ООО «БАЗАЛЬТ СПО»

АЛЬТ ДОМЕН

Инструкция по установке

Ред. 2.0

МОСКВА 2025

СОДЕРЖАНИЕ

1 СОСТАВ ПРОДУКТА

Программный комплекс (ПК) «Альт Домен» функционирует на ОС «Альт Сервер» или ОС «Альт СП Сервер». В данном документе описана процедура установки на ОС «Альт Сервер», для уточнения деталей установки на ОС «Альт СП Сервер» обратитесь к документации на «Альт СП» («Руководство администратора. ЛКНВ.11100-01 90 03»).

Состав «Альт Домен»:

- контроллер домена Samba DC на базе дистрибутива «Альт Сервер»;
- модуль для ввода компьютера в домен;
- модуль удалённого управления базой данных конфигурации (ADMC) – управляет объектами в домене и групповыми политиками, реализован как графический инструмент, работает под Linux;
- модуль редактирования настроек клиентской конфигурации (GPUI) – позволяет редактировать настройки групповых политик;
- шаблоны групповых политик;
- модуль для применения конфигурации на целевой Linux-ОС (gpupdate);
- инструмент диагностики (ADT).

Приложения продукта устанавливаются в следующем порядке:

1. Установка ОС «Альт Сервер».
2. Разворачивание нового домена:

- создание первого контроллера в домене;
- присоединение сервера в роли контроллера домена к существующему домену;
- присоединение сервера или рабочей станции в роли рядового участника существующего домена.

3. Установка административных инструментов (ADMC, GPUI).
4. Установка инструмента диагностики (ADT).

В табл. 1 представлены параметры, используемые в качестве примера в данном разделе.

Таблица 1. Параметры домена

	IP-адрес	Полное доменное имя (FQDN)
Первый контроллер домена	192.168.0.132	dc1.test.alt
Второй контроллер домена	192.168.0.133	dc2.test.alt
Участник домена	192.168.0.135	host-01.test.alt

2 ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

2.1 Системные требования к серверу (контроллеру домена)

Для демонстрационной/тестовой системы рекомендуется 2 ГБ.

Для производственной установки рекомендуется не менее 4 ГБ ОЗУ, а затем 2 ГБ на каждую дополнительную 1000 пользователей.

Примечание. Параметр, который оказывает наибольшее влияние на требования к памяти, – это количество одновременных открытий сеансов.

Примечание. В условиях реальной эксплуатации рекомендуется использовать два или более контроллера домена для обеспечения отказоустойчивости.

2.2 Размеры хранилища

10 ГБ достаточно для доменов с несколькими сотнями пользователей.

При планировании размера хранилища также необходимо учесть:

- уровни журналов и политику хранения журналов;
- использование изображений/аватаров для идентификации пользователей;
- количество пользователей, машин и групп;
- место под резервные копии.

1.3 CPU

Для нескольких сотен пользователей достаточно 4 vCPUs.

Некоторые процессы Samba не являются многопоточными, поэтому увеличение числа процессоров не повысит производительность.

Чтобы сбалансировать нагрузку, необходимо создать второй контроллер домена в репликации с первым и применить политику балансировки нагрузки на уровне клиента.

Необходимое количество контроллеров домена зависит от нескольких параметров:

- количество сторонних приложений LDAP, подключенных к домену;
- качество кода сторонних LDAP-приложений, подключенных к домену;
- количество запросов к файловым серверам.

1.4 DNS

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен верхнего уровня RFC2606 (https://tools.ietf.org/html/rfc2606) для частных тестовых установок, например, alt.test.

Имя домена для разворачиваемого DC должно состоять минимум из двух компонентов, разделённых точкой.

Примечание. Необходимо избегать суффиксов .local. При указании домена, имеющего суффикс .local, потребуется на сервере и подключаемых компьютерах под управлением Linux отключить службу `avahi-daemon`.

Примечание. Имя как контроллера домена, так и всех ПК членов домена, не должно превышать 15 символов (ограничение связано с параметром `sAMAccountName` в Active Directory).

2.3 Синхронизация времени

Для аутентификации Kerberos необходима точная синхронизация времени между рабочими станциями членов домена и контроллером домена. Максимально допустимое отклонение времени по умолчанию составляет 5 минут. Если член домена или DC имеет большую разницу во времени, доступ будет запрещен. В результате пользователь не сможет получить доступ к общим папкам или выполнить запрос к каталогу.

На всех DC домена должен быть настроен сервер времени NTP.

Samba поддерживает как ntpd, так и chrony в качестве сервера NTP. Демон синхронизирует время с внешними источниками и позволяет клиентам получать время с сервера, на котором запущен демон.

Из Рис. 1 видно, что только DC с ролью «Эмулятор PDC» получает свое время от внешних серверов времени, все остальные DC получают время от эмулятора PDC, все рабочие станции получают время от любого DC. Клиенты Windows в конечном итоге получают свое время от DC эмулятора PDC через DC, и если DC эмулятора PDC отключается, другие DC будут продолжать его искать, и время может смещаться. В качестве обходного пути следует установить одинаковые внешние серверы времени на всех DC. В этом случае, если эмулятор PDC отключится и его нельзя будет легко перезапустить, нужно передать или захватить роль эмулятора PDC другому DC.

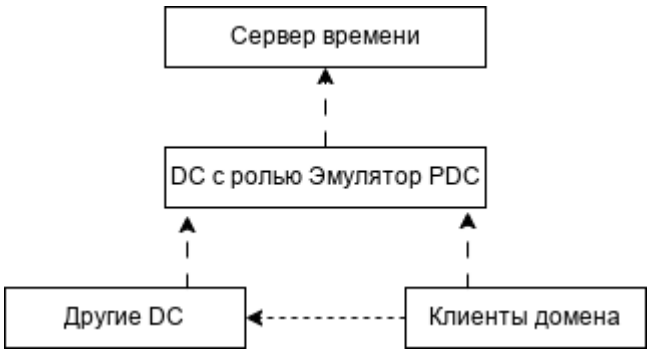

Рис. 1. Схема синхронизации времени

1.5 Требования к портам

Для корректрной работы службы Samba на контроллере домена должны быть открыты порты, указанные в табл. 2.

Таблица 2. Порты, используемые Samba AD DC

Служба	Порт	Протокол	Примечание
DNS	53	TCP и UDP	Для DNS от контроллера домена к контроллеру домена и от клиента к контроллеру домена. Может быть предоставлен внутренним DNS-сервером Samba или DNS-сервером Bind9
Kerberos	88	TCP и UDP	Для аутентификации Kerberos
NTP	123	UDP (опционально)	Если на контроллере домена настроен и работает NTP
End Point Mapper (DCE/RPC Locator Service)	135	TCP	Для операций клиента с контроллером домена и контроллеров домена с операциями контроллера домена
NetBIOS Name Service	137	UDP	
NetBIOS Datagram	138	UDP	Для службы репликации файлов между контроллерами домена
NetBIOS Session	139	TCP	Для службы репликации файлов между контроллерами домена
LDAP	389	TCP и UDP	Для обработки регулярных запросов от клиентских компьютеров к контроллерам домена
SMB over TCP	445	TCP	Для службы репликации файлов
Kerberos	464	TCP и UDP	Используется kadmin для установки и смены пароля Kerberos
LDAPS	636	TCP	Если в файле smb.conf установлен параметр `tls enabled = yes` (по умолчанию)
Global Catalog	3268	TCP	Для глобального каталога от клиента к контроллеру домена
Global Catalog SSL	3269	TCP	Если в файле smb.conf установлен параметр `tls enabled = yes` (по умолчанию)
Динамические порты RPC	49152-65535	TCP	Диапазон соответствует диапазону портов, используемому в Windows Server 2008 и более поздних версиях. Чтобы вручную установить диапазон портов в Samba, необходимо задать требуемый диапазон в параметре `rpc server port` в файле smb.conf.

3 УСТАНОВКА ОС «АЛЬТ СЕРВЕР»

Данный раздел содержит инструкции по установке ОС «Альт Сервер».

2.1 Создание загрузочного flash-диска

Для создания загрузочного flash-диска понадобится файл ISO-образа установочного диска с дистрибутивом. ISO-образы установочных дисков являются гибридными (Hybrid ISO/IMG), что позволяет записать их на flash-накопитель.

Для этого можно воспользоваться командой:

```
dd oflag=direct if=<файл-образа.iso> of=</dev/sdX> bs=1M
status=progress; sync
```

где:

файл-образа.iso – ISO-образ установочного диска с дистрибутивом;

/dev/sdX – устройство, соответствующее flash-диску.

Для удобства показа прогресса записи можно установить пакет pv и использовать команду:

```
pv <файл-образа.iso> | dd oflag=direct of=</dev/sdX> bs=1M; sync
```

где:

файл-образа.iso – ISO-образ установочного диска с дистрибутивом;

/dev/sdX – устройство, соответствующее flash-диску.

Просмотреть список доступных устройств можно командой lsblk или blkid.

Например, так можно определить имя USB-устройства:

```
$ lsblk | grep disk
sda      8:0    0 931,5G  0 disk
sdb      8:16   0 931,5G  0 disk
sdc      8:32   1   7,4G  0 disk
```

USB-диск имеет имя устройства sdc.

Затем записать:

```
# dd oflag=direct if=/iso/alt-server-x86_64.iso of=/dev/sdc bs=1M
status=progress; sync
```

или, например, так:

```
# pv /iso/alt-server-x86_64.iso | dd oflag=direct of=/dev/sdc
bs=1M;sync
dd: warning: partial read (524288 bytes); suggest iflag=fullblock
4GiB 0:10:28 [4,61MiB/s] [=================================>  ] 72%
ETA 0:04:07
```

В операционной системе OS X для создания загрузочного flash-диска можно использовать команду:

```
sudo dd if=alt-server-x86_64.iso of=/dev/rdiskX bs=10M
sync
```

где alt-server-x86_64.iso – образ диска ISO, а /dev/rdiskX – usb-устройство.

Просмотреть список доступных устройств можно командой:

```
diskutil list
```

В операционной системе Windows для создания загрузочного flash-диска можно использовать специальные программы: ALT Media Writer, Win32 Disk Imager и другие.

ALT Media Writer – это инструмент, который помогает записывать образы ALT на портативные накопители, такие как flash-диски. Он может автоматически загружать образы из интернета и записывать их. Для записи образа на flash-диск необходимо:

- скачать и установить ALT Media Writer;
- вставить flash-диск в USB-разъем;
- запустить ALT Media Writer;
- выбрать дистрибутив и нажать кнопку «Создать Live USB…»;
- начнётся загрузка образа из интернета;
- выбрать устройство (flash-диск);
- после окончания загрузки нажать кнопку «Записать на диск» (если был отмечен пункт «Записать образ после загрузки», запись образа начнётся автоматически).

Созданный описанными выше способами, flash-диск является одновременно и загрузочным, и установочным. В результате, установка дистрибутива может быть произведена исключительно с использованием flash-диска.

Для проверки целостности записанного образа необходимо выполнить следующие шаги:

1) определить длину образа в байтах:

```
$ du -b alt-server-x86_64.iso | cut -f1
5491038208
```

2) посчитать контрольную сумму образа (или просмотреть контрольную сумму образа из файла MD5SUM на сервере FTP):

```
$ md5sum alt-server-x86_64.iso
81376b3de7e179bd460311b12c08bab2 alt-server-x86_64.iso
```

3) подсчитать контрольную сумму записанного образа на DVD или USB Flash (выполняется под правами пользователя root):

```
# head -c 5491038208 /dev/sdd | md5sum
```

```
81376b3de7e179bd460311b12c08bab2
```

где размер после -c – вывод в п.1, а /dev/sdd – устройство DVD или USB Flash, на которое производилась запись.

2.2 Установка дистрибутива

2.2.1 Начало установки. Загрузка системы

Примечание. В данной инструкции рассмотрена установка системы в режиме UEFI. Особенности установки в режиме legacy отображены в примечаниях.

Для начала установки ОС «Альт Сервер» необходимо загрузиться с носителя, на котором записан дистрибутив. Для этого может потребоваться включить в BIOS опцию загрузки с оптического привода или с USB-устройства.

Примечание. Способ входа в меню BIOS и расположение конкретных настроек может сильно отличаться в зависимости от используемого оборудования. Чаще всего для входа в BIOS необходимо нажать клавишу <Delete>, как только компьютер начнёт загружаться. За полной инструкцией по настройке обратитесь к документации к вашему оборудованию.

Загрузка с установочного диска или специально подготовленного USB-flash-накопителя начинается с меню (Рис. 2). Чтобы начать процесс установки, нужно клавишами перемещения курсора <↑>, <↓> выбрать пункт меню «Install ALT Server» и нажать <Enter>.

Примечание. Начальный загрузчик в режиме Legacy показан на Рис. 3.

Рис. 2. Установка. Загрузка с установочного диска

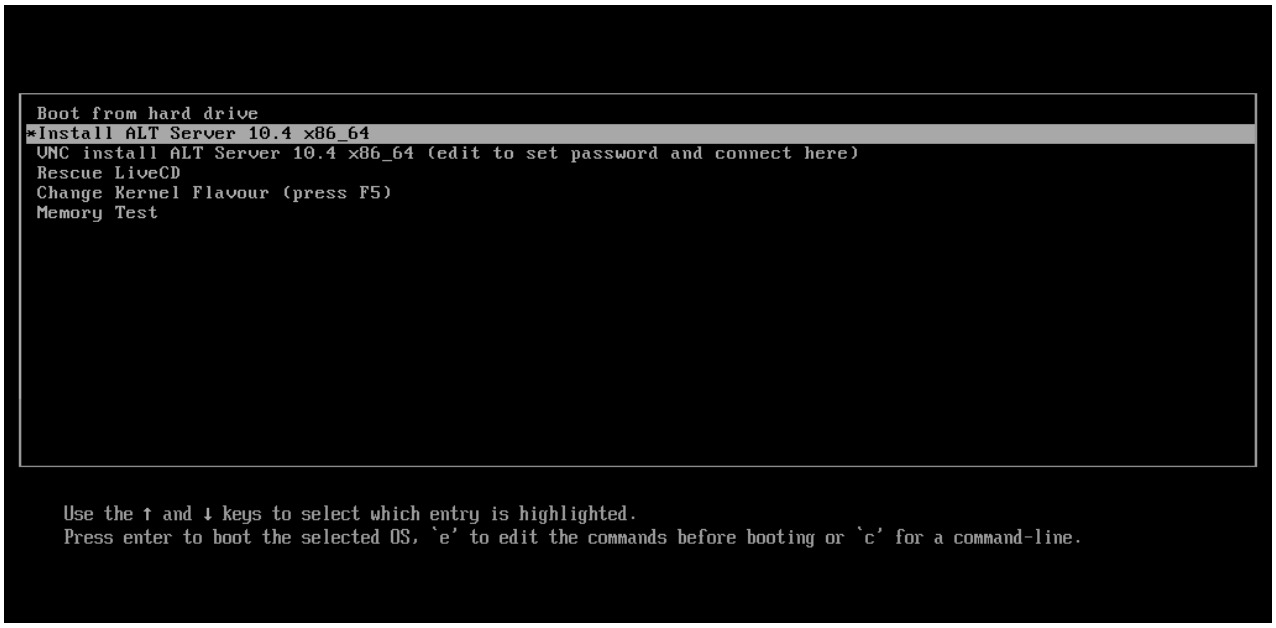

Рис. 3. Установка. Начальный загрузчик в режиме Legacy

2.2.2 Установка системы

Во время установки системы выполняются следующие шаги:

- язык;
- лицензионное соглашение;
- дата и время;
- подготовка диска;
- перемонтирование;
- установка системы;
- сохранение настроек;
- установка загрузчика;
- настройка сети;
- администратор системы;
- системный пользователь;
- установка пароля на LUKS-разделы;
- завершение установки.

Установка начинается с выбора основного языка – языка интерфейса программы установки и устанавливаемой системы (Рис. 4).

После окна выбора языковых параметров ОС «Альт Сервер» программа установки переходит к окну «Лицензионное соглашение» (Рис. 5).

Для подтверждения согласия, необходимо отметить пункт «Да, я согласен с условиями» и нажать кнопку «Далее».

