Комплекс «Межсетевой экран Solar» исполнение 2

Версия 2.0

Инструкция по установке для экспертов

Москва, 2024

Содержание

Список иллюстраций

Список таблиц

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
ИБ	Информационная безопасность
КА	Контентный анализ
МЭ	Межсетевой экран
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface — интерфейс командной строки
CPS	Connection per Second — мера измерения, насколько быстро брандмауэр может создать и сохранить новый сеанс, принятый его политикой.
CSR	Certificate Signing Request — запрос на подпись сертификата
CRL	Certificate Revocation List — список отозванных сертификатов
DC	Domain controller — контроллер домена
DNAT	Destination Network Address Translation — скрытие IP-адреса назначения запроса пользователя путем перенаправления запроса пользователя преобразованием адреса назначения в IP-заголовке пакета
FAQ	Frequently asked questions — «часто задаваемые вопросы», справка с полезной информацией
GUI	Graphical User Interface — графический интерфейс пользователя
FQDN	Fully Qualified Domain Name — полное имя домена (имя домена, не имеющее неоднозначностей в определении)
IPS	Intrusion Prevention System — система обнаружения вторжений
MIME	Multipurpose Internet Mail Extension — спецификация для передачи по сети файлов различного типа: изображений, музыки, текстов, видео, архивов и др.
MITM	Man-In-The-Middle — атака «человек посередине», при которой злоумышленник тайно ретранслирует и при необходимости модифицирует данные между двумя сторонами
NAT	Network Address Translation — преобразование сетевых адресов
OWA	Outlook Web Access — веб-интерфейс почтового сервиса Microsoft Exchange
RFC	Request for Comments — спецификации и стандарты, применяемые в интернете
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты

SNAT	Source Network Address Translation — технология, позволяющая заменить исходный IP-адрес источника сетевого пакета на другой указанный IP-адрес
VLAN	Virtual Local Area Network — технология обмена данными, которая логически делит устройства локальной сети на сегменты для реализации виртуальных рабочих групп
VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
ZIP	Формат архивации файлов и сжатия данных без потерь

1. Введение

1.1. Область применения

Программно-аппаратный комплекс Межсетевой экран Solar (далее – Межсетевой экран Solar) – это комплекс сетевой безопасности для защиты периметра сети организации от вредоносного трафика и вторжений. Для полноценного функционирования весь трафик должен проходить через комплекс "Межсетевой экран Solar".

1.2. Краткое описание возможностей

Комплекс "Межсетевой экран Solar" представляет собой комплексную систему функциональных модулей информационной безопасности, в которую входят:

- фильтрация трафика (по IP-адресам, портам/протоколам),
- контроль приложений, поддерживаемых библиотекой nDPI,
- трансляция адресов (NAT),
- система предотвращения вторжений,
- анализ и фильтрация веб-трафика, передаваемого по протоколам HTTP, HTTPS и FTP over HTTP,
- категоризатор web-ресурсов на базе решения WebCat,
- мониторинг состояния системы и действий пользователей,
- кластеризация комплекса "Межсетевой экран Solar" с отказоустойчивостью.

1.3. Уровень подготовки системного администратора

Квалификация системного администратора комплекса "Межсетевой экран Solar" должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех ее компонентов.

К задачам системного администратора комплекса "Межсетевой экран Solar" относятся:

- установка и настройка компонентов комплекса "Межсетевой экран Solar";
- мониторинг функционирования процессов системы;
- реагирование на служебные уведомления системы.

Администратор информационной системы должен:

- ориентироваться в особенностях работы комплекса "Межсетевой экран Solar";
- понимать работу сетевых протоколов;
- обладать знаниями в области безопасности ОС класса UNIX.

В своей работе администраторы комплекса "Межсетевой экран Solar" должны использовать внутреннюю документацию и документацию по ОС Linux.

1.4. Перечень эксплуатационной документации для ознакомления

Администратор информационной системы должен ознакомиться с эксплуатационными документами:

- *Руководство по установке и настройке*.
- *Руководство администратора безопасности*.

2. Требования и характеристики к программному и аппаратному обеспечению

2.1. Требования к АРМ администратора

2.1.1. Требования к аппаратному обеспечению

АРМ администратора комплекса "Межсетевой экран Solar" должно быть оборудовано персональным компьютером. Особых требований к аппаратному обеспечению нет. Рекомендуются следующие характеристики персонального компьютера:

- процессор P-IV с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 20 ГБ.

2.1.2. Требования к программному обеспечению

В состав программного обеспечения АРМ администратора комплекса "Межсетевой экран Solar" должен входить браузер. Рекомендуемые браузеры:

- Mozilla Firefox (актуальной версии)
- Google Chrome (актуальной версии)

Работа с управляющим интерфейсом комплекса "Межсетевой экран Solar" возможна в других браузерах, но в таком случае полноценная работоспособность комплекса "Межсетевой экран Solar" не гарантируется.

Внимание!

Если вручную увеличить размер шрифта в браузере, дизайн интерфейса комплекса "Межсетевой экран Solar" будет нарушен, и интерфейс станет непригодным к использованию.

2.2. Требования к серверу

2.2.1. Характеристики к аппаратному обеспечению

Компоненты комплекса "Межсетевой экран Solar" устанавливаются на серверы функциональными характеристиками, указанными в таблицах ниже.

Табл. 2.1. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 1)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	2 шт Intel Xeon Silver 4316
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 2 порта 100Gbps Ethernet QSFP28; • 6 портов 10Gbps Ethernet SFP+

Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • 3 шт Сетевой адаптер 10 Гбит/с Ethernet 2 x SFP+ PCI-Ex8; • Сетевая карта Dual Port 10/25/50/100 Gigabit Ethernet Server Adapter, 2 x QSFP28(QSFP28 Cage) 100GBASE-SR4/100GBASE-LR4, Intel E810, OCP 3.0 SFF NIC Card
Интерфейсы	• 2 порта USB 3.0 Type A; • 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)
Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Табл. 2.2. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 2)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	Intel Xeon Gold 5318Y
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 2 порта 100Gbps Ethernet QSFP28; • 6 портов 10Gbps Ethernet SFP+
Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • 3 шт Сетевой адаптер 10 Гбит/с Ethernet 2 x SFP+ PCI-Ex8; • 1 шт Mellanox ConnectX-5 2 x QSFP28 MCX556A-ECAT
Интерфейсы	• 2 порта USB 3.0 Type A; • 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)
Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Табл. 2.3. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 3)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	2 шт Intel Xeon Gold 5318Y
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 8 портов 100Gbps Ethernet QSFP28
Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • 4 шт Mellanox ConnectX-5 2 x QSFP28 MCX556A-ECAT
Интерфейсы	• 2 порта USB 3.0 Type A;

	• 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)
Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Табл. 2.4. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 4)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	2 шт Intel Xeon Gold 5318Y
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 4 порта 100Gbps Ethernet QSFP28; • 8 портов 10Gbps Ethernet SFP+
Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • 2 шт Сетевая карта Quad Port 10 Gigabit Ethernet Server Adapter, 4 x 1/10 Gbit/s SFP+(SFP+ Cage) ports, Intel XL710, PCI-E 3.0 x8 RP7219; • 2 шт Mellanox ConnectX-5 2 x QSFP28 MCX556A-ECAT
Интерфейсы	• 2 порта USB 3.0 Type A; • 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)
Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Табл. 2.5. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 5)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	2 шт Intel Xeon Gold 5318Y
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 4 порта 100Gbps Ethernet QSFP28; • 8 портов 1Gbps Ethernet RJ-45
Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • 2 шт Сетевая карта Quad Copper Port Gigabit Ethernet Server Adapter, 4 шт RJ-45 10/100/1000 Mbit/sec, Intel I350AM4, PCI-E v2.1 (5.0GT/s) x4 RP7238; • 2 шт Mellanox ConnectX-5 2 x QSFP28 MCX556A-ECAT
Интерфейсы	• 2 порта USB 3.0 Type A; • 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)

Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Табл. 2.6. Функциональные характеристики сервера комплекса "Межсетевой экран Solar" (Тип 6)

Оперативная память	128 GB (8 модулей памяти 16GB DDR4-3200)
Процессор	2 шт Intel Xeon Gold 5318Y
Хранение данных	2 накопителя SSD M.2 2280 PCIe Gen3x4 1TB 980
Тип интерфейсов	• 4 порта 1Gbps Ethernet RJ-45; • 4 порта 1Gbps Ethernet RJ-45*; • 4 порта 100Gbps Ethernet QSFP28; • 4 порта 10Gbps Ethernet SFP+
Сетевая карта	• Сетевой адаптер 1 Гбит/с Ethernet 4 x RJ-45 PCI-Ex4; • Сетевая карта Quad Copper Port Gigabit Ethernet Server Adapter, 4 шт RJ-45 10/100/1000 Mbit/sec, Intel I350AM4, PCI-E v2.1 (5.0GT/s) x4 RP7238; • Сетевая карта Quad Port 10 Gigabit Ethernet Server Adapter, 4 x 1/10 Gbit/s SFP+(SFP+ Cage) ports, Intel XL710, PCI-E 3.0 x8 RP7219; • 2 шт Mellanox ConnectX-5 2 x QSFP28 MCX556A-ECAT
Интерфейсы	• 2 порта USB 3.0 Type A; • 1 порт HDMI (microHDMI); • 1 порт консоли управления RS-232 (RJ-45)
Питание	AC-DC 220 В 50 Гц отказоустойчивый «1+1», с двумя модулями питания мощностью не менее 800Вт каждый

Для установки и корректной работы комплекса "Межсетевой экран Solar" требуется как минимум 150 ГБ свободного дискового пространства. Системный диск разбивается исходя из рекомендаций:

- Не менее 50 ГБ для раздела **/var** , т.к. в зависимости от политики сервис skvt-wizor по умолчанию записывает в этот каталог файлы, загружаемые из интернета.
- Не менее 30 ГБ для корневого каталога, в который будет устанавливаться операционная система.
- Не менее 70 ГБ для раздела **/opt**, в который будут установлены непосредственно рабочие файлы комплекса "Межсетевой экран Solar".

2.3. Операционная система

Данная версия комплекса "Межсетевой экран Solar" функционирует под управлением ОС Astra Linux Special Edition версии 1.7.4 (версия ядра 5.10.176-1-generic) с максимальным уровнем защиты «Смоленск».

2.4. Рекомендации по размещению в сетевой инфраструктуре

Аппаратное и программное обеспечение сервера должно располагаться на сетевом периметре безопасности для исключения несанкционированного доступа.

2.5. Требования к паролю

Комплекс "Межсетевой экран Solar" обеспечивает стойкость паролей для доступа в систему. При создании пользователей система проверяет качество паролей, которое определяется следующими параметрами:

1. Минимально разрешенная длина пароля - 8 символов.
2. Пароль не может содержать имя или часть имени учетной записи пользователя.
3. Пароль не должен совпадать ни с одним из 10 предыдущих паролей.
4. Известная и задокументированная максимальная длина пароля.
5. В пароле должны присутствовать символы трех категорий из числа следующих четырех:
   - заглавные буквы латиницы (от A до Z);
   - прописные буквы латиницы (от a до z);
   - цифры (от 0 до 9);
   - служебные символы: ~ ! @ # $ % ^ & * ( ) + - = ` ' _ / \ | ".

При создании пароля система рассчитывает уровень его сложности (от 0 до 10). Система не позволит создать пароль, если он не соответствует заданному в настройках уровню сложности – например, если он содержит более двух символов подряд из одного набора. По умолчанию уровень сложности пароля должен быть не менее 8. Расчет уровня сложности пароля выполняется на основании следующих условий:

1. Если длина пароля равна или больше минимальной, прибавляется 1.
2. Если длина пароля максимальная, прибавляется 2.
3. Если пароль содержит символы из двух наборов, прибавляется 1.
4. Если пароль содержит символы из трех наборов, прибавляется 1.
5. Если пароль содержит символы из четырех наборов, прибавляется 1.
6. Если пароль не содержит более двух символов из одного набора подряд, прибавляется 1.
7. Если пароль не содержит более одного символа из одного набора подряд, прибавляется 2.
8. Если количество разных символов больше минимальной длины пароля, прибавляется 1.
9. Если пароль выполняет условия пунктов 1, 5, 7, 8, прибавляется 1.

Если сумма условий больше 10, уровень сложности пароля считается равным 10.

В настройках по умолчанию минимальная длина пароля равна 8, максимальная – 12, минимально допустимый уровень сложности пароля – 8. Таким образом, если уровень сложности меньше 8, система не позволит создать пароль.

Настройки по умолчанию можно изменить, отредактировав в GUI следующие параметры (раздел **Система > Расширенные настройки >Интерфейс**, секция **Сервер веб-интерфейса**):

- **Мин. длина пароля**;
- **Макс. длина пароля**;
- **Уровень сложности пароля**.

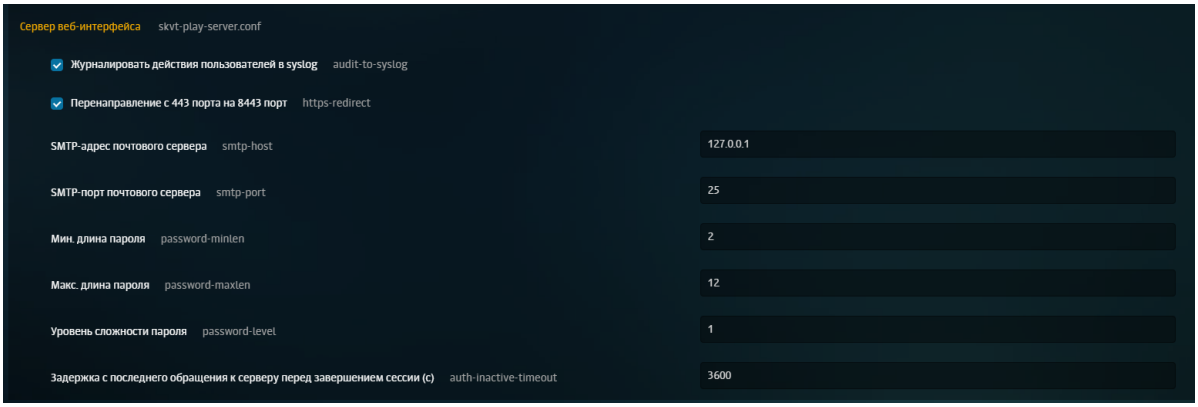


Рис. 2.1. Настройки сложности пароля

В системе реализована защита от взлома путем перебора учетных данных (брутфорс). После заданного количества неудачных попыток входа перед каждой следующей попыткой вводится временная задержка, которая увеличивается экспоненциально после каждой последующей неудачной попытки входа. Настройки защиты можно задать, используя следующие параметры конфигурации (раздел **Система > Расширенные настройки > Интерфейс**, секция **Сервер веб-интерфейса**):

- **Макс. количество неудачных попыток входа в систему до задержки**;
- **Начальное значение задержки для входа в систему (с)**;
- **Макс. значение задержки для входа в систему (с)**.

