по использованию информационных ресурсов и управлению средствами и системами ИК ТСО «Равелин»;
- хранение всей информации о работе ИК ТСО «Равелин» и действиях пользователей;
- защиту от несанкционированного изменения алгоритмов функционирования и (или) отключения функциональных систем, входящих в них СЧ и ИК ТСО «Равелин» в целом.

1.2.2 СПО СКУД

СПО СКУД. Контроль доступа, СПО СКУД. Автоматизированная система биоидентификации, СПО СКУД. Автомобильная досмотровая система, СПО СКУД. Железнодорожная досмотровая система обеспечивают:

- выполнение типовых алгоритмов доступа;
- формирование точек доступа;
- работу локальной сети контроллеров СКУД;
- возможность автономной работы контроллеров с сохранением контроллерами основных функций при отказе связи с центральным сервером СКУД;
- контроль и учет доступа персонала (посетителей) на объект охраны (помещение, зону);
- назначение индивидуальных временных зон для персонала и транспортных средств на проход/проезд рубежей контроля в течение буднего, выходного и праздничного дня;
- управление доступом посредством идентификации персонала по индивидуальным признакам;
- управление доступом посредством назначения постоянных индивидуальных кодов для считывания их на устройстве считывания кода и идентификации персонала;
- управление доступом посредством назначения сменных индивидуальных и групповых кодов для ввода их персоналом на кодонаборном устройстве и идентификации персонала;
- автоматизацию процессов приема/снятия рубежей (зон) охраны (точек доступа, помещений) под охрану/с охраны;
- управление доступом по правилу «нескольких лиц»; контроль за проносом/провозом запрещенных предметов и веществ; временной, зональный и глобальный контроль повторного прохода; контроль местонахождения персонала и транспортных средств на объекте (количество персонала в охраняемых зонах с указанием идентификационных данных);
- формирование запросов на получение информации, получение и анализ информации от устройств СКУД, формирование и отображение тревожных сообщений;
- сбор информации от устройств системы, ее обработку и хранение в базе СКУД, передачу управляющей информации на периферийные устройства системы;
- защиту разрешительных данных;
- защиту от несанкционированного доступа к техническим и аппаратно-программным средствам контроля управления доступом;
- автоматический и автоматизированный контроль работоспособности устройств, входящих в состав системы, отображение и протоколирование результатов контроля;
- ежедневную смену цифровых кодов-паролей (при наличии) для вскрытия и прохода в особо важные зоны;
- запрет прохода (проезда) при срабатывании средств досмотра и обнаружения запрещенных предметов и веществ, прохода в неустановленное графиком работы время, а также не совпадении идентификационных признаков;
- блокирование нарушителя в шлюзе (преграждающем устройстве) до выяснения причин срабатывания средств досмотра и обнаружения запрещенных предметов и веществ;
- возможность подключения дополнительных средств специального контроля, средств досмотра;
- возможность интеграции автоматизированных средств досмотра днища транспортного средства;
- перевод технических средств контроля и управления доступом в режим «свободного доступа» с центрального пункта управления (ЦПУ) или локального пункта управления (ЛПУ) при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т.п.);

– блокировку прохода по точкам доступа командой с пункта управления (ЦПУ/ЛПУ) в случае возникновения нештатной ситуации (попытки проникновения, нападения на объект и т.п.).

1.2.3 СПО СОН

СПО СОН обеспечивает:

- непрерывный круглосуточный контроль (прямое визуальное наблюдение) оператором АРМ (дежурным из состава сил охраны) за обстановкой на участках контроля охраняемого объекта и прилегающих территориях;
- автоматический вывод видеоинформации на монитор в случае возникновения сигнала «Тревога» с изображением участка, на котором произошло нарушение;
- подтверждение с помощью ВК и НТПВ факта несанкционированного проникновения в контролируруемую (охраняемую) зону и выявление ложных срабатываний (видеоверификацию сигналов «Тревога»);
- управление исполнительными устройствами (поворотными ВК и НТПВ) как средствами СПО, так и с использованием специальных устройств (пультов управления);
- запись видеоинформации (непрерывную, по расписанию, по выбору оператора) в архив для последующего анализа состояния охраняемого объекта (зоны), нештатных и нерегламентированных событий, идентификации нарушителей и других задач;
- выдачу информации о номере зоны наблюдения и ВК (НТПВ);
- формирование не менее четырех зон наблюдения.
- возможность цифровой обработки видеоинформации с функциями многоэкранного режима наблюдения на одном мониторе;
- циклический просмотр видеоинформации ВК и НТПВ, и программирование циклов просмотра (последовательности включения ВК и НТПВ);
- возможность автоматического переключения режимов просмотра в рабочее и нерабочее время (постановка под охрану / снятие с охраны);
- задание и выбор нескольких предустановок для поворотных ВК и НТПВ;
- возможность «предтревожной» записи видеоинформации с изменяемым периодом времени «предтревоги» (начало записи до получения сигнала «Тревоги» со средств обнаружения);
- возможность записи изображения с выбранного ВК и НТПВ щелчком манипулятора «мыши» по пиктограмме ВК и НТПВ, окну выведенного видео на АРМ;
- возможность воспроизведения записанной видеоинформации по произвольной записи программного журнала событий;
- возможность одновременного и независимого от записи доступа к данным и воспроизведения видеоданных с нескольких АРМ в соответствии с правами доступа к информации;
- возможность автоматического улучшения качества записываемого по сигналу «Тревога» изображения путем увеличения частоты записи кадров и разрешающей способности записываемого видеоизображения;
- автоматический разворот платформы ВК и НТПВ или непосредственно поворотным ВК и НТПВ на тревожный участок или движущийся объект (при использовании детектора движения).
- автоматическое обнаружение целей (человек, группа людей, наземное транспортное средство) при помощи ВК и НТПВ;
- автоматическую классификацию целей (человек, группа людей, транспортное средство) на расстоянии не менее 70 метров при помощи ВК, допустимая минимальная относительная погрешность 0,1 %;
- сопровождение (автоматическое и автоматизированное) целей (человек, группа людей, наземное транспортное средство, неопознанный объект) при помощи поворотных ВК и НТПВ (или ВК и НТПВ на поворотных платформах).

- запись видеоинформации и ее хранение в видеоархиве на период от 14 суток в максимальном разрешении ВК и НТПВ с темпом записи не менее 10 кадров в секунду;
- возможность записи «по кольцу» с автоматической перезаписью видеоинформации;
- возможность защиты от перезаписи фрагментов видеоархива, на которых присутствует информация, определенная как «важная»;
- возможность сохранять кадры или фрагменты видеозаписи на стороннем носителе;
- просмотр видеофайлов с возможностью увеличения изображения в три и более раза;
- самодиагностику работоспособности системы с выводом тревожного сообщения при отказе ее элементов;
- индикацию текущего состояния ВК и НТПВ (включено, выключено, исправно, неисправно, тревога и пр.), а также линий связи и шлейфов подключения этих средств;
- управление состоянием (включение, выключение, сброс) ВК и НТПВ;
- проведение регламентных работ по подстройке параметров ВК и НТПВ (сезонные, ежегодные) без непосредственного контакта с ВК и НТПВ в месте его установки.
- возможность поиска видеозаписей:
 - 1) по дате и времени;
 - 2) по тревожным событиям в системе;
 - 3) по определенным ВК и НТПВ или группе ВК и НТПВ;
 - 4) в режиме ускоренной перемотки, паузы, покадрового просмотра.

1.2.4 СПО модулей сопряжения

СПО модулей сопряжения обеспечивает:

- обмен с ССКУ (компонентом ССКУ — сервером оборудования) через ЛВС по унифицированному протоколу верхнего уровня следующей информацией:
 - 1) получение общесистемной конфигурации от сервера оборудования;
 - 2) получение конфигурации устройств от сервера оборудования;
 - 3) загрузка описаний моделей оборудования в сервер оборудования;
 - 4) пересылка в сервер оборудования событий от устройств
- обеспечивает обмен следующей информацией с УКУ через аппаратный интерфейсный модуль по специализированному протоколу УКУ:
 - 1) получение информации о событиях от устройств;
 - 2) управление, подключенными устройствами контроля и управления.

2 УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТОВ СПО ИК ТСО «РАВЕЛИН»

Перед установкой СПО ИК ТСО «Равелин» требуется установить и настроить ОС «Astra Linux Special Edition» (очередное обновление не ниже 1.7, сертификат Минобороны РФ) (далее – ОС «Astra Linux SE»). Необходимые действия по установке и настройке описаны ниже, дополнительная настройка ОС «Astra Linux SE» проводится согласно документации на ОС.

2.1 Установка и настройка ОС «Astra Linux SE» (очередное обновление 1.7)

2.1.1 Установка ОС «Astra Linux SE» (очередное обновление 1.7)

Установку ОС рекомендуется проводить в режиме **Графическая установка** (рис. 1).

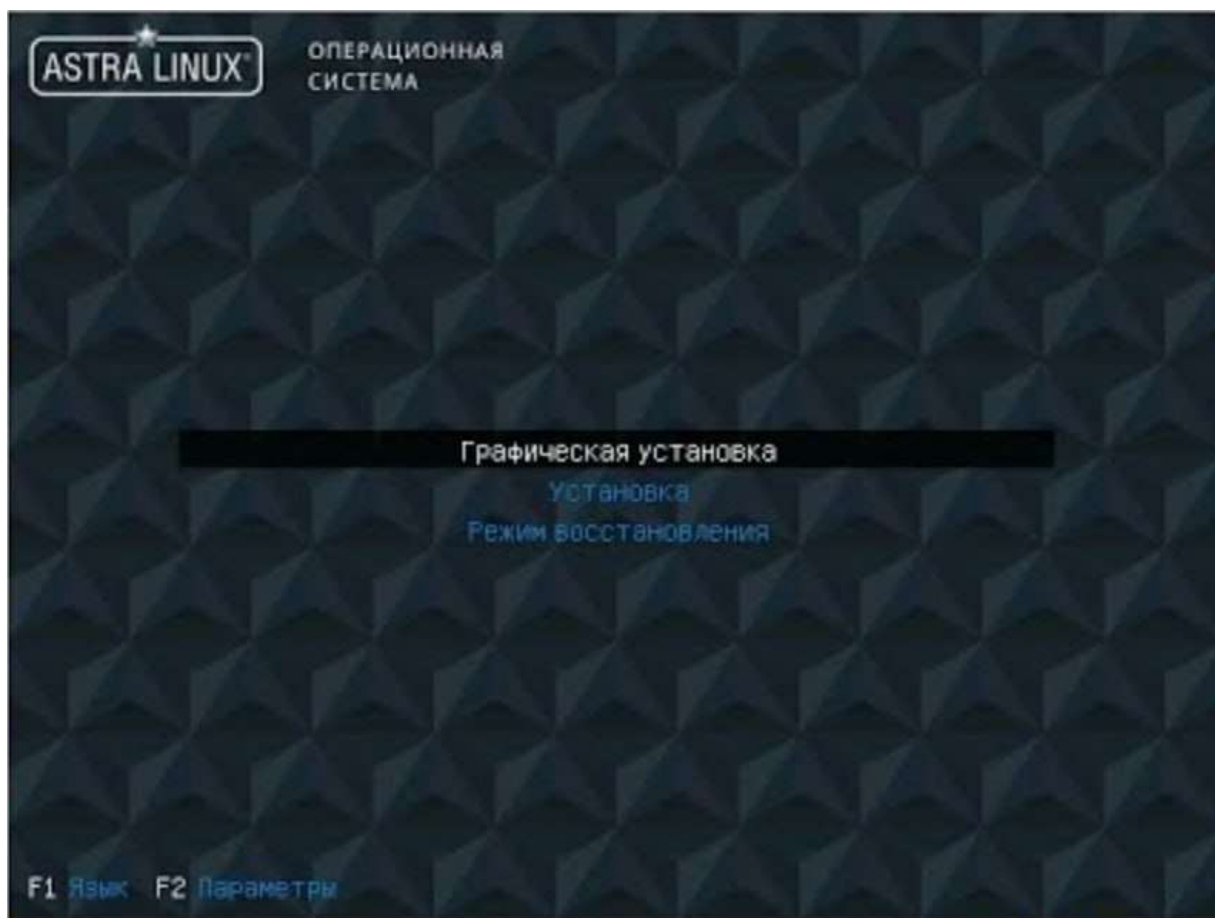


Рисунок 1 — Выбор режима Графическая установка

В окне **Лицензия**, после прочтения лицензионного соглашения, нажать кнопку **Продолжить**.

В окне **Выберите язык** выбрать язык **Russian – Русский**, в окне **Выберите местонахождение**, выбрать **Российская Федерация**.

В окне **Настройка клавиатуры**, выбрать способ переключения национальной и стандартной латинской раскладкой, либо оставить по умолчанию комбинацию клавиш «Alt+Shift». Нажать кнопку **Продолжить**.

В окне **Настройка сети** ввести уникальное имя компьютера например, **astra** или **rav-arm**. Нажать кнопку **Продолжить**.

В окне **Настройка учетных записей пользователей и паролей** создать пользователя с именем **algot** и паролем **12345678** (рис. 2, 3). Пароль пользователя будет изменен во время установки СПО ИК ТСО «Равелин». Нажать кнопку **Продолжить**.

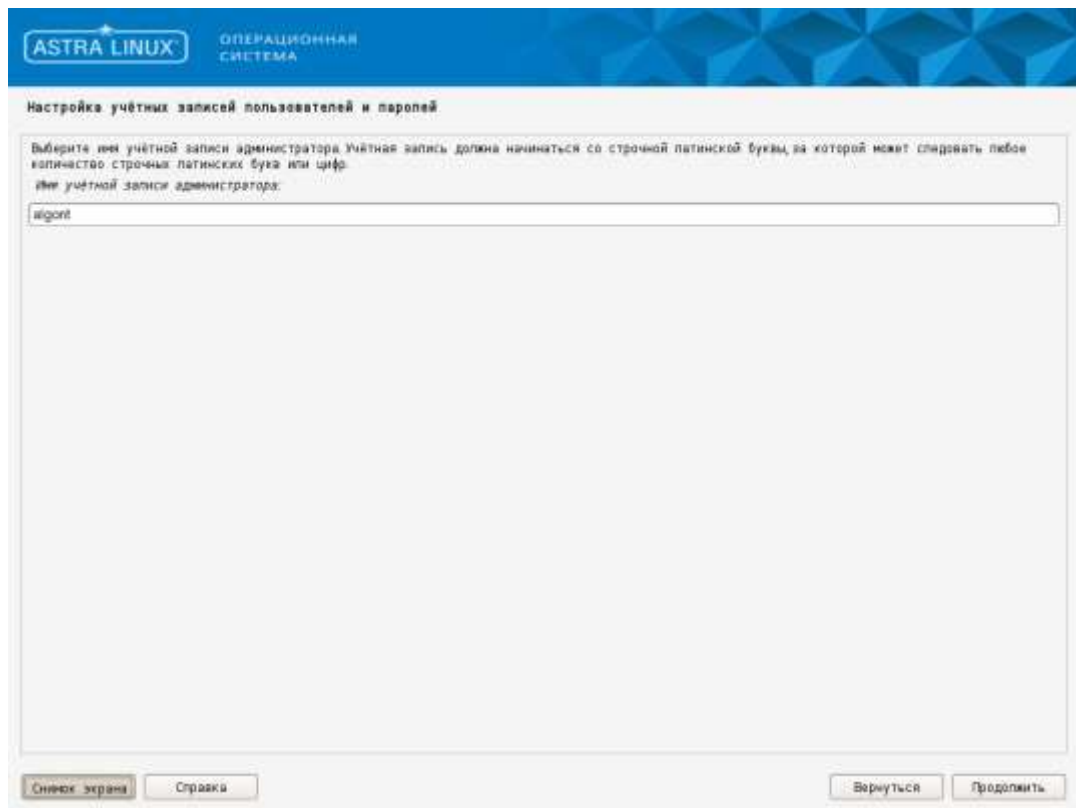


Рисунок 2 — Настройка учетных записей пользователей и паролей. Ввод имени учетной записи

ASTRA LINUX[®] ОПЕРАЦИОННАЯ СИСТЕМА

Настройка учётных записей пользователей и паролей

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.
Введите пароль для нового администратора:

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.
Введите пароль ещё раз:

Снимок экрана Справка Вернуться Продолжить

Рисунок 3 — Настройка учетных записей пользователей и паролей. Ввод пароля учетной записи

В окне **Настройка времени** выбрать часовой пояс по названию крупного города или региона, который находится в этом же поясе (рис. 4). Нажать кнопку **Продолжить**.

