



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ»**

РУКОВОДСТВО ПО БЫСТРОЙ НАСТРОЙКЕ

RU.33654484.0004-02 91 03

Листов 30

СОДЕРЖАНИЕ

1 Введение.....	3
1.1 Область применения.....	3
1.2 Краткое описание возможностей.....	3
1.3 Уровень подготовки администратора.....	4
2 Назначение и условия работы СКДПУ.....	5
2.1 Назначение СКДПУ.....	5
2.2 Требования к техническим и программным средствам.....	5
3 Установка.....	7
3.1 Начало процесса установки ОС Astra Linux 1.6SE.....	7
3.2 Разметка диска ОС Astra Linux 1.6SE под установку СКДПУ.....	11
3.3 Процесс установки ОС Astra Linux 1.6SE.....	15
3.4 Настройка ОС Astra Linux 1.6SE.....	16
4 4 Порядок развертывания СКДПУ.....	18
4.1 Проверка целостности дистрибутива СКДПУ.....	18
4.2 Установка СКДПУ.....	18
4.3 Фиксация контрольных сумм исполняемых файлов СКДПУ.....	19
5 Доступ к СКДПУ.....	21
5.1 Администрирование ОС после установки.....	21
5.2 Доступ к веб-интерфейсу СКДПУ.....	21
5.3 Настройка подключения к почтовому серверу.....	22
5.4 Добавление файла лицензии.....	23
5.5 Включение режима ЗПС ОС Astra Linux 1.6SE.....	23
Перечень сокращений.....	24
Перечень рисунков.....	28
Перечень таблиц.....	29
Лист регистрации изменений.....	30

1 ВВЕДЕНИЕ

1.1 Область применения

Настоящий документ предназначен для администраторов СКДПУ и содержит описание действий для развертывания и быстрой настройки СКДПУ.

1.2 Краткое описание возможностей

Основные возможности СКДПУ приведены в [таблица 1](#).

Таблица 1 – Основные возможности СКДПУ

Основные возможности	Описание
Контроль доступа	СКДПУ позволяет создать политику управления доступом на основе прав пользователей: целевые учетные записи, протоколы, интервалы времени и типы сеансов.
Единая точка входа в систему (SSO)	Для доступа к учетным записям достаточно предоставить имя пользователя и пароль в СКДПУ.
Поддержка нескольких протоколов администрирования	СКДПУ поддерживает следующие протоколы администрирования устройств и серверов: RDP/TSE, SSH, TELNET, VNC, SFTP/SCP и т.д.
Отслеживание активности и запись сеансов	Регистрация и возможность записи всех действий, выполненных на управляемых устройствах в течение графического сеанса (RDP/TSE или VNC) или сеанса командной строки (SSH, TELNET).
Управление паролями	СКДПУ позволяет изменять пароли на управляемых устройствах по запросу или через заданные интервалы времени.
Работа без использования агентов	СКДПУ работает без использования специальных агентов на администрируемых устройствах или на рабочих станциях администраторов.
Статистика и отчеты о действиях	Возможность формировать рабочую статистику/отчеты и экспортировать эти данные в формате CSV через интерфейс администратора.

Основные возможности	Описание
Делегирование функций администрирования СКДПУ	Средства управления профилями позволяют определить, какие действия будут доступны каждому пользователю СКДПУ (например, создание пользователей, управление правами и т.д.)
Анализ потока и распознавание текста	СКДПУ позволяет в реальном времени обнаруживать определенные строки символов в сессиях SSH и анализировать содержимое сеансов подключения к удаленному рабочему столу (RDP/TSE).
Контроль в реальном времени	Администраторы СКДПУ могут просматривать активные сеансы подключения к удаленному рабочему столу и SSH в СКДПУ в реальном времени.
Поддержка Web Service	Вся информация о пользователях, учетных записях, устройствах, правах доступа в СКДПУ может вводиться или быть доступна с помощью Web Service API.