Рис. 2.2. Настройка параметров входа в систему

Примечание

Максимальное число попыток ввода пароля – 3. Если было сделано 3 неудачные попытки входа в систему, то выставить блокировку учетной записи пользователя на 15 минут.

При неправильном вводе пароля воспользуйтесь сервисом **user-tool**.

3. Установка ОС Astra 1.7.4

Для установки ОС Astra 1.7.4 запустите сервер с использованием установочного диска или USB-носителя «Astra 1.7.4» версии и выполните следующие действия:

1. В окне приветствия оставьте выбор параметров программы установки по умолчанию (**Графическая установка**, **Русский**) и нажмите **Enter**.

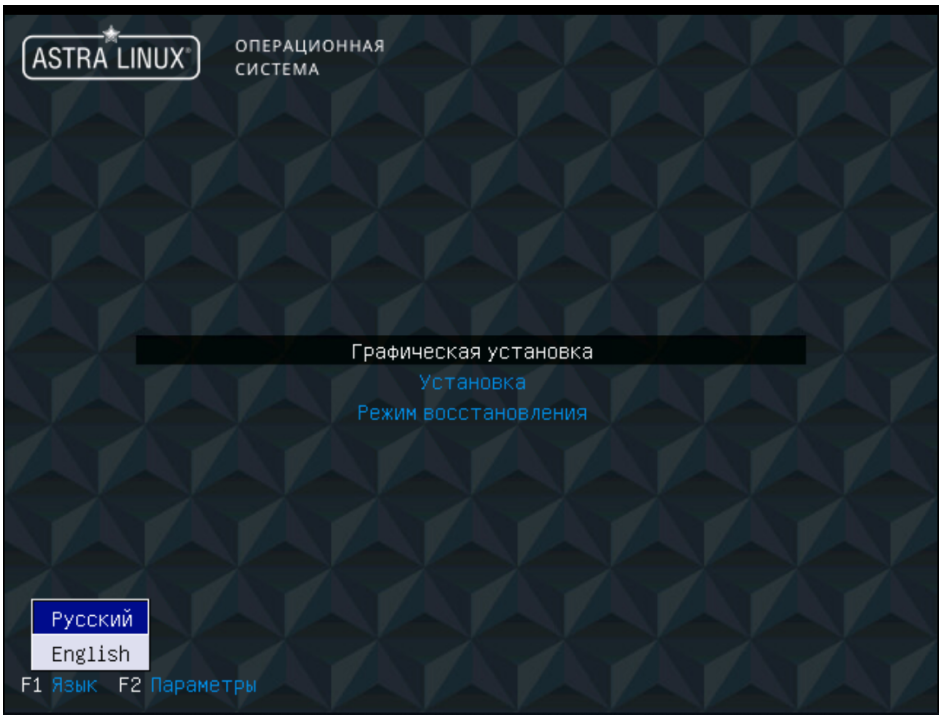


Рис. 3.1. Окно приветствия

2. В окне **Лицензия** нажмите **Продолжить**.

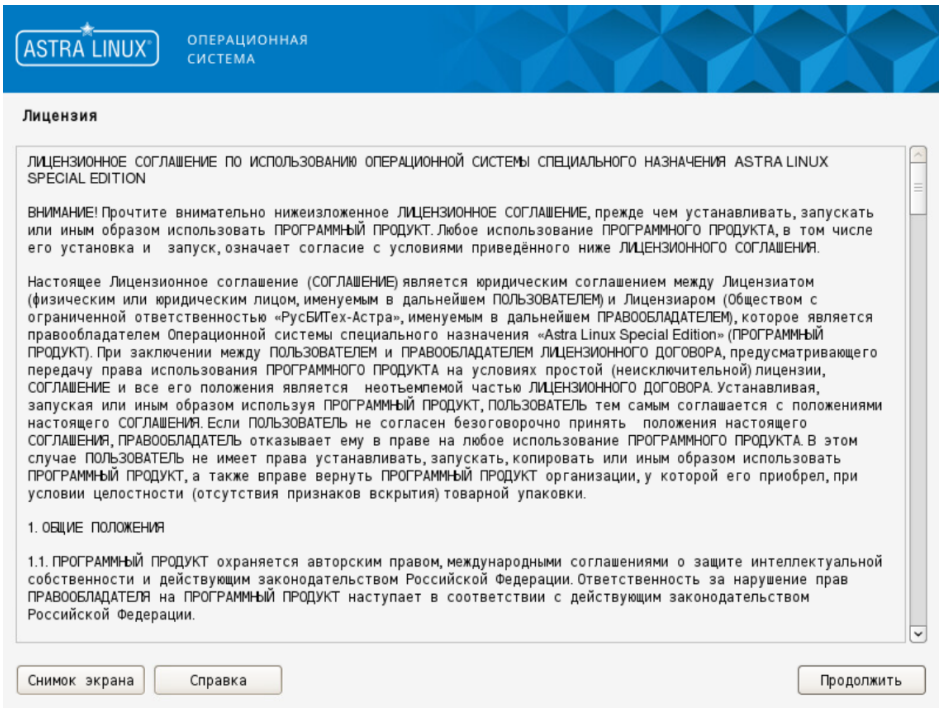


Рис. 3.2. Окно Лицензия

3. В окне **Настройка клавиатуры** выберите удобный способ переключения раскладки ввода с клавиатуры и нажмите **Продолжить**.

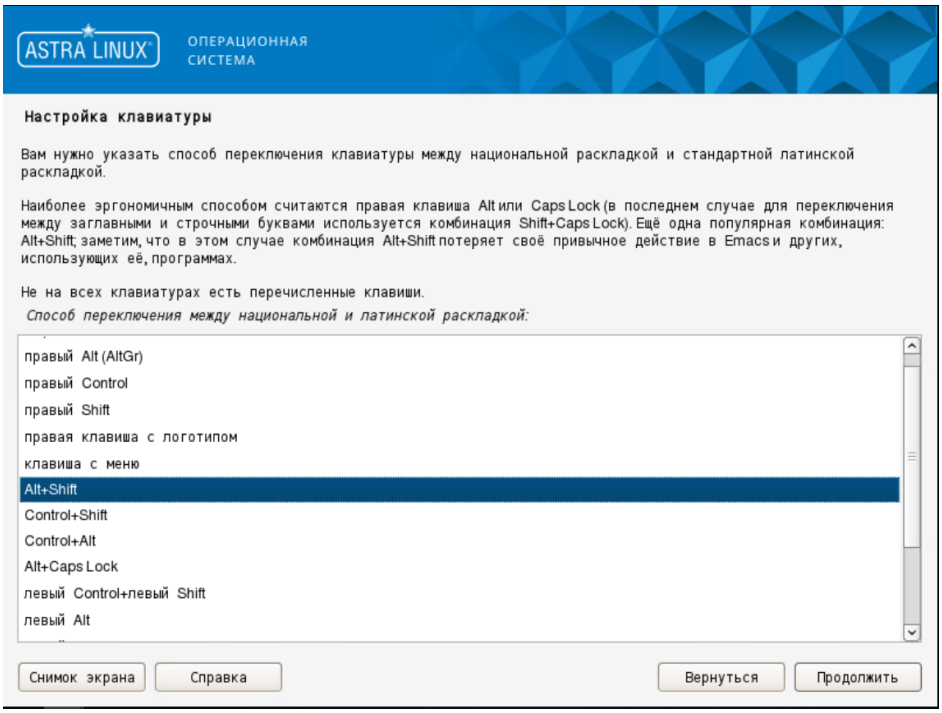


Рис. 3.3. Настройка клавиатуры

4. Дождитесь загрузки компонентов программы установки. В появившемся окне **Настройка сети** укажите краткое сетевое имя сервера (должно совпадать с прежним именем сервера).

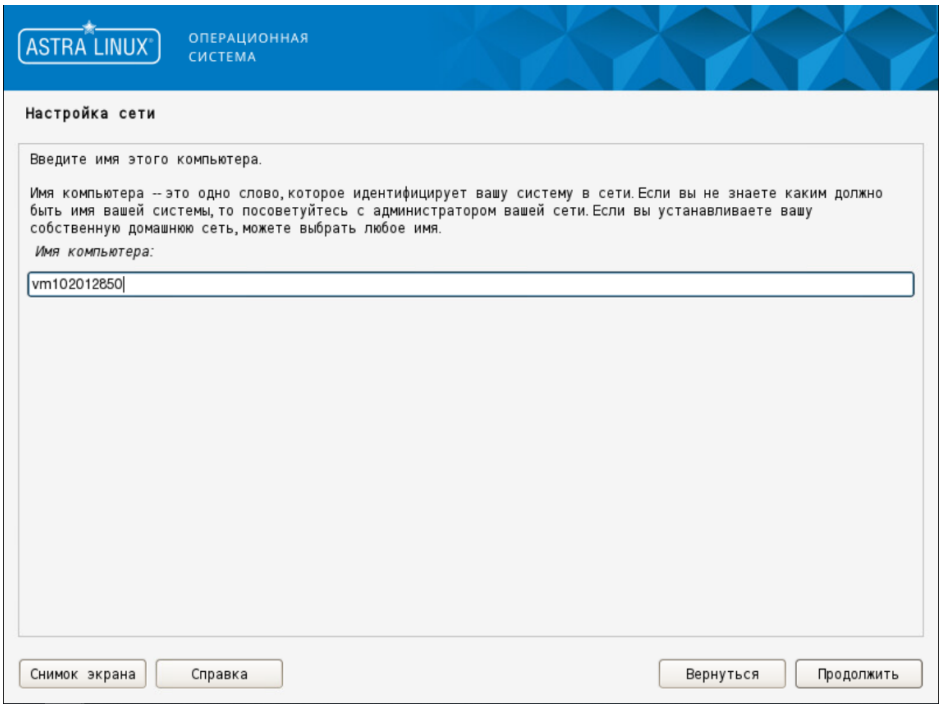


Рис. 3.4. Настройка сети

5. В окне **Настройка учётных записей пользователей и паролей** в поле **Имя учётной записи администратора** укажите произвольное имя и нажмите **Продолжить**. Не следует использовать имя **dozor**, поскольку оно зарезервировано в комплексе "Межсетевой экран Solar".

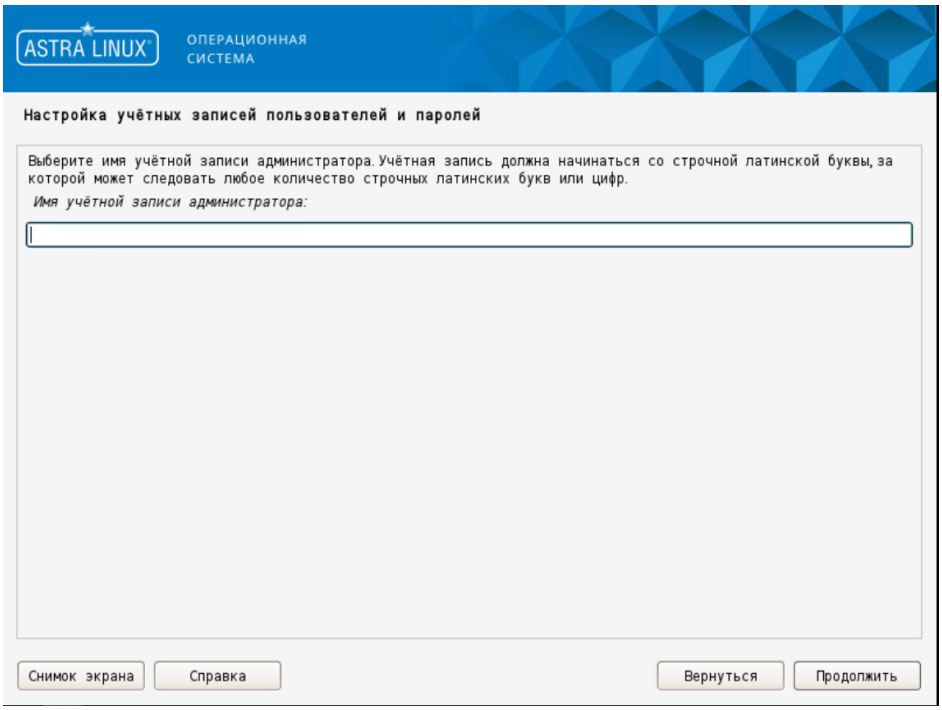


Рис. 3.5. Окно Настройка учётных записей пользователей и паролей

6. В появившемся окне задайте пароль для созданной учетной записи и подтвердите его. Нажмите **Продолжить**.

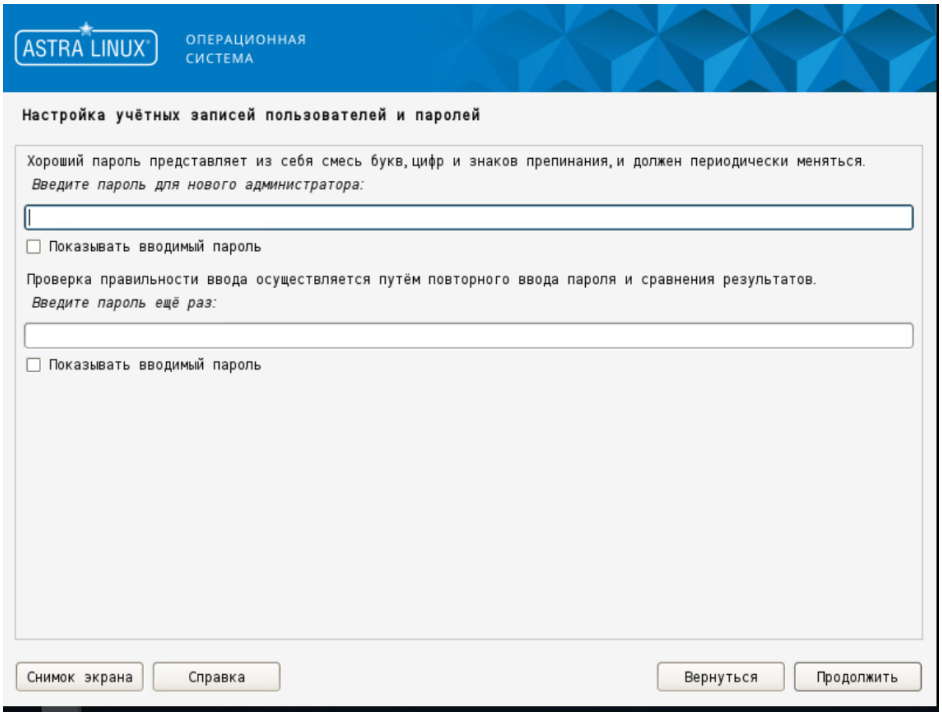
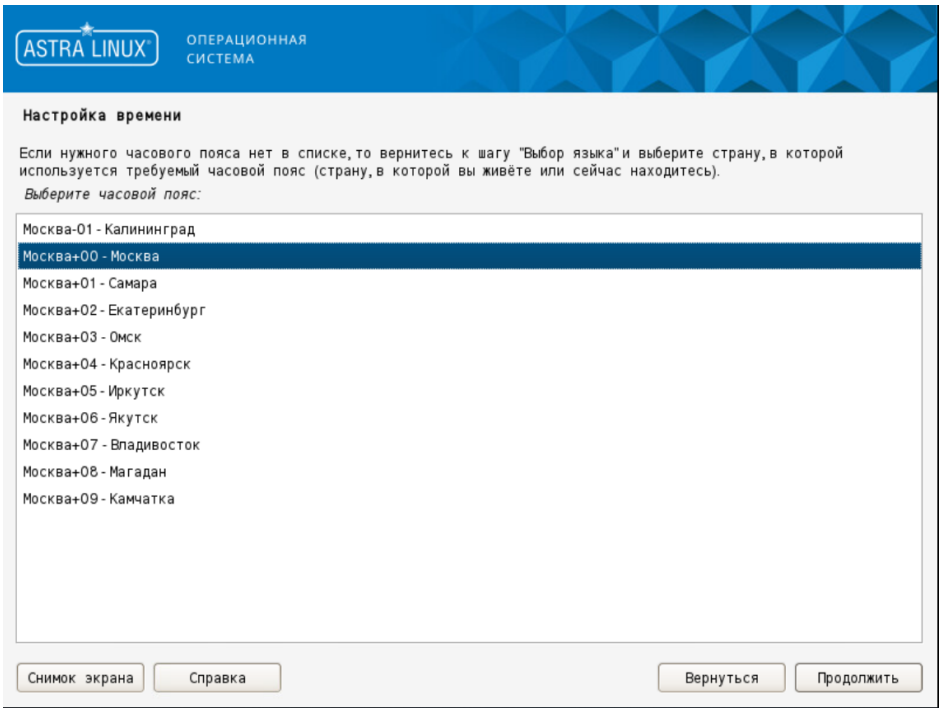


Рис. 3.6. Создание пароля для учетной записи администратора

7. В окне **Настройка времени** задайте требуемый часовой пояс и нажмите **Продолжить**.