ASTRA LINUX[®] ОПЕРАЦИОННАЯ СИСТЕМА

Настройка времени

Если нужного часового пояса нет в списке, то вернитесь к шагу "Выбор языка" и выберите страну, в которой используется требуемый часовой пояс (страну, в которой вы живёте или сейчас находитесь).
Выберите часовой пояс:

Москва-01 - Калининград
Москва-00 - Москва
Москва-01 - Самара
Москва-02 - Екатеринбург
Москва-03 - Омск
Москва-04 - Красноярск
Москва-05 - Иркутск
Москва-06 - Якутск
Москва-07 - Владивосток
Москва-08 - Магадан
Москва-09 - Камчатка

Снимок экрана Справка Вернуться Продолжить

Рисунок 4 — Настройка времени

В окне **Разметка дисков** выбрать «Авто – использовать весь диск», нажать **Продолжить**. В следующем окне **Разметка дисков** выбрать «**SCSI1 (0.0.0) (sda) - ...**», нажать кнопку **Продолжить**. Далее, рекомендуется использовать схему **Все файлы в одном разделе** (рис. 5). Нажать кнопку **Продолжить**.

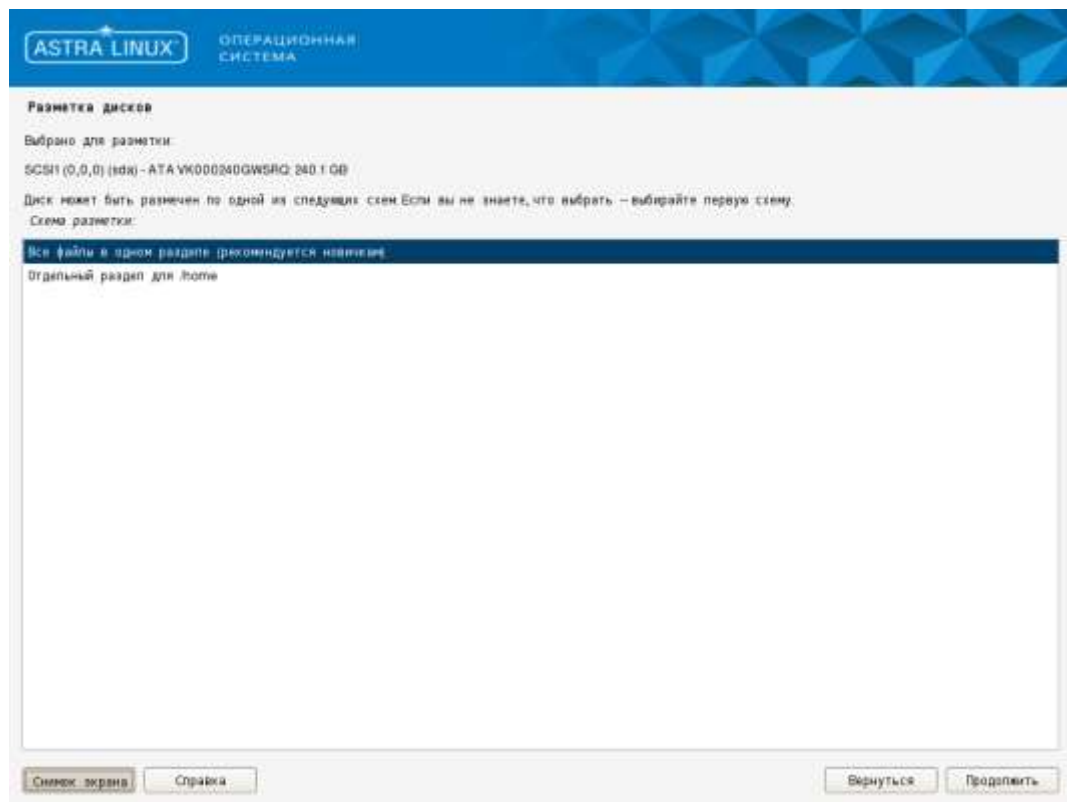


Рисунок 5 — Разметка дисков

Выбрать **Закончить разметку и записать изменения на диск** (рис. 6). Нажать кнопку **Продолжить**. Произвести запись изменений на диск, выбрав **Да** (рис. 7) и нажать кнопку **Продолжить**.



Рисунок 6 — Разметка дисков

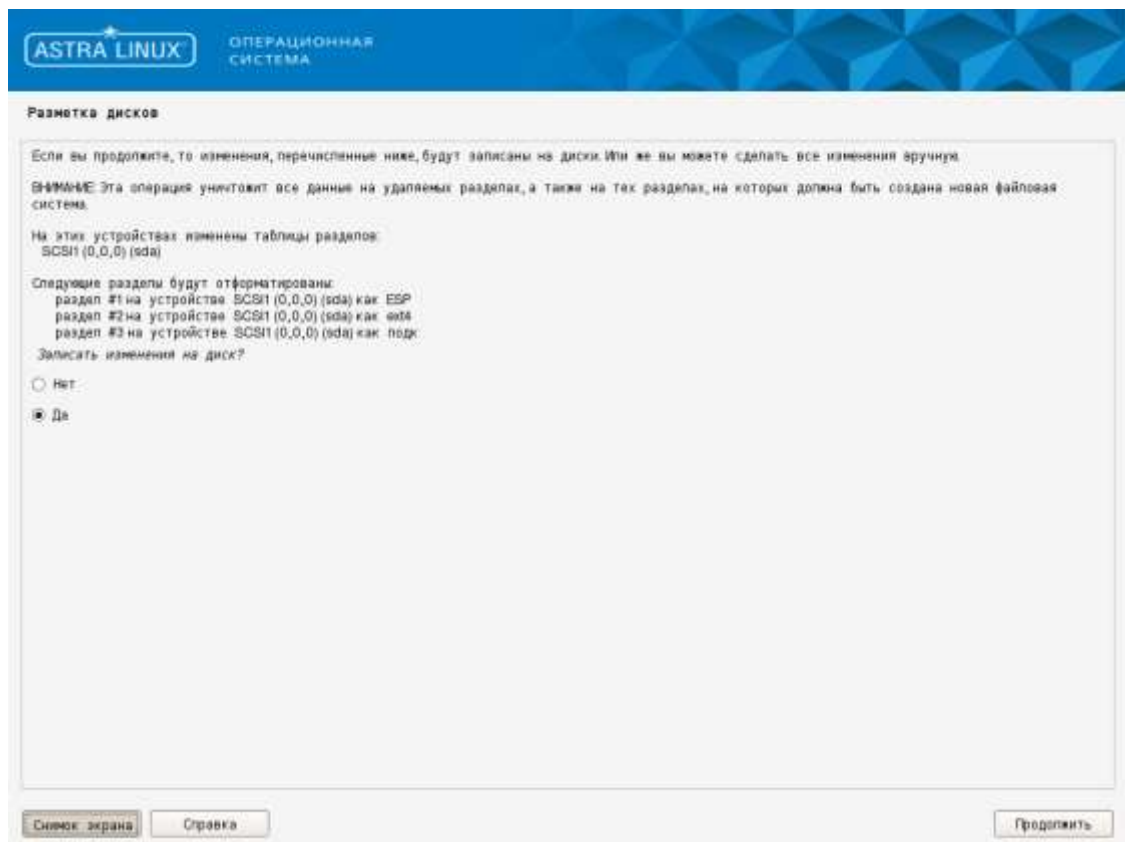


Рисунок 7 — Разметка дисков

В окне **Выбор программного обеспечения** (рис. 8) выбрать Графический интерфейс Fly, Средства работы с Интернет, Консольные утилиты, Средства удаленного подключения.

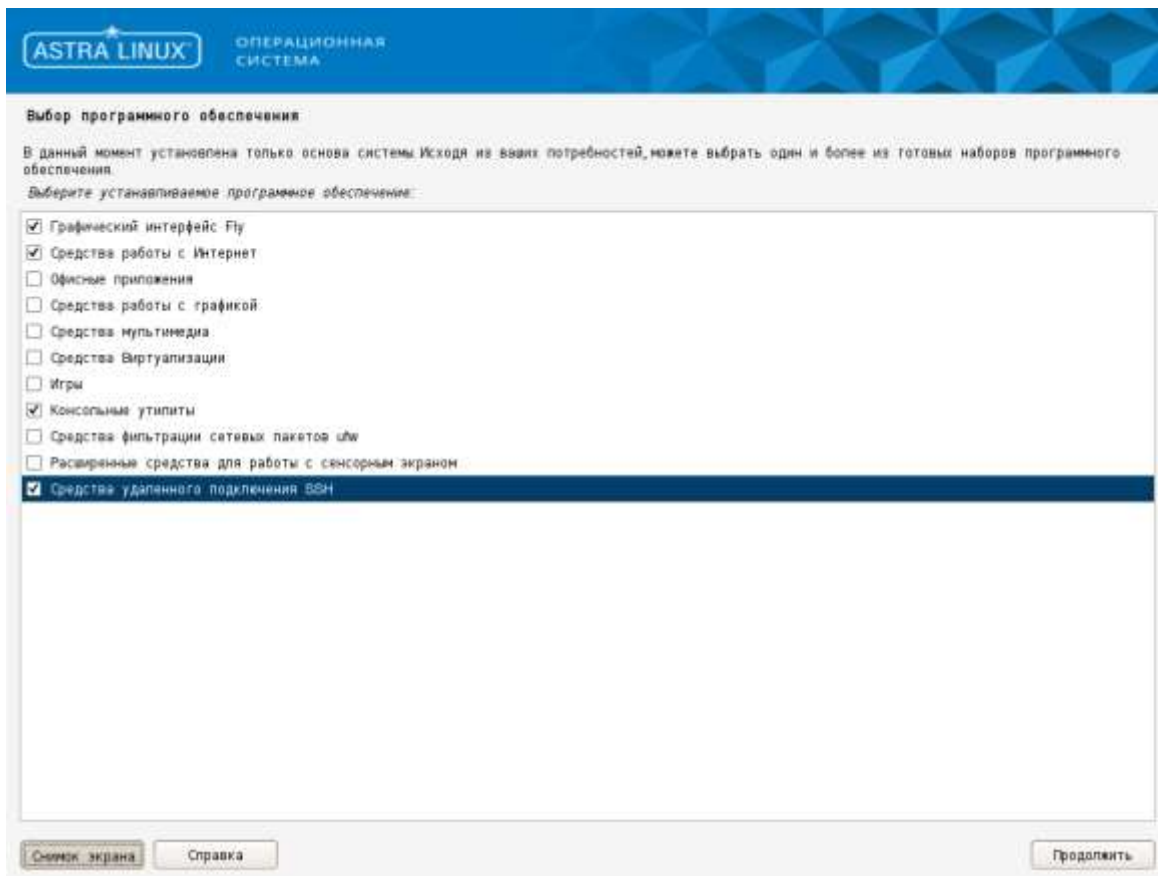


Рисунок 8 — Выбор программного обеспечения

В окне **Дополнительные настройки ОС** выбрать **Максимальный уровень защищенности «Смоленск»** (рис. 9), нажать кнопку **Продолжить**.

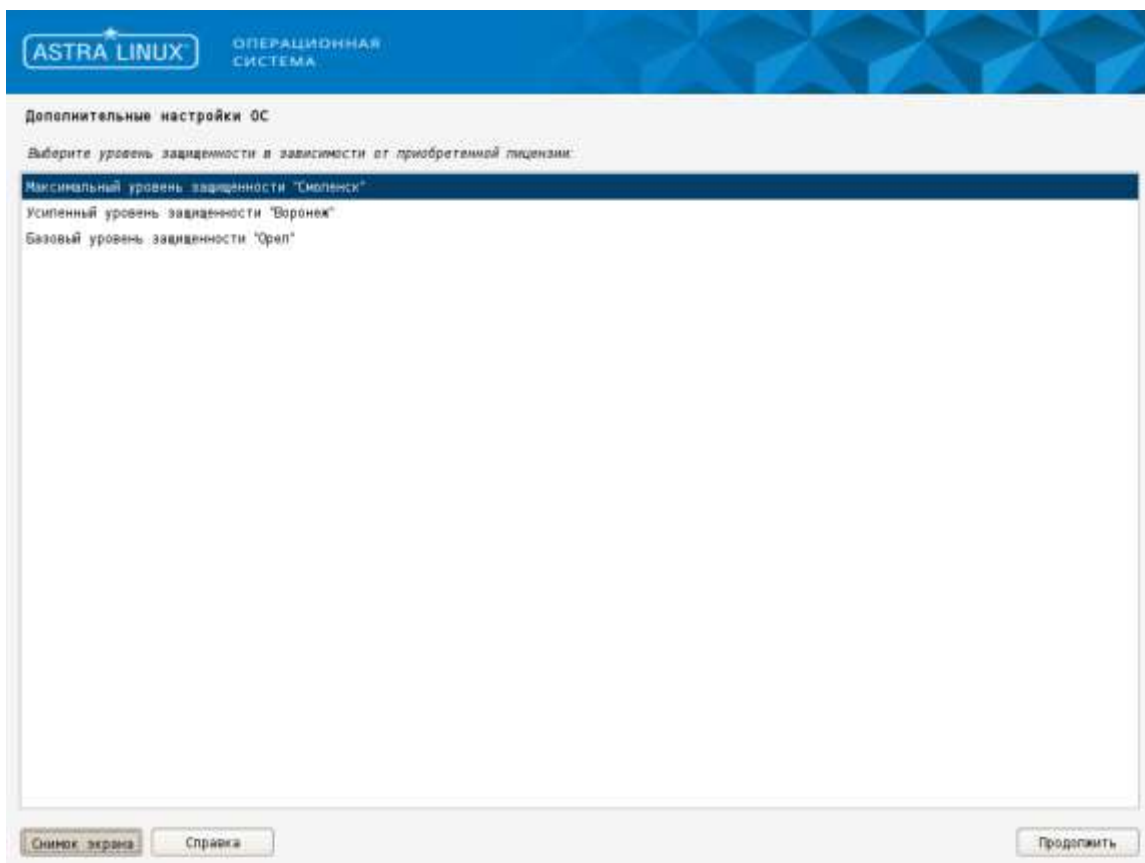


Рисунок 9 — Дополнительные настройки ОС

Выбрать **Запрет автонастройки сети** (рис. 10), нажать кнопку **Продолжить**.