1.3 Уровень подготовки администратора

Администратор должен обладать следующими знаниями:

- Системное администрирование ОС Windows/Linux и активного сетевого оборудования;
- Базовые знания сетевых протоколов;
- Администрирование СКДПУ и умение с его помощью реализовывать корпоративную политику безопасности, в части относящейся к информационному обмену;
- Знание и соблюдение требований конфиденциальности (секретности) при проведении работ.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ РАБОТЫ СКДПУ

2.1 Назначение СКДПУ

СКДПУ предназначена для мониторинга и аудита действий поставщиков ИТ-услуг и других третьих лиц на администрируемых устройствах с целью контроля доступа внутренних и внешних поставщиков ИТ-услуг, владельцев учетных записей с расширенными правами и пользователей с повышенными рисками.

СКДПУ своевременно уведомляет Администратора о любых попытках подключения к устройствам, определенным как критичные, о неудачных попытках входа в СКДПУ или о невозможности автоматического входа с использованием заданной учетной записи.

СКДПУ предназначена для записи рабочих сеансов для последующего просмотра с целью аудита, управления инцидентами и проведения расследований.

СКДПУ анализирует все команды, вводимые в ходе сеансов SSH, в реальном времени и в случае обнаружения запрещенных строк отправляет соответствующее уведомление или разрывает сеанс подключения. Кроме того, СКДПУ использует технологию оптического распознавания символов (OCR) сеансов подключения к удаленному рабочему столу (RDP и VNC) в реальном времени, что упрощает процесс выявления причин сбоев или инцидентов безопасности.

СКДПУ поддерживает следующие протоколы передачи данных:

- HTTP (RFC 2616) и HTTPS (HTTP Over TLS – RFC 2818);
- SSH (RFC 4250 – 4256) и подсистемы указанного протокола;
- TELNET (RFC 854);
- RLOGIN (RFC 1282);
- произвольные TCP протоколы (RAWTCPIP) в рамках сессий SSH;
- RDP (v. 5 – 8.1) и VNC (на основе RFB 3.8, RFC 6143) в домене пользователя.

2.2 Требования к техническим и программным средствам

Минимальные характеристики программного и аппаратного обеспечения для развертывания сервера СКДПУ см. [таблица 2](#).

Таблица 2 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	интерфейс для подключения к LAN
ОС	ОС Astra Linux 1.6 Special Edition
Веб-сервер	HTTP Apache 2.4

Компонент	Описание
База данных	СУБД PostgreSQL версии 9.6
Брокер сообщений	RabbitMQ версии 3.6
Другое ПО	Интерпретаторы языка программирования Python 2.7, Python 3.5
	Библиотеки Python, обеспечивающие удовлетворение зависимостей для *.py части ПО

3 УСТАНОВКА

СКДПУ - это программное решение, которое может быть развернуто на ОС Astra Linux 1.6SE на платформе x86_64. Он предоставляет веб-интерфейс для работы с данными и утилиты CLI для обслуживания системы.



32-битные платформы не поддерживаются

Для установки СКДПУТ необходимо наличие сервера (аппаратного или виртуального), на котором будет работать СКДПУ.



Решение СКДПУ разработано для работы в рамках защищенного периметра локально на выделенном оборудовании или в качестве виртуального хоста

СКДПУ необходимо установить в защищенную среду для защиты от возможных вторжений или несанкционированного доступа к данным системы.

3.1 Начало процесса установки ОС Astra Linux 1.6SE

Для установки программного обеспечения подготовьте ОС и минимальный требуемый «базовый» набор.

Порядок установки ОС Astra Linux 1.6SE аналогичен любой другой установке ОС и подразумевает наличие дистрибутивного диска.



Для успешной установки требуется установить локализацию в UTF-8.

Шаг 1. Установить носитель в устройство считывания дисков.