8. В появившемся окне **Разметка дисков** выберите метод разметки **Вручную** и нажмите **Продолжить**.

Внимание!

При выборе любого другого метода разметки все данные на диске будут потеряны.

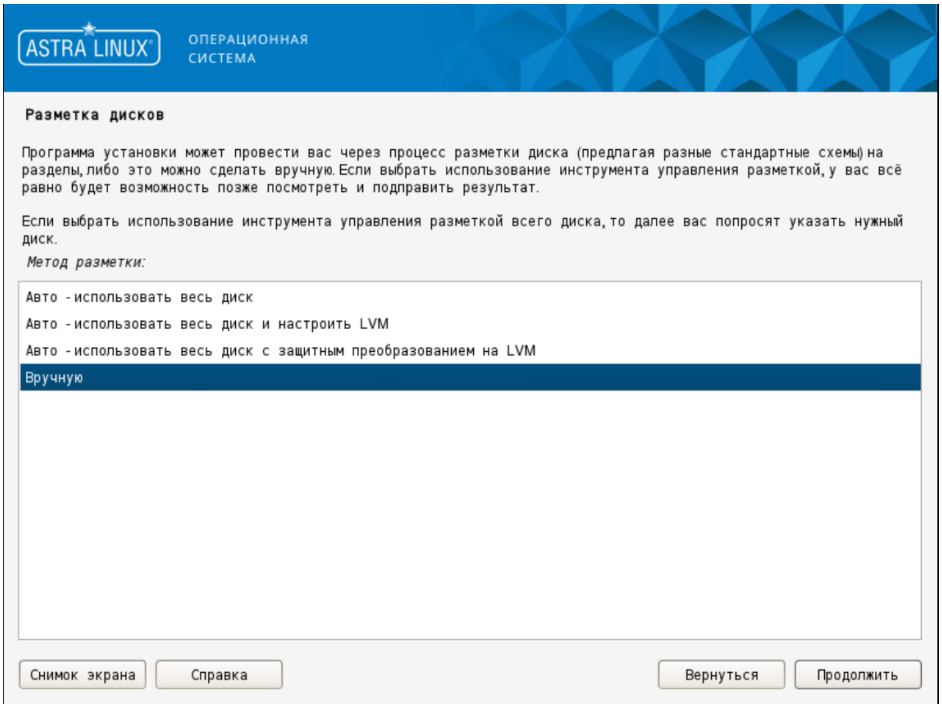


Рис. 3.7. Окно Разметка дисков

9. В появившемся окне выберите область для разметки, например, как показано ниже. Нажмите **Продолжить**.

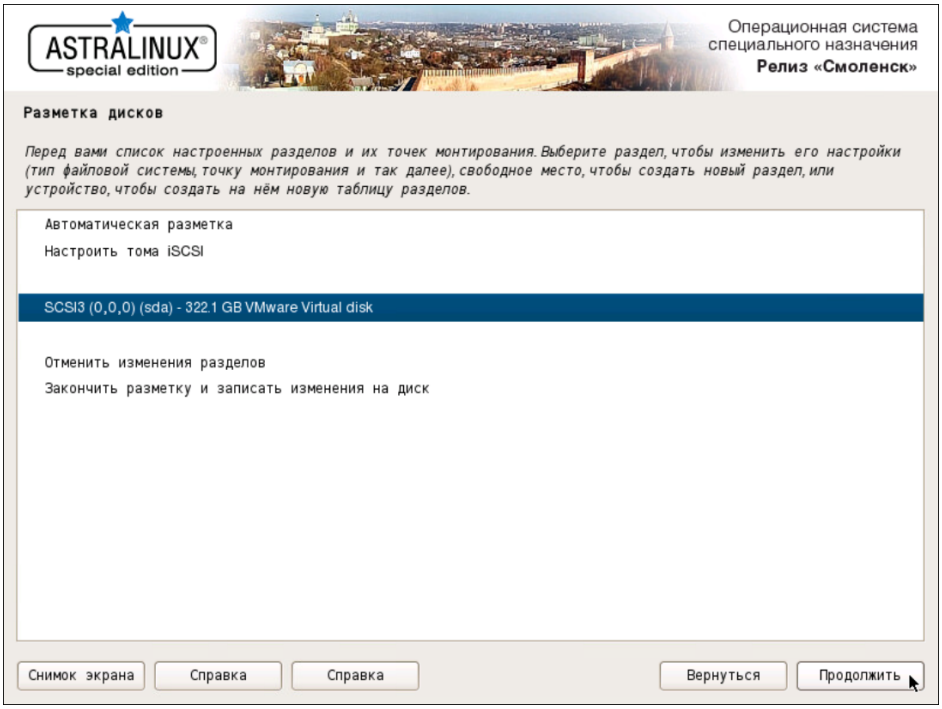


Рис. 3.8. Выбор области для разметки

10. В появившемся окне с запросом **Создать новую пустую таблицу разделов?** выберите вариант **Да**. Нажмите **Продолжить**.

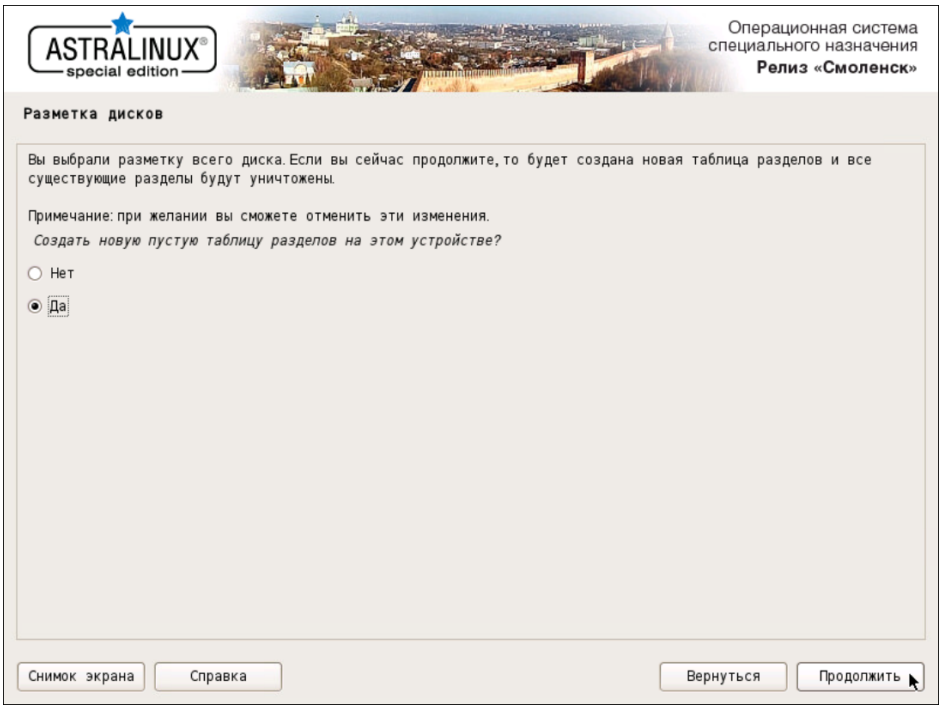


Рис. 3.9. Создание таблицы разделов

11. В появившемся окне выделите строку, помеченную как **СВОБОДНОЕ МЕСТО**, и нажмите **Продолжить**.

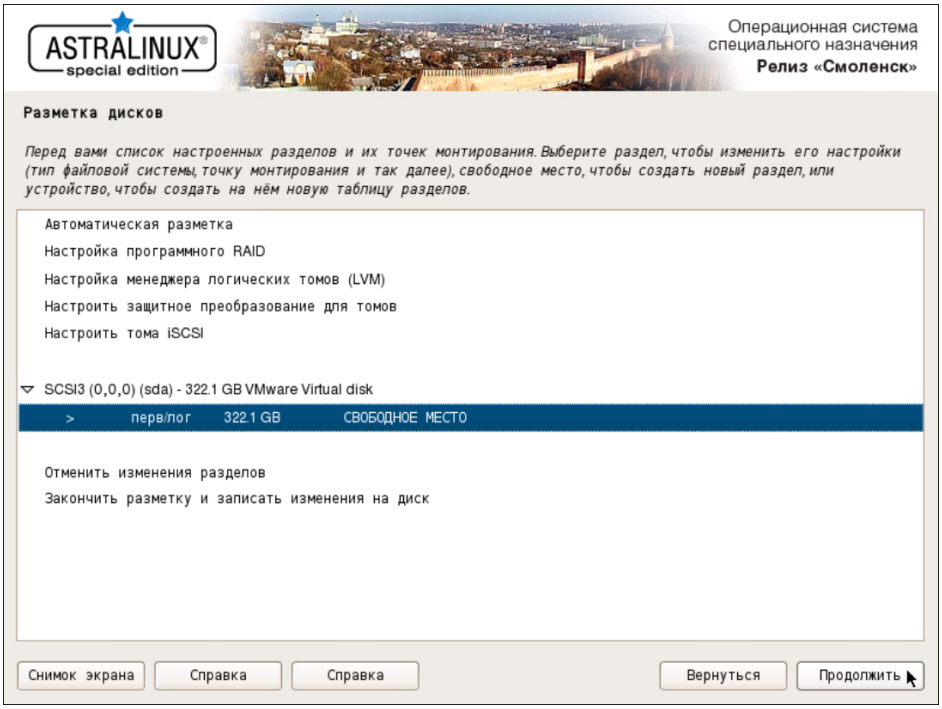


Рис. 3.10. Выбор пространства для создания разделов

12. В появившемся окне с запросом **Что делать со свободным пространством** выберите вариант **Создать новый раздел**. Нажмите **Продолжить**.

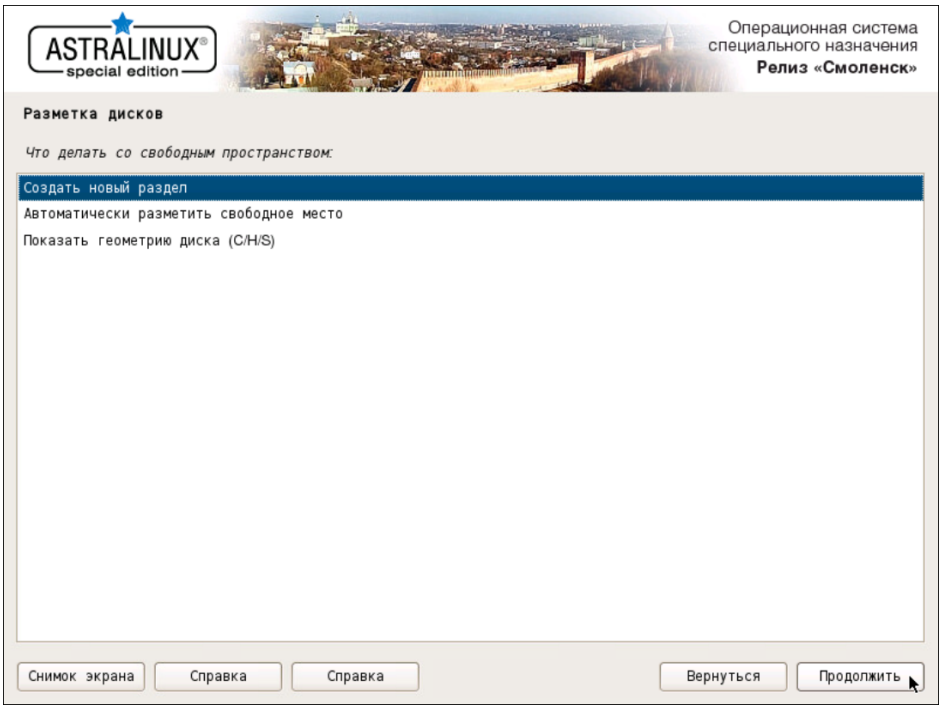


Рис. 3.11. Выбор варианта для создания раздела

13. В появившемся окне задайте размер диска **1 GB**. Нажмите **Продолжить**.