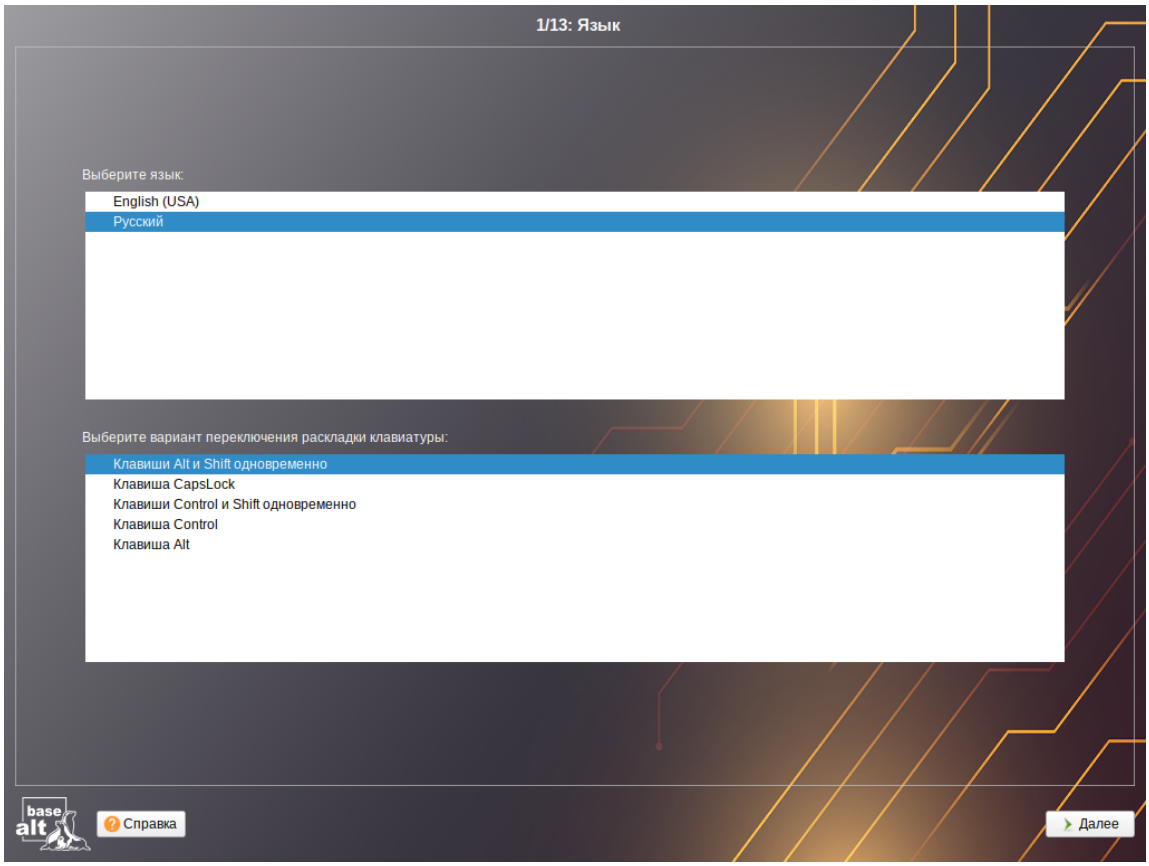

Рис. 4. Установка. Выбор языка

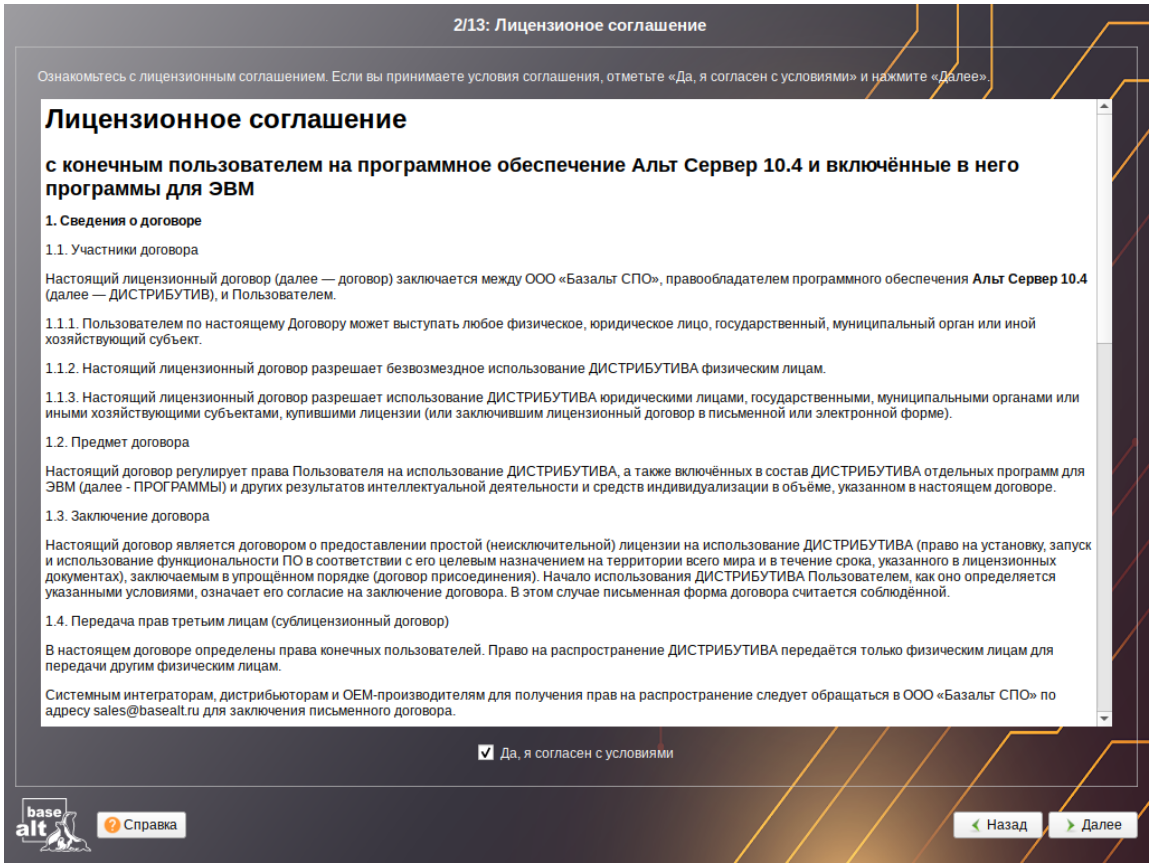

Рис. 5. Установка. Лицензионное соглашение

На этапе «Дата и время» выполняется выбор региона и города, по которым будет определен часовой пояс и установлены системные часы (Рис. 6). Для корректной установки даты и времени достаточно правильно указать часовой пояс и выставить желаемые значения для даты и времени. Для ручной установки текущих даты и времени нужно нажать кнопку «Изменить…».

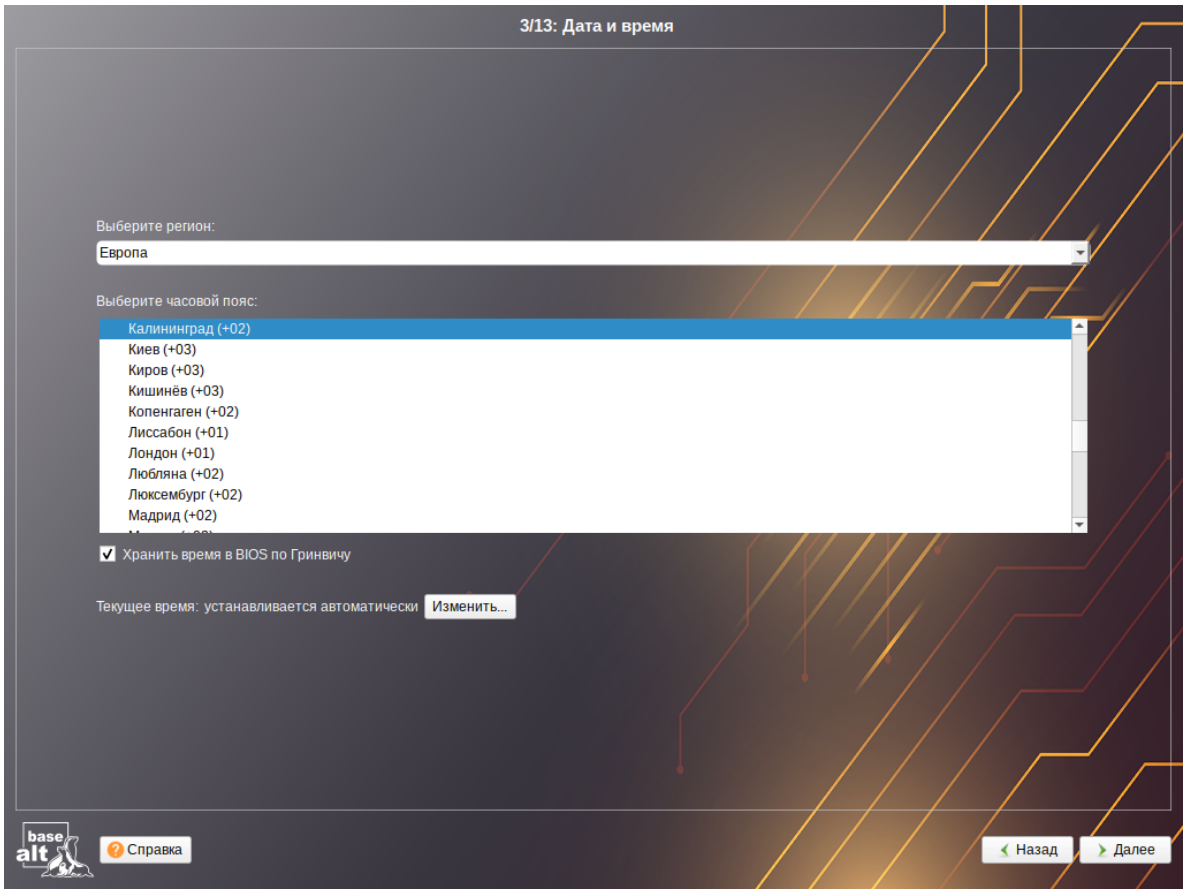

Рис. 6. Установка. Выбор часового пояса

На этапе «Подготовка диска» (Рис. 7) подготавливается площадка для установки ОС «Альт Сервер», в первую очередь – выделяется свободное место на диске.

В списке разделов перечислены уже существующие на жестких дисках разделы (в том числе здесь могут оказаться съемные USB-носители, подключенные к компьютеру в момент установки).

В списке «Выберите профиль» перечислены доступные профили разбиения диска. Профиль – это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

- «Установка сервера»;
- «Вручную».

Примечание. При установке системы в режиме UEFI рекомендуется выбрать автоматическое разбиение диска для создания необходимых разделов для загрузки с EFI.

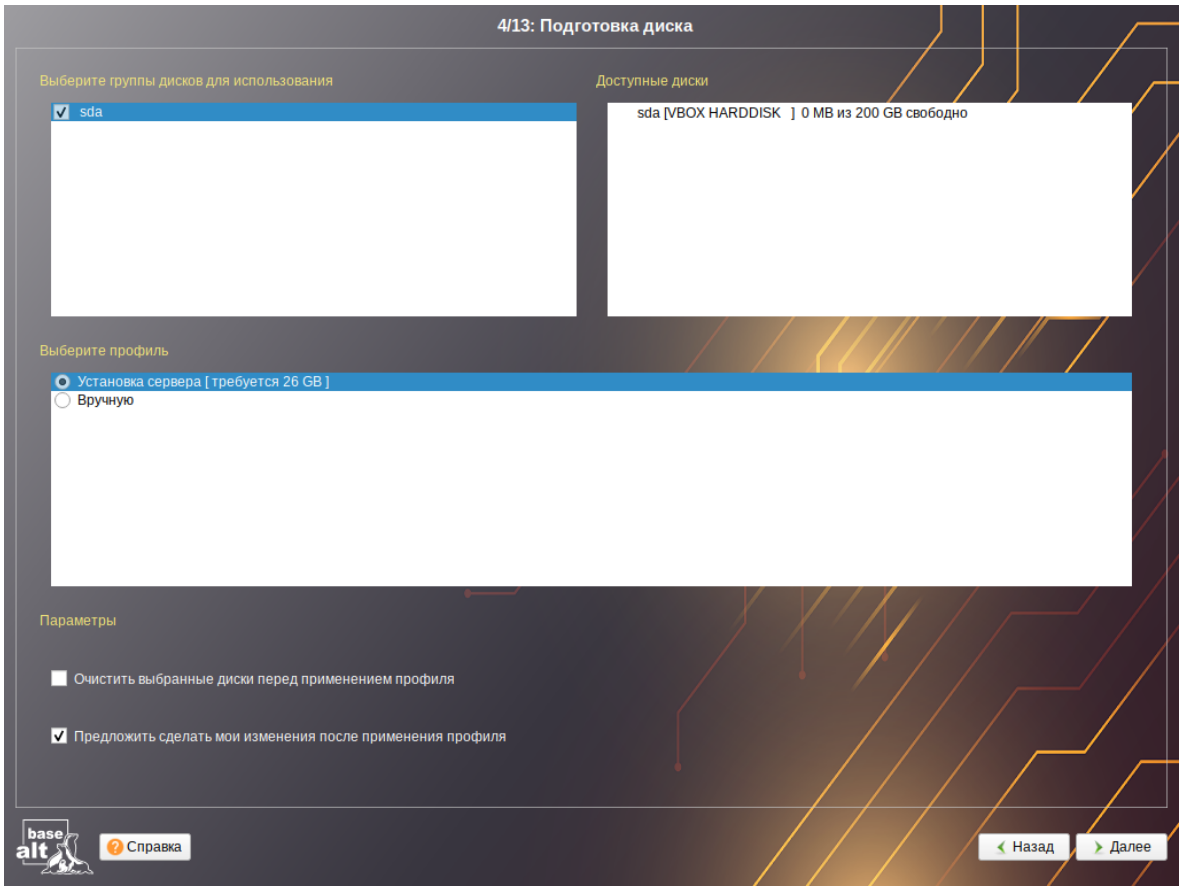

Рис. 7. Установка. Выбор профиля разбиения диска(ов)

Примечание. При отмеченном пункте «Очистить выбранные диски перед применением профиля» будут удалены все данные с выбранных дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

По завершении этапа подготовки диска начинается шаг перемонтирования. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения (Рис. 8).

На этапе «Установка системы» происходит распаковка ядра и установка набора программ, необходимых для работы дистрибутива ОС «Альт Сервер».

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав ОС «Альт Сервер» и установлены вместе с ней на диск (Рис. 9).