Шаг 2. Настроить область `/boot` для загрузки этого носителя в приоритете, либо запустить в ручном режиме с данного носителя, если система BIOS рассчитана на ручной режим выбора устройства загрузки.

Шаг 3. В появившемся интерфейсе автозагрузки выбрать язык English



Рисунок 1 – Выбор языка установки

Шаг 4. Выбрать в меню вариант неграфической установки Install

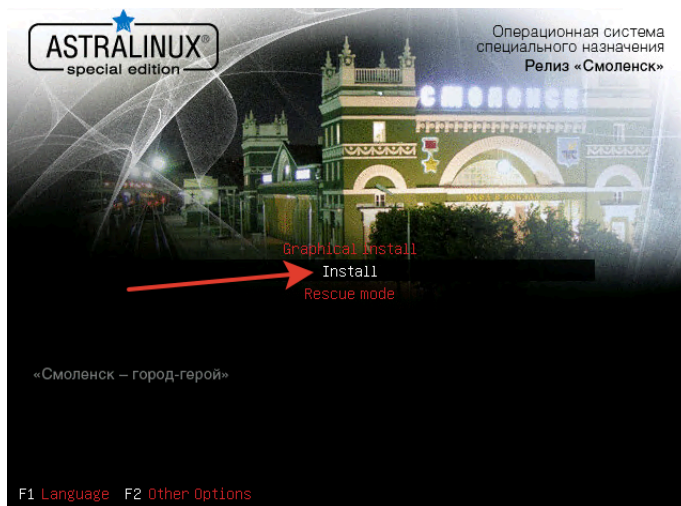


Рисунок 2 – Выбор текстового режима установки

Шаг 5. Выбрать язык

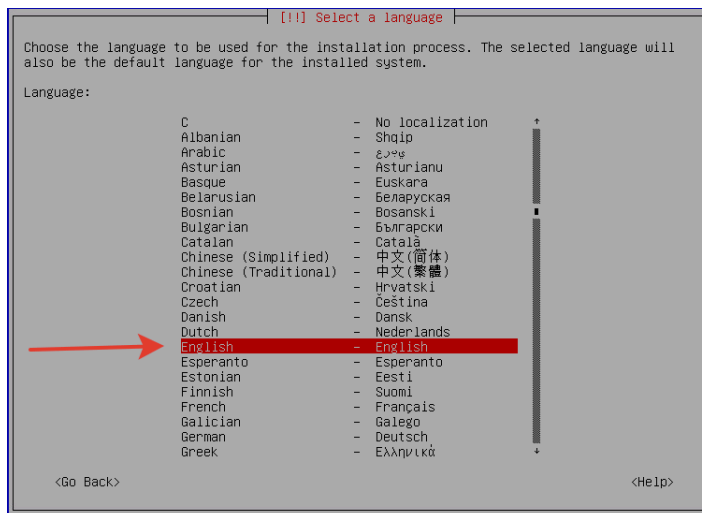


Рисунок 3 – Выбор языка установки

Шаг 6. Сконфигурировать локализацию