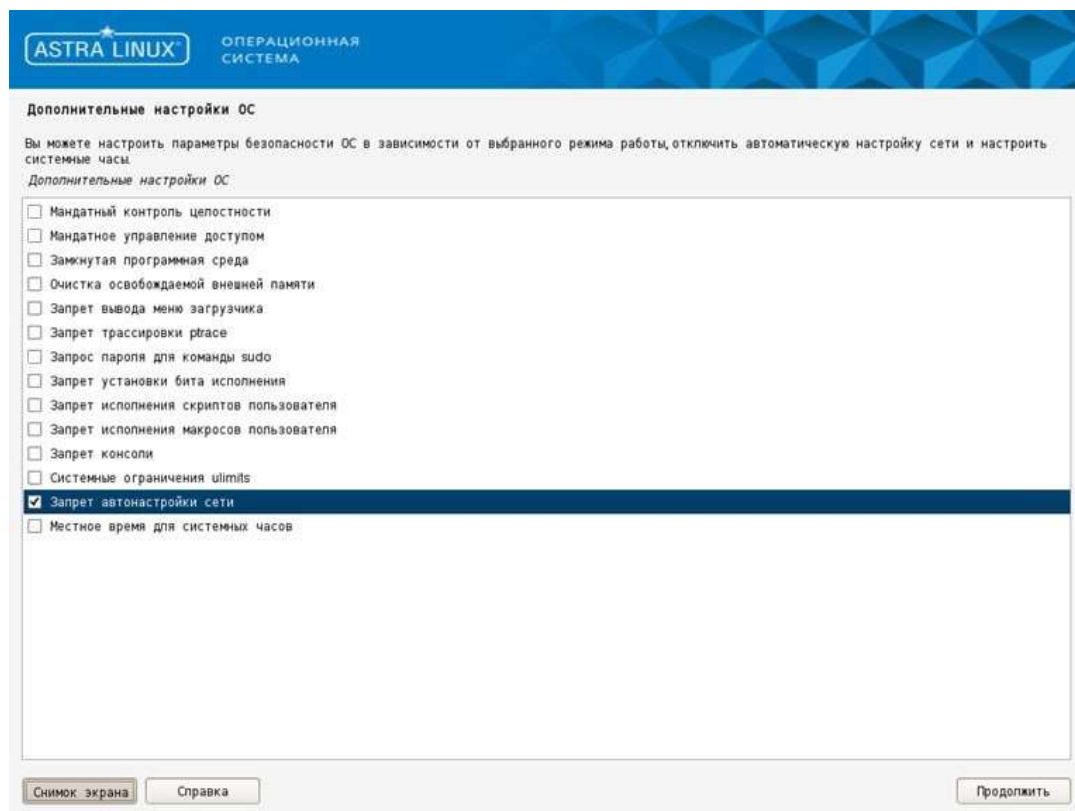


Рисунок 10 — Дополнительные настройки ОС

В окне **Установка системного загрузчика GRUB на жесткий диск** выбрать **Да**, нажать кнопку **Продолжить**.

Ввести пароль для GRUB: **12345678** (рис. 11), для защиты от несанкционированного доступа, нажать кнопку **Продолжить**. Повторно ввести пароль для GRUB, нажать кнопку **Продолжить**.

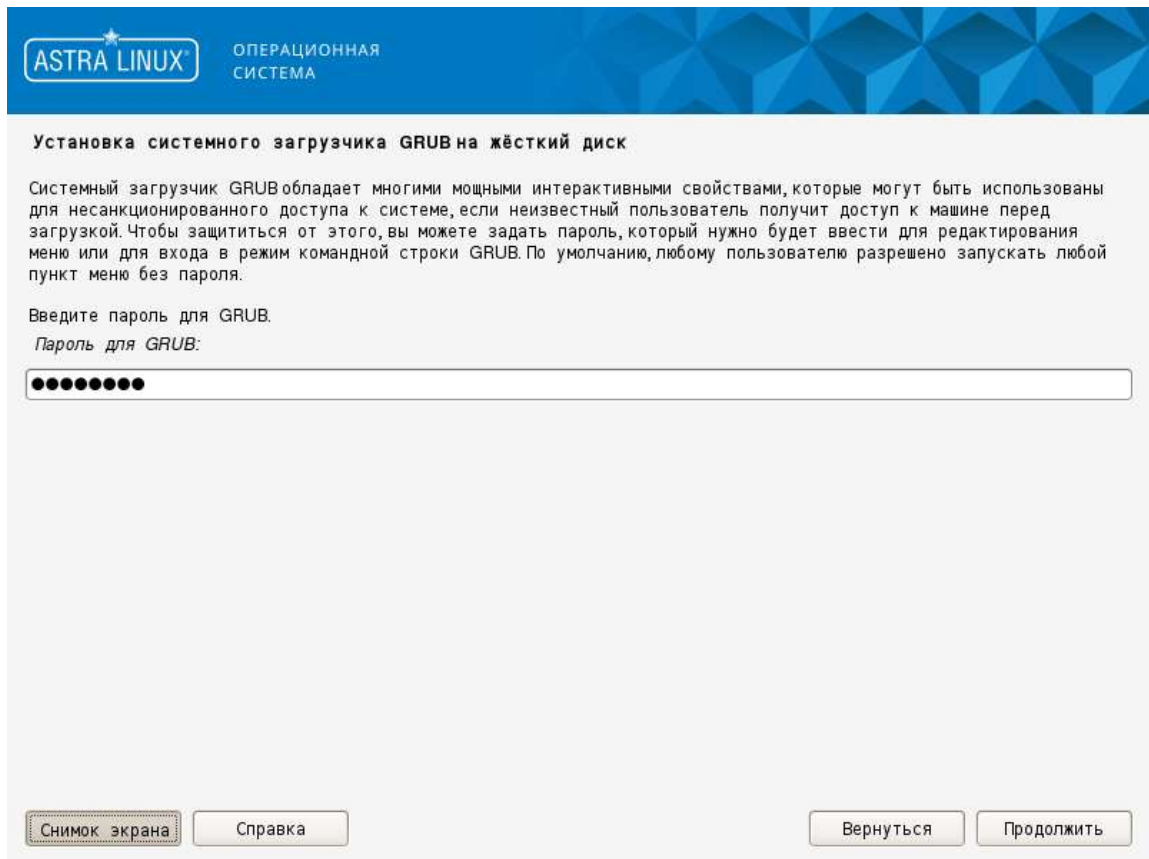


Рисунок 11 — Установка пароля для GRUB

После появления окна **Завершение установки**, извлечь установочный носитель и нажать кнопку **Продолжить**.

После завершения процесса установки произойдет автоматическая перезагрузка.

2.1.2 Настройка учетной записи root и разрешение административного входа

Войти в ОС «Astra Linux SE» под учетной записью пользователя **algont**. Открыть меню **Пуск** → **Панель управления** (рис. 12). Выбрать раздел **Безопасность** → **Политика безопасности** → **Пользователи** (рис. 13)

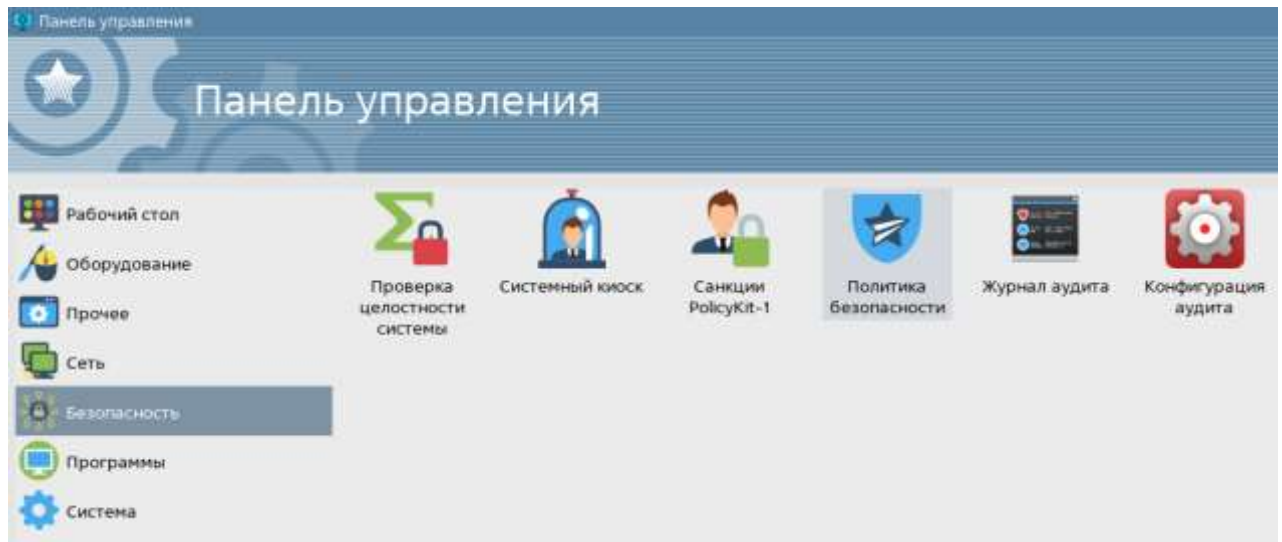


Рисунок 12 — Политика безопасности

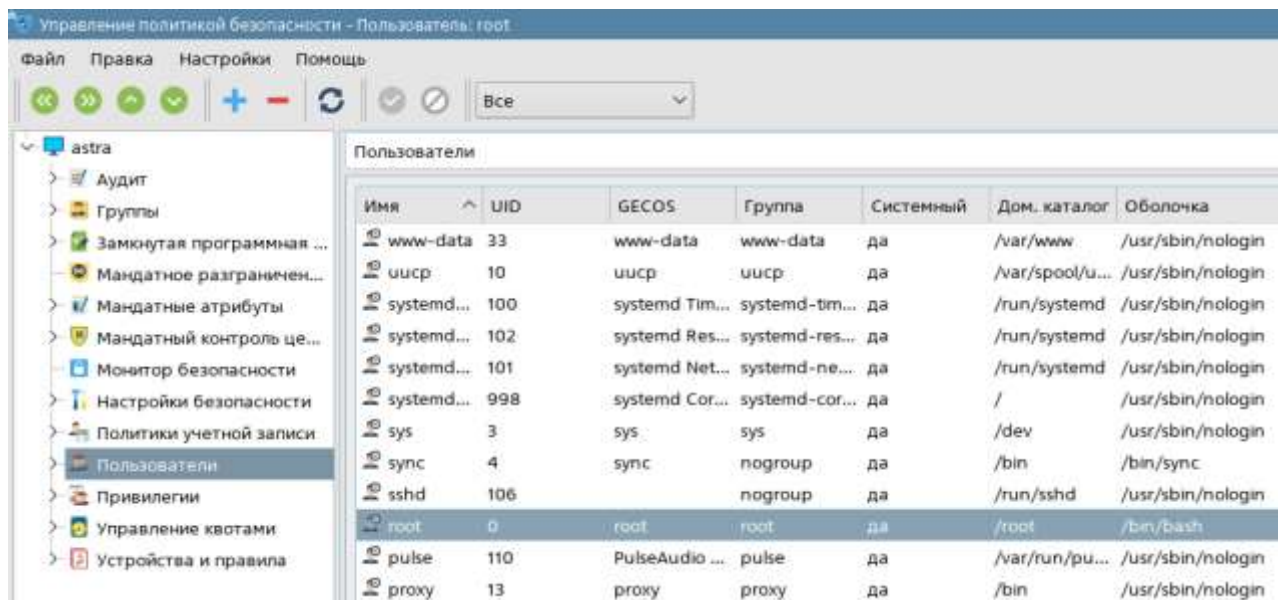


Рисунок 13 — Пользователи

В выпадающем списке выбрать **Все**. Нажать два раза левой кнопкой мыши по пользователю **root**. Нажать кнопку **Изменить**. В открывшемся окне ввести новый пароль и повтор пароля. Появится сообщение об успешном вводе пароля. Открыть вкладку **Привилегии**. Активировать все чекбоксы в разделах **Linux** и **Parsec** и применить изменения (рис. 14).

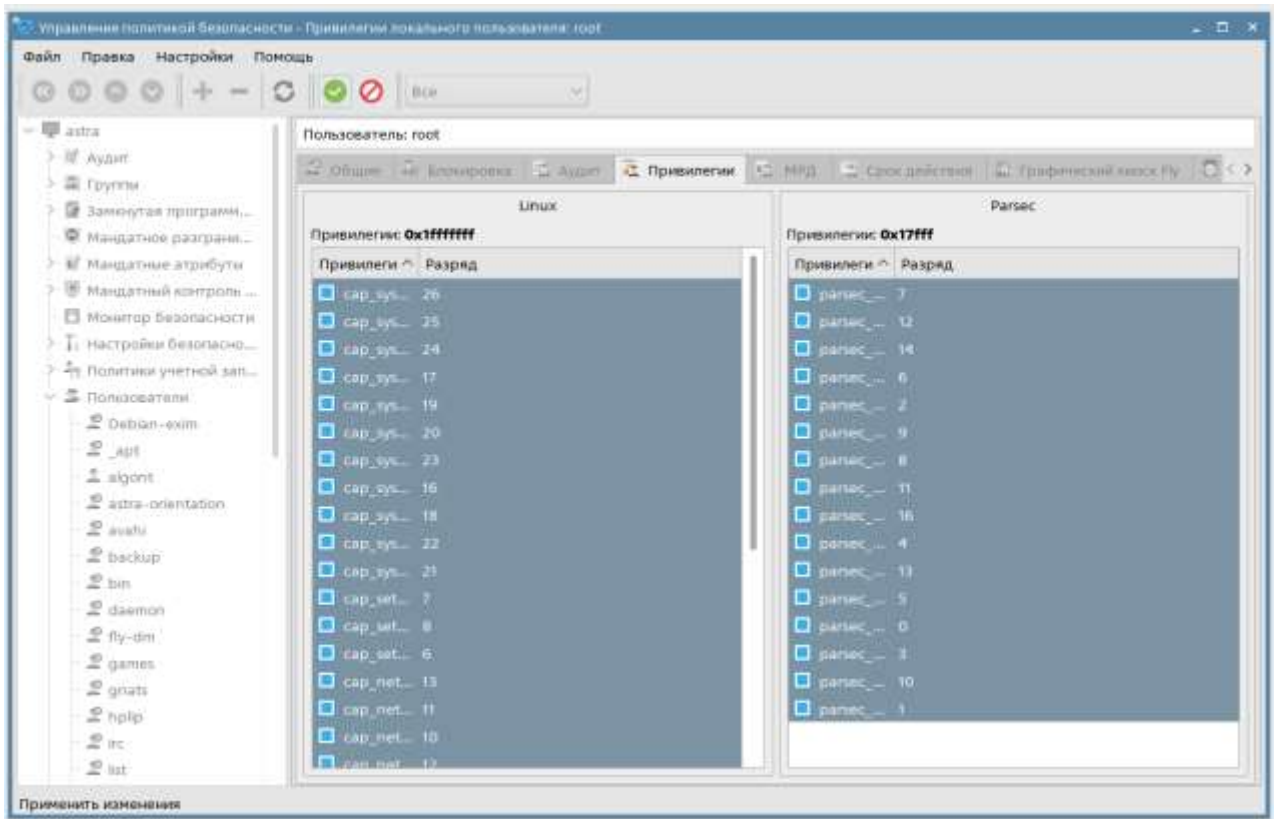


Рисунок 14 — Пользователь: root. Вкладка Привилегии

Закреть окно. Перейти **Панель управления** → **Система** → **Вход в систему**, выбрать вкладку **Пользователи**, активировать чекбокс **Разрешить вход администратору root** (рис. 15). Нажать **Да**. Перезагрузить компьютер.