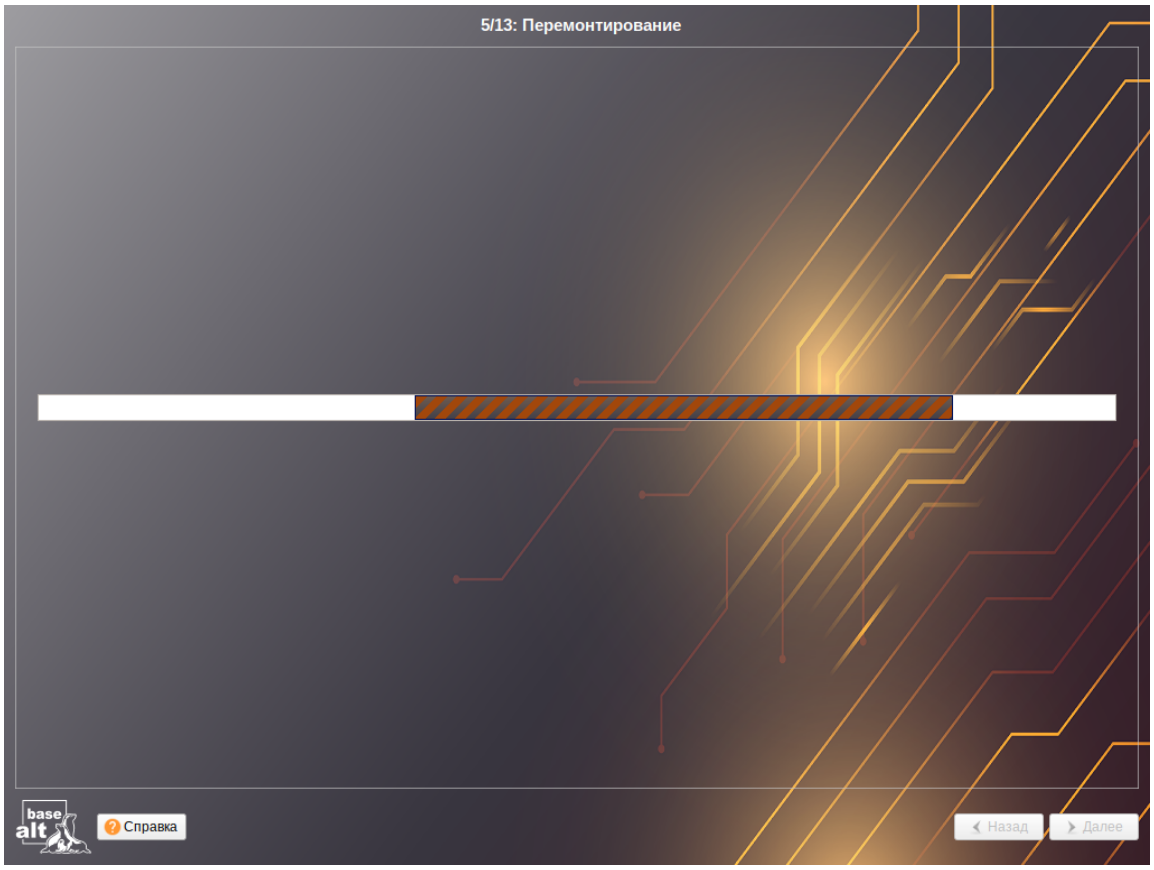

Рис. 8. Установка. Перемонтирование

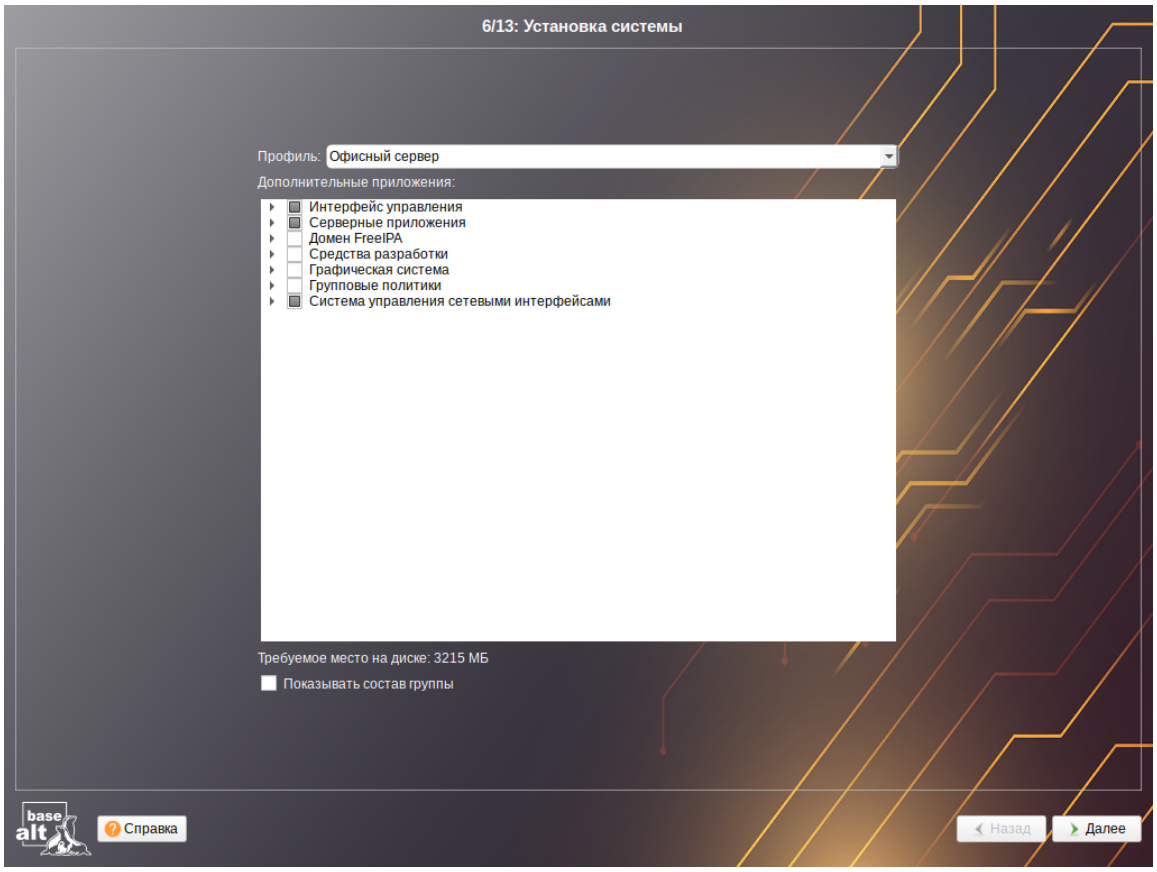

Рис. 9. Установка. Выбор групп пакетов

Для установки пакетов, необходимых для разворачивания контроллера домена, следует выбрать профиль «Контроллер Альт Домена (Сервер Samba DC)», в группе пакетов «Групповые политики» отметить пункт «Шаблоны групповых политик» и нажать кнопку «Далее» (Рис. 10).

Примечание. Если административные инструменты планируется использовать на контроллере домена, то необходимо установить графическую среду MATE. Для этого следует установить отметку в поле «Графическая система». Для установки административных инструментов в группе пакетов «Групповые политики» отметить пункт «Инструменты администрирования».

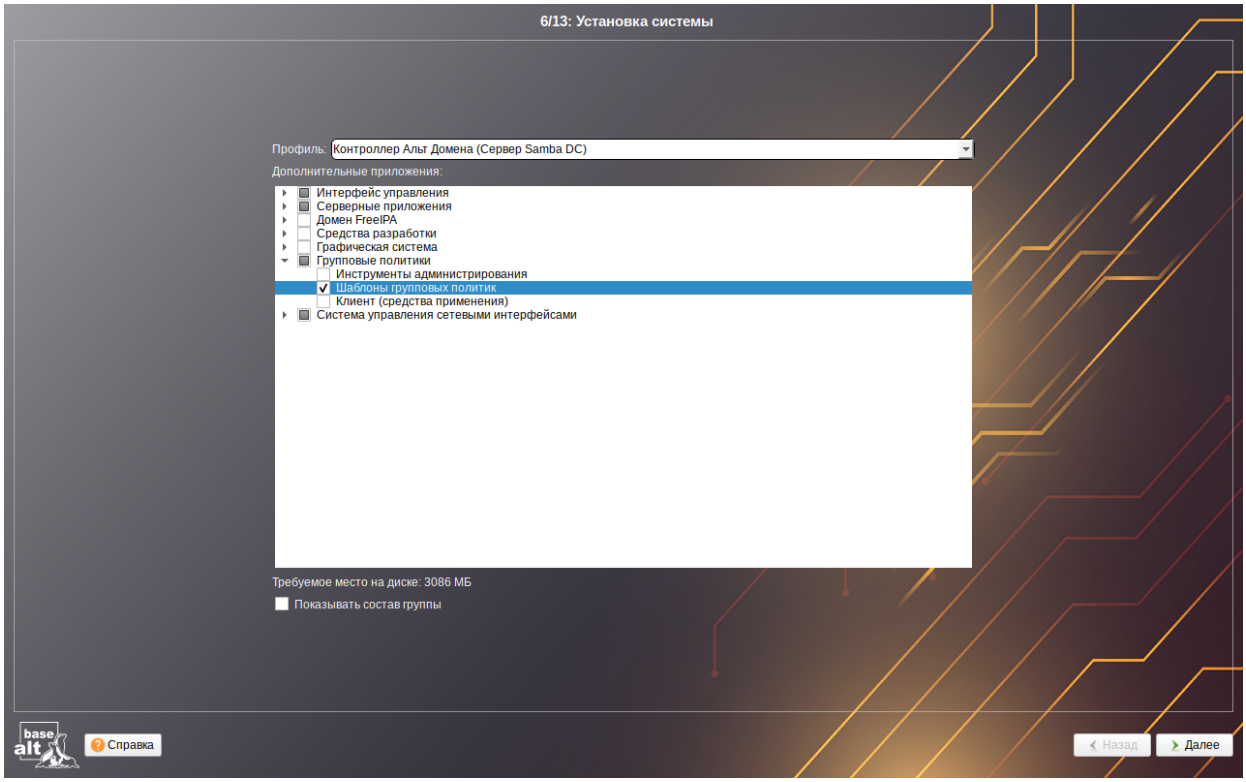

Рис. 10. Профиль «Контроллер Альт Домена (Сервер Samba DC)»

Установка пакетов (Рис. 11) происходит автоматически в два этапа:

- получение пакетов;
- установка пакетов.

После завершения установки базовой системы выполняется шаг сохранения настроек (Рис. 12). Он проходит автоматически и не требует вмешательства пользователя, на экране отображается индикатор выполнения. После сохранения настроек осуществляется автоматический переход к следующему шагу.

Рис. 11. Установка. Установка пакетов

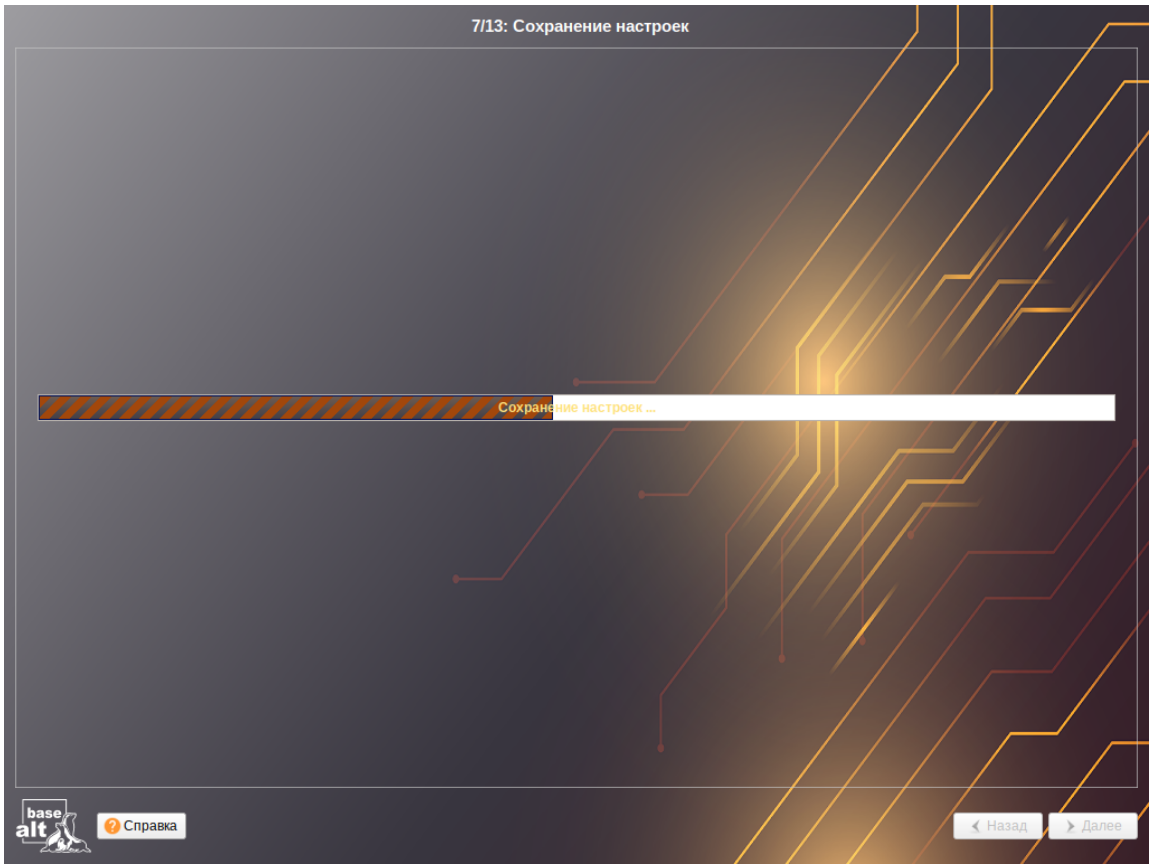

Рис. 12. Установка. Сохранение настроек

На этапе «Установка загрузчика» программа установки автоматически определяет, в каком разделе жёсткого диска следует располагать загрузчик для возможности корректного запуска ОС «Альт Сервер».

При установке системы в режиме UEFI следует выбрать в качестве устройства для установки специальный раздел «EFI» (Рис. 13).

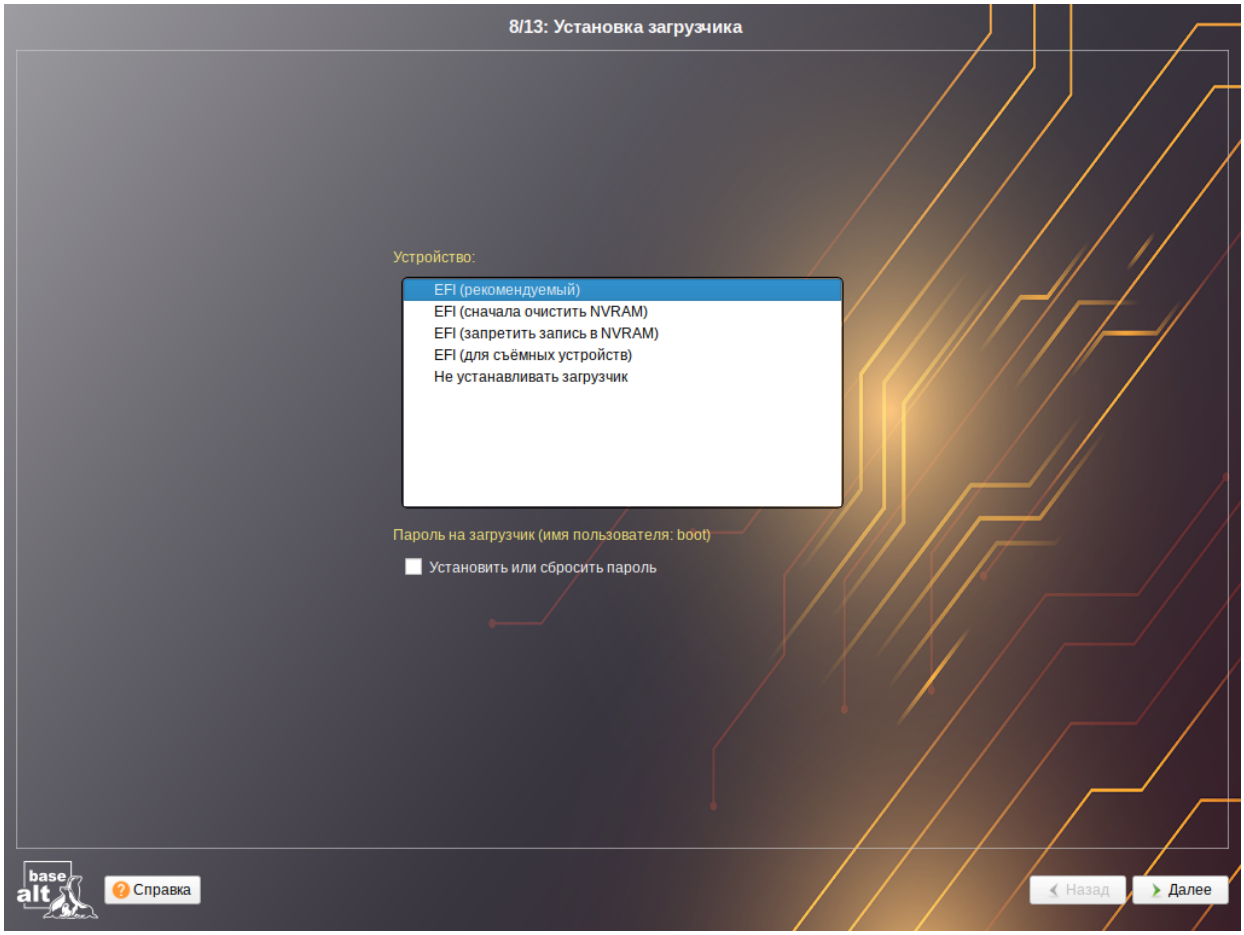

Рис. 13. Установка. Установка загрузчика

Для подтверждения выбора и продолжения работы программы установки необходимо нажать кнопку «Далее».

П р и м е ч а н и е . Установка загрузчика при установке в режиме Legacy показана на Рис. 14.

На этапе «Настройка сети» необходимо задать имя компьютера, IP-адрес, шлюз по умолчанию и DNS-серверы (Рис. 15).

П р и м е ч а н и е . Имя домена, для разворачиваемого контроллера домена, должно состоять минимум из двух компонентов, разделённых точкой.