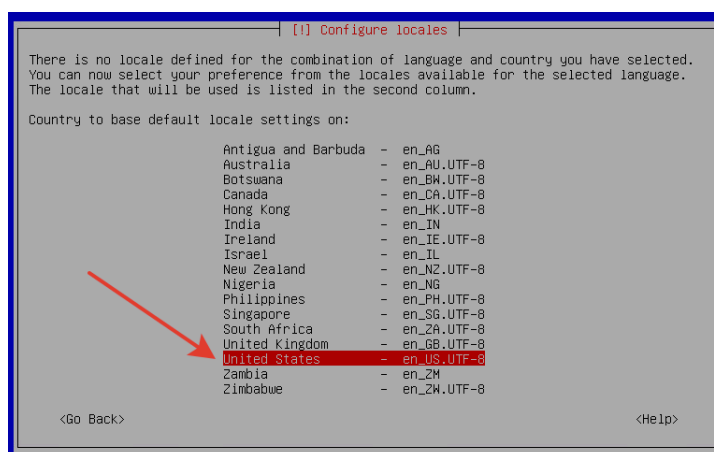


Рисунок 4 – Выбор параметров локализации

Шаг 7. Принять лицензионное соглашение

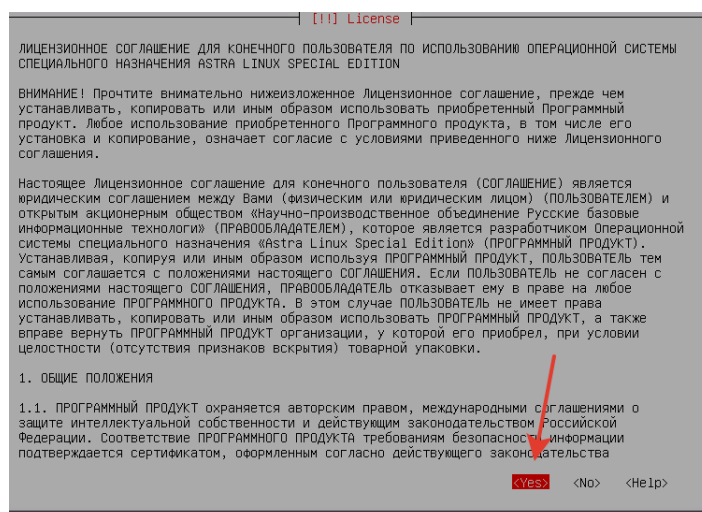


Рисунок 5 – Лицензионное соглашение ОС

Шаг 8. Выбрать раскладку клавиатуры



Рисунок 6 – Выбор раскладки клавиатуры

Шаг 9. После загрузки первичных пакетов ввести имя хоста `skdpu`

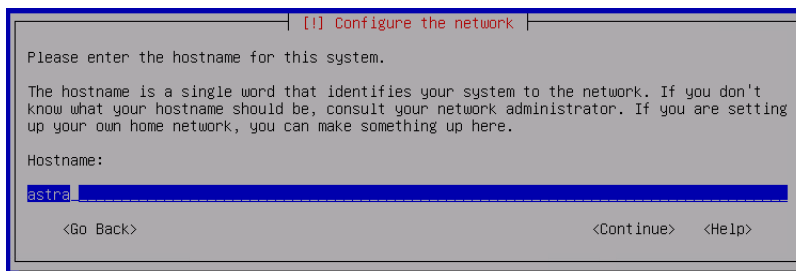


Рисунок 7 – Задание имени хоста



При установке базовой ОС рекомендуется первым пользователем добавлять именно `wabadmin`. Этот пользователь будет реализован как низкоуровневый, но с разрешением удаленного доступа, в т.ч. по SSH.