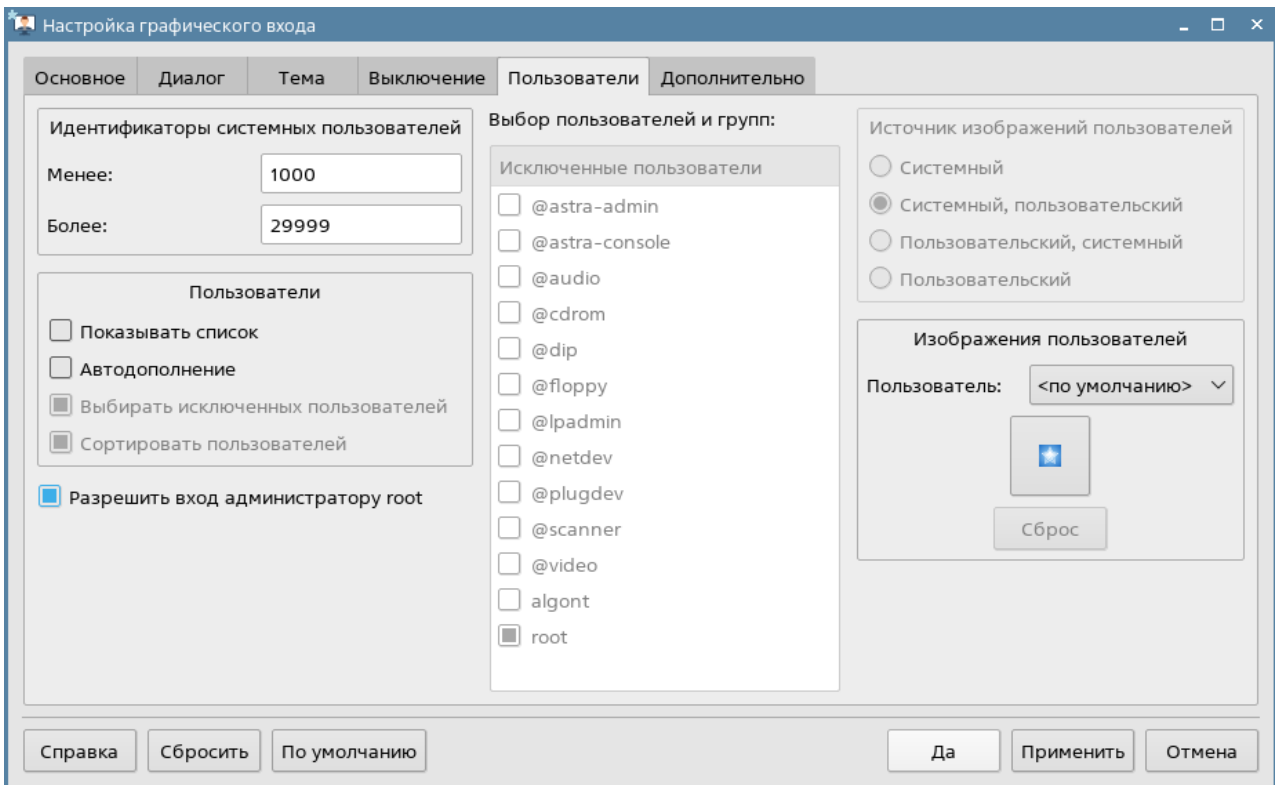


Рисунок 15 — Активация чекбокса

2.1.3 Создание локального репозитория с установочного диска ОС «Astra Linux SE»

Для работы СПО ИК ТСО «Равелин» необходимы пакеты с установочного диска ОС «Astra Linux SE», для этого необходимо создать копию установочного диска ОС «Astra Linux SE» и подключить его как репозиторий:

1) Подключить DVD-привод из комплекта ЗИП-О ЦРПА.424933.238 к USB-разъему ПК.

2) Вставить установочный диск ОС «Astra Linux SE» в DVD-привод. Примечание — необходимо использовать установочный диск ОС «Astra Linux SE» для ПК (APM, сервер), прописанный в формуляре на выбранный ПК.

3) Войти в ОС «Astra Linux SE» под логином и паролем `algotn`.

Запустить Терминал Fly, если ОС загружена в графическом режиме. При отсутствии графического режима работать в консоли.

Примечание — все последующие команды выполнять через механизм `sudo`, или выполнить команду `sudo su` и ввести пароль.

4) Определить название DVD-привода командой

```
lsblk | awk '/rom/ {print $1}'
```

5) Примонтировать устройство к файловой системе ОС «Astra Linux SE» командой

```
mount /dev/<sr1> /media/cdrom
```

где `<sr1>` — название устройства с типом `<rom>`, которое было определено в перечислении 4) п. 2.1.2 настоящего руководства. Дождаться окончания процесса монтирования.

6) Создать директорию для будущего репозитория командой

```
mkdir -p /srv/repo/astra/main
```

Убедиться, что директория пуста, выполнив команду

```
rm -rf /srv/repo/astra/main/*
```

7) Скопировать содержимое установочного диска в созданную директорию командой

```
cp -a /media/cdrom/* /srv/repo/astra/main
```

8) Для определения источника локального репозитория необходимо создать файл `/etc/apt/sources.list.d/astra_main.list` и написать в нём следующую строку:

```
deb file:/srv/repo/astra/main 1.7_x86-64 contrib main non-free
```

Данное действие выполнить следующей командой:

```
echo "deb file:/srv/repo/astra/main 1.7_x86-64 contrib main non-free" >/etc/apt/sources.list.d/astra_main.list
```

9) Размонтировать устройство командой

```
umount /media/cdrom
```

Извлечь установочный диск ОС «Astra Linux SE» из DVD-привода.

10) В файлах `/etc/apt/sources.list` и `/etc/apt/sources.list_astra` закомментировать все строки, чтобы при обновлении ОС «Astra Linux SE» не требовался установочный диск.

11) Выполнить обновление информации о пакетах из всех настроенных источников командой

```
apt update
```

Теперь пакеты, входящие в диск установки, доступны без использования самого диска.

2.1.4 Установка обновления (изменения) репозитория установочного диска (Бюллетень № 2023-0426SE17)

Оперативное обновление 1.7.4 (Бюллетень № 2023-0426SE17) представляет собой кумулятивное обновление безопасности, предназначенное для нейтрализации угроз эксплуатации выявленных уязвимостей и совершенствования функциональных возможностей операционных систем специального назначения «Astra Linux SE» РУСБ.10015-01 (очередное обновление 1.7).

Для установки необходимо выполнить следующие действия:

1) Войти в ОС «Astra Linux SE» под логином и паролем `algont`.

Запустить Терминал Fly, если ОС загружена в графическом режиме. При отсутствии графического режима работать в консоли.

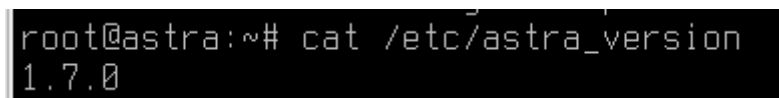
Примечание — все последующие команды выполнять через механизм `sudo`, или выполнить команду `sudo su` и ввести пароль.

2) Проверить текущую версию ОС «Astra Linux SE» командой

```
cat /etc/astra_version
```

Если результат выполнения команды — 1.7.4, то дальнейших действий не требуется.

Если результат выполнения команды — 1.7.0 (рис. 16), то необходимо выполнить действия п. 2.1.2 настоящего руководства, если не были выполнены ранее и продолжить выполнение действий далее.



```
root@astra:~# cat /etc/astra_version
1.7.0
```

Рисунок 16 — Результат выполнения команды

3) Убедиться в наличии пакета `astra-update`.

Проверить информацию о пакете командой

```
apt-cache policy astra-update
```

В случае отсутствия установленной версии, установить командой

```
apt install -y astra-update
```

Примечание — если не удалось найти пакет `astra-update`, необходимо выполнить п. 2.1.2 настоящего руководства.

4) Проверить версию ядра Linux командой

```
uname -r
```

Если версия ядра менее чем 5.10 (например, 5.4.0-81-generic), то необходимо установить актуальное ядро Linux в соответствии с п.2.1.5 настоящего руководства и только потом переходить к выполнению следующего перечисления.

Примечание — работоспособность операционной системы не гарантируется при комбинировании ядер и пакетов из разных обновлений.

5) Подключить DVD-привод из комплекта ЗИП-О ЦРПА.424933.238 к USB-разъему ПК.

6) Вставить диск РУСБ.10015-01 (оперативное обновление 1.7.4) ОС «Astra Linux Special Edition». Бюллетень № 2023-0426SE17 в DVD-привод, примонтировать его в папку /iso-update командами:

```
mkdir -p /media/iso-update  
mount /media/cdrom/repository-update.iso /media/iso-update
```

7) Создать каталог для локального репозитория с файлами оперативного обновления командой:

```
mkdir /srv/repo/astra/update
```

8) Скопировать из /media/iso-update файлы в локальный репозиторий /srv/repo/astra/update командой
cp -a /media/iso-update/* /srv/repo/astra/update

Для определения источника локального репозитория необходимо создать файл /etc/apt/sources.list.d/astra_update.list и добавить в него следующую строку

```
deb file:/srv/repo/astra/update stable main contrib non-free
```

Для этого выполнить команду

```
echo "deb file:/srv/repo/astra/update stable main contrib non-free" >/etc/apt/sources.list.d/astra_update.list
```

9) Размонтировать устройство командами

```
umount /media/iso-update  
umount /media/cdrom
```

10) Выполнить обновление информации о пакетах из всех настроенных источников командой

```
apt update
```

11) Выполнить команду

```
sudo astra-update -A -r
```

Дождаться выполнения обновления.

12) Перезагрузить компьютер командой `reboot`

13) Рекомендуется выполнить Обновление ядра Linux до актуальной версии для ОС «Astra Linux SE» 1.7 с использованием модификации ядра 5.15 в соответствии с п.2.1.5 настоящего руководства.

2.1.5 Обновление ядра Linux до актуальной версии для ОС «Astra Linux SE» 1.7

Примечание — Обязательно должен быть создан локальный репозиторий с использованием актуального (с целевой версией ОС «Astra Linux SE») диска установки (п. 2.1.2 настоящей инструкции).

1) Войти в ОС «Astra Linux SE» под логином и паролем суперпользователя `root`.

Запустить Терминал Fly, если ОС загружена в графическом режиме. При отсутствии графического режима работать в консоли.

Примечание — все последующие команды выполнять через механизм `sudo`, или выполнить команду `sudo su ~` и ввести пароль.

2) Определить версию ОС «Astra Linux SE» командой

```
cat /etc/astra_version
```

3) Для ОС «Astra Linux SE». Бюллетень № 2023-0426SE17 (оперативное обновление 1.7.4) необходимо установить ядро модификации 5.15.

Примечание — Целевая модификация ядра в зависимости от версии ОС «Astra Linux SE»:

- ядро модификации 5.4 доступно при версии 1.7.0;
- ядро модификации 5.10 доступно при версии 1.7.1;
- ядро модификации 5.15 доступно при версии 1.7.2 — 1.7.4;
- ядро модификации 6.1 доступно при версии 1.7.5.

Примечание — работоспособность операционной системы при комбинировании ядер и пакетов из разных обновлений не гарантируется.

Для определения текущей версии ядра выполнить команду

```
uname -r
```

Если текущая версия ядра меньше целевой модификации ядра (например, текущая версия ОС «Astra Linux SE» — 1.7.1, а текущая версия ядра 5.4.0-81-generic), то необходимо выполнить обновление целевой модификации ядра (в указанном примере до 5.10). В противном случае обновление целевой модификации ядра (перечисление 4)-13) п. 2.1.5 настоящего руководства) не требуется.

4) Выполнить обновление целевой модификации ядра Linux, для этого необходимо определить текущие установленные ядра командой

```
dpkg --get-architecture | grep "linux-image-"
```

Вывод команды покажет фактически установленные ядра на ОС.

Если целевая модификация ядра присутствует в этом списке, то необходимо добавить её в автозагрузку выполнив перечисления 14)-17) п. 2.1.5 настоящей инструкции, а действия по установке целевой модификации ядра не требуются (перечисление 10)-13) п. 2.1.5 настоящей инструкции).

5) Вставить диск РУСБ.10015-01 (оперативное обновление 1.7.4) ОС « Astra Linux Special Edition ». Бюллетень № 2023-0426SE17 в DVD-привод, примонтировать его в папку `/iso-update` командами:

```
mkdir -p /media/iso-update
```

```
mount /media/cdrom/repository-update.iso /media/iso-update
```

6) Создать каталог для локального репозитория с файлами оперативного обновления командой:

```
mkdir /srv/repo/astra/update
```

7) Скопировать из `/media/iso-update` файлы в локальный репозиторий `/srv/repo/astra/update` командой

```
cp -a /media/iso-update/* /srv/repo/astra/update
```

Для определения источника локального репозитория необходимо создать файл

/etc/apt/sources.list.d/astra_update.list и добавить в него следующую строку

```
deb file:/srv/repo/astra/update stable main contrib non-free
```

Для этого выполнить команду

```
echo "deb file:/srv/repo/astra/update stable main contrib non-free" >/etc/apt/sources.list.d/astra_update.list
```

8) Размонтировать устройство командами

```
umount /media/iso-update
```

```
umount /media/cdrom
```

9) Извлечь диск РУСБ.10015-01 (оперативное обновление 1.7.4) ОС «Astra Linux Special Edition». Бюллетень № 2023-0426SE17 из DVD-привода.

10) Для установки целевой модификации ядра необходимо проверить доступность целевой модификации ядра для установки. Выполнить обновление информации о пакетах командой

```
sudo apt update
```

Определить доступные для установки ядра:

```
apt-cache policy linux-image* | grep linux-image
```

Вывод команды покажет все доступные для установки ядра. Чтобы отсортировать вывод команды, можно добавить номер модификации, например

```
apt-cache policy linux-image* | grep linux-image-5.15
```

Вывод последней команды не должен оказаться пустым.

11) Запуск установки метапакета модификации ядра Linux выполнить командой

```
sudo apt install -y linux-X.X
```

где, X.X — номер модификации

Например, для установки модификации ядра 5.15 выполнить команду

```
sudo apt install -y linux-5.15
```

Примечание — не рекомендуется использовать установку ядер через метапакеты linux-X.X-generic, linux-X.X-hardened, linux-X.X-lowlatency, так как автоматическое обновление пакетов выполняться не будет.

12) Выполнить перезагрузку ОС командой

```
sudo reboot now
```

13) После перезагрузки выполнить проверку используемого ядра командой

```
uname -r
```

Если окажется, что текущая версия ядра не совпадает с установленной, необходимо добавить новую модификацию ядра в автозагрузку, выполнив действия перечислений 14)-17).

14) Для изменения стандартного пункта загрузки GRUB необходимо получить список возможных значений пунктов загрузки ядра Linux выполнив команду

```
sudo awk '/^menuentry/ { for(i=1; i<=NF; i++) if($i ~ /gnulinux/) {print$i} }' /boot/grub/grub.cfg
```

Пример вывода команды показан на рисунке 17.

```
'gnulinux-5.15.0-70-lowlatency-advanced-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.15.0-70-lowlatency-recovery-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.15.0-70-hardened-advanced-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.15.0-70-hardened-recovery-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.15.0-70-generic-advanced-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.15.0-70-generic-recovery-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.4.0-110-generic-advanced-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
'gnulinux-5.4.0-110-generic-recovery-792a2f2f-d3b8-4c0a-a56e-321258823c3e'
```

Рисунок 17 — Результат выполнения команды

15) Изменить пункт загрузки GRUB по умолчанию, выполнив команду

```
sudo sed -i 's/^GRUB_DEFAULT=.* /GRUB_DEFAULT={TARGET_KERNEL} /'
/etc/default/grub
```

где {TARGET_KERNEL} — значение для установки, например

```
sudo sed -i 's/^GRUB_DEFAULT=.* /GRUB_DEFAULT=gnulinux-5.10.190-1-generic-
advanced-48ca7bb5-cc8b-43d0-9a38-8ae7c43a92b8 /' /etc/default/grub
```

Примечание — для нормальной работы прикладного ПО рекомендуется использовать значение `generic-advanced`.