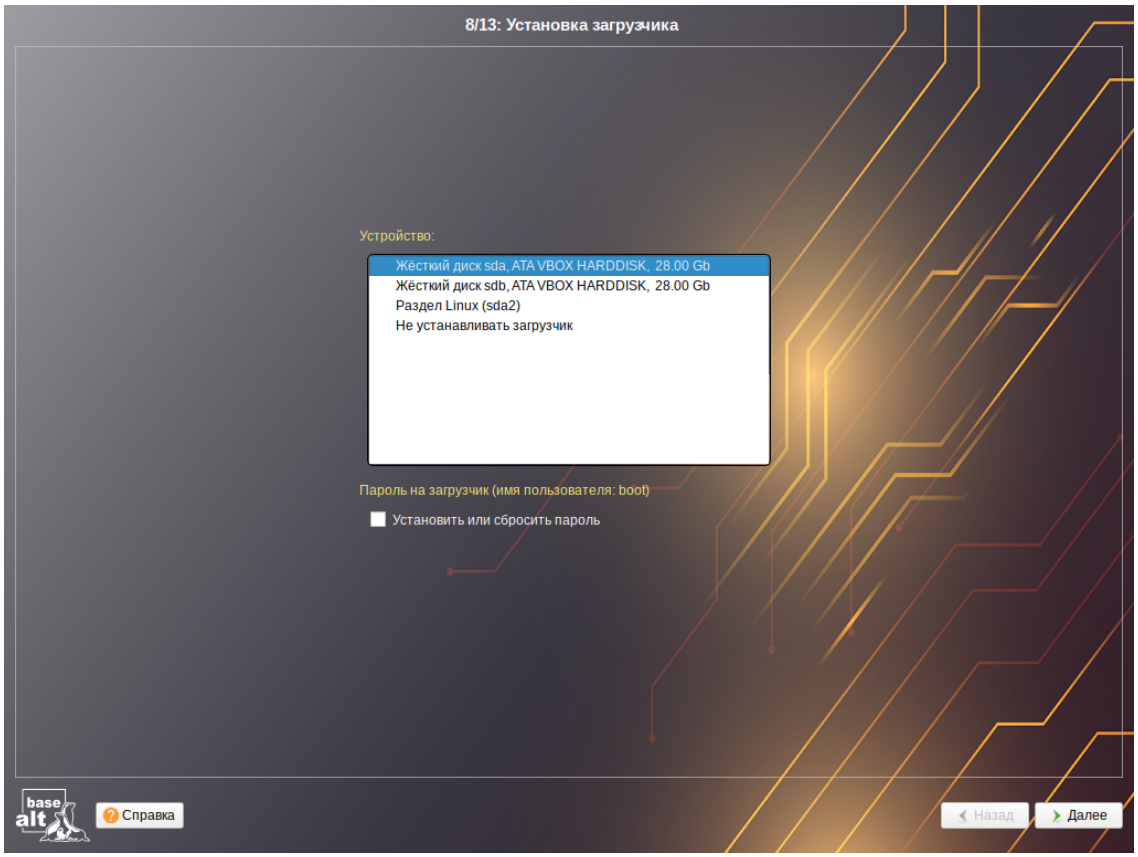

Рис. 14. Установка. Установка загрузчика в режиме Legacy

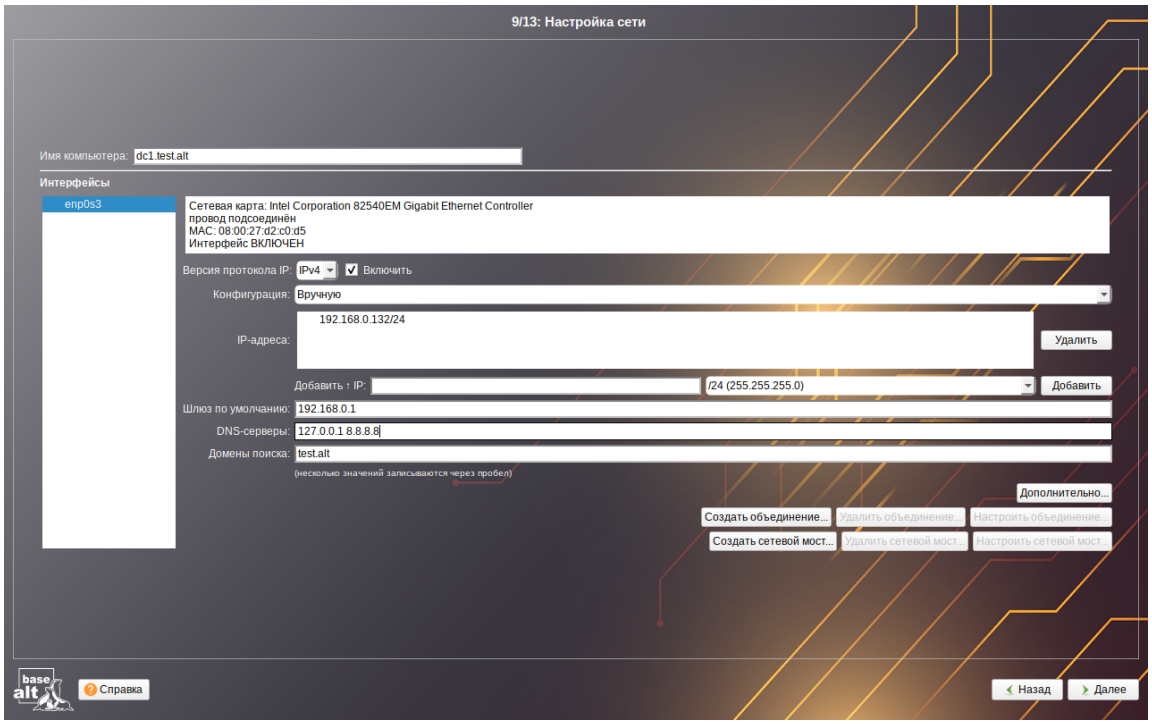

Рис. 15. Установка. Настройка сети

На вторичном сервере обязательно нужно указать первичный сервер в поле DNS-серверы (Рис. 16).

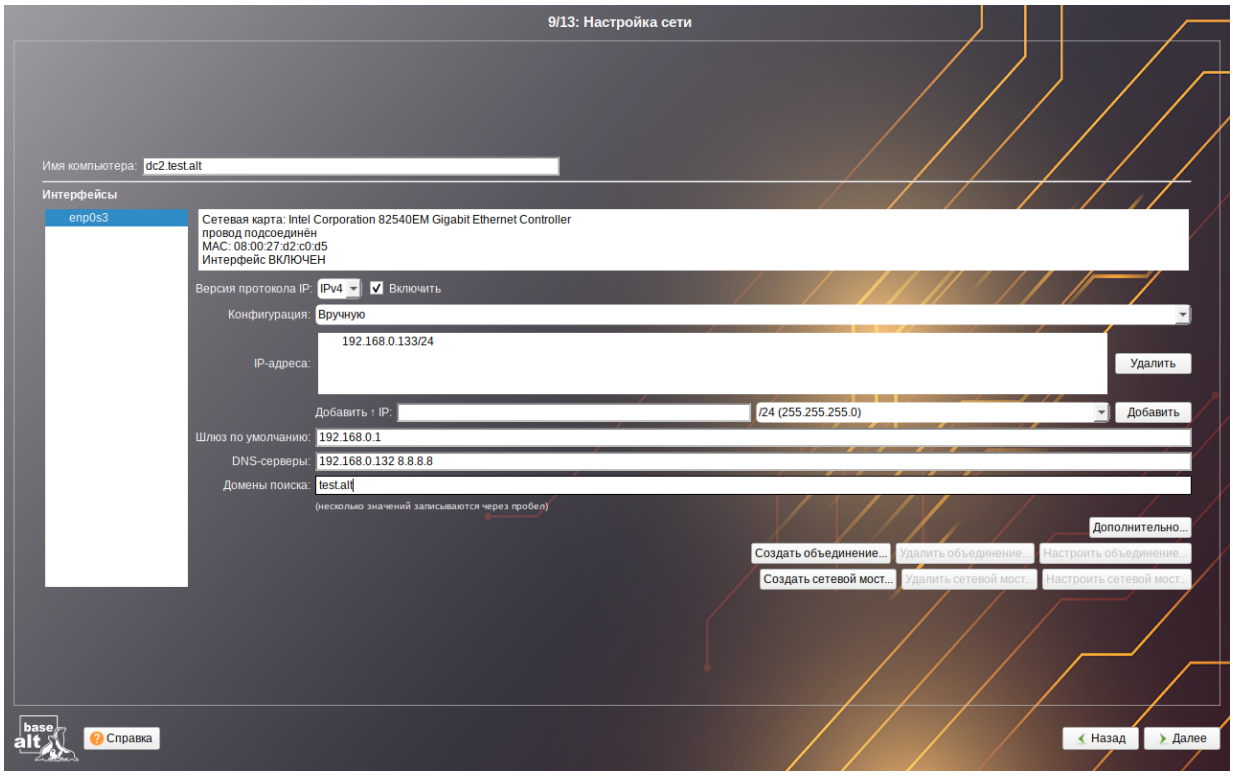

Рис. 16. Установка. Настройка сети на вторичном сервере

В окне (Рис. 17), открываемом при нажатии кнопки «Дополнительно», необходимо выбрать сетевую подсистему Etcnet.

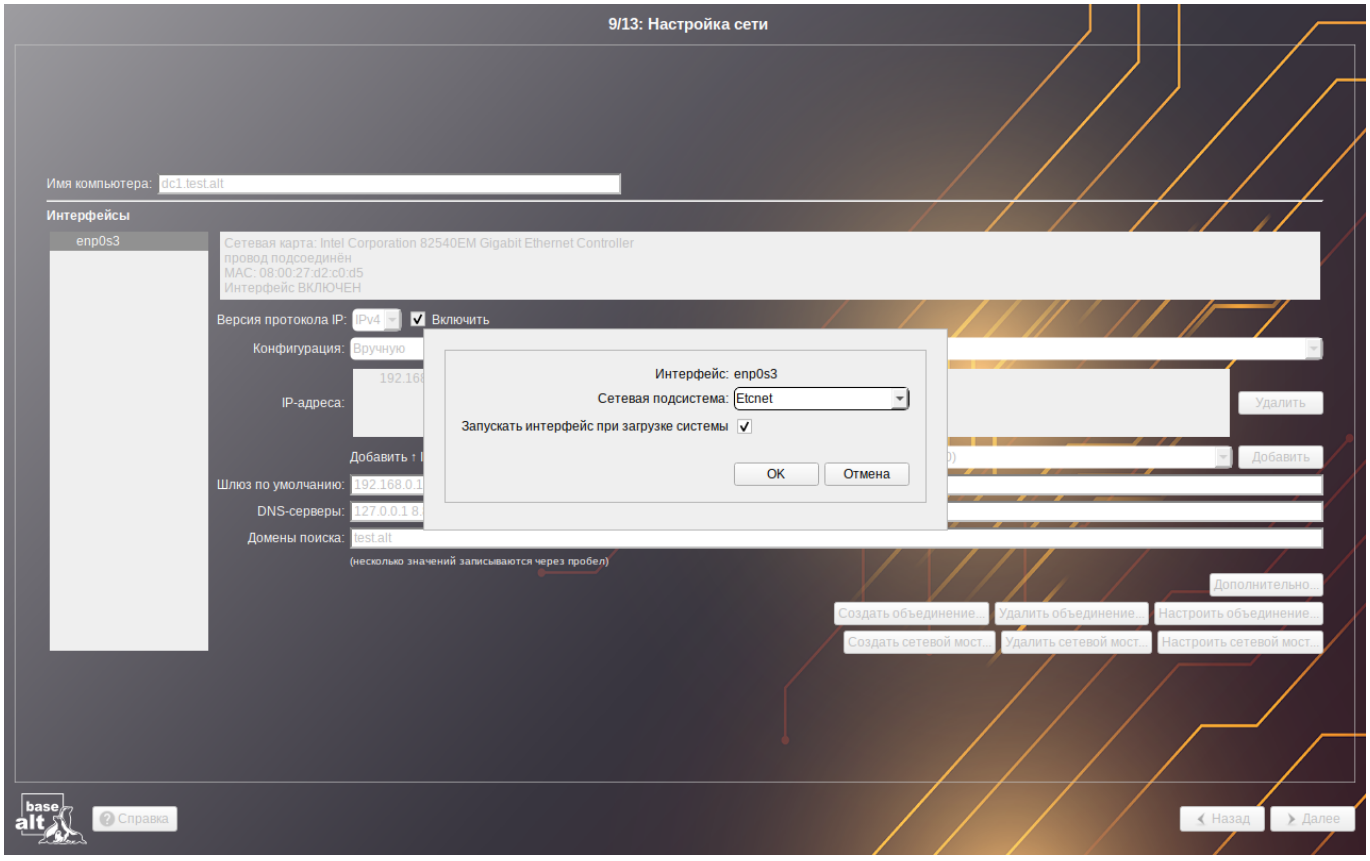

Рис. 17. Установка. Настройка сетевой подсистемы

П р и м е ч а н и е . По умолчанию при выборе профиля «Контроллер Альт Домена (Сервер Samba DC)» будет выбрана сетевая подсистема systemd-networkd. В этом случае при разворачивании домена потребуется дополнительно настроить или отключить systemd-resolved.

Для сохранения настроек сети и продолжения работы программы установки необходимо нажать кнопку «Далее».

На этапе «Администратор системы» программа установки создает учетную запись администратора (Рис. 18). В открывшемся окне необходимо ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды. Подтверждение введенного (или сгенерированного) пароля учетной записи администратора (root) и продолжение работы программы установки выполняется нажатием кнопки «Далее».

На этапе «Системный пользователь» программа установки создает учетную запись системного пользователя (пользователя) ОС «Альт Сервер» (Рис. 19).

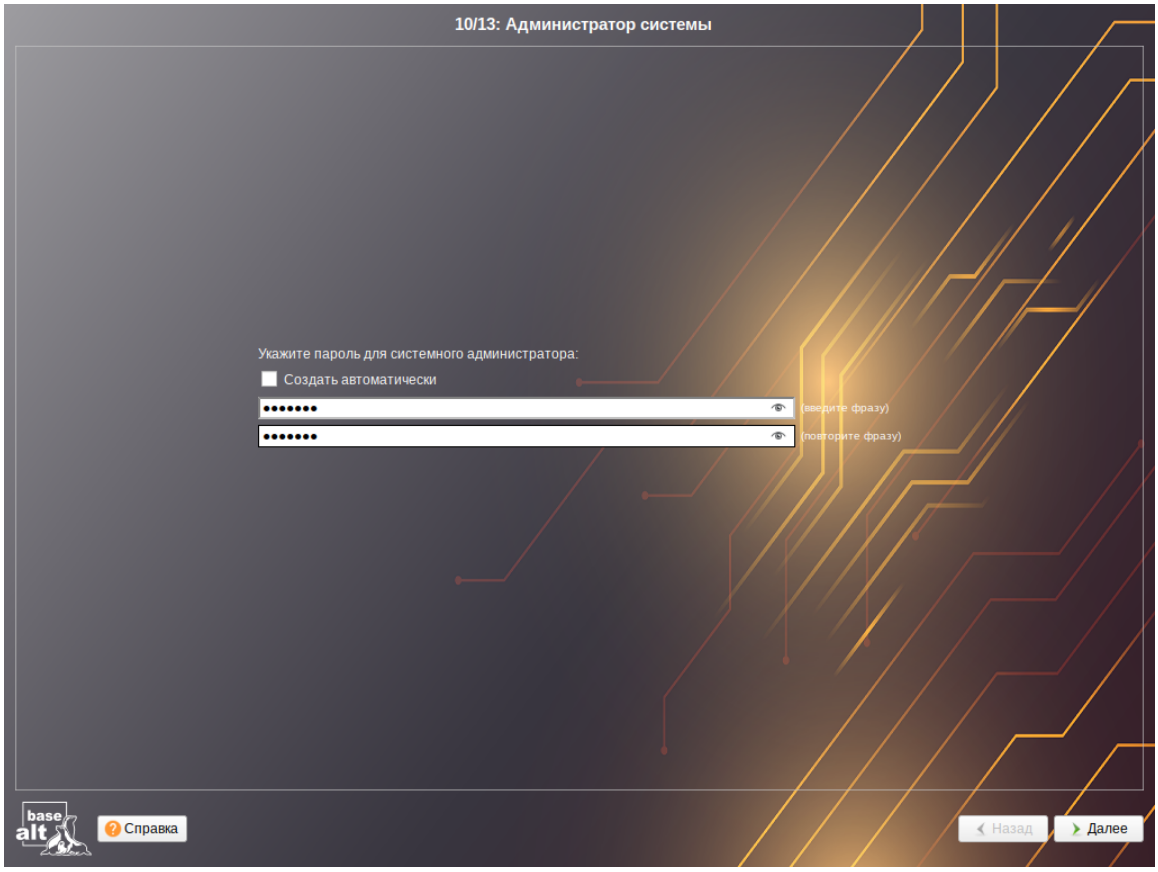

Рис. 18. Установка. Задание пароля администратора

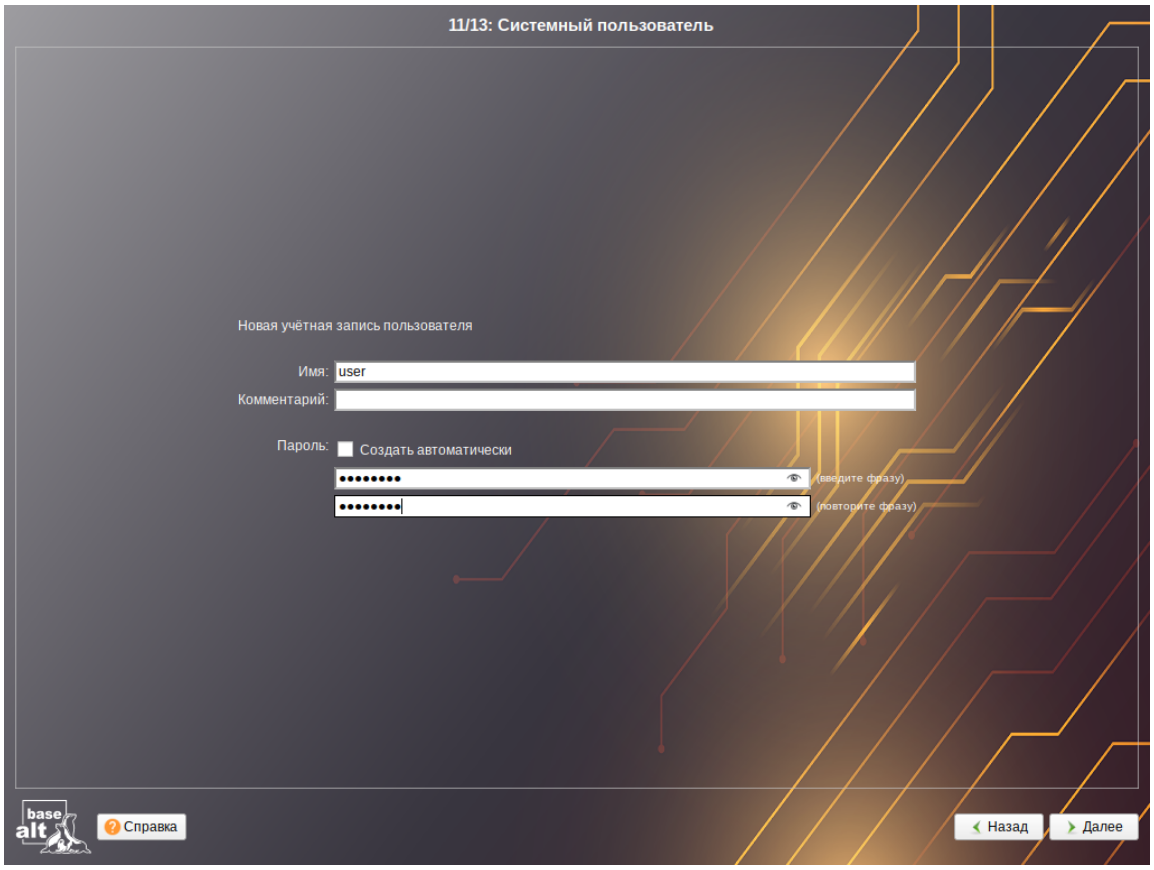

Рис. 19. Установка. Создание пользователя

В этом окне необходимо заполнить следующие поля:

- «Имя» – имя учётной записи пользователя ОС «Альт Сервер» (слово, состоящее только из строчных латинских букв, цифр и символа подчеркивания «_», причем цифра и символ «_» не могут стоять в начале слова);
- «Пароль» – пароль учётной записи пользователя (чтобы исключить опечатки при вводе пароля, пароль пользователя вводится дважды).