Шаг 10. Создать пользователя wabadmin и задать для него пароль !QAZ2wsx

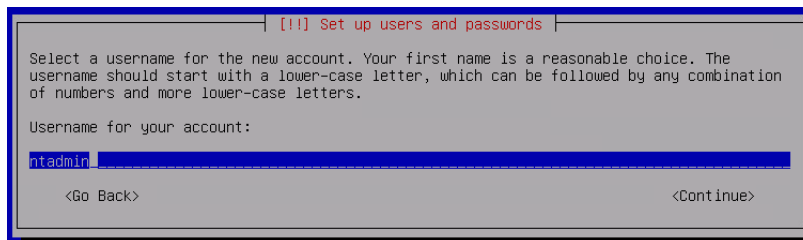


Рисунок 8 – Создание пользователя

Шаг 11. Подтвердить пароль повторным вводом

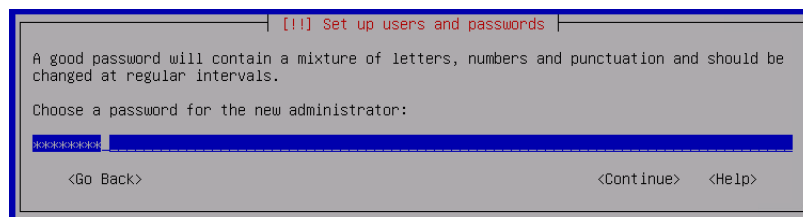


Рисунок 9 – Подтверждение пароля

Шаг 12. Выбрать часовой пояс

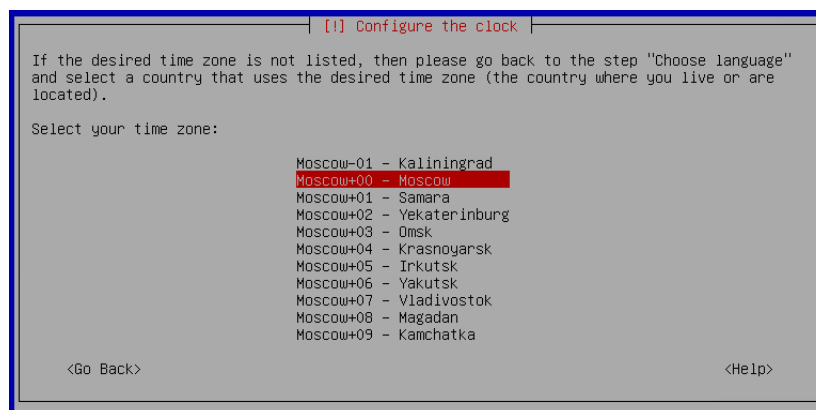
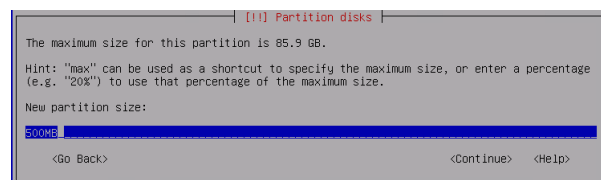
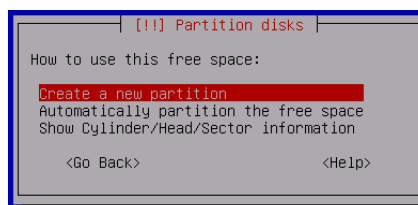
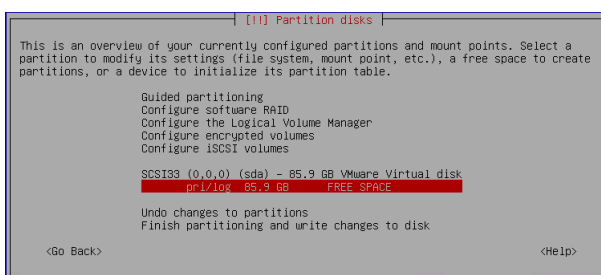
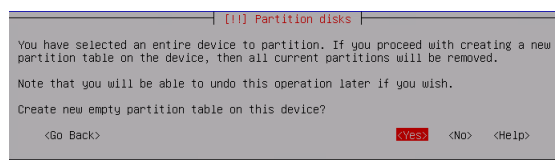
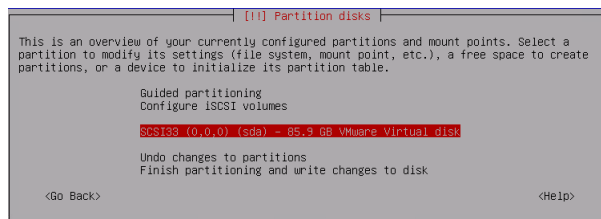
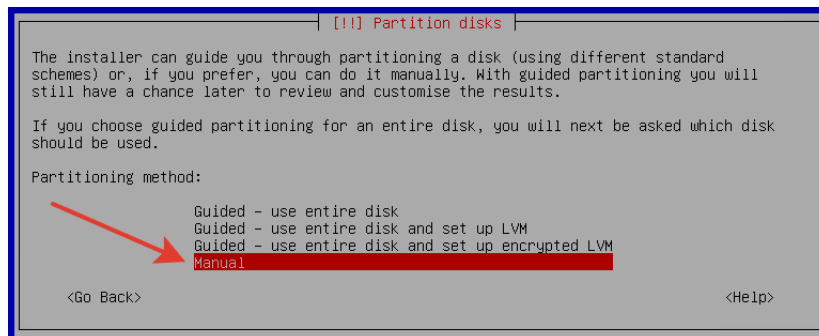