16) Обновить параметры загрузчика GRUB командой

```
sudo update-grub
```

17) Перезагрузить ОС и убедиться, что в меню с выбором загрузки ОС автоматически выбрана ОС «Astra Linux SE» с необходимым ядром, а также, что после загрузки ОС используется целевая версия ядра, для этого выполнить команду

```
uname -r
```

2.2 Установка и настройка ОС «Astra Linux SE» (очередное обновление 1.8)

2.2.1 Установка ОС «Astra Linux SE» (очередное обновление 1.8)

После запуска инсталлятора ОС Astra Linux SE» необходимо выполнить следующие настройки:

1) В поле **Язык программы установки** выбрать значение **Русский**, в поле **Уровень защищенности** выбрать значение **Максимальный «Смоленск»**.

2) Ознакомиться с лицензионным соглашением на продукт. После ознакомления сделать отметку в поле **Принимаю условия лицензионного соглашения** и нажать кнопку **Далее** (рис. 18).

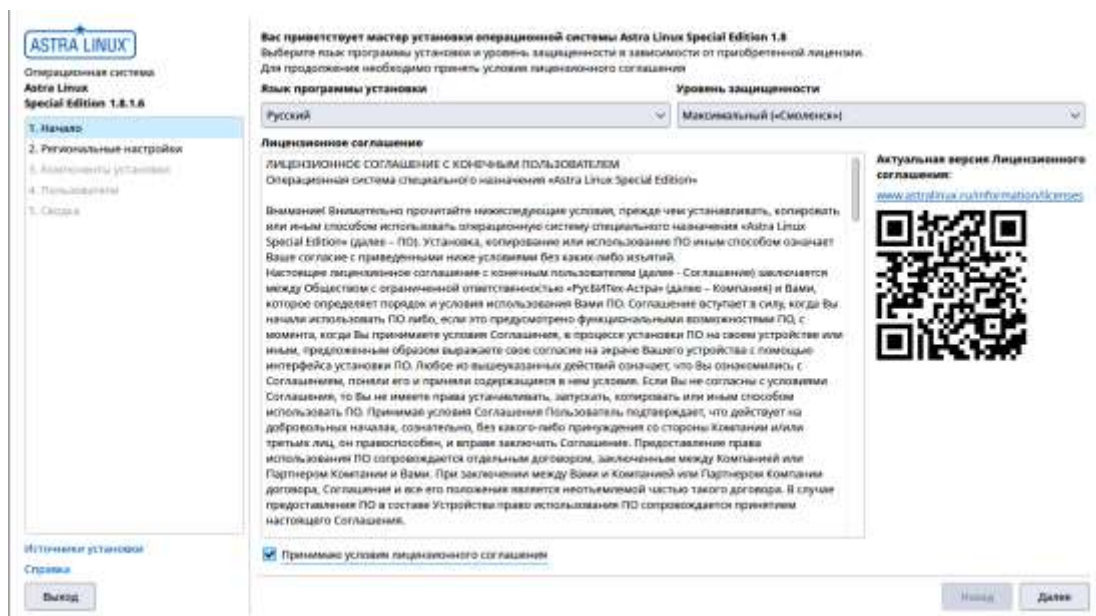


Рисунок 18 — Лицензионное соглашение

3) На странице **Региональные настройки** выбрать текущий часовой пояс (рис. 19), нажать кнопку **Далее**.



Рисунок 19 — Региональные настройки

4) На странице **Компоненты установки** (рис. 20) в разделе **Компоненты операционной системы** выбрать Графический интерфейс Fly, Средства работы с Интернет, Консольные утилиты, Средства удаленного подключения, в разделе **Дополнительные настройки** выбрать **Запрет автонастройки сети** и **Запрет трассировки traceroute**.

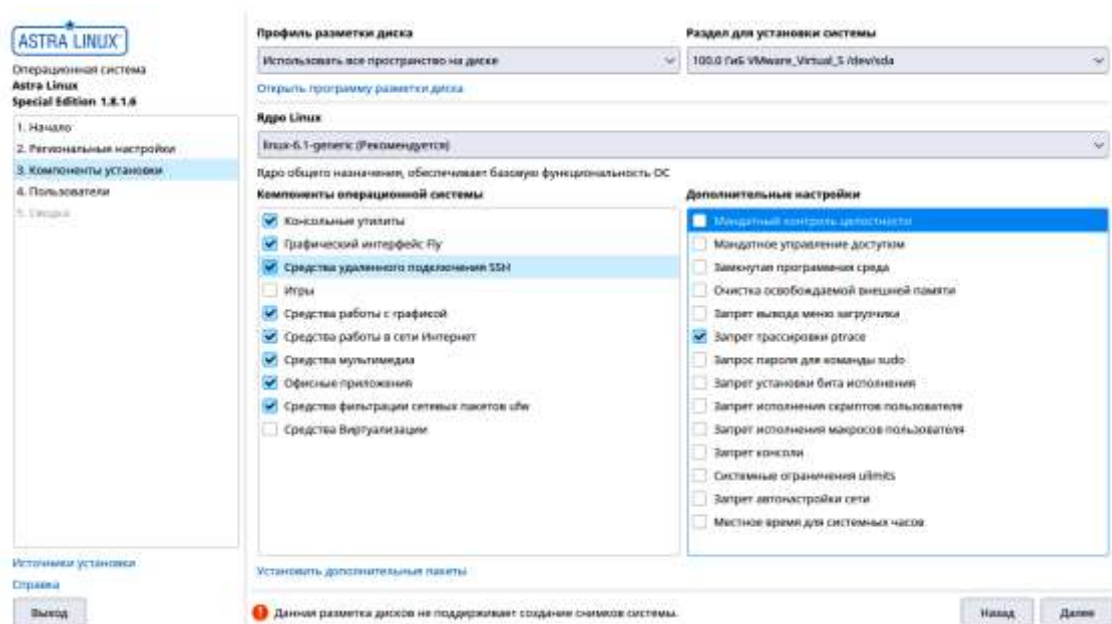


Рисунок 20 — Выбор компонентов установки

ВНИМАНИЕ: В связи с особенностями работы механизмов выделения и очистки памяти в ОС «Astra Linux SE», при установке ОС «Astra Linux SE» необходимо задать размер файла подкачки, равный объему установленной оперативной памяти.

5) В поле **Профиль разметки диска** выбрать значение **Использовать всё пространство на диске**. Нажать **Открыть программу разметки диска** (рис. 21).

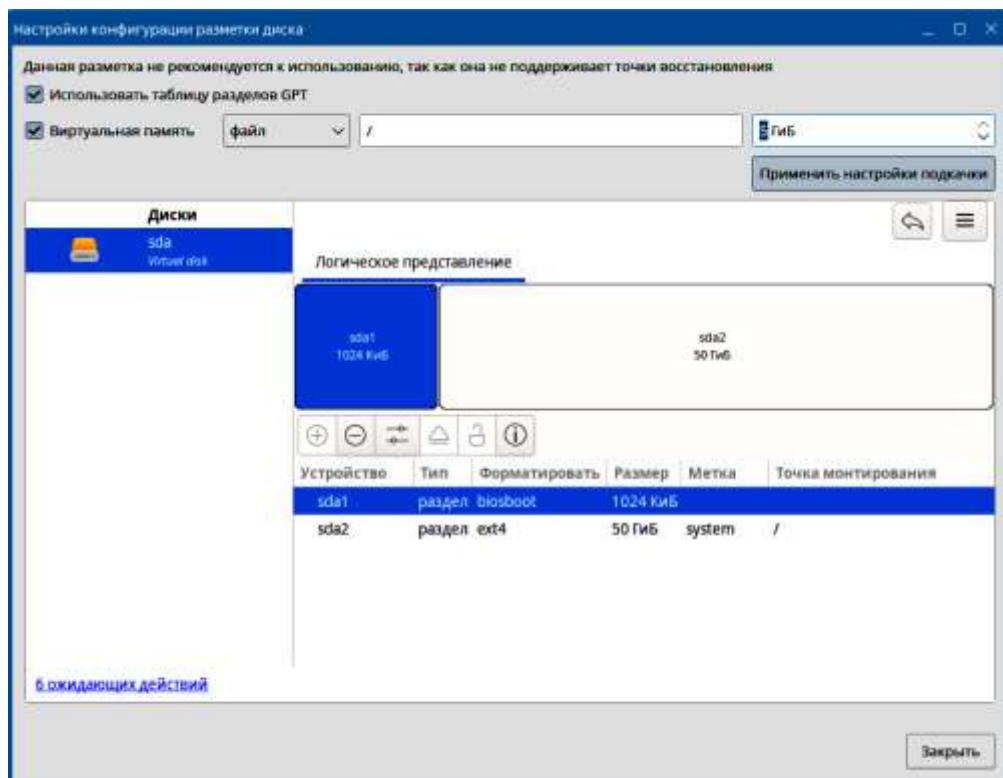


Рисунок 21 — Настройки конфигурации разметки диска

6) В строке **Виртуальная память** установить значение, равное размеру ОЗУ и нажать кнопку **Применить настройки подкачки**.

7) На странице **Пользователи** ввести имя нового пользователя **algont**, пароль **12345678** и имя компьютера, например, **srv1** (рис. 22). Дождаться завершения процесса установки и автоматической перезагрузки.

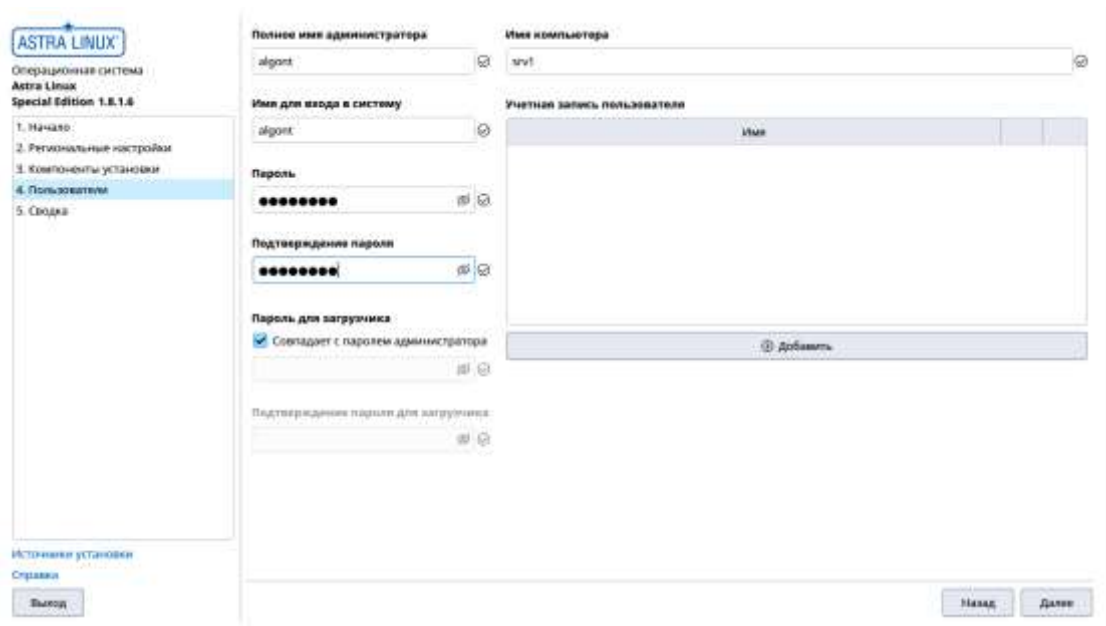


Рисунок 22 — Страница «Пользователи»

2.2.2 Установка PostgreSQL

Выполнить установку СУБД PostgreSQL следующими командами:

```
sudo apt update  
sudo apt install -y postgresql
```

2.2.3 Настройка учетной записи root и разрешение административного входа

Войти в ОС «Astra Linux SE» под учетной записью пользователя **algont**. Открыть меню **Пуск** → **Параметры** → **Параметры системы** (рис. 23).

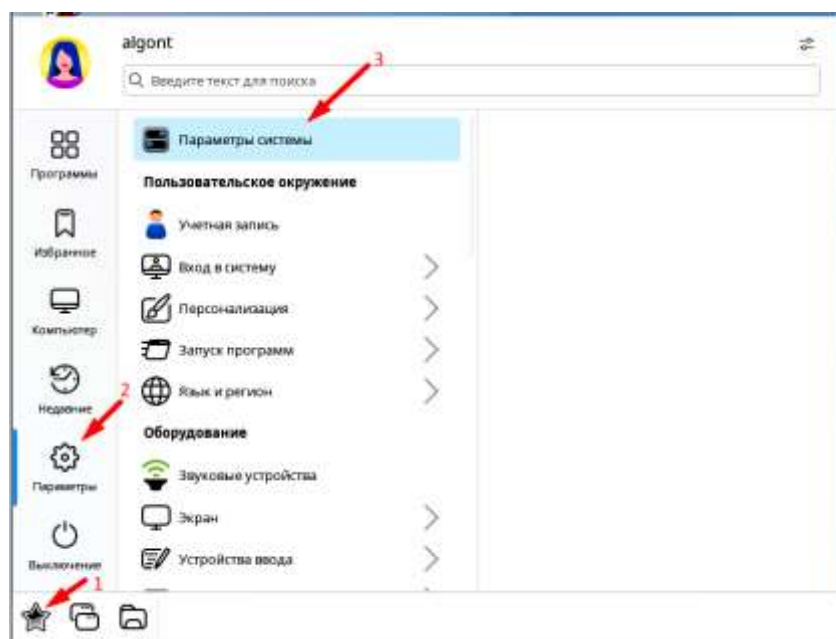


Рисунок 23 — Параметры системы

В окне **Для доступа к текущим настройкам вам нужна аутентификация** нажать **Нажмите сюда, для запроса аутентификации** (рис. 24). В открывшемся окне ввести пароль, указанный при установке операционной системы и нажать кнопку **Да**.