Подтверждение введенного (или сгенерированного) пароля учётной записи системного пользователя и продолжение работы программы установки выполняется нажатием кнопки «Далее».

Если на этапе подготовки диска были созданы кодируемые разделы (LUKS-разделы), на этапе «Установка пароля на LUKS-разделы» необходимо ввести пароль для обращения к этому разделу (Рис. 20).

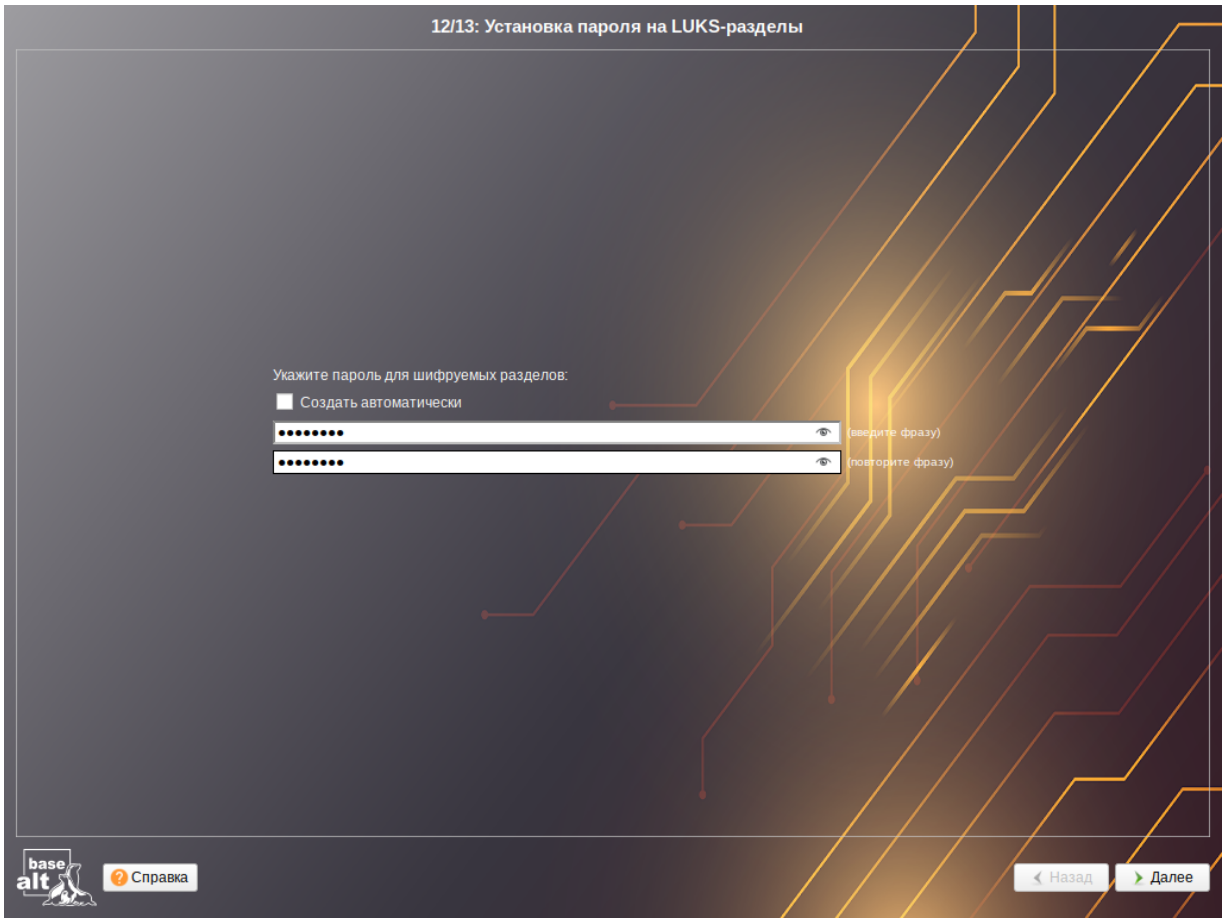

Рис. 20. Установка. Установка пароля на кодированные разделы

П р и м е ч а н и е . Если кодируемые разделы, не создавались, этот шаг пропускается автоматически.

На экране последнего этапа установки отображается информация о завершении установки (Рис. 21).

После нажатия кнопки «Завершить» автоматически начнется перезагрузка системы.

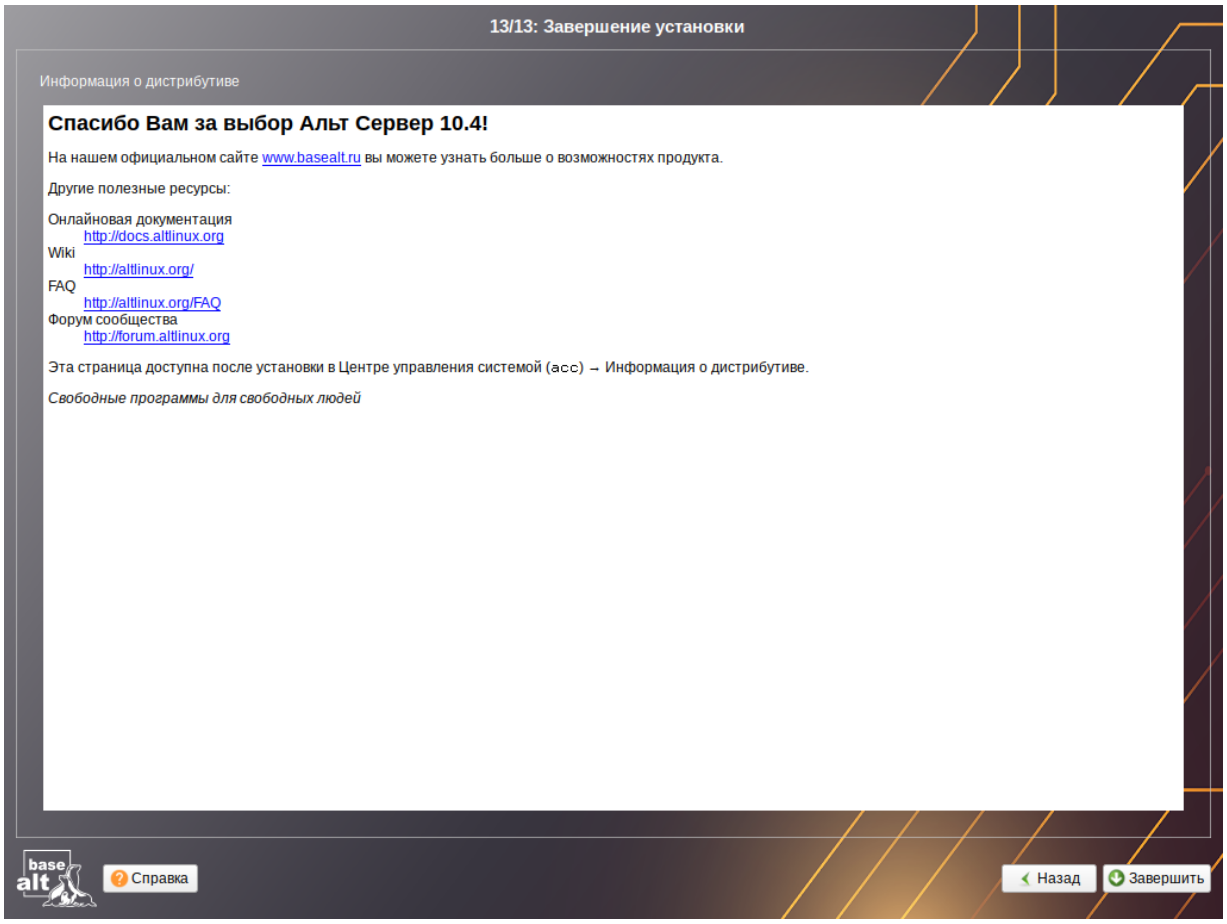

Рис. 21. Установка. Завершение установки

3.1 Обновление системы до актуального состояния

После установки системы, её следует обновить до актуального состояния.

Для обновления системы необходимо выполнить команды (с правами администратора):

```
# apt-get update
# apt-get dist-upgrade
# update-kernel
# apt-get clean
# reboot
```

Примечание. Получить права администратора можно, зарегистрировавшись в системе под именем root или выполнив команду:

```
$ su -
```

4 РАЗВОРАЧИВАНИЕ ДОМЕНА

4.1 Создание первого контроллера домена

Все действия выполняются на узле dc1.test.alt (192.168.0.132).

Для управления службой DNS Samba поддерживает работу с двумя DNS-бэкендами:

- внутренний DNS-сервер (SAMBA_INTERNAL);
- внешний DNS-сервер BIND 9 (BIND9_DLZ).

В данной инструкции рассмотрен внутренний DNS-сервер, разворачивание домена с внешним DNS-сервером рассмотрено в руководстве администратора.

4.1.1 Установка пакетов

Samba поддерживает две реализации Kerberos: Heimdal и MIT.

Установить пакет `task-samba-dc` для Samba DC на базе Heimdal Kerberos (этот шаг можно пропустить, если при установке системы на этапе «Установка системы» был выбран профиль «Контроллер Альт Домена (Сервер Samba DC)»):

```
# apt-get install task-samba-dc
```

или `task-samba-dc-mitkrb5` для Samba DC на базе MIT Kerberos:

```
# apt-get install task-samba-dc-mitkrb5
```

Примечание. Samba на базе Heimdal Kerberos использует KDC несовместимый с MIT Kerberos, поэтому на контроллере домена на базе Heimdal Kerberos из пакета samba-dc, для совместимости с клиентской библиотекой libkrb5, в файле krb5.conf (в блоке – `libdefaults`) необходимо отключить использование ядерного кеша ключей – `KEYRING:persistent:%{uid}`:

```
# control krb5-conf-ccache default
```

4.1.2 Остановка конфликтующих служб

Так как Samba в режиме контроллера домена (Domain Controller, DC) использует свой сервер LDAP, свой центр распределения ключей Kerberos и свой сервер DNS (если не включен плагин BIND9_DLZ), перед установкой домена необходимо остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service; systemctl stop $service; done
```

Выключить автозагрузку служб и отключить службы можно в ЦУС (см. Центр управления системой) в разделе «Система» → «Системные службы».

4.1.3 Настройка NTP-сервера

Настройка сервера времени chrony в качестве NTP-сервера:

- установить пакет chrony:

```
# apt-get install chrony
```

- включить доступ к серверу chrony:

```
# control chrony server
```

- установить синхронизацию с российским пулом NTP:

```
# sed -i -r 's/^(pool.*)/#\1\npool ru.pool.ntp.org iburst/' /etc/chrony.conf
```

или указать серверы NTP в директиве server или pool в файле конфигурации NTP `/etc/chrony.conf`:

```
pool pool.ntp.org iburst
```

- включить и запустить службу по умолчанию:

```
# systemctl enable --now chronyd
```

- убедиться в нормальной работе NTP-сервера:

```
# systemctl status chronyd.service
```

Примечание. Параметр iburst используется для ускорения начальной синхронизации.

4.1.4 Установка имени домена

Этот раздел можно пропустить, если имя компьютера было задано при установке системы на этапе «Настройка сети».

Имя домена, для разворачиваемого DC, должно состоять минимум из двух компонентов, разделённых точкой.

Примечание. Необходимо избегать суффиксов .local. При указании домена, имеющего суффикс .local, на сервере и подключаемых компьютерах под управлением Linux потребуется отключить службу `avahi-daemon`.

Для установки имени узла и домена следует выполнить команды:

```
# hostnamectl set-hostname <имя узла>
# domainname <имя домена>
```

Например:

```
# hostnamectl set-hostname dc1.test.alt
# domainname test.alt
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

4.1.5 Сетевые настройки

Для корректной работы сервера должны соблюдаться следующие условия:

- для сервера должно быть задано полное доменное имя (FQDN);
- IP-адрес сервера не должен изменяться;
- в настройках сетевого интерфейса должен быть указан IP-адрес 127.0.0.1 в качестве первичного DNS.

Настройку сети можно выполнить как в ЦУС: в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера и указать в поле «DNS-серверы» 127.0.0.1 (Рис. 22).

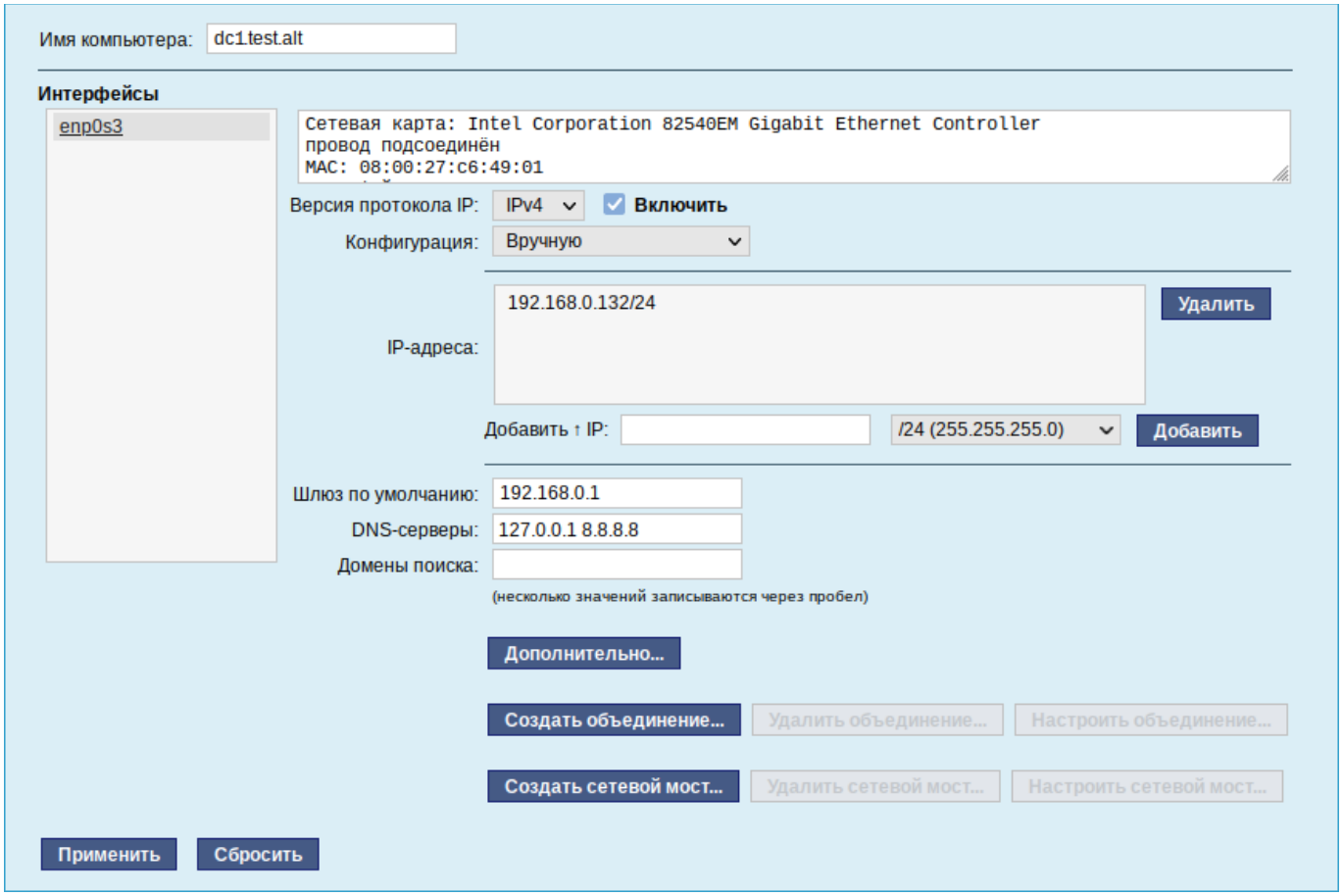

Рис. 22. Модуль «Ethernet-интерфейсы»