Рисунок 10 – Задание часового пояса

3.2 Разметка диска ОС Astra Linux 1.6SE под установку СКДПУ

СКДПУ не предъявляет особых требований к названиям директорий, но при этом разметать диск рекомендуется следующим образом:

Шаг 1. Выбрать ручной режим разметки



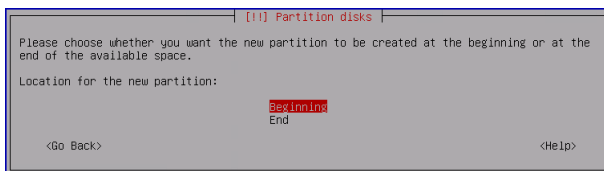


Рисунок 11 – Разметка дискового пространства

- Шаг 2.** Создать в главной партии физический раздел *boot* размером 500 Мб, файловой системой ext2 и точкой монтирования */boot*

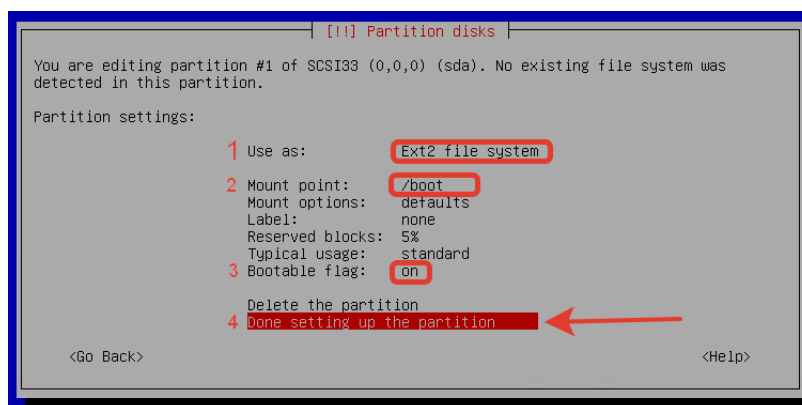
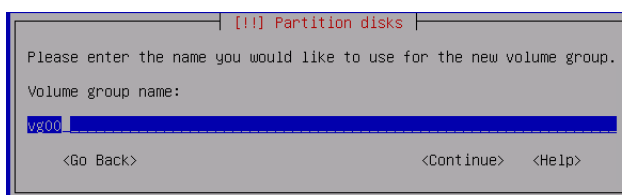
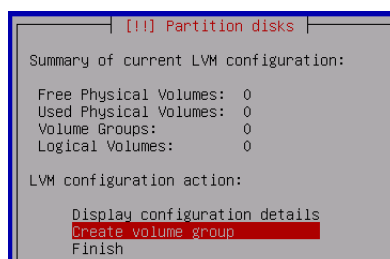
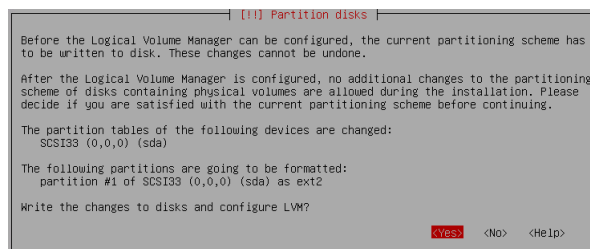
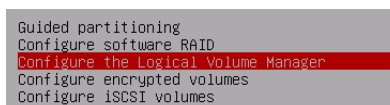