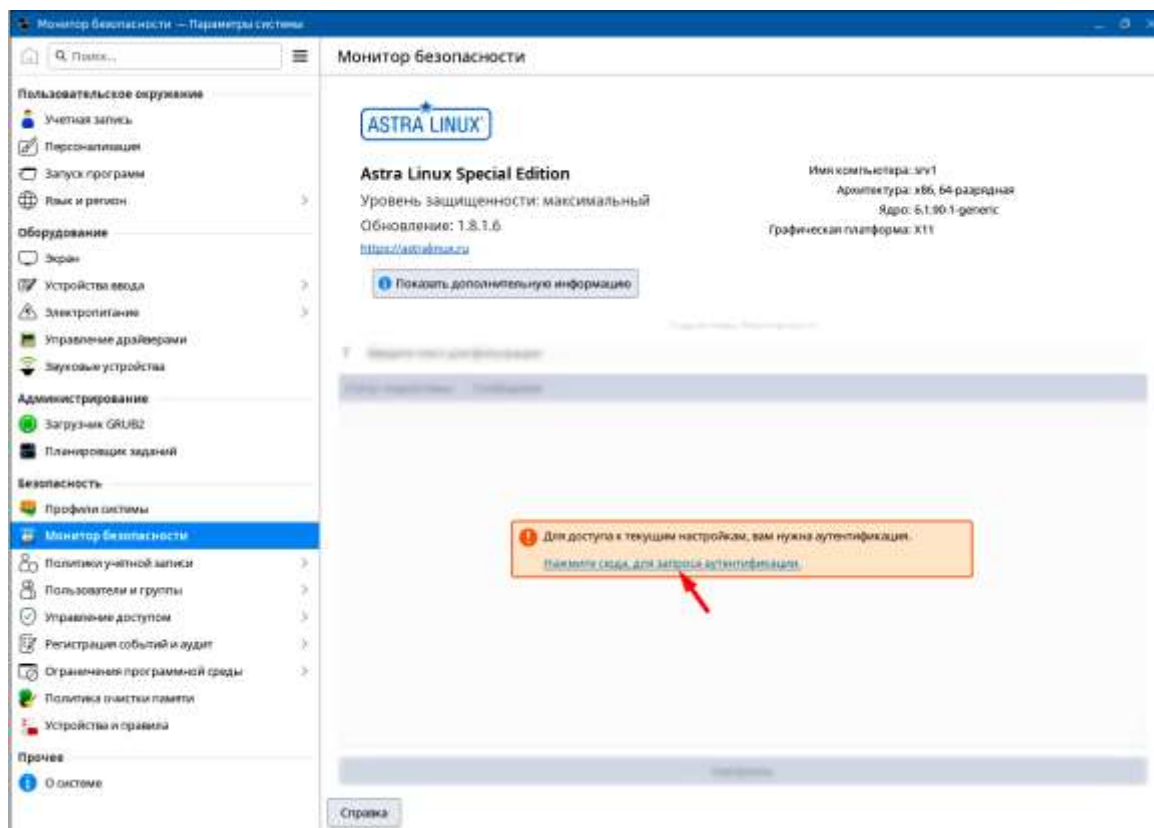


Рисунок 24 — Запрос аутентификации

В разделе **Безопасность** выбрать **Пользователи и группы**. В выпадающем списке выбрать **Все**. Выбрать пользователя **root** (рис. 25). В поле **Пароль** нажать кнопку . В открывшемся окне **Изменить пароль** ввести пароль root нажать кнопку **Да**. В окне с сообщением об успешной смене пароля нажать кнопку **Да**.

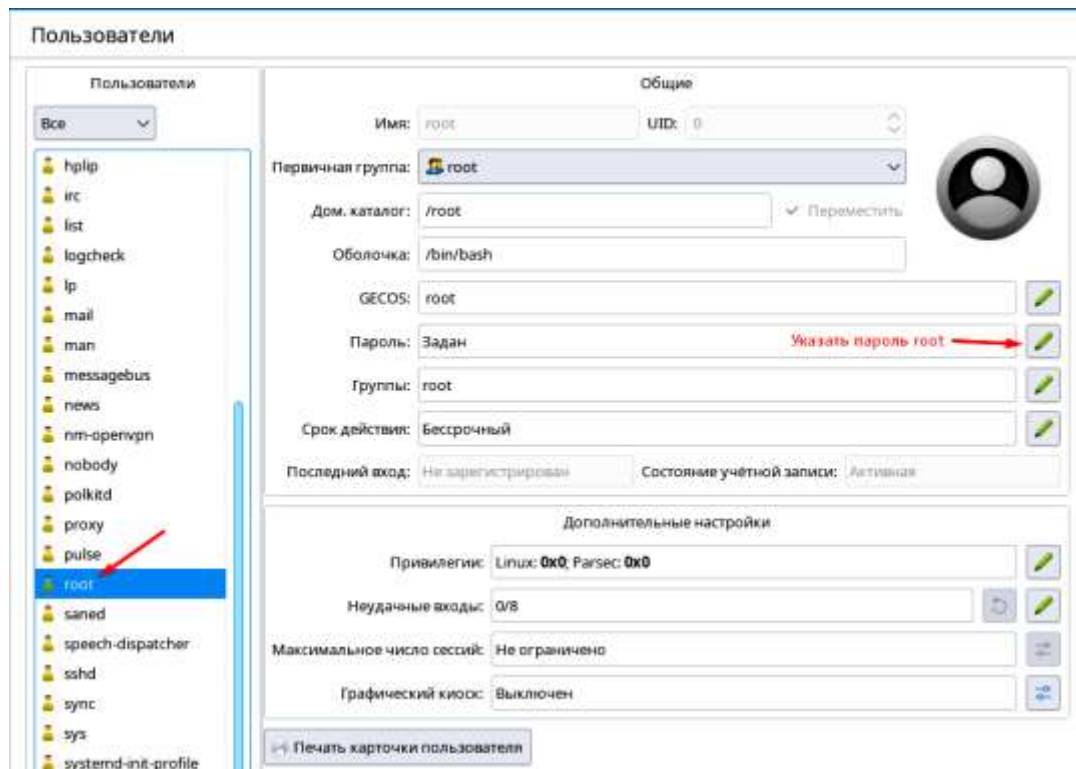


Рисунок 25 — Смена пароля

В поле **Привилегии** нажать кнопку . Отметить все строки списков **Привилегий** в разделах **Linux** и **Parsec** и применить изменения, нажав кнопку **Да** (рис. 26). Для сохранения внесенных изменений нажать кнопку **Применить**.

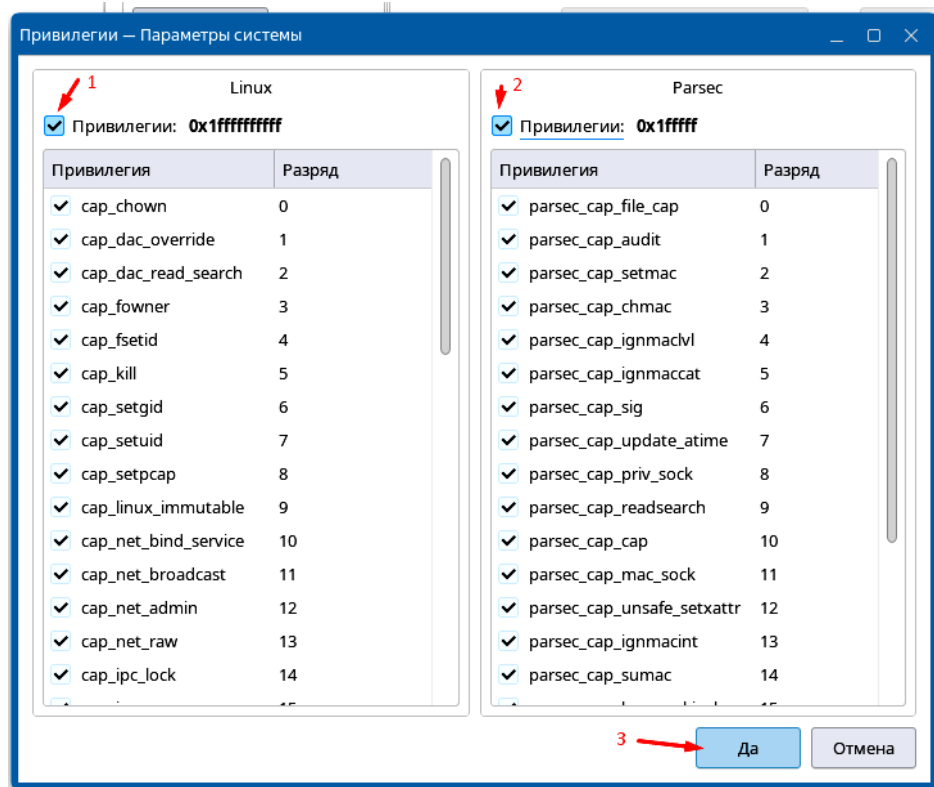


Рисунок 26 — Привилегии

В разделе **Безопасность** выбрать **Политики учетной записи**. В разделе **Вход в систему** выбрать вкладку **Пользователи** (рис. 27), отметить пункт **Разрешить вход администратору**. Нажать кнопку **[Применить]**. Перезагрузить компьютер.

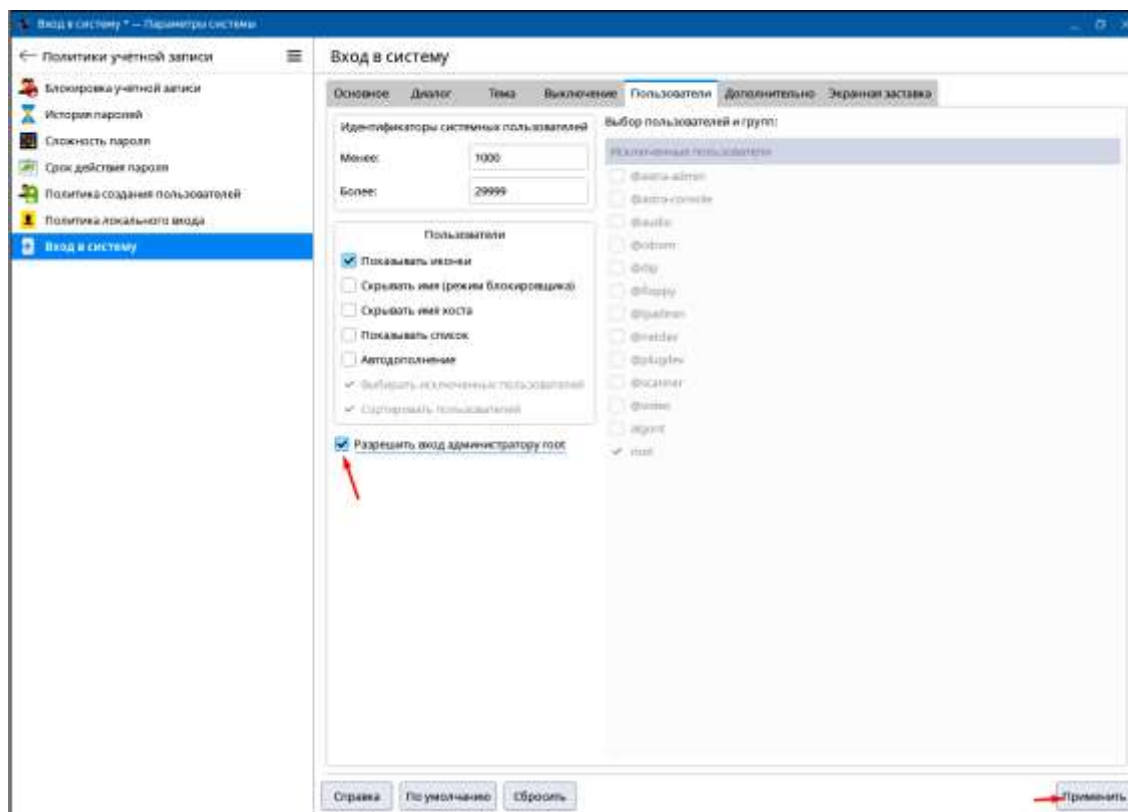


Рисунок 27 — Разрешение на вход администратору root

2.3 Смена пароля системного загрузчика GRUB

Для смены пароля системного загрузчика необходимо сгенерировать хеш нового пароля и заменить им старый:

- 1) Для генерации хеша выполнить команду и дважды ввести новый пароль:

```
grub-mkpasswd-pbkdf2
```

- 2) Полученный хеш (начиная со слова grub) скопировать в буфер (например, выделив его с помощью мыши, и нажав правую кнопку мыши выбрать «копировать»).

- 3) Открыть в редакторе с правами суперпользователя root файл `/etc/grub.d/07_password`. Например, для редактирования с помощью встроенного редактора с графическим интерфейсом kate можно воспользоваться командой: `sudo kate /etc/grub.d/07_password`

В результате редактирования должен получиться текст вида:

```
#!/bin/bash

cat << EOF
set superusers="username"
password_pbkdf2 username grub.pbkdf2.sha512.10000.9C319610666.....
EOF
```

Цветом условно обозначены имя пользователя (красный) и ранее сгенерированный кеш (зелёный), в редакторе никаких цветов нет.

4) Сохранить файл, и выйти из редактора.

5) Для того, чтобы эти изменения вступили в силу обновить загрузчик командой:

```
sudo update-grub2
```

2.4 Установка антивируса

Установка, настройка, обновление Dr.Web Enterprise Security Suite подробно описаны в документе ЦРПА.424356.509 И15 Инструкция по организации антивирусной защиты информации. После установки и настройки Dr.Web выполнить:

- 1) Антивирусный сторож SpIDer Guard отключить на всех АРМ и серверах.
- 2) Сканер Dr.Web выключить на всех серверах.
- 3) Отключить на серверах сканирование по расписанию.

2.5 Установка принтера для печати карт доступа

Драйвер принтера для печати карт доступа расположен на поставочном диске ЦРПА.2.00397.01.00 «Специальное программное обеспечение интегрированного комплекса технических средств охраны «Равелин» (Том 2/7). Для подключения принтера необходимо выполнить следующие действия:

- 1) Подключить привод для чтения компакт-дисков к рабочей станции АРМ-Б, вставить поставочный диск (Том 2/7) в привод;
- 2) Выбрать необходимый драйвер для установки с помощью диспетчера файлов (рис. 28);

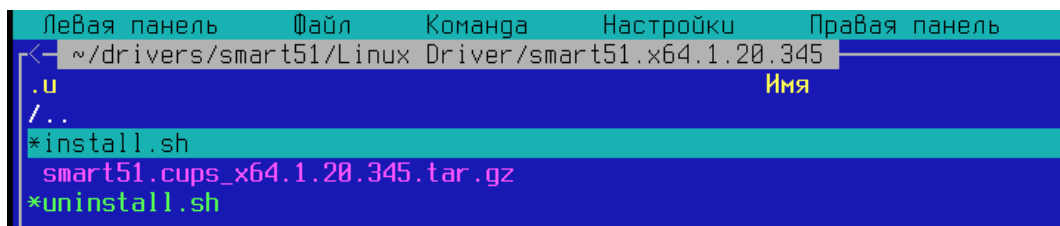


Рисунок 28 — Выбор драйвера принтера

- 3) Запустить менеджер печати Fly, выбрать пункт **Добавить** (рис. 29);

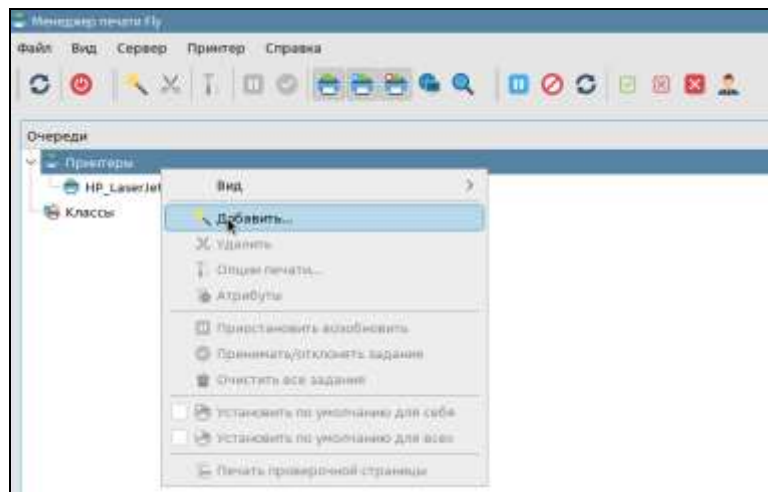


Рисунок 29 — Мастер установки принтера. Добавить принтер

4) На странице выбора принтера или класса принтеров выбрать пункт **Принтер** (рис. 30);