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

Примечание. Если используется сетевая подсистема systemd-networkd, то для того чтобы DNS-сервер Samba управлял зоной test.alt, нужно настроить systemd-resolved для использования Samba в качестве основного DNS-сервера. По умолчанию systemd-resolved прослушивает DNS-запросы на локальном сокете. Чтобы избежать конфликтов с Samba DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле `/etc/resolv.conf`:

```
nameserver 127.0.0.1
search test.alt
```

4.1.6 Настройка файла /etc/resolvconf.conf

Для корректного распознавания всех локальных DNS-запросов в файле `/etc/resolvconf.conf` должна присутствовать строка:

```
name_servers=127.0.0.1
```

Если этой строки в файле `/etc/resolvconf.conf` нет, то в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

4.1.7 Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba:

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Примечание. Перед созданием домена необходимо обязательно удалить /etc/samba/smb.conf:

```
# rm -f /etc/samba/smb.conf
```

4.1.8 Создание домена

4.1.8.1 Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание. Чтобы принять значение по умолчанию, необходимо нажать <Enter>.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
```

```
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
```

При запросе «DNS forwarder IP address» можно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена:

```
DNS forwarder IP address (write 'none' to disable forwarding)
[127.0.0.1]:  8.8.8.8
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
```

```
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3617232745-2316959539-2936900449
```

4.1.8.2 Создание домена в пакетном режиме

Команда `samba-tool domain provision` имеет множество опций, которые можно использовать для предоставления дополнительной информации при интерактивной установке сервера. Их также можно использовать в скриптах.

Для пакетной установки необходимо указать следующие параметры домена:

- `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- `--domain=DOMAIN` – имя домена (имя рабочей группы);
- `--adminpass=PASSWORD` – пароль основного администратора домена;

- `dns forwarder` – внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;
- `--server-role=ROLE` – тип серверной роли;
- `--dns-backend=NAMESERVER-BACKEND` – бэкенд DNS-сервера;
- `--use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt \
--domain=test --adminpass='Pa$$word' \
--dns-backend=SAMBA_INTERNAL --server-role=dc –use-rfc2307 \
--option="dns forwarder=8.8.8.8"
```

Если уровень не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt \
--domain=test --adminpass='Pa$$word' \
--dns-backend=SAMBA_INTERNAL --option="dns forwarder=8.8.8.8" \
--option="ad dc functional level = 2016" \
--server-role=dc --function-level=2016
```

Примечание. Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2.

Примечание. Полный список параметров команды `samba-tool domain provision` можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

4.1.8.3 Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС (см. Центр управления системой) следует в модуле «Домен» указать имя домена, отметить пункт «Active Directory», указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку «Применить» (Рис. 23).

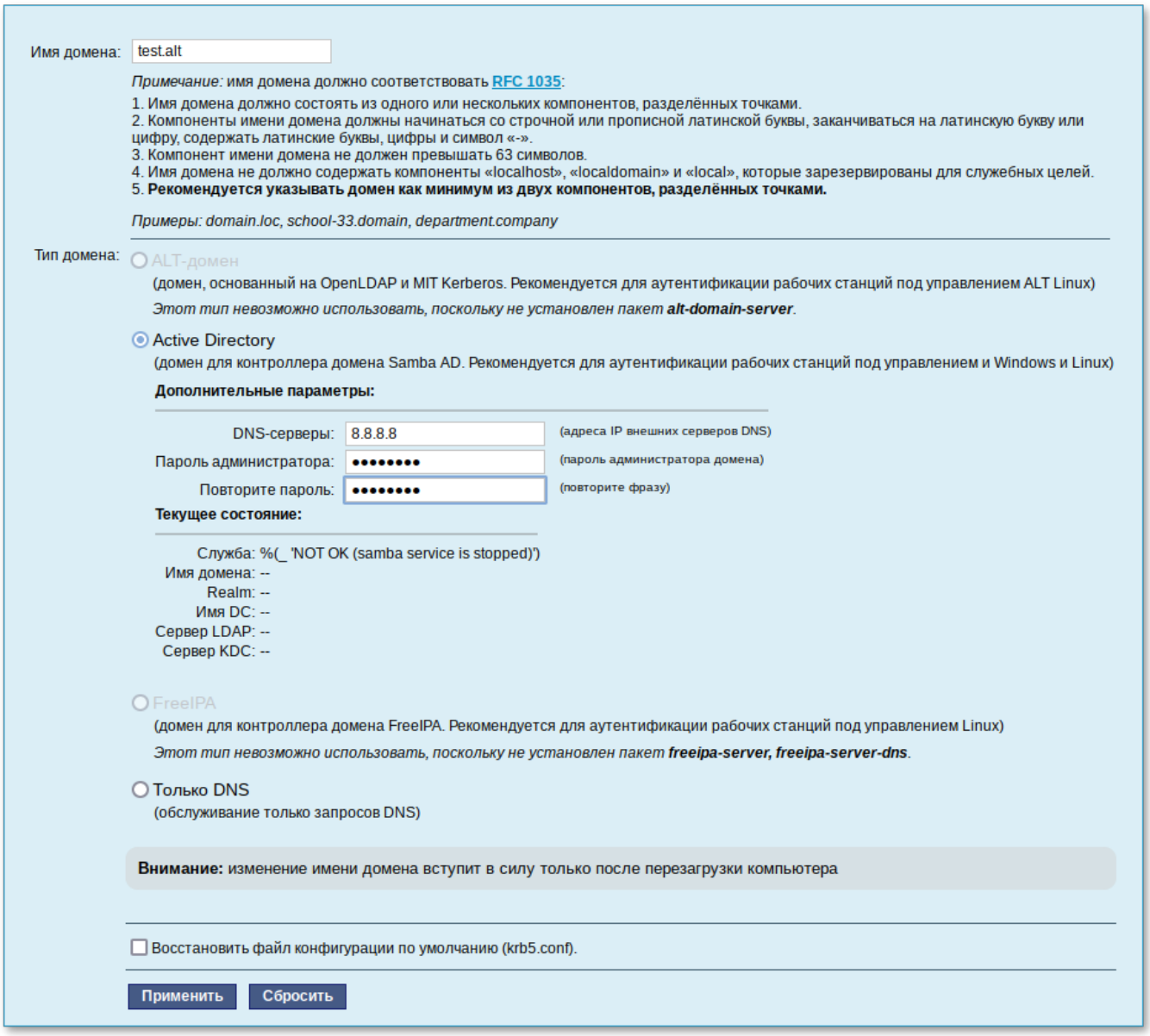

Рис. 23. Создание домена в ЦУС

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

После успешного создания домена, будет выведена информация о домене (Рис. 24).

Перегрузить сервер для применения изменений.

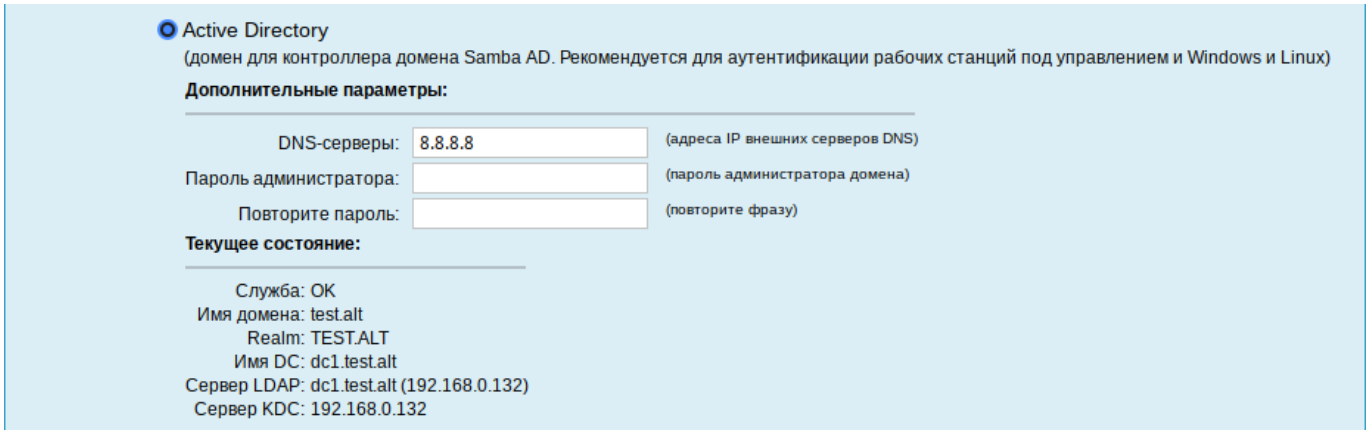

Рис. 24. Информация о домене

4.1.9 Запуск службы каталогов

Установить службу samba запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание. Если служба samba после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание. Пример файла /etc/samba/smb.conf после создания домена с SAMBA_INTERNAL:

```
 Global parameters
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

4.2 Настройка Kerberos

Далее необходимо настроить Kerberos, для этого следует внести изменения в файл /etc/krb5.conf.

В файле /etc/krb5.conf нужно раскомментировать строку `default_realm` и содержимое разделов `realms` и `domain_realm` и указать название домена (следует обратить внимание на регистр символов), в строке `dns_lookup_realm` должно быть установлено значение false:

```
includedir /etc/krb5.conf.d/

[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
TEST.ALT = {
default_domain = test.alt
}

[domain_realm]
dc = TEST.ALT
```

Примечание. В момент создания домена Samba конфигурирует шаблон файла krb5.conf для домена в каталоге /var/lib/samba/private/. Можно просто заменить этим файлом файл, находящийся в каталоге /etc/:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

4.3 Проверка работоспособности домена

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    IPC$            IPC       IPC Service (Samba 4.19.9)
SMB1 disabled -- no workgroup available
```

Создаваемые по умолчанию общие ресурсы netlogon и sysvol нужны для функционирования сервера AD и создаются в файле smb.conf в процессе развертывания/модернизации.

Проверка конфигурации DNS:

- проверка наличия nameserver 127.0.0.1 в /etc/resolv.conf:

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1

# host test.alt
test.alt has address 192.168.0.132
```

- проверка имён узлов:

- адрес _kerberos._udp.<адрес домена с точкой>:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

- адрес _ldap._tcp.<адрес домена с точкой>:

```
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
```

- адрес адрес узла.<адрес домена с точкой>:

```
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.132
```

Если имена не находятся, следует проверить выключение службы bind.

Проверка Kerberos (имя домена должно быть в верхнем регистре):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
Warning: Your password will expire in 41 days on Ср 03 июл 2024
11:18:36
```

Просмотр полученного билета:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
22.05.2024 11:28:23  22.05.2024 21:28:23  krbtgt/TEST.ALT@TEST.ALT
   renew until 29.05.2024 11:28:20
```

Создать пользователя:

```
# samba-tool user create ivanov --given-name='Иван Иванов' \
--mail-address='ivanov@test.alt'
# samba-tool user setexpiry ivanov --noexpiry
```

4.4 Установка административных шаблонов

Для задания конфигурации необходимо установить административные шаблоны (ADMX-файлы). Для этого:

1. Установить пакеты политик admx-basealt, admx-chromium, admx-firefox, admx-yandex-browser и утилиту admx-msi-setup:

```
# apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-
browser admx-msi-setup
```

2. Запустить утилиту admx-msi-setup, которая загрузит и установит ADMX-файлы от Microsoft:

```
# admx-msi-setup
```

3. После установки, политики будут находиться в каталоге /usr/share/PolicyDefinitions. Скопировать локальные ADMX-файлы в сетевой каталог sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/), выполнив команду:

```
# samba-tool gpo admxload -U Administrator
```

4.5 Присоединение к домену в роли контроллера домена

Для обеспечения отказоустойчивости и балансировки нагрузки в домен могут добавляться дополнительные контроллеры домена.

Системные требования к дополнительному DC такие же, как и для первого контроллера домена (см. Системные требования к серверу (контроллеру домена)).

Примечание. В терминологии контроллеров домена нет понятия PDC/BDC, т.е. все контроллеры равны, но один из них выступает владельцем ролей FSMO.

Заведение дополнительного контроллера домена выполняется путём присоединения дополнительного DC к существующему домену.

На добавляемом DC в `/etc/resolv.conf` обязательно должен быть добавлен первый DC как nameserver. Указать DNS и домен для поиска можно, например в ЦУС. Пример содержимого файла `/etc/resolv.conf`:

```
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

Примечание. Если используется сетевая подсистема systemd-networkd, то для того чтобы избежать конфликтов systemd-resolved с Samba DNS, следует отключить DNSStubListener:

- в файле конфигурации systemd-resolved (/etc/systemd/resolved.conf) установить значение:

```
DNSStubListener=no
```

- перезапустить службу systemd-resolved:

```
# systemctl restart systemd-resolved
```

- убедиться в наличии следующих строк в файле /etc/resolv.conf:

```
nameserver 192.168.0.132
search test.alt
```

Примечание. Для выполнения операции присоединения к домену требуется пароль администратора домена.

Все действия выполняются на узле dc2.test.alt (192.168.0.133), если не указано иное.

1. Установить пакет `task-samba-dc`, который установит все необходимое (этот шаг можно пропустить, если при установке системы на этапе «Установка системы» был выбран профиль «Контроллер Альт Домена (Сервер Samba DC)»):

```
# apt-get install task-samba-dc
```

2. Остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service; systemctl stop $service; done
```

3. Для сервера должно быть установлено правильное имя узла и домена (этот шаг можно пропустить, если имя компьютера было задано при установке системы на этапе «Настройка сети»). Для этого необходимо выполнить команды:

```
# hostnamectl set-hostname dc2.test.alt
# domainname test.alt
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

4. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

5. На существующем контроллере домена завести IP-адрес для нового контроллера домена (команда выполняется на узле dc1.test.alt):

```
# samba-tool dns add 192.168.0.132 test.alt DC2 \
A 192.168.0.133 -Uadministrator

Password for [TEST\administrator]:
Record added successfully
```

Примечание. Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примечание. Синтаксис команды `samba-tool dns add`:

```
samba-tool dns add <server> <zone> <name> <A|AAAA|PTR|CNAME|NS|MX|SRV|TXT> <data>
```

6. На дополнительном контроллере домена установить следующие параметры в файле конфигурации клиента Kerberos /etc/krb5.conf):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

7. Для проверки настройки следует запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Примечание. Имя домена должно быть указано в верхнем регистре.

Убедиться, что билет получен:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
22.05.2024       13:35:08              22.05.2024       23:35:08
krbtgt/TEST.ALT@TEST.ALT
   renew until 29.05.2024 13:35:05
```

8. Ввести дополнительный сервер в домен test.alt в качестве контроллера домена (DC):

```
# samba-tool domain join test.alt DC \
-Uadministrator@TEST.ALT --realm=test.alt
```

В случае успешного выполнения присоединения, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772)
as a DC
```

Примечание. При использовании SAMBA_INTERNAL, необходимо указать значение `dns forwarder`, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex, например:

```
--option="dns forwarder=8.8.8.8"
```

Если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9. Сделать службу samba запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание. Для получения дополнительной информации о параметрах команды `samba-tool domain join` можно воспользоваться командой:

```
# samba-tool domain join –help
```

После успешного ввода в домен в resolvconf необходимо сменить адрес первого контроллера домена на адрес второго DC (в данном примере 192.168.0.132 на 192.168.0.133). Для этого внести изменения в файл /etc/net/ifaces/enp0s3/resolv.conf и перезагрузить систему.

4.5.1 Проверка результатов присоединения

Примечание. После присоединения к домену службе синхронизации данных может понадобиться до 15 минут для автоматического формирования подключений для репликации.

Проверка корректности присоединения:

1. Проверить работу DNS:

```
$ host -t A test.alt
test.alt has address 192.168.0.132
test.alt has address 192.168.0.133
```

В списке адресов должен отображаться IP-адрес добавленного контроллера домена.

2. Проверить статус репликации между контроллерами домена. Для этого на добавленном DC выполнить команду:

```
# samba-tool drs showrepl
```

В случае успешного выполнения репликации в каждом блоке отображаются сообщения вида:

```
Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 10e22808-960e-4cb3-8724-abd2223555cd
        Last attempt @ Sat Jun 15 10:27:21 2024 EET was successful
        0 consecutive failure(s).
        Last success @ Sat Jun 15 10:27:21 2024 EET
```

В пункте «Last attempt» должны стоять актуальные дата и время, идентичные указанным в строке «Last success» (отображает время последней репликации). Также должно быть «0 consecutive failure(s)».

3. На добавленном DC создать нового пользователя домена:

```
# samba-tool user add testuser --random-password
User 'testuser' added successfully
```

4. Убедиться, что учетная запись созданного пользователя доступна на первом контроллере домена:

```
# samba-tool user list | grep  testuser
testuser
```

4.6 Присоединение к домену в роли участника

В данном разделе рассмотрен процесс ввода в домен узла host-01.test.alt (192.168.0.135) с ОС «Альт Рабочая станция».

В данном разделе описывается использование демона служб безопасности системы (SSSD) для подключения системы к домену. Особенности использования Winbind для подключения системы к «Альт Домен» рассмотрены в руководстве администратора.

Примечание. Для выполнения операции присоединения к домену требуется пароль администратора домена.

4.6.1 Установка пакетов

Для ввода компьютера в «Альт Домен» потребуется установить пакет task-auth-ad-sssd и все его зависимости и пакет alterator-gpupdate для включения групповых политик:

```
# apt-get install task-auth-ad-sssd alterator-gpupdate
```

4.6.2 Настройка сети

Необходимо произвести настройку сети, если она не выполнялась при установке. Настройку сети можно выполнить как в графическом интерфейсе, так и в консоли.

В ЦУС (см. Центр управления системой) «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (Рис. 25).

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname host-01.test.alt
```

- в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл /etc/net/ifaces/enp0s3/resolv.conf со следующим содержимым:

```
nameserver 192.168.0.132
```

где 192.168.0.132 – IP-адрес DNS-сервера домена.