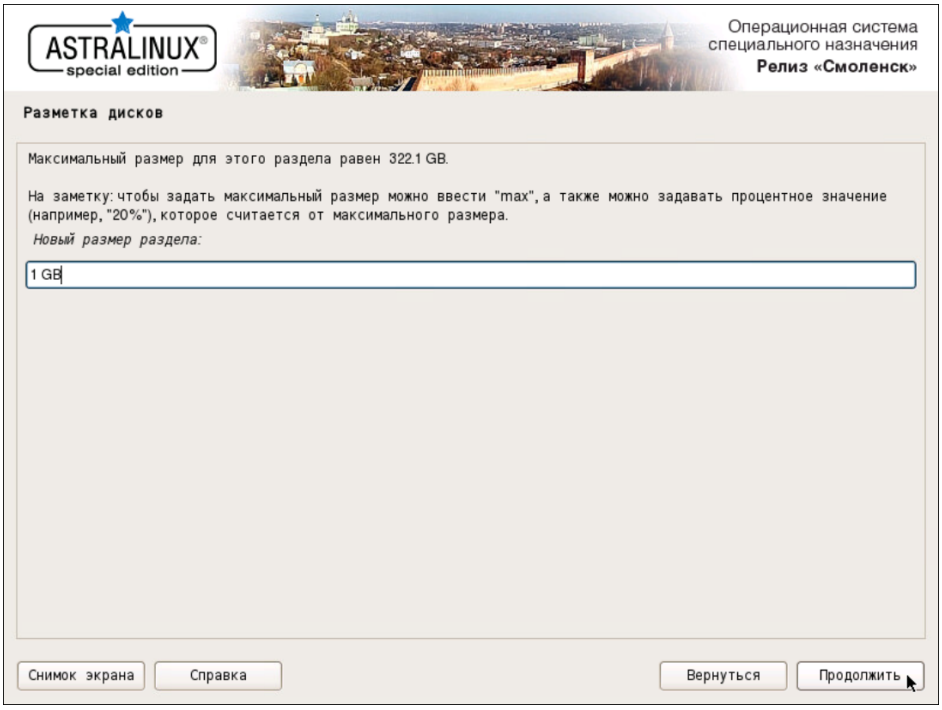


Рис. 3.12. Задание размера раздела

14. В появившемся окне выберите тип раздела **Первичный**. Нажмите **Продолжить**.

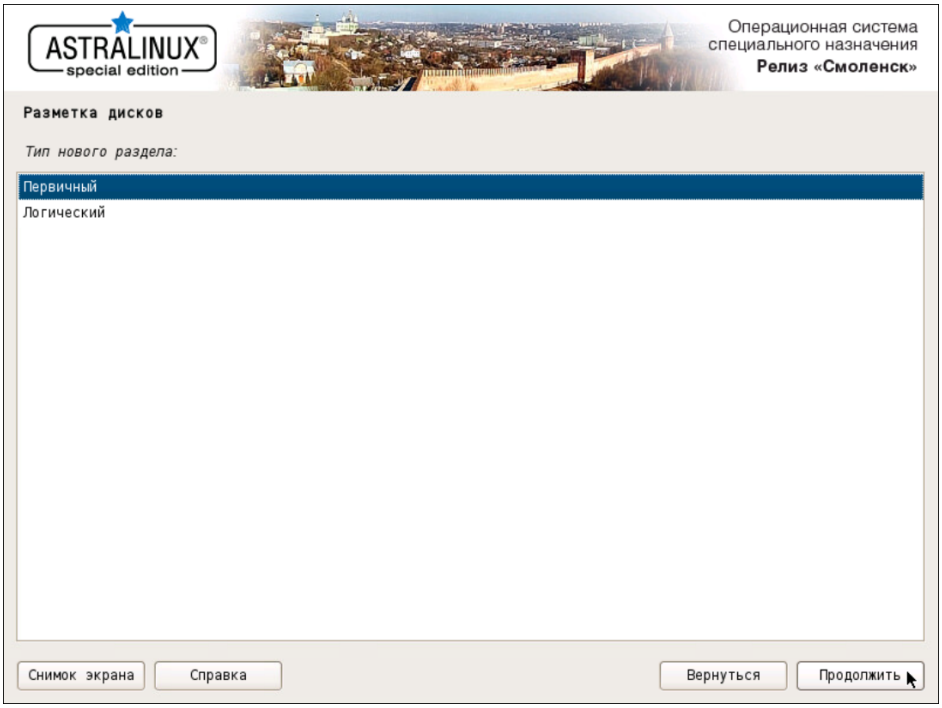


Рис. 3.13. Выбор типа раздела

15. В появившемся окне выберите расположение раздела **Начало**. Нажмите **Продолжить**.

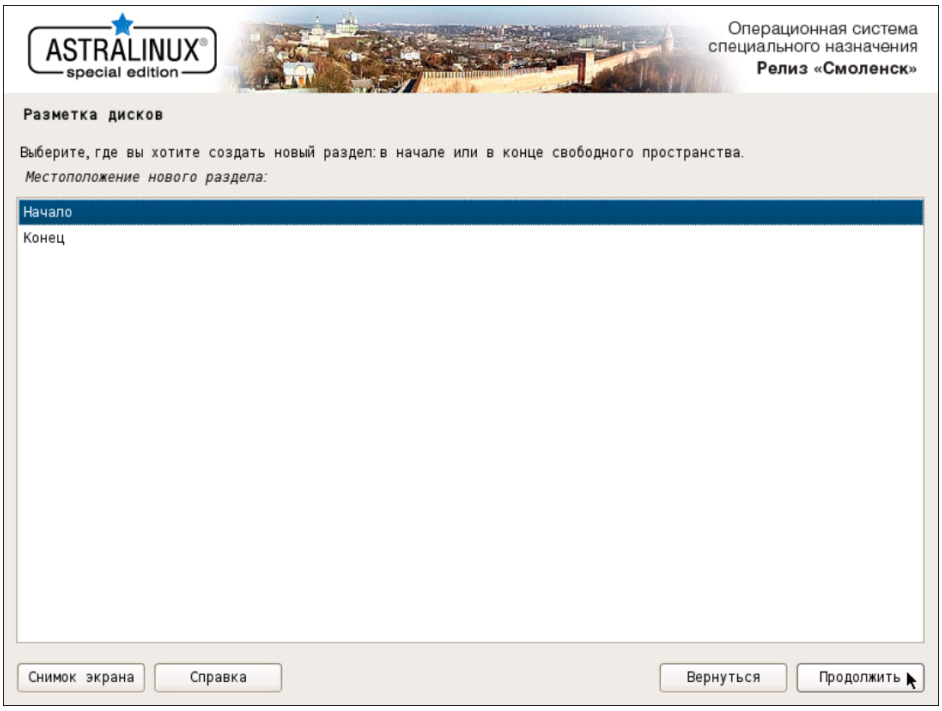


Рис. 3.14. Выбор местоположения раздела

16. Двойным щелчком мыши откройте параметры строки **Точка монтирования** и в появившемся окне выберите вариант **/boot**. Убедитесь, что на строке **Метка 'загрузочный'** выбрано значение **вкл**. Нажмите **Продолжить**.

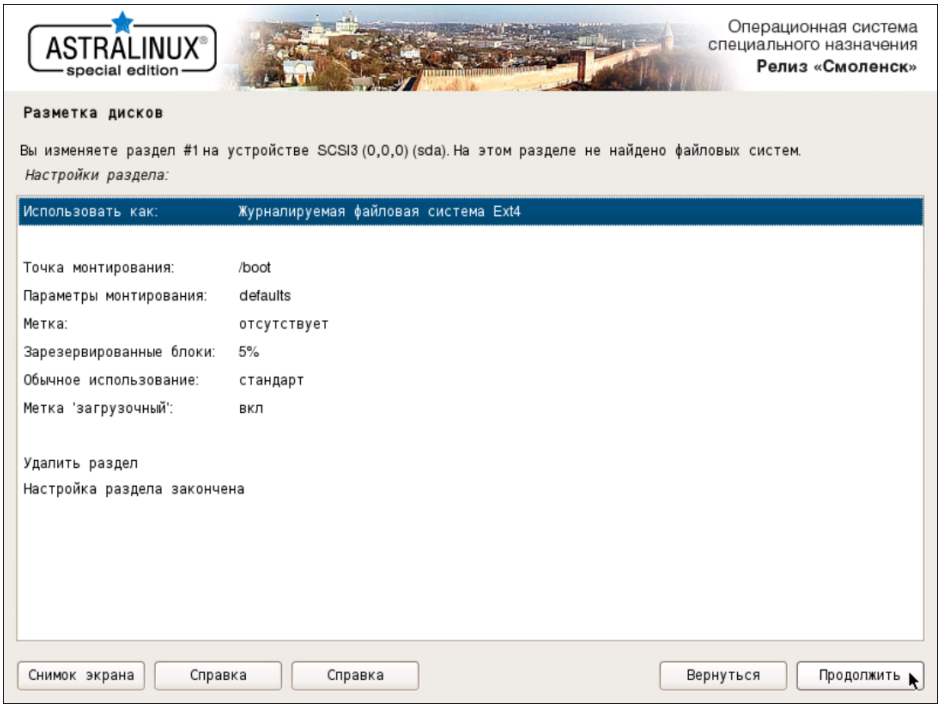


Рис. 3.15. Параметры монтирования раздела

17. Выделите строку **Настройка раздела закончена** и нажмите **Продолжить**.

18. Создайте новый раздел, выполнив шаги 11 и 12.

19. В появившемся окне выбора размера раздела оставьте максимальное значение по умолчанию. Нажмите **Продолжить**.

20. В появившемся окне выберите тип раздела **Логический**. Нажмите **Продолжить**.

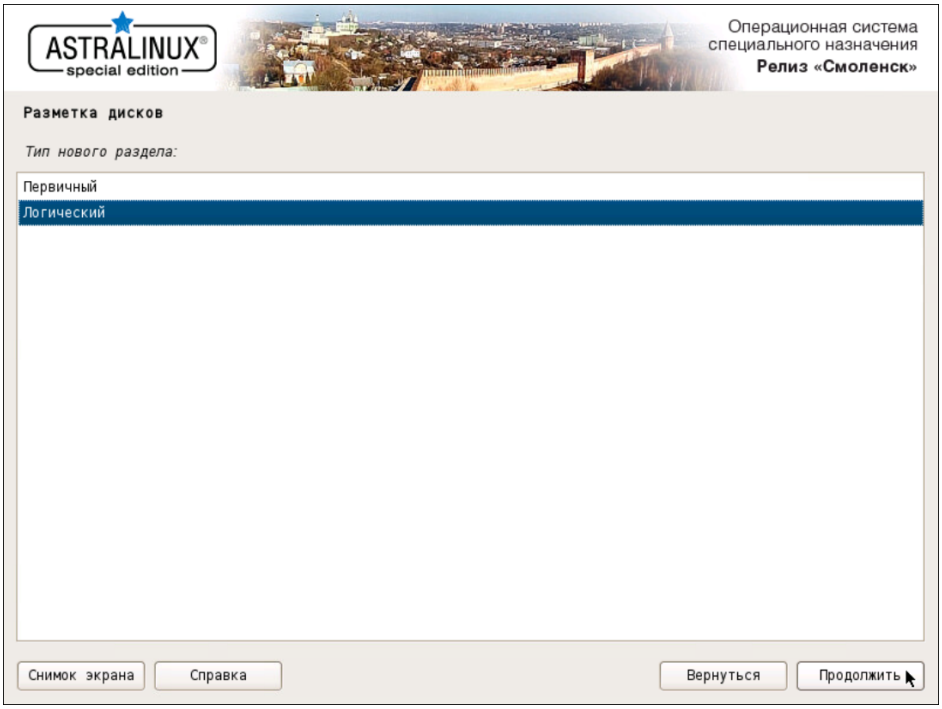


Рис. 3.16. Выбор типа раздела

21. В появившемся окне нажмите строку **Использовать как:**, выберите вариант **физический том для LVM** и нажмите **Продолжить**. Выделите строку **Настройка раздела закончена** и нажмите **Продолжить**.

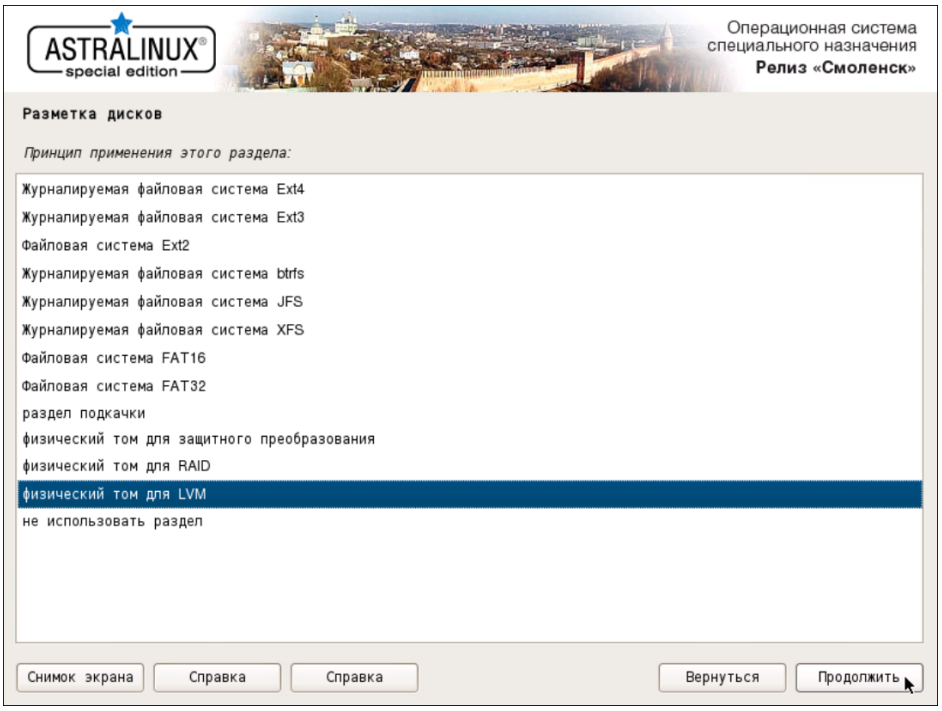


Рис. 3.17. Выбор варианта использования раздела

22 Двойным щелчком мыши откройте параметры строки **Настройка менеджера логических томов (LVM)** и в появившемся окне выберите **Да**. Нажмите **Продолжить**.

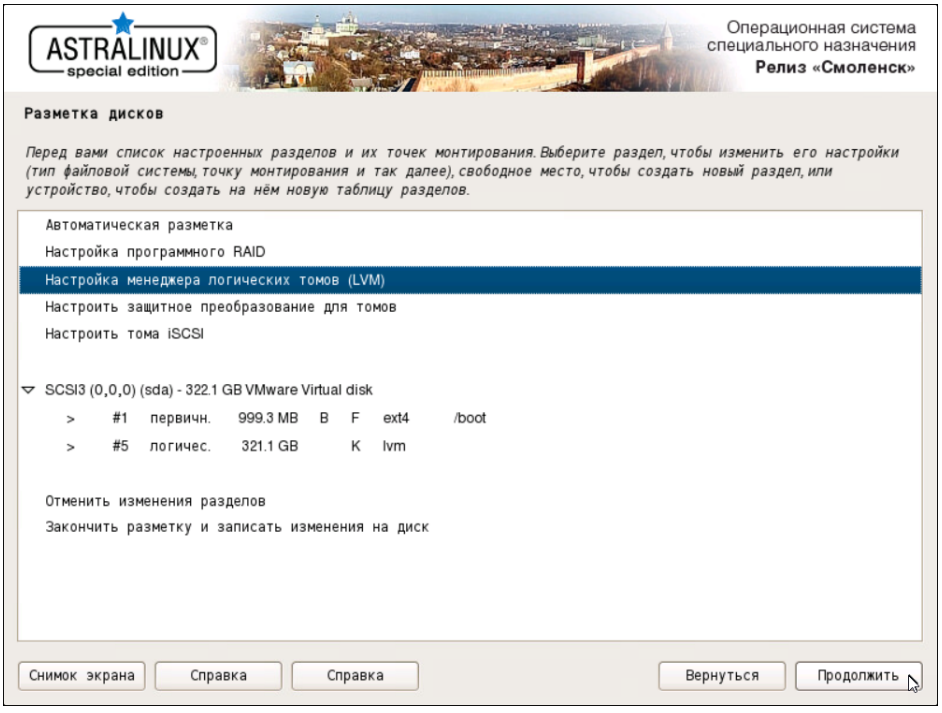


Рис. 3.18. Пункт настройки менеджера логических томов

23 В появившемся окне выберите вариант **Создать группу томов**. Нажмите **Продолжить**.