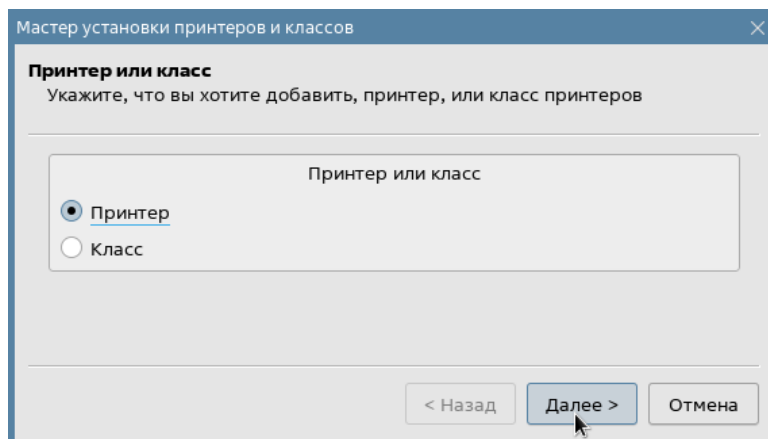


Рисунок 30 — Мастер установки принтера

5) На странице **Выберите принтера** выбрать модель принтера (рис. 31);

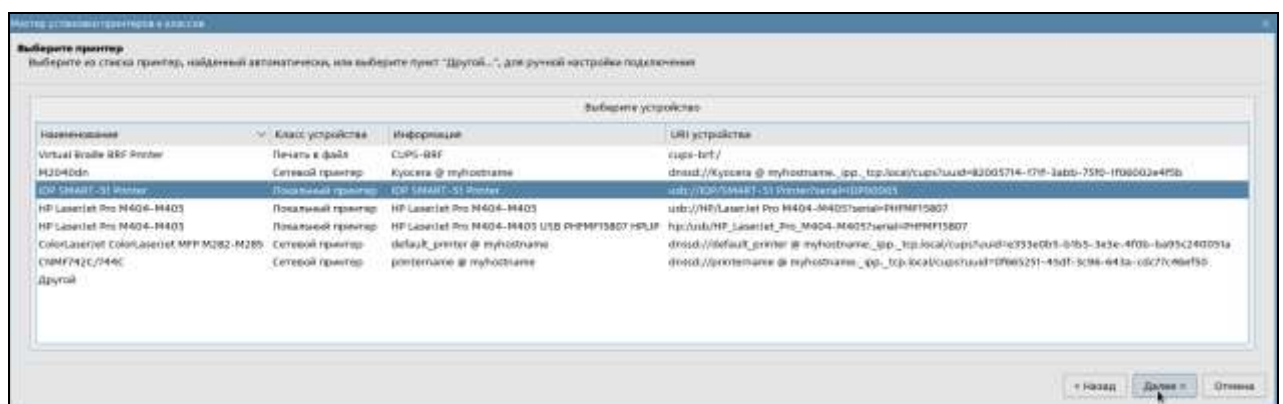


Рисунок 31 — Выбор принтера из списка

6) На странице **Информация** ввести необходимую информацию о местонахождении принтера и описание. В строке **Драйвер** вызвать меню выбора драйвера по кнопке «...» (рис. 32);

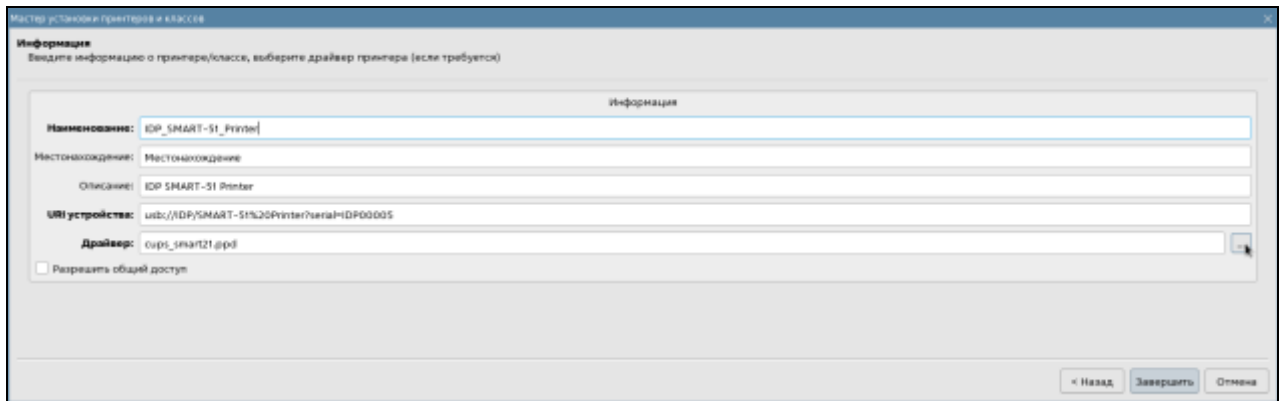


Рисунок 32 — Запуск меню выбора драйвера

7) На странице **Драйверы** выбрать производителя принтера и модель из списка (рис. 33);

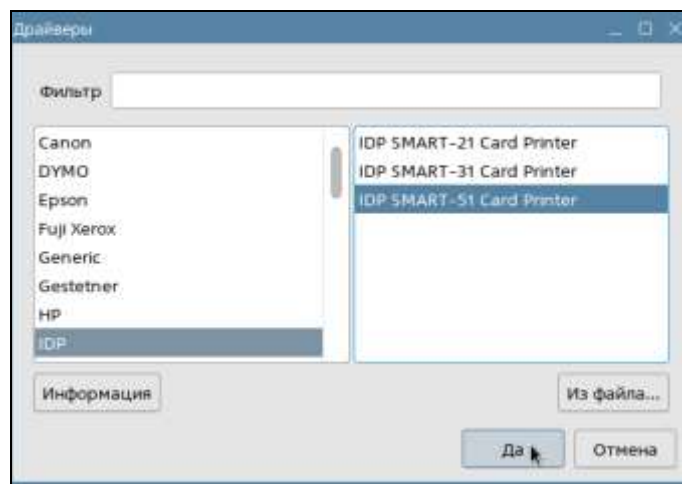


Рисунок 33 — Выбор драйвера

8) На странице **Информация** нажать на кнопку **Завершить** (рис. 34) и дождаться окончания процесса установки драйвера принтера;

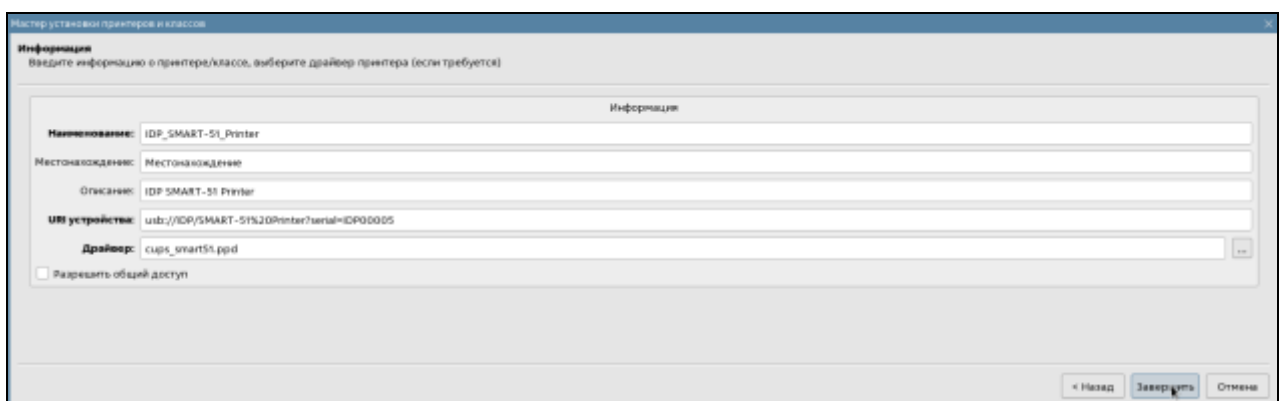


Рисунок 34 — Завершение настроек установки драйвера

9) Открыть веб-браузере, в адресной строке ввести **127.0.0.1:631**, откроется страница подсистемы печати CUPS (рис. 35);

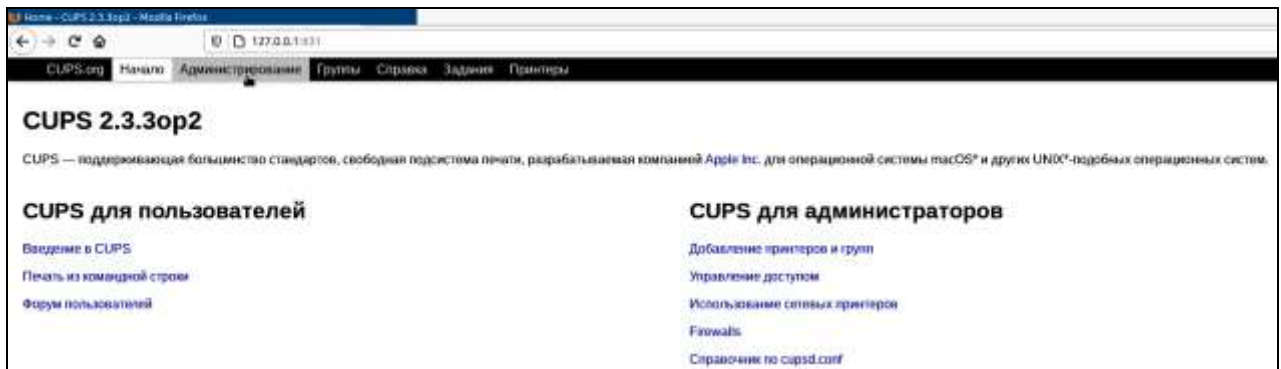


Рисунок 35 — Подсистема печати CUPS. Стартовая страница

10) Перейти на вкладку **Администрирование**, нажать на кнопку **Добавить принтер** (рис. 36);

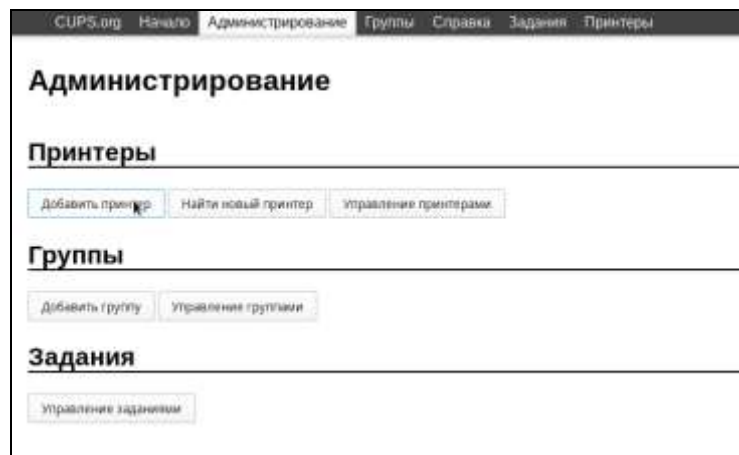


Рисунок 36 — Подсистема печати CUPS. Вкладка Администрирование

11) На странице **Добавить принтер** выбрать установленный принтер из списка, нажать на кнопку **Продолжить** (рис. 37);

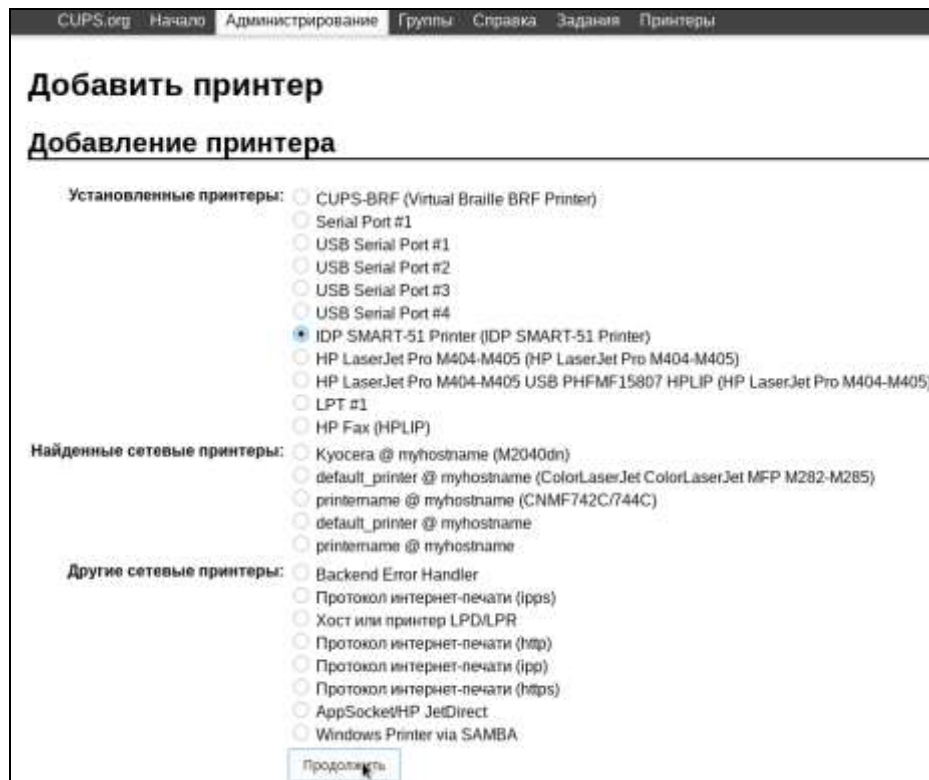


Рисунок 37 — Подсистема печати CUPS. Страница Добавить принтер

12) Далее ввести необходимую информацию в полях **Название**, **Описание**, **Расположение**, **Подключение**, нажать кнопку **Продолжить** (рис. 38);

Рисунок 38 — Подсистема печати CUPS. Страница Добавить принтер

13) Выбрать модель принтера, нажать кнопку **Добавить принтер** (рис. 39);

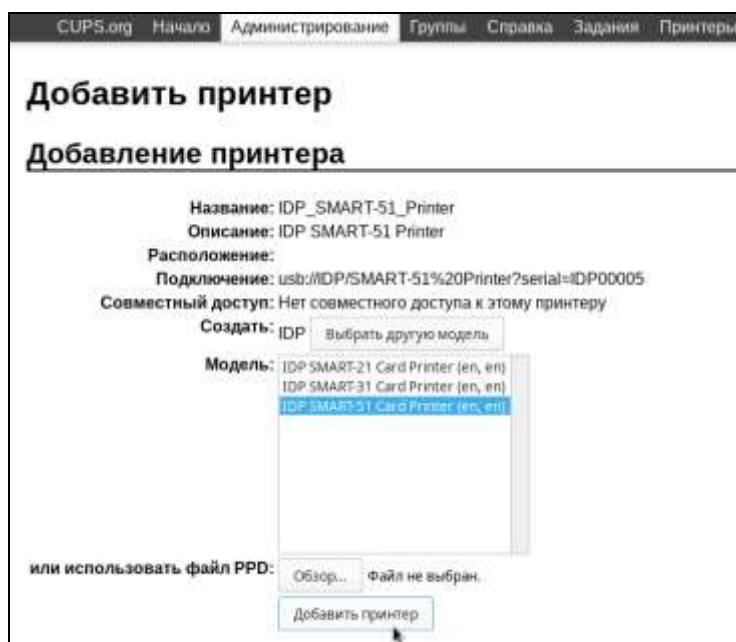


Рисунок 39 — Подсистема печати CUPS. Страница Добавить принтер

14) На странице **Настроить параметры принтера** установить параметры (рис. 40), нажать кнопку **Сохранить параметры**;