- указать службе resolvconf использовать DNS контроллера домена и домен для поиска. Для этого в файле /etc/resolvconf.conf3добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
search_domains=test.alt
```

где enp0s3 – интерфейс на котором доступен контроллер домена, test.alt – домен.

- обновить DNS адреса:

```
# resolvconf -u
```

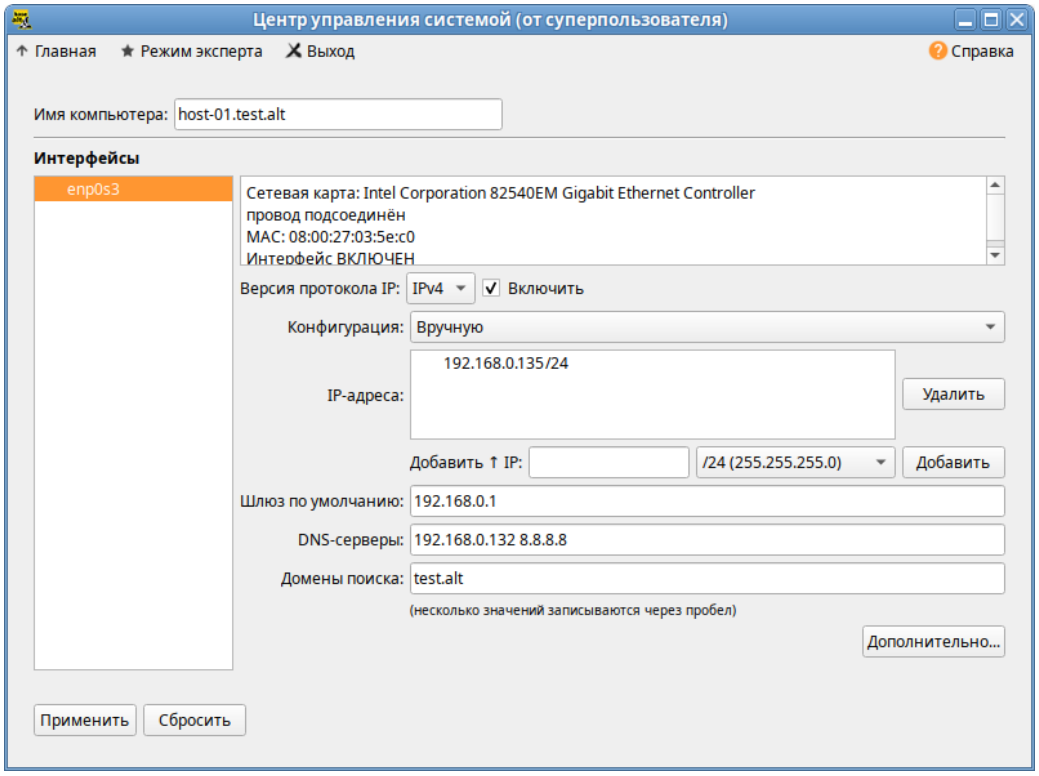

Рис. 25. Настройка сети

В результате выполненных действий в файле /etc/resolv.conf должны появиться строки:

```
search test.alt
nameserver 192.168.0.132
```

4.6.3 Ввод клиентской машины в домен

4.6.3.1 Ввод в домен в командной строке

Для ввода машины в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-01 test 'administrator' 'Pa$
$word'
Joined 'HOST-01' to dns domain 'test.alt'
```

Перезагрузить рабочую станцию.

4.6.3.2 Ввод в домен в ЦУС

Для ввода компьютера в домен в ЦУС (см. Центр управления системой) необходимо выбрать пункт «Пользователи»→«Аутентификация».

В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory», заполнить поля («Домен», «Рабочая группа», «Имя компьютера»), выбрать пункт «SSSD (в единственном домене)» и нажать кнопку «Применить» (Рис. 26).

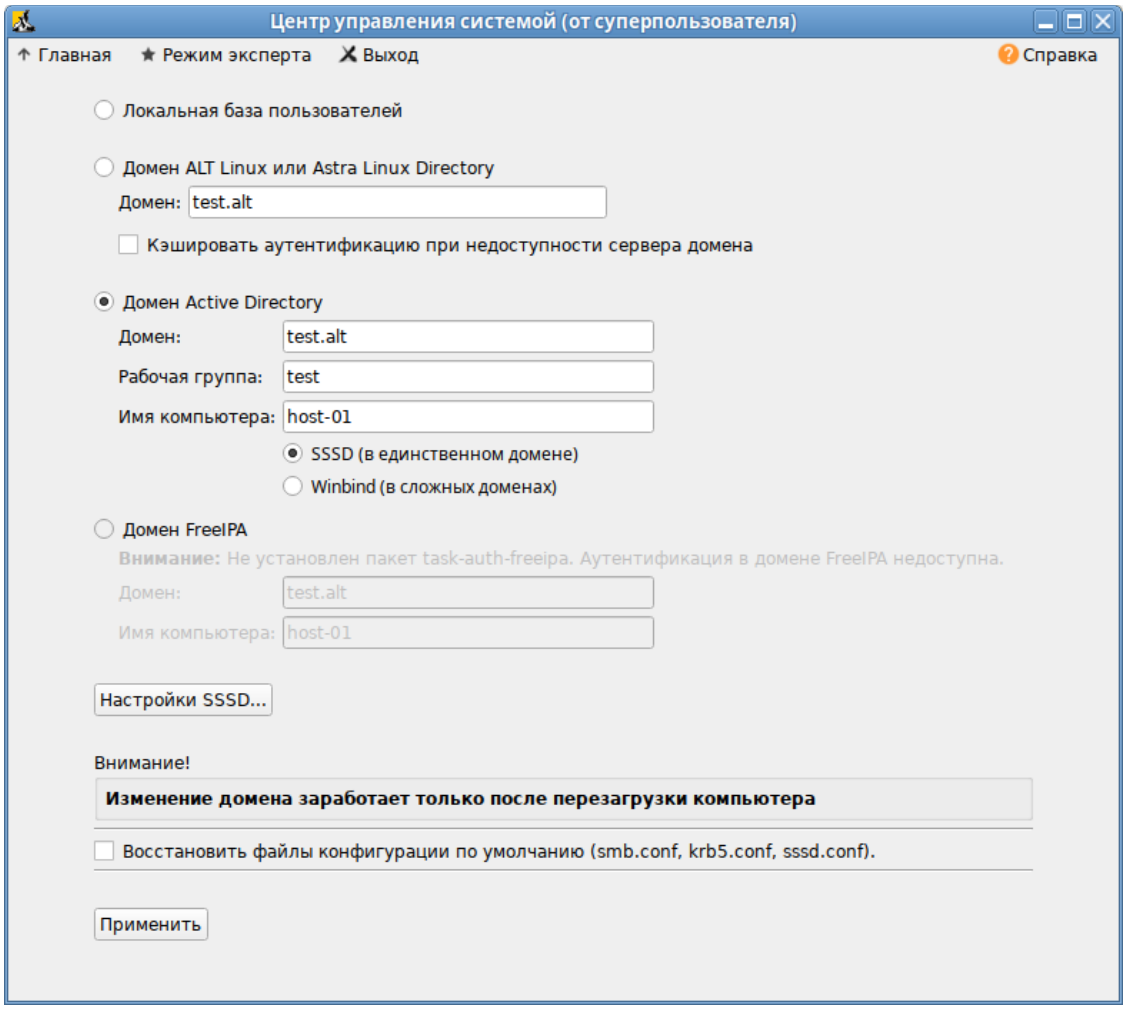

Рис. 26. Ввод в домен в ЦУС

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, установить отметку в поле «Включить групповые политики» и нажать кнопку «ОК» (Рис. 27).

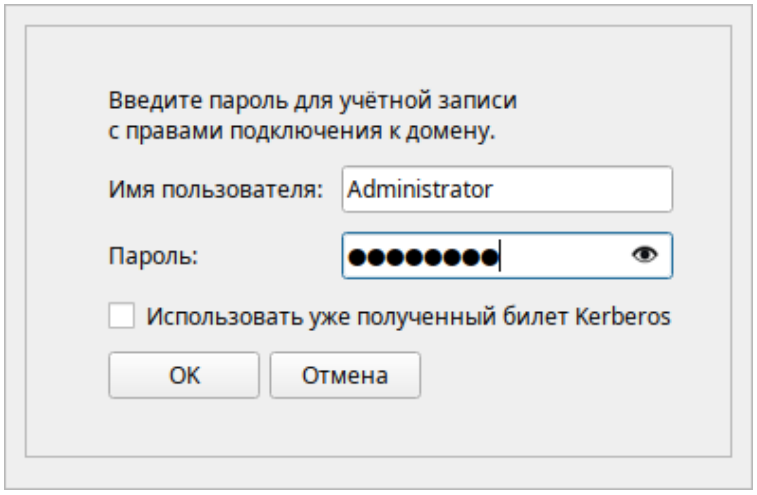

Рис. 27. Параметры учетной записи с правами подключения к домену

При успешном подключении к домену, отобразится соответствующая информация (Рис. 28).

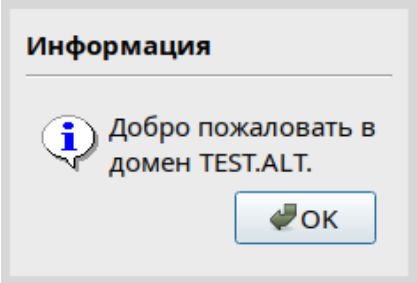

Рис. 28. Успешное подключение к домену

Перезагрузить рабочую станцию.

4.6.4 Проверка подключения к домену

Отображение сведений о доменном пользователе (ivanov – пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET

# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

5 УСТАНОВКА АДМИНИСТРАТИВНЫХ ИНСТРУМЕНТОВ

Раздел содержит инструкции по установке административных инструментов. Административные инструменты обычно устанавливаются на рабочей станции, введенной в домен, но могут быть установлены и на контроллере домена если на нем установлена графическая среда.

5.1 Модуль удаленного управления базой данных конфигурации (ADMC)

Установить пакет admc:

```
# apt-get install admc
```

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные»→«ADMC» или из командной строки (команда `admc`).

Примечание. Для использования ADMC необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

Интерфейс ADMC представлен на Рис. 29.

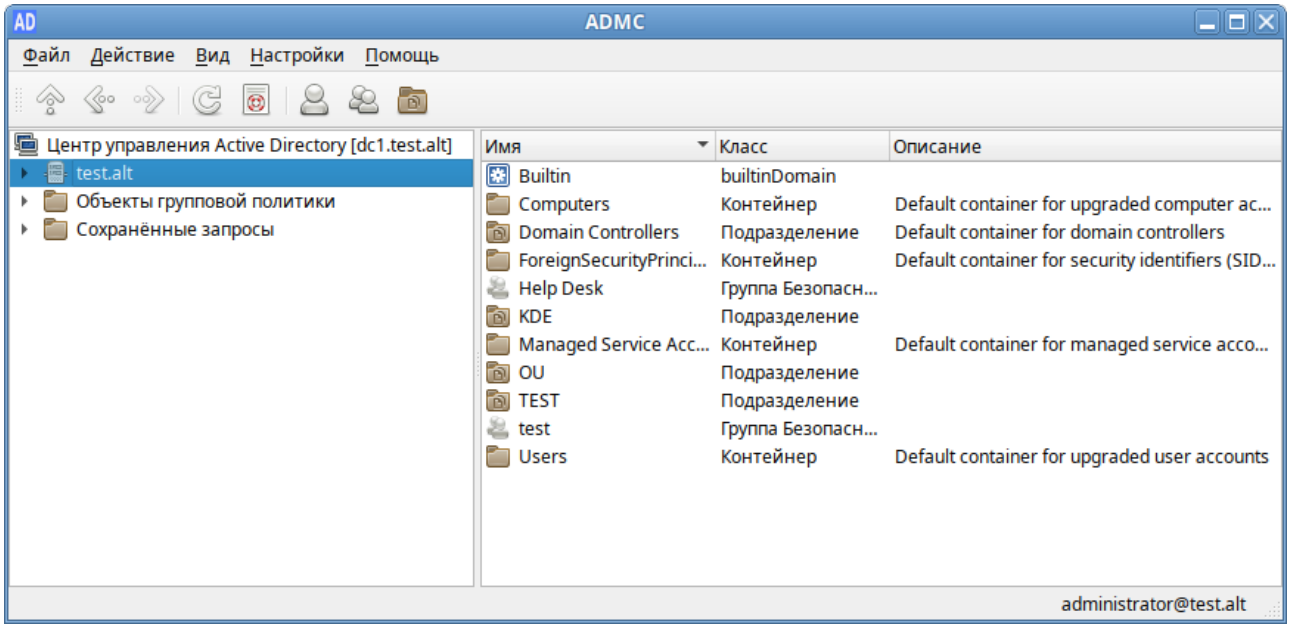

Рис. 29. Интерфейс ADMC

5.2 Модуль редактирования настроек клиентской конфигурации (GPUI)

Установить пакет gpui:

```
# apt-get install gpui
```

Примечание. В настоящее время GPUI не умеет читать файлы ADMX с контроллера домена. Для корректной работы необходимо установить пакеты admx и файлы ADMX от Microsoft:

```
# apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-browser admx-msi-setup
# admx-msi-setup
```

Для использования модуля необходимо предварительно получить ключ Kerberos для администратора домена:

```
$ kinit administrator
Password for administrator@TEST.ALT:
```

Интерфейс GPUI представлен на Рис. 30.

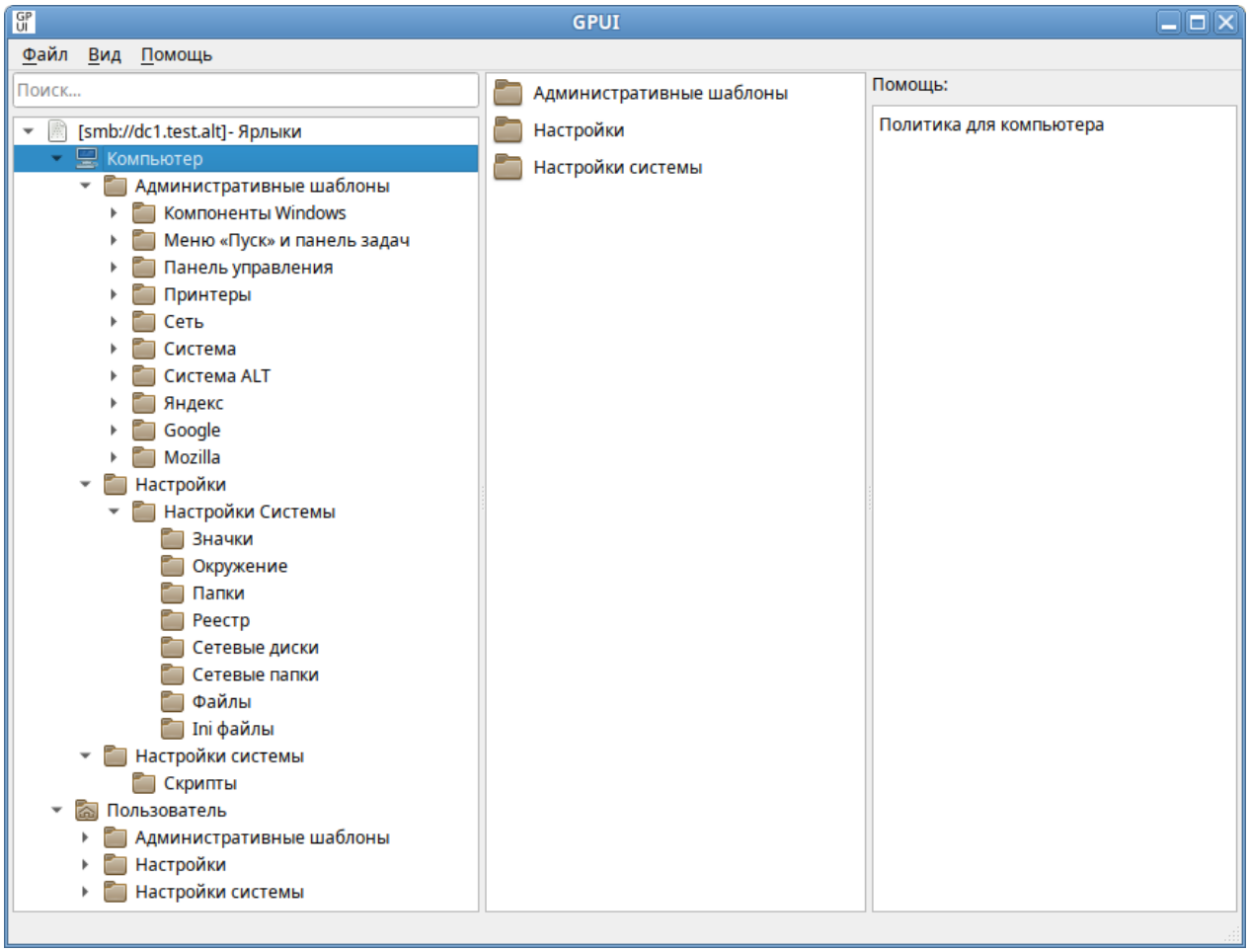

Рис. 30. Окно GPUI

По умолчанию GPUI не редактирует никаких политик. Для того чтобы редактировать политику, GPUI нужно запустить либо из ADMC, выбрав в контекстном меню объекта групповой политики пункт «Изменить…» (Рис. 31), либо с указанием каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}"
```

Ключ `-p` позволяет указать путь к шаблону групповой политики, который нужно редактировать, dc1.test.alt – имя контроллера домена, а "{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}" – GUID шаблона групповой политики для редактирования. Можно указывать как каталоги smb, так и локальные каталоги.

Примечание. GUID шаблона групповой политики можно узнать в ADMC (это дочерний контейнер Policies контейнера System), в настройках должен быть отмечен пункт «Дополнительные возможности».

Пример запуска GPUI для редактирования политики:

```
$ gpui-main -p "smb://dc.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

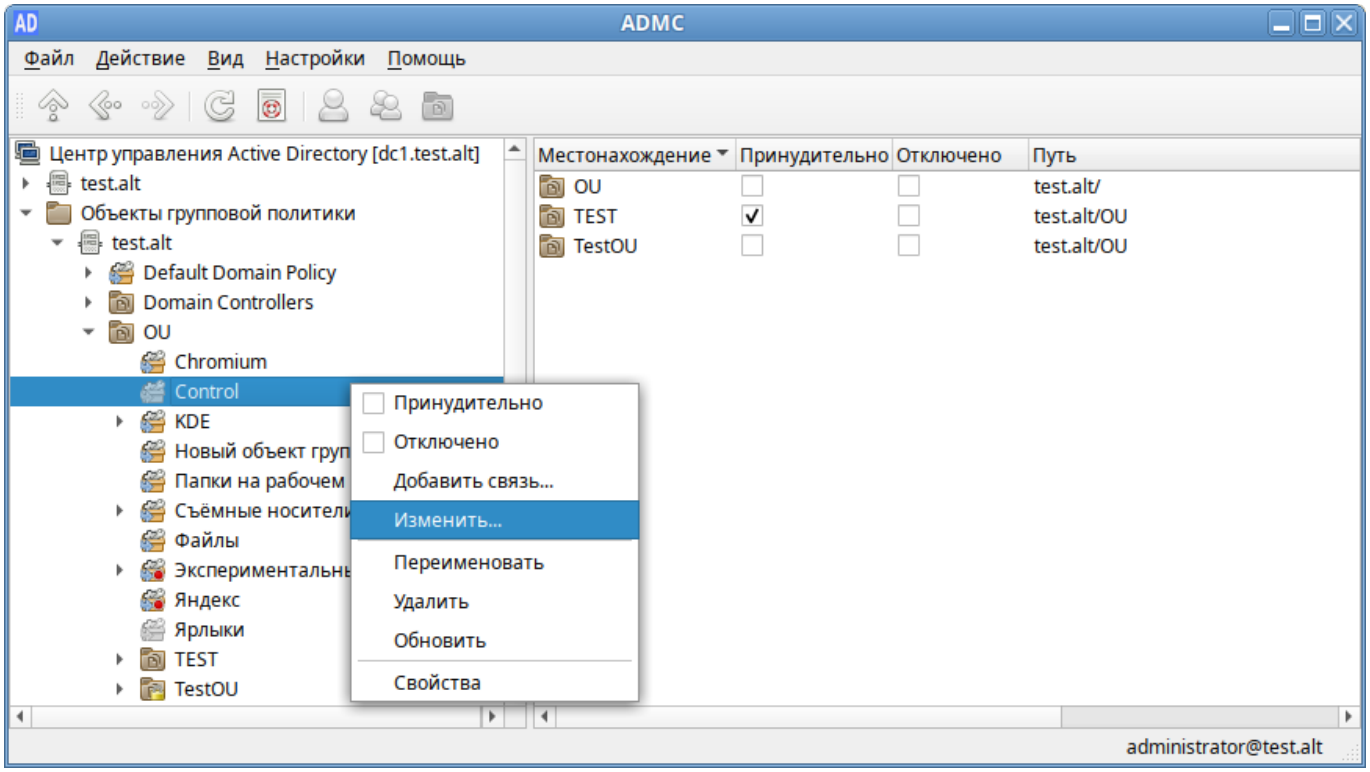

Рис. 31. Запуск GPUI из ADMC

6 ПРИЛОЖЕНИЯ

6.1 Центр управления системой

Центр управления системой (ЦУС, альтератор) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

Запустить ЦУС в графической среде можно следующими способами:

- в графической среде MATE: «Система» → «Администрирование» → «Центр управления системой»;
- в графической среде XFCE, KDE: «Меню запуска приложений» → «Настройки» → «Центр управления системой»;
- из командной строки: командой `acc`.

Запуск ЦУС требует административных прав, и если запустить его от обычного пользователя, он запросит пароль администратора системы (Рис. 32).

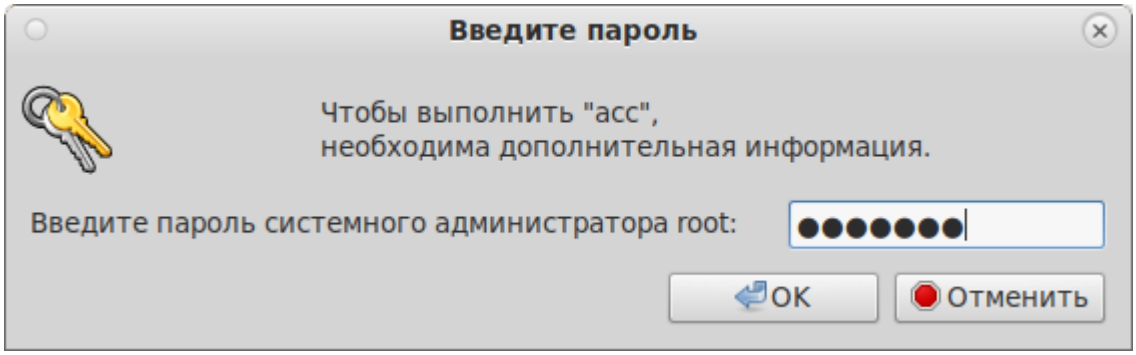

Рис. 32. Запрос пароля администратора

ЦУС (Рис. 33) состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

ЦУС имеет также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет alterator-fbi:

```
# apt-get install alterator-fbi
```

И запущены сервисы ahttpd и alteratord:

```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

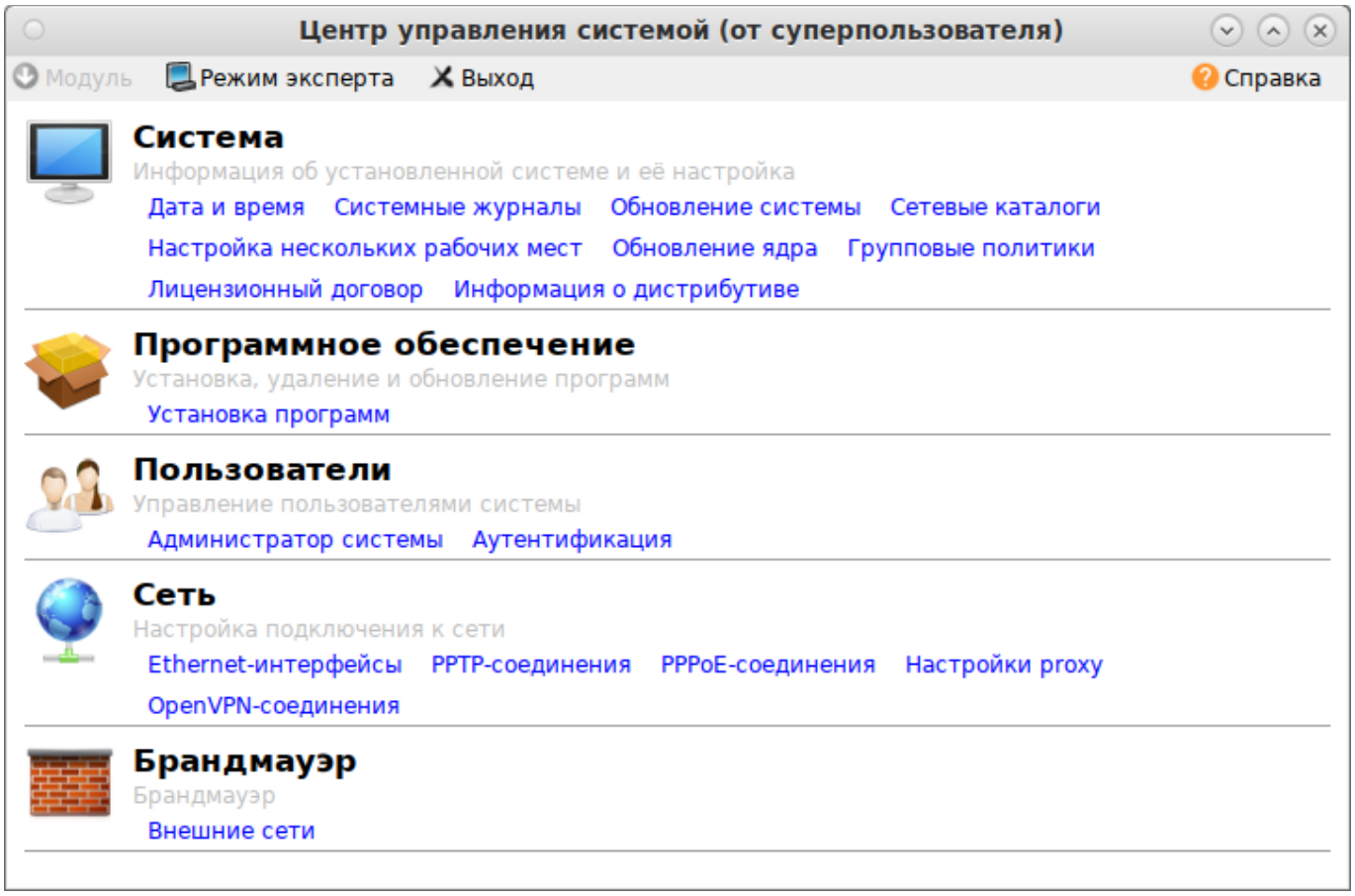

Рис. 33. Центр управления системой

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу https://ip-адрес:8080/.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (root) и пароль пользователя (Рис. 34).

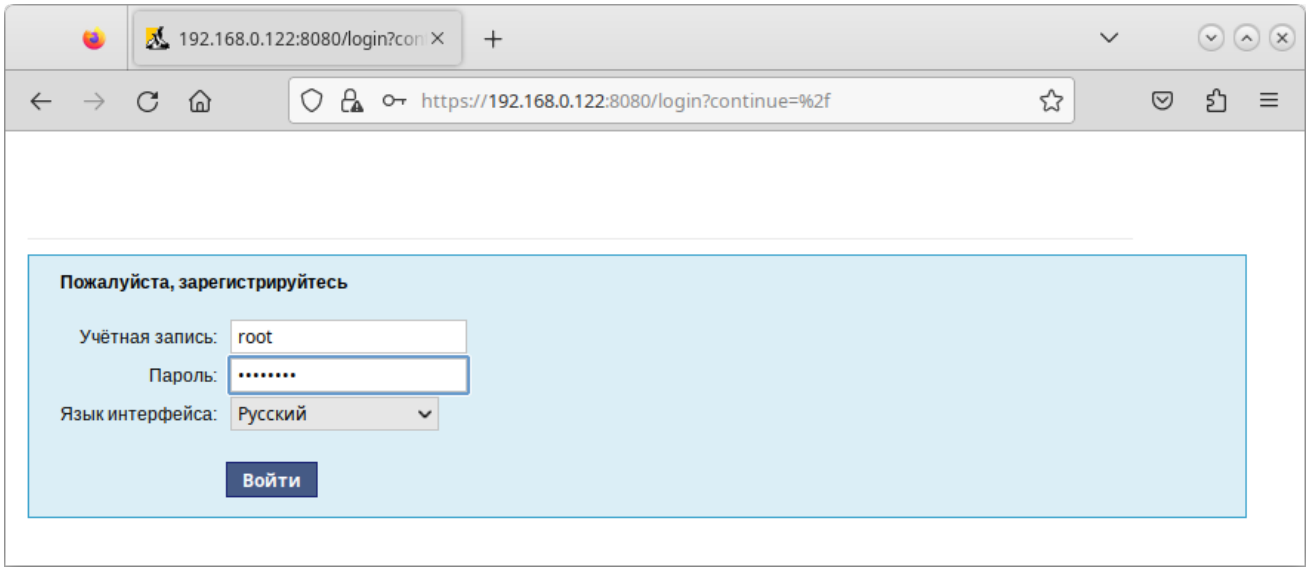

Рис. 34. Вход в систему

После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс (Рис. 35).

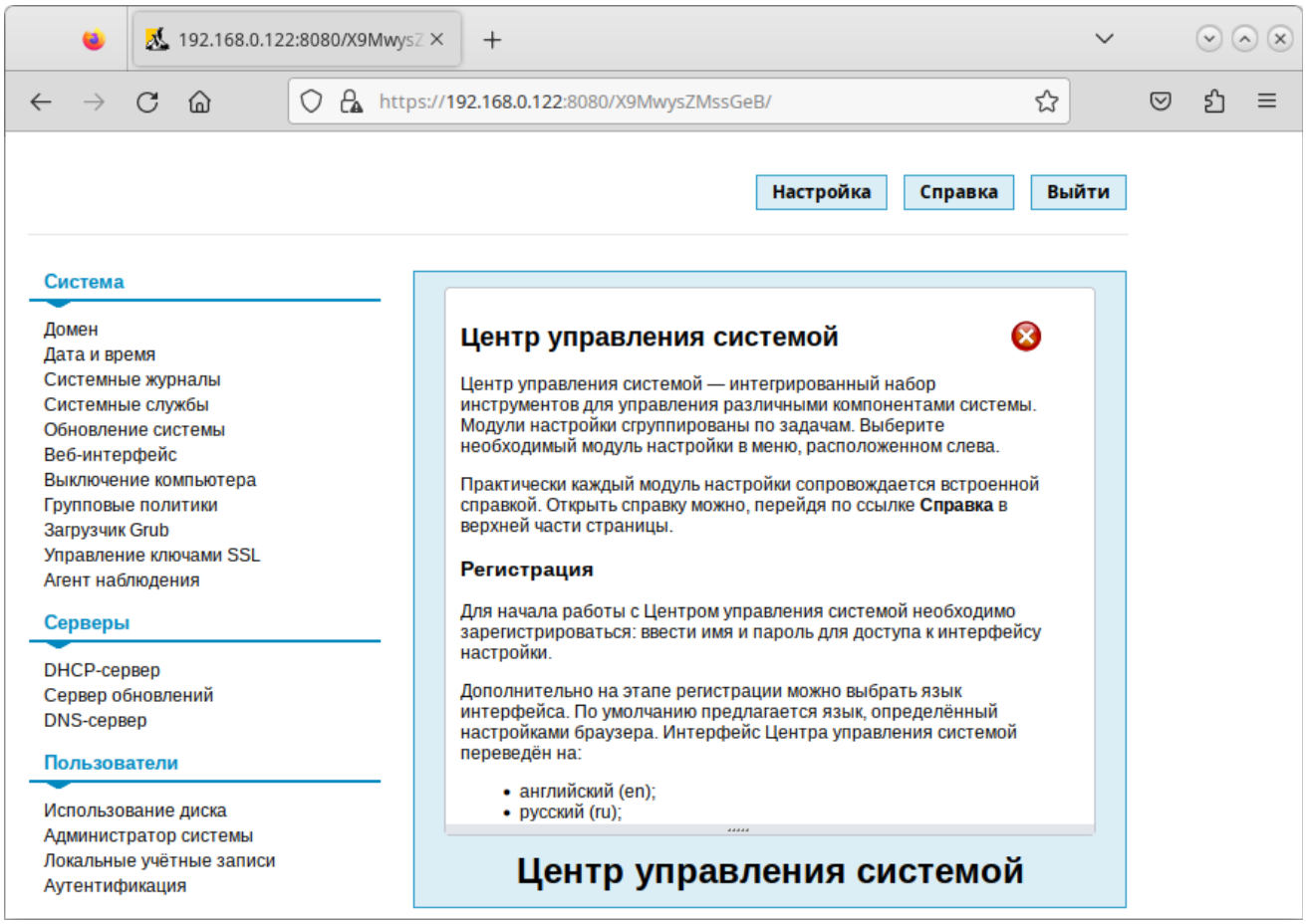

Рис. 35. Веб-интерфейс центра управления системой

Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
$ rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
$ apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```