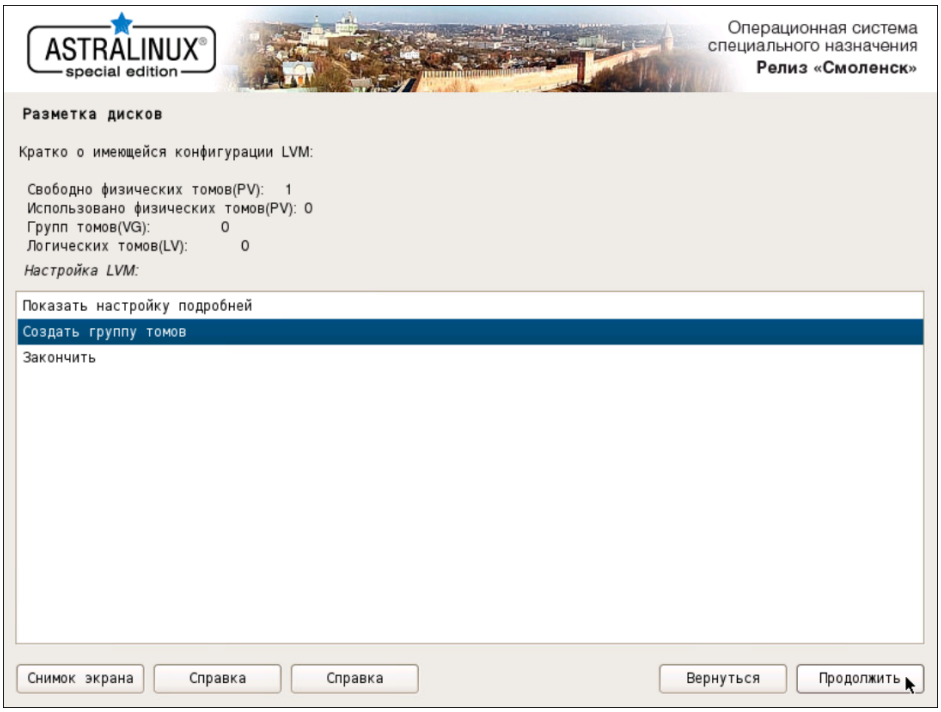


Рис. 3.19. Создание группы томов для LVM

24. В появившемся окне задайте название для группы томов, например, **ngfw**. Нажмите **Продолжить**.

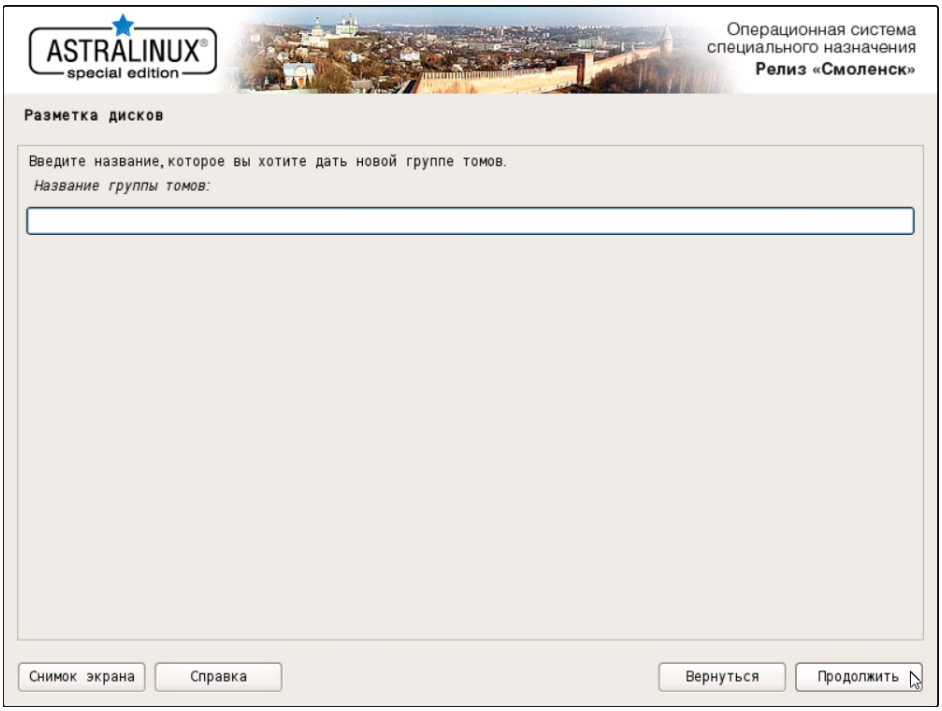


Рис. 3.20. Ввод имени группы томов

25. В появившемся окне выберите раздел, созданный на шаге 18. Нажмите **Продолжить**.

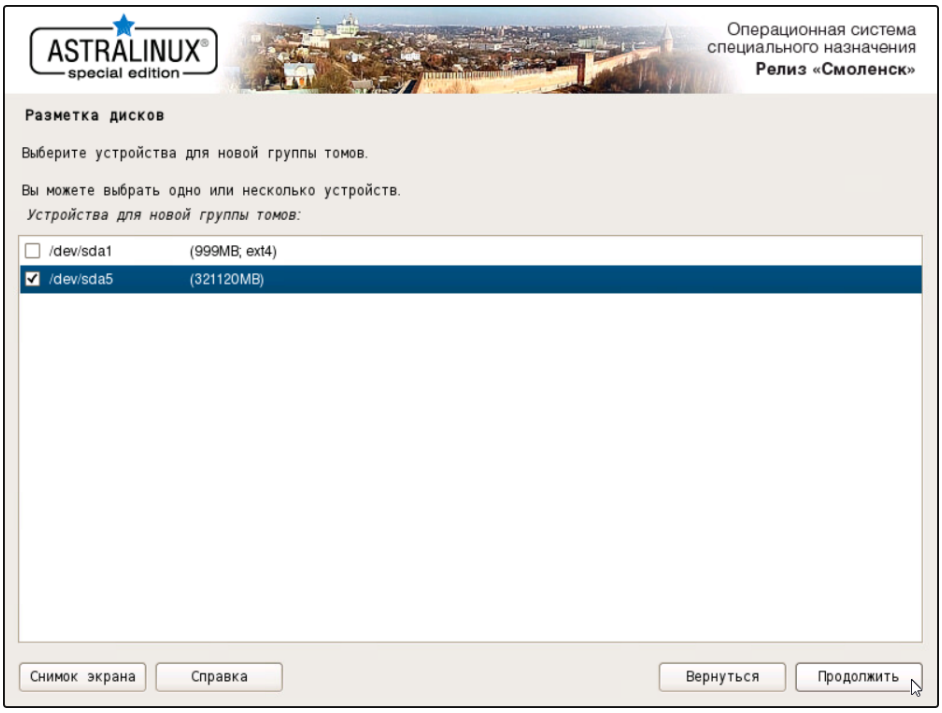


Рис. 3.21. Выбор устройства для размещения группы томов

26. В появившемся окне выберите вариант **Создать логический том**, нажмите **Продолжить** и укажите группу томов, созданную на шаге 23. Нажмите **Продолжить**.

27. В появившемся окне для нового логического тома задайте имя **root**. Нажмите **Продолжить**.

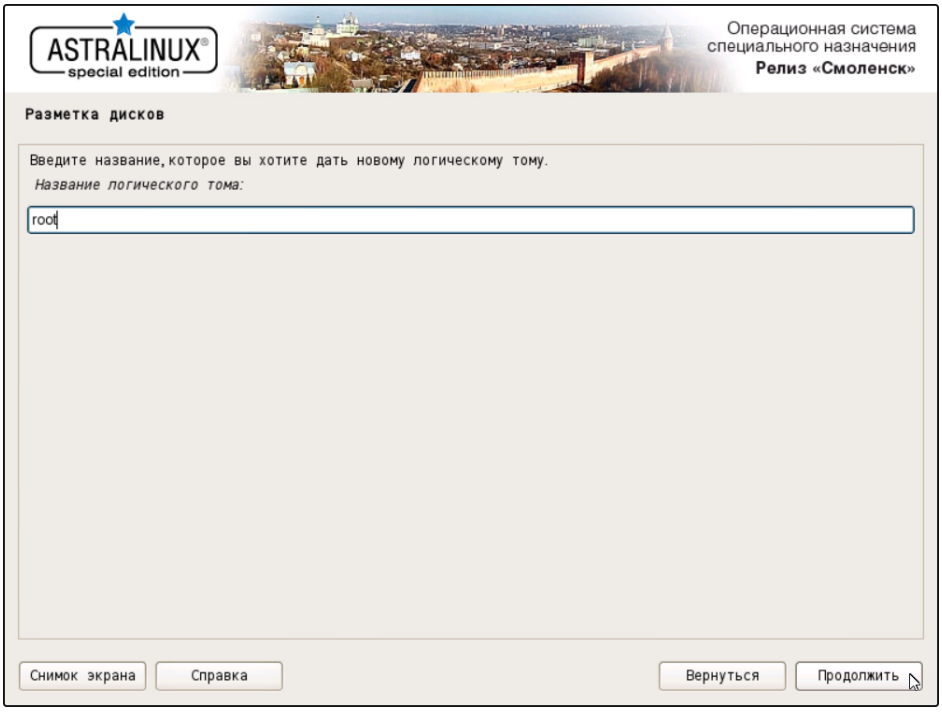


Рис. 3.22. Задание имени логического тома root

28. В следующем окне для нового логического тома задайте размер **25G**. Нажмите **Продолжить**.

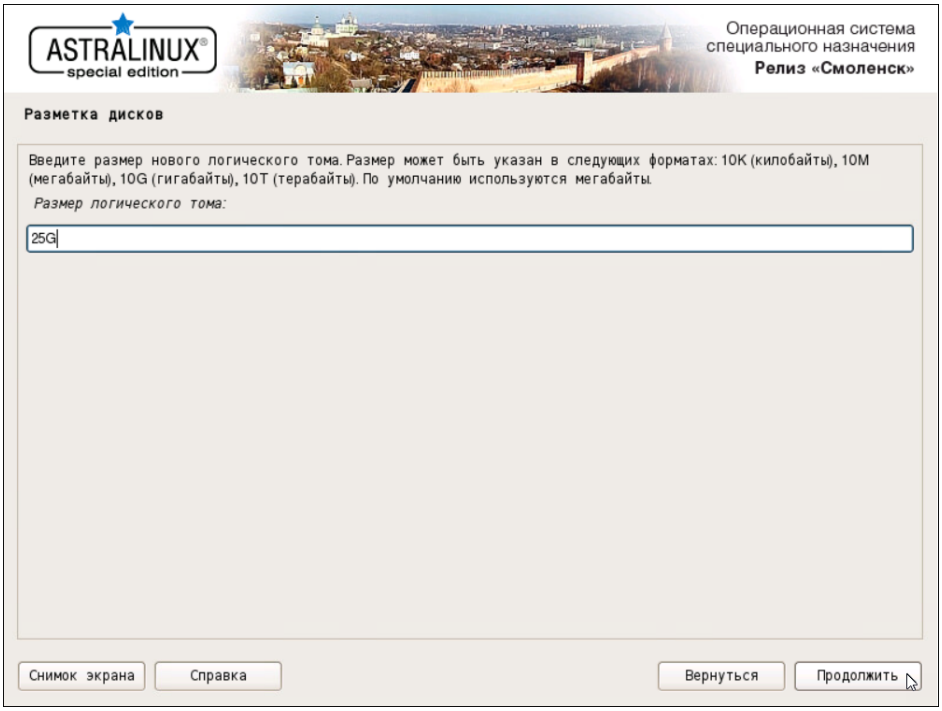


Рис. 3.23. Выделение размера для логического тома root

29. Создайте том с названием **var** и выделите для него 50 ГБ, выполняя действия шагов 26, 27 и 28.

30. Создайте тома, выполняя действия шагов 26, 27 и 28, в зависимости от назначения узла:

- При установке на master-узел – создайте тома **data** и **opt**. Для тома **data** выделите дисковое пространство в соответствии с требованиями к размеру хранилища. Рекомендуется выделить не менее 100 ГБ дискового пространства. Для тома **opt** выделить все оставшееся дисковое пространство.

  Внимание!

  *Крайне желательно, чтобы объем пространства, выделенного для тома **opt**, составлял не менее 40 ГБ. Этот том в процессе эксплуатации комплекса "Межсетевой экран Solar" активно наполняется данными, и исчерпание свободного места на нем приведет к аварийной остановке комплекса "Межсетевой экран Solar".*

- При установке на slave-узел – создайте тома **opt** и **data**. Для тома **opt** выделите не менее 40 ГБ дискового пространства, а для тома **data** – все оставшееся дисковое пространство.

31. В появившемся окне **Настройка LVM** выберите вариант **Закончить**. Нажмите **Продолжить**.