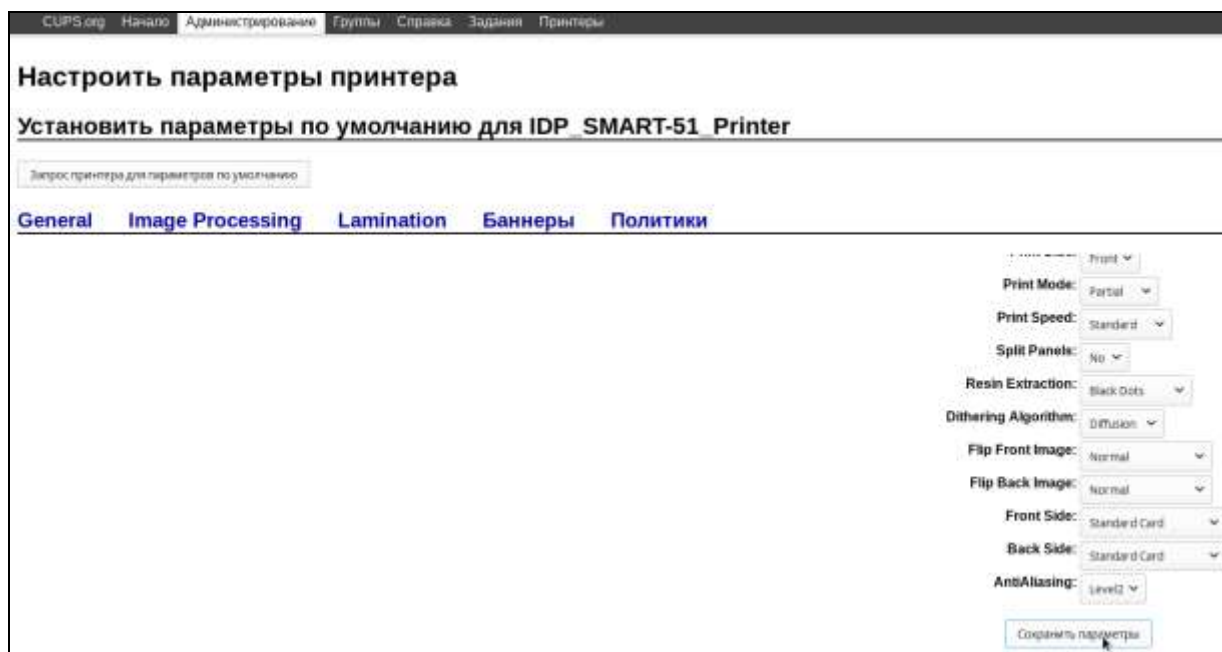


Рисунок 40 — Подсистема печати CUPS. Страница настройки параметров принтера

2.6 Установка принтера для печати на бумаге

Для установки принтера печати на бумаге отдельные драйвера не требуются. Стандартный драйвер входит в состав ОС «Astra Linux SE», установленной на АРМ-Б. Для подключения принтера необходимо:

1) В панели управления ОС «Astra Linux SE» запустить **Утилиту настройки принтеров HP** (рис. 41);

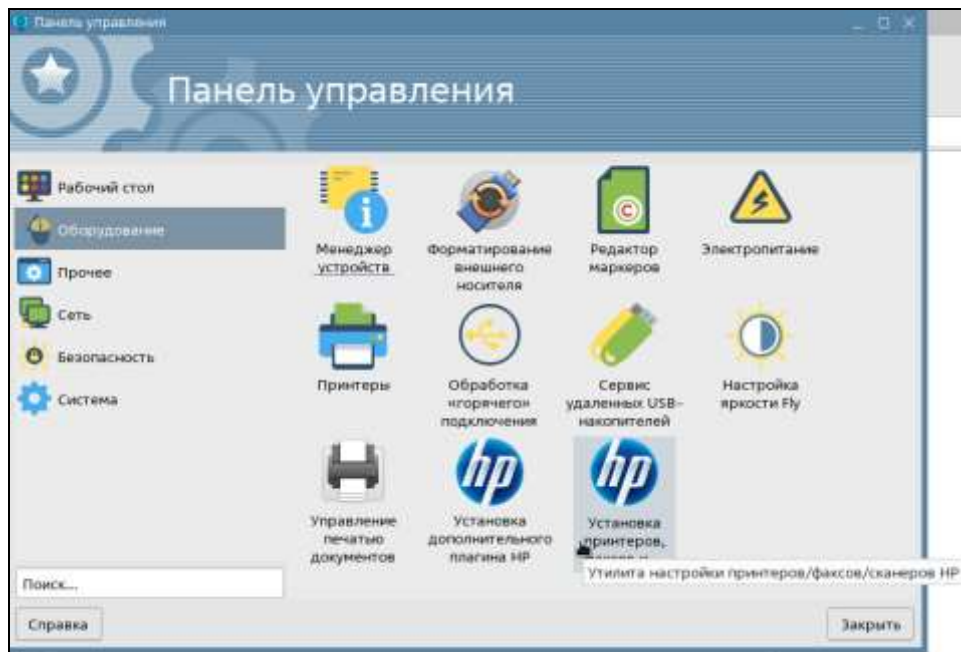


Рисунок 41 — Панель управления. Подключение оборудования

2) На странице **Обнаружение устройств** выбрать тип подключения **Универсальная последовательная шина** (рис. 42);

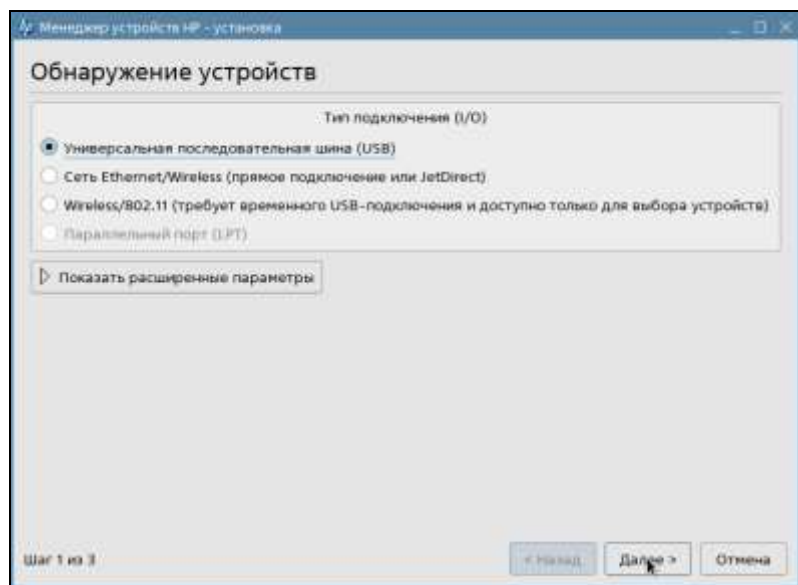


Рисунок 42 — Менеджер устройств HP. Обнаружение устройств

3) На странице **Выбор обнаруженных устройств** найти и отметить устанавливаемый принтер, нажать кнопку **Далее** (рис. 43);

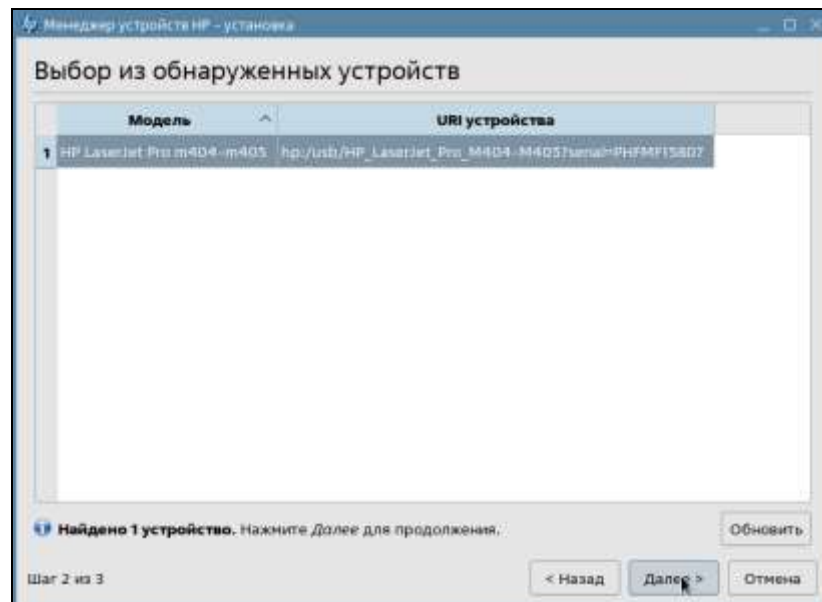


Рисунок 43 — Менеджер устройств HP. Выбор устройства

4) На странице **Настройка устройства** Ввести **Имя принтера** нажать на кнопку **Завершить** (рис. 44).

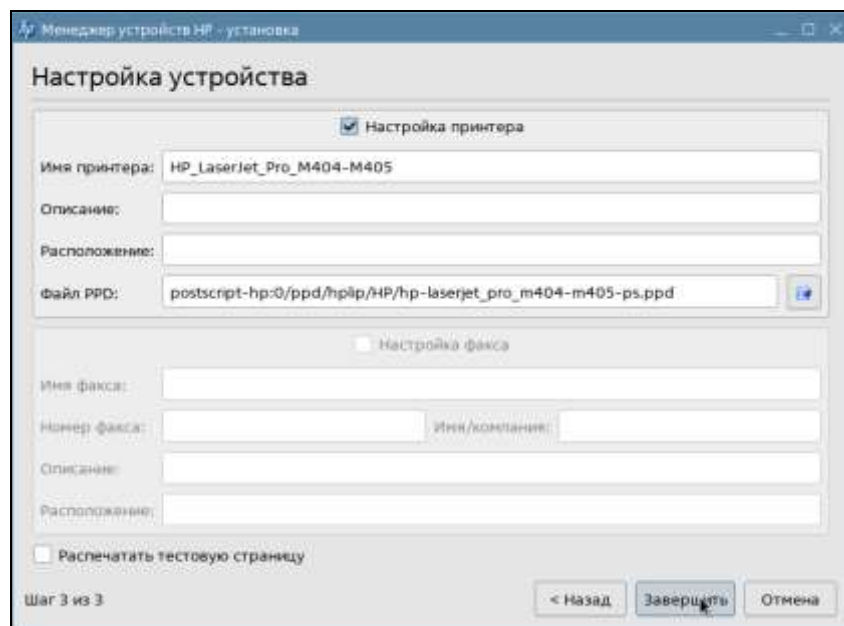


Рисунок 44 — Менеджер устройств HP. Настройка устройства

2.7 Установка компонентов СПО ИК ТСО «Равелин»

Установка компонента СПО ССКУ описана в ЦРПА.2.00330.01.00 32.

Установка компонента СПО СКУД. Контроль доступа описана в ЦРПА.2.00341.01.00 32.

Установка компонента СПО СКУД. Автоматизированная система биоидентификации описана в ЦРПА.2.00342.01.00 32.

Установка компонента СПО СКУД. Автомобильная досмотровая система описана в ЦРПА.2.00343.01.00 32.

Установка компонента СПО СКУД. Железнодорожная досмотровая система описана в ЦРПА.2.00344.01.00 32.

Установка компонента СПО СОН описана в ЦРПА.2.00345.01.00 32.

Установка компонента СПО модулей сопряжения описана в ЦРПА.2.00331.01.00 32.

2.8 Установка средств защиты информации

Установку средств защиты информации необходимо производить после установки ОС «Astra Linux SE» и компонентов ИК ТСО «Равелин».

Установка средств защиты информации производится в соответствии с документацией на соответствующее средство защиты информации.

2.9 Блокировка доступа к учетной записи суперпользователя

После установки ОС, СПО и необходимых средств СЗИ интерактивный вход в систему суперпользователя root следует заблокировать. Для блокировки доступа к учетной записи суперпользователя root необходимо выполнить следующие команды:

```
passwd -l root  
usermod -p '!' root
```

3 ПРОВЕРКА ПРОГРАММЫ

3.1 Проверка компонентов СПО ИК ТСО «Равелин»

Проверка работоспособности компонента СПО ССКУ описана в ЦРПА.2.00330.01.00 32.

Проверка работоспособности компонента СПО СКУД. Контроль доступа описана в ЦРПА.2.00341.01.00 32.

Проверка работоспособности компонента СПО СКУД. Автоматизированная система биоидентификации описана в ЦРПА.2.00342.01.00 32.

Проверка работоспособности компонента СПО СКУД. Автомобильная досмотровая система описана в ЦРПА.2.00343.01.00 32.

Проверка работоспособности компонента СПО СКУД. Железнодорожная досмотровая система описана в ЦРПА.2.00344.01.00 32.

Проверка работоспособности компонента СПО СОН описана в ЦРПА.2.00345.01.00 32.

Проверка работоспособности компонента СПО модулей сопряжения описана в ЦРПА.2.00331.01.00 32.

4 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Дополнительные возможности в СПО ИК ТСО «Равелин» не предусмотрены.

5 СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

Сообщения системному программисту компонентов ИК ТСО «Равелин» приведены в руководстве системного программиста:

ЦРПА.2.00330.01.00 32 СПО ССКУ;

ЦРПА.2.00341.01.00 32 СПО СКУД. Контроль доступа;

ЦРПА.2.00342.01.00 32 СПО СКУД. Автоматизированная система биоидентификации;

ЦРПА.2.00343.01.00 32 СПО СКУД. Автомобильная досмотровая система.

ЦРПА.2.00344.01.00 32 СПО СКУД. Железнодорожная досмотровая система.

ЦРПА.2.00345.01.00 32 СПО СОН.

ЦРПА.2.00331.01.00 32 СПО модулей сопряжения.

ПРИЛОЖЕНИЕ А
(обязательное)

ПРАВИЛА РАСПРЕДЕЛЕНИЯ IP-АДРЕСОВ

При назначении IP-адресов оборудованию системы следует пользоваться данными правилами для создания понятной, бесконфликтной топологии сети.

Маска сети принимается: 255.240.0.0

По назначенному IP-адресу можно понять какого типа это устройство и где оно расположено. Поэтому IP-адреса имеют вид **10.Локализация.Тип.Номер**, где:

- Локализация — локализация сетевых устройств по географическому признаку, например, сооружение 1, ЦПУ, периметр, КПП;
- Тип — тип оборудования;
- Номер — номер оборудования данного типа.

Оборудование ИК ТСО «Равелин» с примерными адресами перечислено в таблице А.1.

Таблица А.1 — Пример IP-адресов

Тип оборудования	Назначенный номер для данного типа оборудования	Адрес	Пример для сооружения 1
Шлюз по умолчанию		10.0.0.254/255.240.0.0	е
Адрес кластера серверов баз данных ССКУ	1	10.0.1.1	10.0.1.1
Серверы баз данных ССКУ	1	10.Локализация.1.номер	10.1.1.1
Серверы ССКУ (управляющие компьютеры)	2	10.Локализация.2.номер	10.1.2.1
Автоматизированные рабочие места	3	10.Локализация.3.номер	10.1.3.1
Сетевые видеорегистраторы	4	10.Локализация.4.номер	10.1.4.1
Серверы видеоаналитики	5	10.Локализация.5.номер	10.1.5.1
IP-видеокамеры	6	10.Локализация.6.номер	10.1.6.1
Видеокодеры	7	10.Локализация.7.номер	10.1.7.1
Сетевое оборудование (коммутаторы, маршрутизаторы)	8	10.Локализация.8.номер	10.1.8.1
Принтеры	9	10.Локализация.9.номер	10.1.9.1
Преобразователи интерфейсов	10	10.Локализация.10.номер	10.1.10.1
Сетевые карты ИБП и прочее	11	10.Локализация.11.номер	10.1.11.1

[illegible]