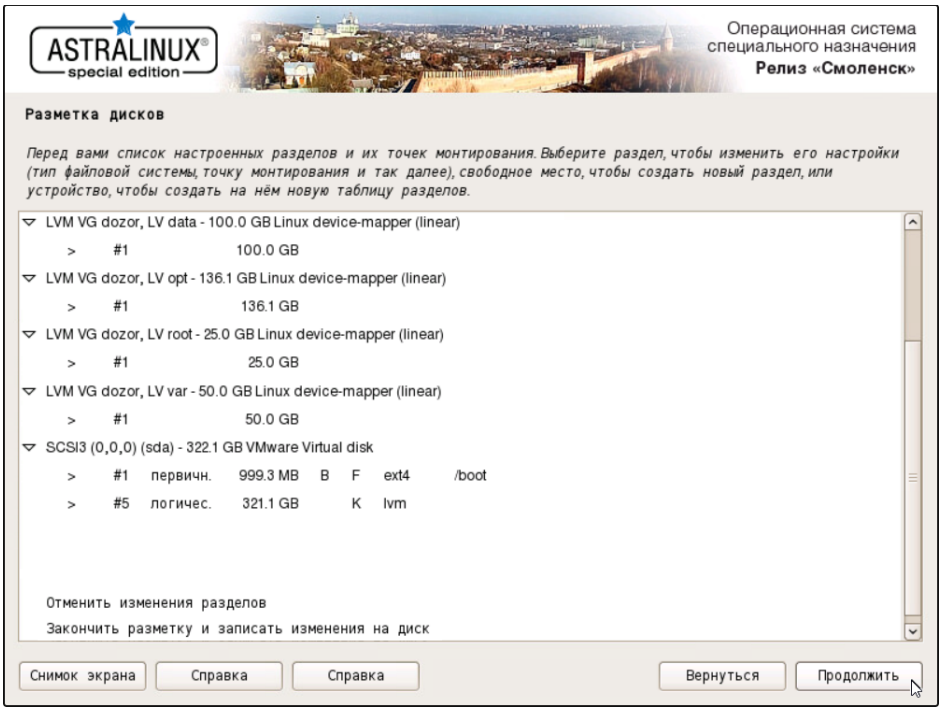


Рис. 3.24. Разметка дисков для master-узла

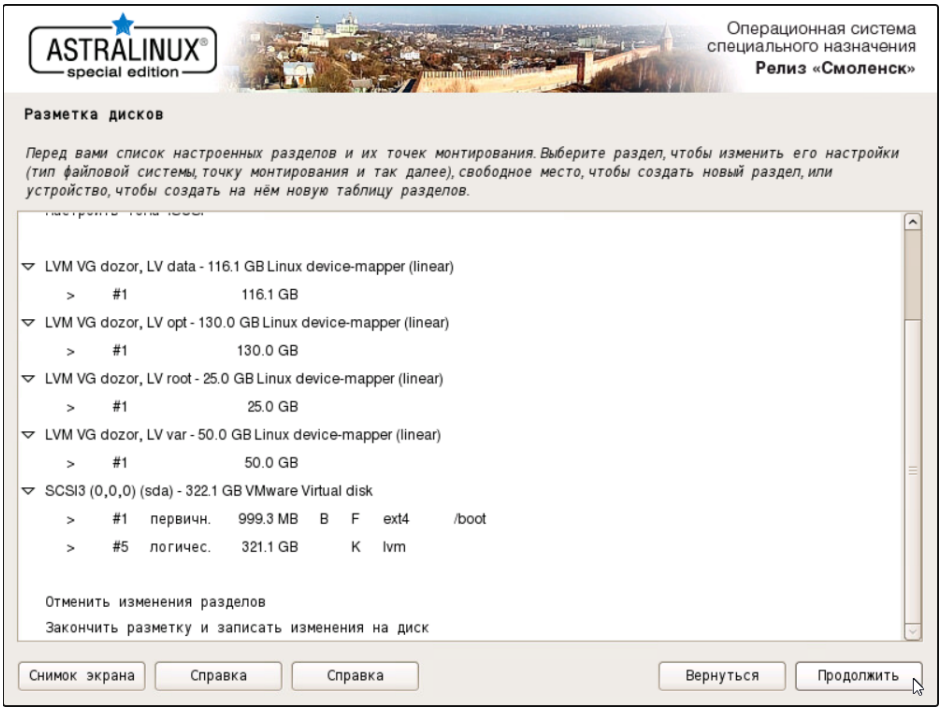


Рис. 3.25. Разметка дисков для slave-узла

32 Задайте точки монтирования и файловые системы для созданных томов. Например, для тома **root** выделите строку:

```
>   #1      25.0 GB
```

Нажмите **Продолжить** (или выполните двойной щелчок на этой строке). В появившемся окне двойным щелчком мыши откройте параметры строки **Использовать как: не использовать**. В появившемся окне выберите строку **Журналируемая файловая система Ext4** и нажмите **Продолжить**. В окне настроек тома откройте параметры строки **Точка монтирования** и выберите точку монтирования **/ -- корневая файловая система**. В окне настроек тома выполните двойной щелчок по строке **Настройка раздела закончена**.

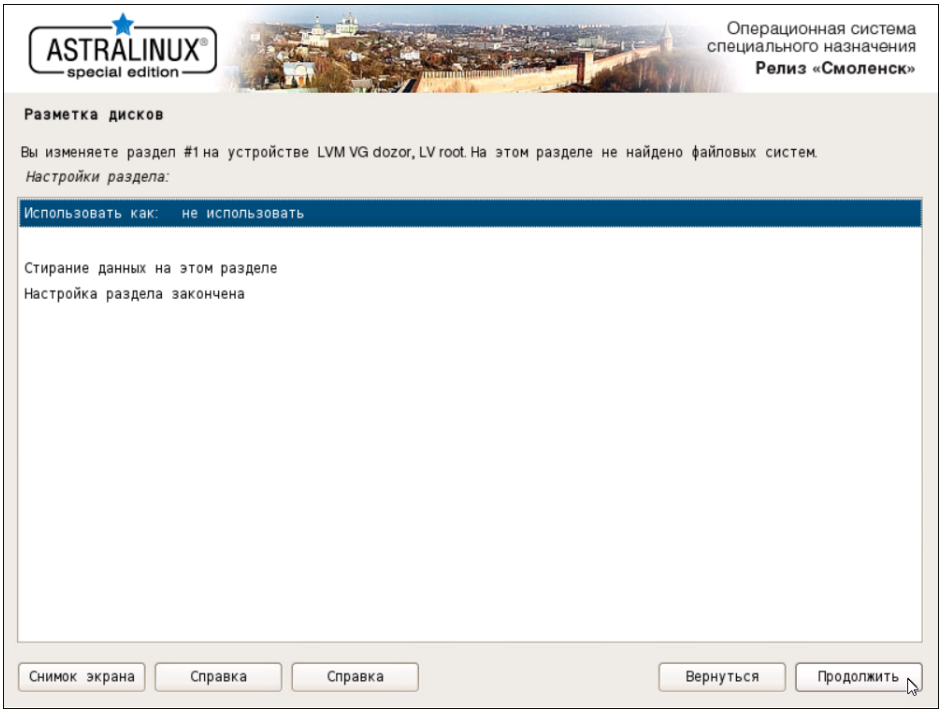


Рис. 3.26. Настройки тома root

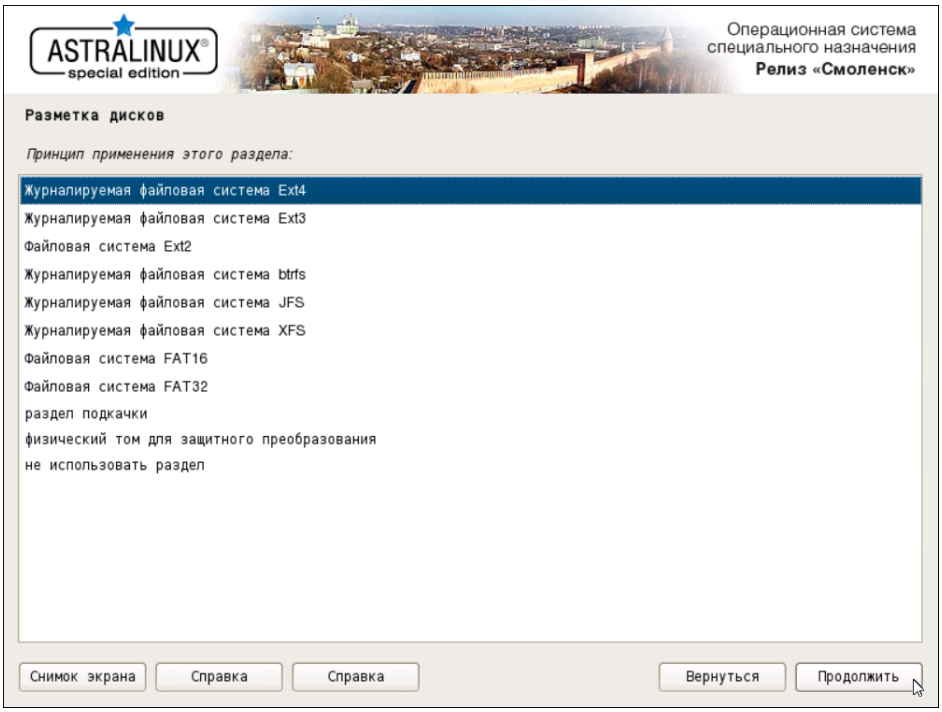


Рис. 3.27. Выбор файловой системы

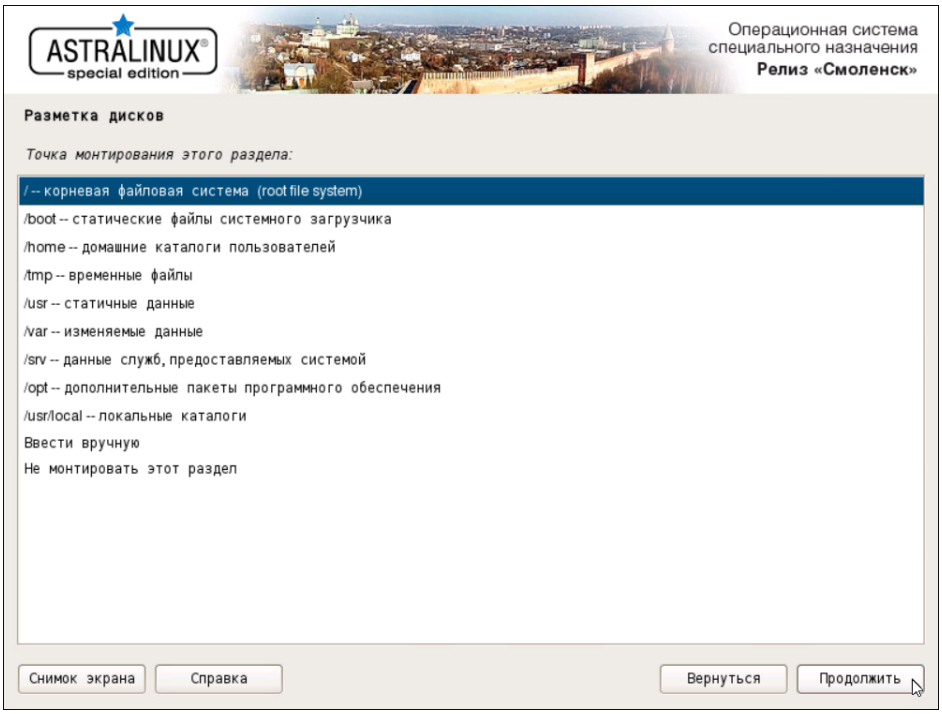


Рис. 3.28. Выбор точки монтирования

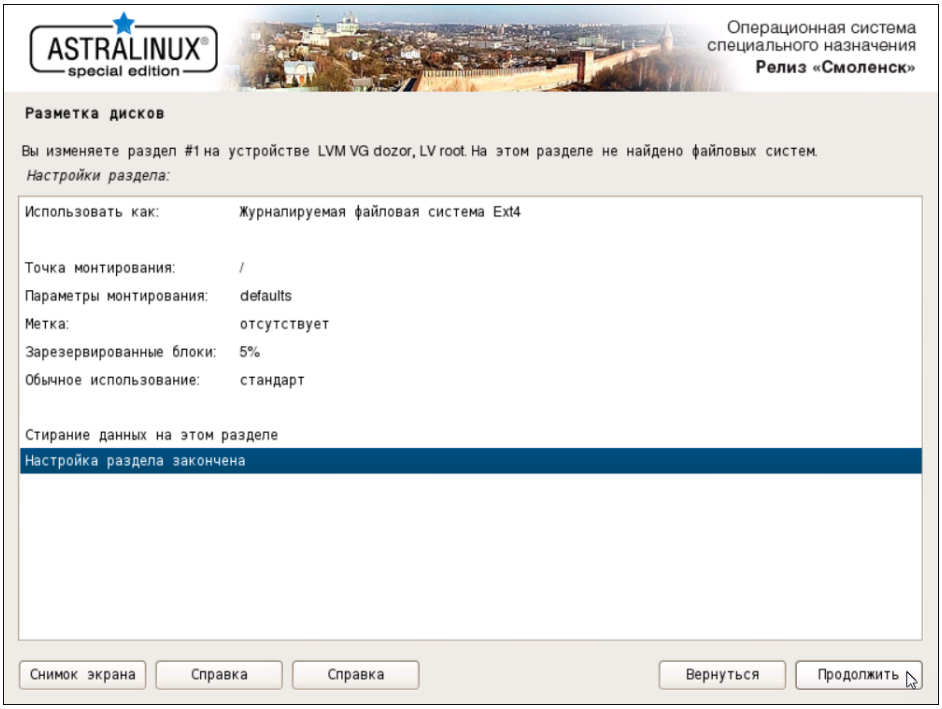


Рис. 3.29. Заполненные настройки тома root

33. Выполните действия предыдущего шага, задавая следующие точки монтирования и файловые системы:

- **var** – **/var**, **ext4**
- **data** – **/data**, **ext4** либо **xfs** (см. примечание)

- **opt – /opt, ext4**

Примечание

*Выберите значение **ext4** или **xfs** в зависимости от задач.*

При выборе точек монтирования для тома **data** следует выбирать пункт **Ввести вручную**.

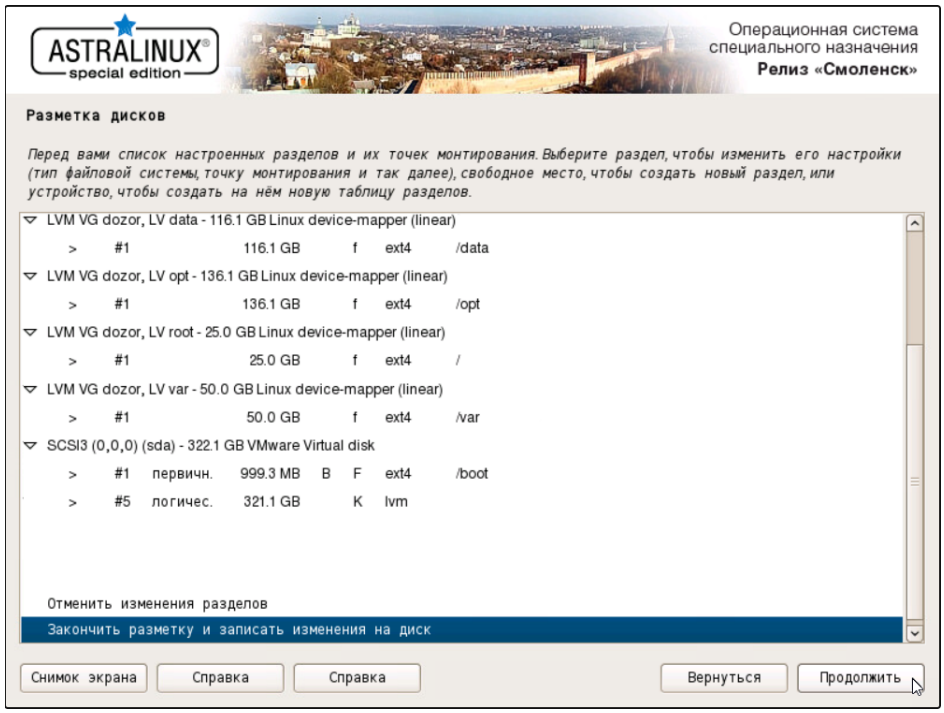


Рис. 3.30. Заполненные настройки томов для master-узла

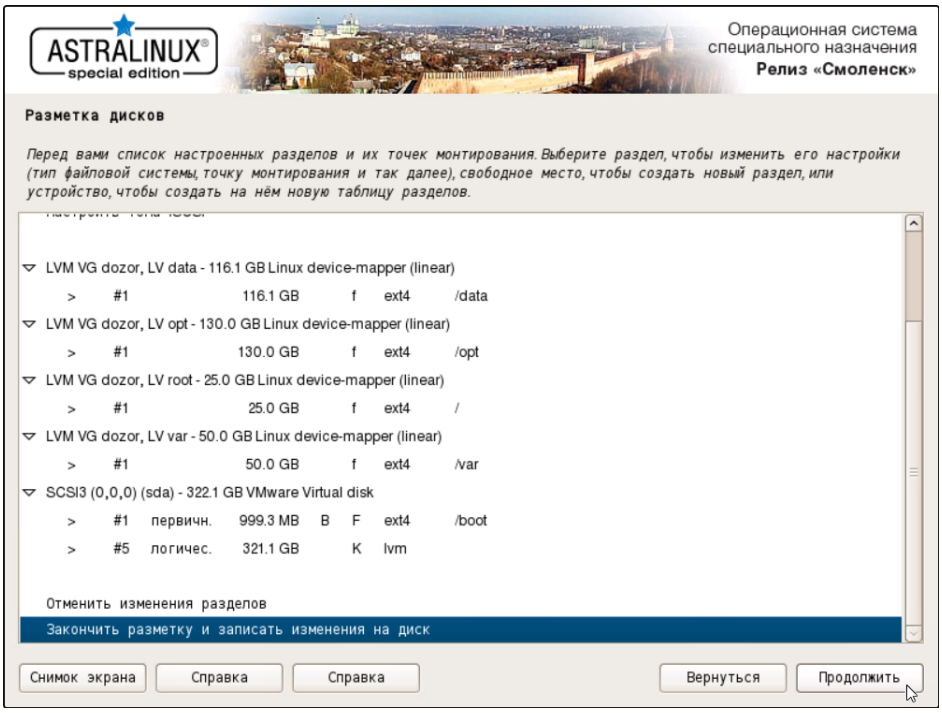


Рис. 3.31. Заполненные настройки томов для slave-узла

34. Выберите строку **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.

35. В появившемся окне будет отображено предупреждение об отсутствии разделов для пространства подкачки. Следует выбрать **Нет** и нажать **Продолжить**.

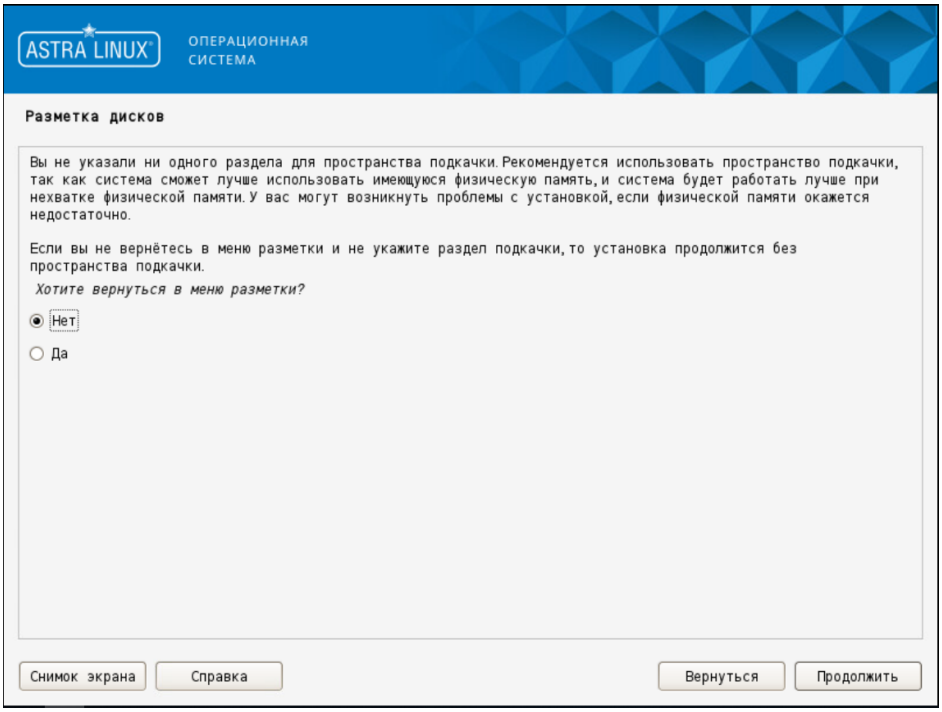


Рис. 3.32. Предупреждение об отсутствии разделов для пространства подкачки

36. В появившемся окне будет отображена информация о разметке дисков. Убедитесь, что эта информация верна, выберите **Да** и нажмите **Продолжить**.

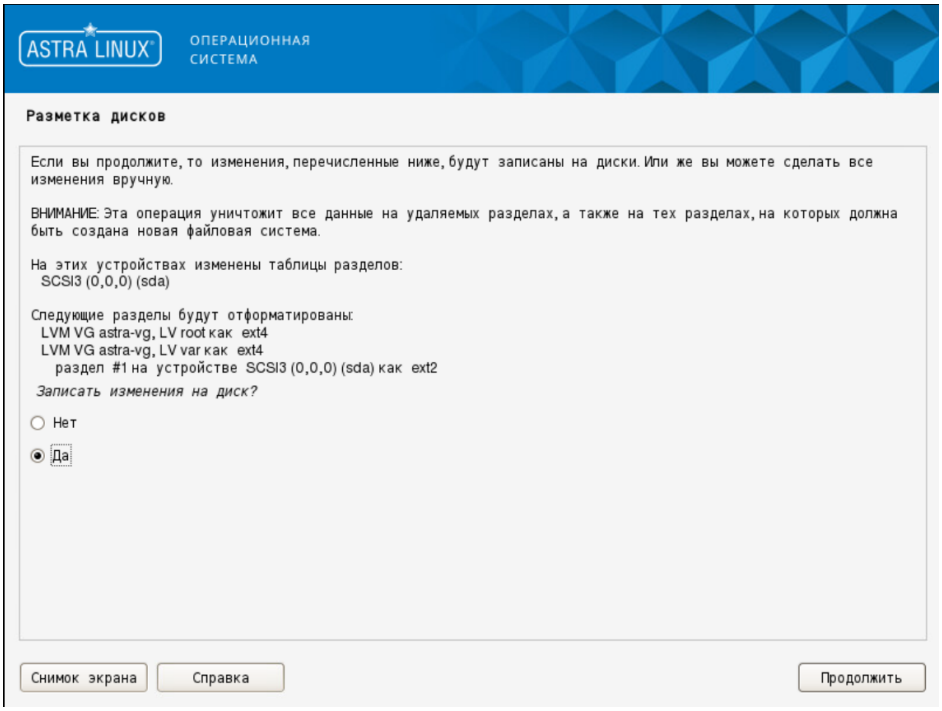


Рис. 3.33. Информация о разметке дисков

37. Дождитесь установки базовой системы. В появившемся окне выберите ядро **linux-5.10-generic**.

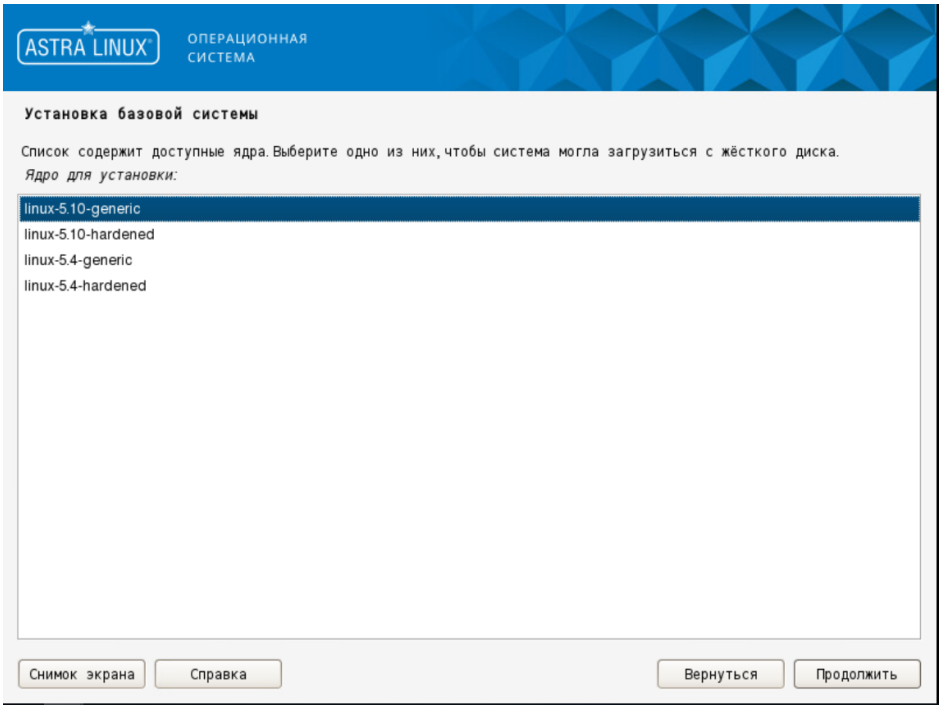


Рис. 3.34. Выбор ядра

Примечание

Версия ядра может меняться в зависимости от установленной версии ОС Astra Linux.

38. После окончания установки в появившемся окне **Выбор программного обеспечения** выберите варианты **Консольные утилиты** и **Средства удаленного доступа SSH**. Нажмите **Продолжить**.

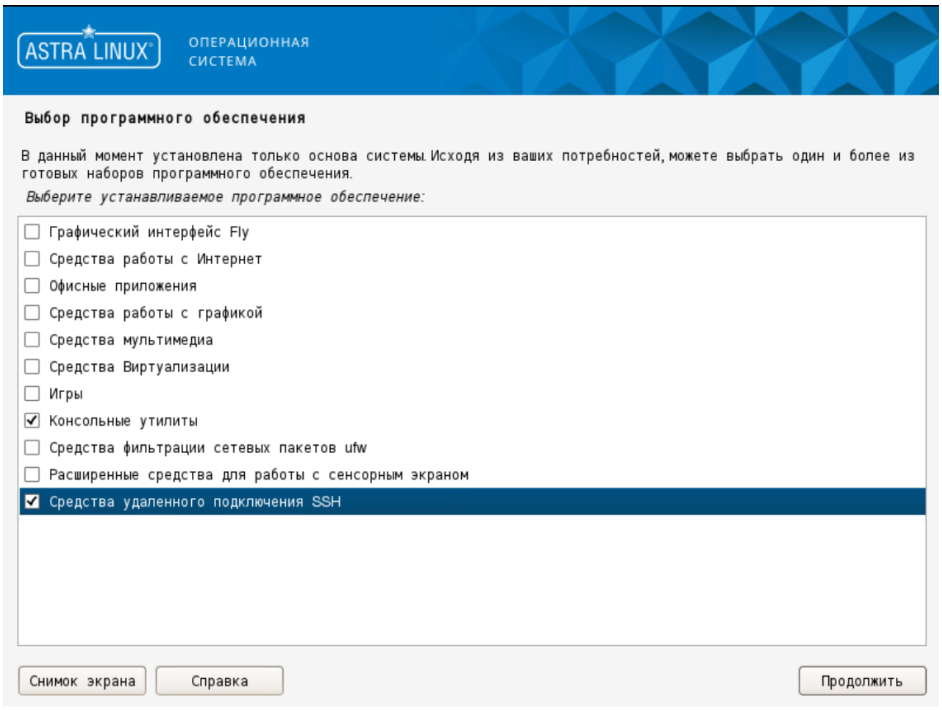


Рис. 3.35. Выбор программного обеспечения

39. В появившемся окне **Дополнительные настройки ОС** выберите **Максимальный уровень защищенности "Смоленск"**, если позволяет лицензия. Нажмите **Продолжить**.

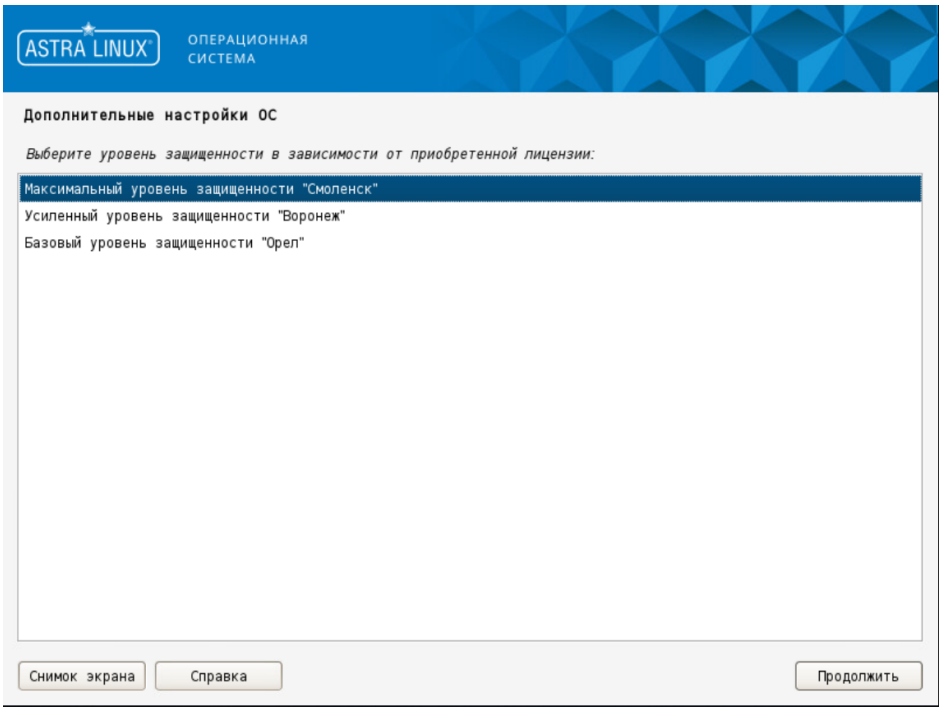


Рис. 3.36. Выбор уровня защищенности

40. В следующем окне снимите все флажки и нажмите **Продолжить**.

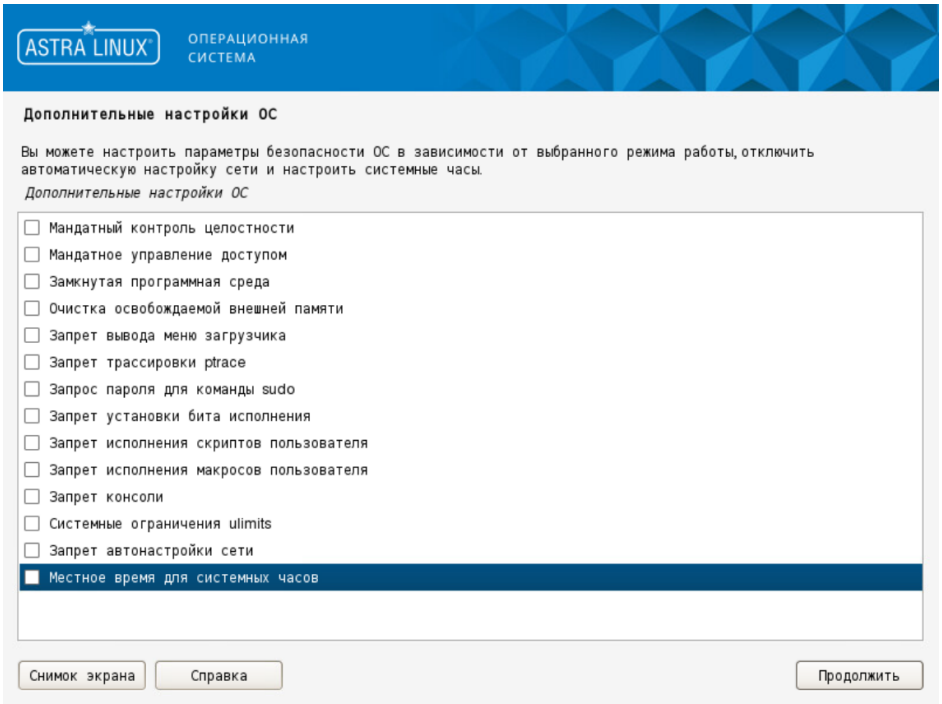


Рис. 3.37. Дополнительные настройки ОС

41. В появившемся окне **Установка системного загрузчика GRUB на жесткий диск** нажмите **Продолжить**.

42. В появившемся окне задайте пароль для системного загрузчика GRUB. Нажмите **Продолжить**, повторите ввод пароля и нажмите **Продолжить**.

43. После запроса системы отключите установочный носитель и нажмите **Продолжить**.

44. Перезагрузите систему и войдите под учетной записью администратора..

45. Запустите SSH-сервер, выполнив команды:

    ~$ sudo systemctl start ssh

    ~$ sudo systemctl enable ssh

    Примечание

    Здесь и далее команды CLI следует выполнять от имени суперпользователя, используя команду ***sudo*** *.*

46. Узнайте имя сетевого интерфейса, выполнив команду:

    ~$ ip a

    Вывод команды будет содержать пронумерованный список имен сетевых интерфейсов (включая локальную петлю под номером 1).

47. Откройте для редактирования файл **/etc/network/interfaces.d/eth0** (где **eth0** – имя сетевого интерфейса, полученного на предыдущем шаге) и внесите необходимые изменения в соответствии с существующей в компании сетевой архитектурой:

```
auto eth0
iface eth0 inet static
address <IP>/<mask>
gateway <IP>
```

    Если каталог **/etc/network/interfaces.d/eth0** пуст, выполните следующие действия:

    a. Откройте для редактирования файл **/etc/network/interfaces** и задайте конфигурацию сети. Пример для автоматического конфигурирования с использованием DHCP:

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

    Пример для ручного конфигурирования:

```
auto eth0
iface eth0 inet static
address <IP>
netmask <mask>
gateway <gateway>
dns-nameservers <dns>
```

    где:

- **<IP>** – статический IP-адрес сервера.
- **<mask>** – маска сети.
- **<gateway>** – адрес сетевого шлюза.
- **<dns-nameservers>** – IP-адрес сервера DNS. Можно указать несколько адресов, перечисляя их через пробел.

b. При ручном конфигурировании откройте или создайте файл **/etc/resolv.conf** и настройте параметры DNS:

```
nameserver 192.168.11.1
domain example.com
```

где:

- **<nameserver>** – IP-адрес сервера DNS,
- **<example.com>** – имя домена.

c. Выполните действия шага **a** для всех остальных сетевых интерфейсов.

48. Перезапустите сетевую службу, выполнив команду:

~$ sudo systemctl restart networking

49. Выполните команды:

~$ sudo ufw disable

~$ sudo init 6

~$ sudo astra-mic-control disable

Примечание

Для корректной работы Журнала соединений выполните действия:

a. *Авторизуйтесь под учетной записью **root**, выполнив команду:*

~$ sudo su -

b. *Задайте пароль этой учетной записи, выполнив команду:*

~# passwd

c. *Разрешите авторизацию и вход под этой учетной записью, выполнив команду:*

~# echo "PermitRootLogin yes" >> /etc/ssh/sshd_config

d. *Перезапустите сервис ssh, выполнив команду:*

~# systemctl restart ssh

4. Рекомендации к установке комплекса "Межсетевой экран Solar"

4.1. Подготовка оборудования перед установкой

Выполняйте при работе следующие требования по безопасности:

- Рабочую зону и оборудование необходимо содержать в чистоте.
- Не производите действий, которые могут создать опасность для окружающих или оборудования.
- При монтаже необходимо обесточить оборудование и проверьте. что отсутствует напряжение цепях электропитания.
- Не производите работы в одиночку в потенциально опасных условиях.

После транспортировки оборудование необходимо оставить в помещении, где оно будет установлено, не менее 5 часов.

При работе оборудования крышка корпуса должна быть закрыта. Конструкция корпуса обеспечивает достаточную циркуляцию воздуха для охлаждения оборудования.

Перед установкой оборудования проверьте комплект поставки.

При монтаже подключите монитор, клавиатуру и кабель сети управления. Чтобы обезопасить оборудование от скачков напряжения, необходимо подключить сначало его к внешнему источнику питания.

4.2. Настройка DNS

Внимание!

Необходимо настроить FQDN на master-узле до установки комплекса "Межсетевой экран Solar".

Проверьте содержимое следующих файлов настройки DNS на всех узлах комплекса "Межсетевой экран Solar":

- **/etc/hostname**
- **/etc/hosts**

Файл **/etc/hostname** должен содержать единственную строку, представляющую собой краткое доменное имя сервера.

Файл **/etc/hosts** должен содержать строки для всех узлов ПК комплекса "Межсетевой экран Solar", каждая из которых состоит из IP-адреса узла, FQDN (состоящего из краткого доменного имени и доменного суффикса) и краткого (домен нижнего уровня) доменного имени, например:

```
10.199.21.148 ngfw-master.company.local ngfw-master
10.199.21.149 filter1.company.local filter1
10.199.21.147 filter2.company.local filter2
```

Примечание

*При наличии адреса 127.0.1.1 в файле **/etc/hosts** необходимо его скрыть или удалить, а FQDN явно прописывать для IP-адреса, с которого происходит вход в комплекс "Межсетевой экран Solar".*

IP-адрес и записи доменного имени должны быть разделены символом табуляции.

Внимание!

*Полное доменное имя (FQDN) и краткое доменное имя (hostname) могут состоять только из прописных латинских букв, цифр или служебного символа **-**. Для разделения уровней доменных зон в FQDN используйте точку. Краткое доменное имя должно начинаться только с прописной латинской буквы и не должно содержать в себе точки. При подключении комплекса "Межсетевой экран Solar" к NTLM-домену Windows краткое доменное имя (hostname) не должно превышать 15 символов. Пример правильного написания FQDN: **ngfw-01.example.org**, где краткое доменное имя будет **ngfw-01**.*

4.3. Настройка синхронизации времени

Для корректной работы комплекса "Межсетевой экран Solar" необходима синхронизация времени. В отсутствие контроллера домена или другого источника точного времени возникнут проблемы из-за разного времени в журналах и метках времени на данных, а также возможны проблемы с работой протокола HTTPS. Для синхронизации времени могут быть использованы один или несколько серверов точного времени, находящихся как в корпоративной сети, так и в сети Интернет.

Для настройки синхронизации времени на всех узлах комплекса "Межсетевой экран Solar" выполните следующие действия:

1. Найдите нужную временную зону, выполнив следующую команду:

   # timedatectl list-timezones

   Для удобства поиска можно воспользоваться сортировкой, например:

   # timedatectl list-timezones | grep Europe

2. Установите нужную временную зону, выполнив команду следующего вида:

   # timedatectl set-timezone <timezone>

   где **<timezone>** – значение, найденное в предыдущем шаге.

3. Убедитесь в правильности настройки временной зоны, выполнив следующую команду:

   # timedatectl

4. Установите пакет **ntp**, выполнив команду:

   # sudo apt-get install ntp

5. Откройте для редактирования файл **/etc/ntp.conf** и добавьте в него одну или несколько строк следующего вида:

   ```
   server <timeserver> iburst
   ```

   где **<timeserver>** – FQDN или IP-адрес NTP-сервера (внешнего или принадлежащего организации). Параметр **iburst** является необязательным и служит для повышения точности синхронизации за счет увеличенного количества пакетов, отправляемых при обмене данными с NTP-сервером.

   Наличие нескольких записей позволяет продолжать синхронизацию в случае отказа какого-либо из NTP-серверов. Серверы опрашиваются по очереди, в порядке их перечисления в файле **ntp.conf**.

6. Запустите службу NTP и добавьте ее в автозагрузку, выполнив команды:

   # systemctl start ntp

   # systemctl enable ntp

Узнать список работающих используемых серверов точного времени можно выполнив следующую команду:

 # ntpq -p

4.4. Проверка и настройка БД Clickhouse (инструкции sse4_2)

Комплекс "Межсетевой экран Solar" использует БД Clickhouse. Для корректного функционирования этой БД аппаратное обеспечение поддерживает набор инструкций **sse4_2**. Проверить наличие этой поддержки можно с помощью команды:

 # grep sse4_2 /proc/cpuinfo

Вывод команды не должен быть пустым.

4.5. Настройка функционирования под управлением systemd

По умолчанию подсистема инициализации **systemd** принудительно завершает процессы пользователя **dozor**, от имени которого впоследствии должна быть создана БД архива, а также будут выполняться некоторые другие действия. Для исправления этой ситуации выполните следующие действия:

1. Откройте для редактирования файл **/etc/systemd/logind.conf**.

2. Найдите следующие строки:

   ```
   #KillExcludeUsers=root
   #RemoveIPC=yes
   ```

3. Замените найденные строки на следующие:

```
KillExcludeUsers=root dozor
RemoveIPC=no
```

4. Сохраните и закройте файл.
5. Перезапустите ОС, выполнив команду:

   ~$ sudo init 6

5. Установка комплекса "Межсетевой экран Solar"

Для установки комплекса "Межсетевой экран Solar" на master-узле в CLI выполните команду:

 # /var/tmp/solar-ngfw-1.2.astra17-1.7.4-signed.run --install

где **/var/tmp/solar-ngfw-1.2astra17-1.7.4-signed.run** – путь к инсталлятору.

Примечание

Для просмотра установленных пакетов на программно-аппаратном комплексе МЭ Solar в CLI введите следующую команду:

apt list –installed| grep solar

5.1. Настройка сетевых интерфейсов

Для управления сетевыми интерфейсами в комплексе "Межсетевой экран Solar" необходимо перенести состояния сетевых интерфейсов, настроенных через службу networking или другими методами, в службу Network Manager. Состояния сетевых интерфейсов переносятся автоматически во время установки комплекса "Межсетевой экран Solar".

Примечание

Возможно перенесение настроек только Ethernet-интерфейсов простого типа.

Переносятся настройки только активной конфигурации. Из конфигурационных файлов перенос настроек не происходит.

При перенесении настроек сетевых интерфейсов значимой информацией являются действующие IP-адреса, маршруты и состояния интерфейсов. Другая информация не обрабатывается.

Условия переноса настроек сетевых интерфейсов:

- *В системе определен как минимум один интерфейс, позволяющий проводить удаленное управление (SSH).*
- *Одному интерфейсу соответствует один IP-адрес.*
- *В системе используется только статическая маршрутизация.*
- *Из таблицы маршрутизации импортируются только активные маршруты (в том числе только один активный маршрут по умолчанию).*

Перед переносом не рекомендуется оставлять ненастроенные интерфейсы в активном состоянии, т.к. при наличии DHCP-протокола их IP-адреса будут также обработаны. В таком случае, например, может быть добавлен активный маршрут, который не был выбран в явном виде, что может привести к потере связи.

Чтобы перенести состояния сетевых интерфейсов в службу Network Manager:

1. Определите и настройте интерфейс для удаленного управления системой. Для этого задайте настройки статической маршрутизации для удаленного входа в конфигурационном файле **/etc/network/interfaces**, добавив строки:

   # iface <название интерфейса управления> inet static

   # address <IP-адрес с префиксом маски>

   Примечание

   Также можно задать дополнительные статические маршруты для интерфейса управления. Для этого добавьте строки:

   # iface <название интерфейса управления> inet static

   # address <IP-адрес с префиксом маски>

   # gateway <IP-адрес шлюза>

   # up /bin/ip route add <подсеть назначения> via <адрес шлюза>

2. Все интерфейсы, кроме управляющего, переведите в режим ручного управления. Для этого для каждого интерфейса (кроме управляющего) в файле конфигурации **/etc/network/interfaces** добавьте строку:

   # iface <название интерфейса> inet manual

   Пример записи:

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth4
iface eth4 inet static
        address 10.199.28.49/22
        up /bin/ip route add 10.201.160.0/19 via 10.199.28.1
        up /bin/ip route add 10.201.196.0/22 via 10.199.28.1
        up /bin/ip route add 10.201.208.0/20 via 10.199.28.1
        up /bin/ip route add 10.201.28.10/32 via 10.199.28.1
        up /bin/ip route add 10.201.11.10/31 via 10.199.28.1
        up /bin/ip route add 10.201.11.36/32 via 10.199.28.1
        up /bin/ip route add 10.201.28.9/32 via 10.199.28.1
        up /bin/ip route add 10.201.28.238/32 via 10.199.28.1
        up /bin/ip route add 10.199.11.2/32 via 10.199.28.1

iface eth0 inet manual

iface eth1 inet manual

iface eth2 inet manual

iface eth3 inet manual

iface usb0 inet manual
root@main:~#
```

3. Перезапустите сервис networking с помощью команды:

   # systemctl restart networking

После завершения переноса состояния сетевых интерфейсов в службу Network Manager файл конфигурации **/etc/network/interfaces** будет переименован в **/etc/network/interfaces.bak**.