Рисунок 12 – Создание загрузочной области

- Шаг 3.** Создать LVM с названием *vg00*. В качестве места создания обязательно ставим отметку напротив незанятого пространства



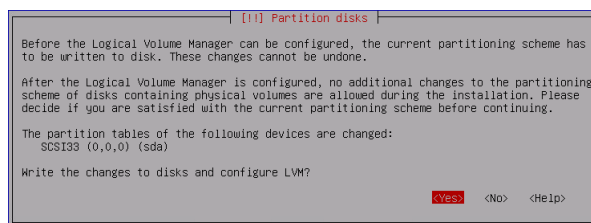
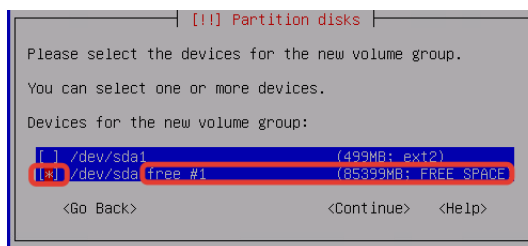


Рисунок 13 – Создание LVM

Шаг 4. Внутри LVM создать логические партиции, например

Таблица 3 – Пример разметки разделов

Имя раздела	Размер	Точка монтирования	Тип файловой системы
<i>boot</i>	500 MB	/boot	Ext2, флаг автозагрузки
Логические разделы LVM <i>vg00</i>			
<i>lvroot</i>	10 GB	/	Ext3 или Ext4
<i>lvvar</i>	2 GB	/var	Ext3 или Ext4
<i>lvopt</i>	10 GB	/opt	Ext3 или Ext4
<i>lvdrbdmeta</i>	160 MB	-	-
<i>lvswap</i>	4 GB	-	swap area
<i>lvfree</i>	4 GB	-	do not use
<i>lvwab</i>	все оставшееся место	/var/wab	Ext4

lvdata выделяется все оставшееся место, так как в данном разделе будут храниться самые многочисленные и увесистые файлы - записи сессий, со всеми доп. материалами к ним, потому, чем больше выделено место, тем реже придется чистить партицию от устаревших файлов.

Шаг 5. После создания и задания параметров логических разделов выбираем `Finish ... and write to disk` и запускаем программу разметки диска по принятым параметрам

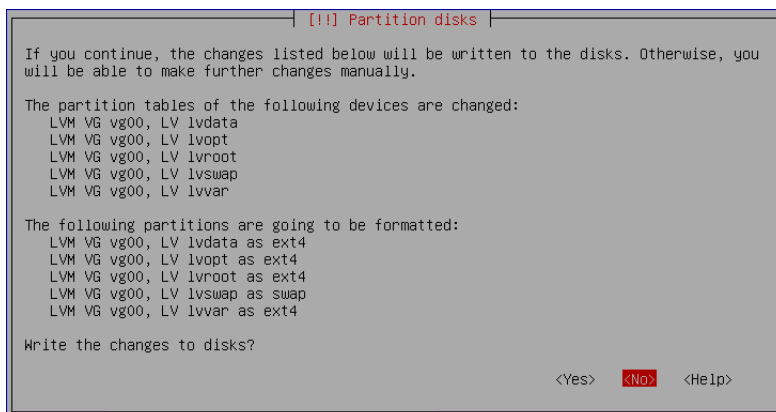


Рисунок 14 – Запуск процесса разбиения диска с установленными параметрами

3.3 Процесс установки ОС Astra Linux 1.6SE

Шаг 1. При выборе дополнительных устанавливаемых модулей к ОС Astra Linux 1.6SE необходимо снять отметки со всех модулей кроме Base

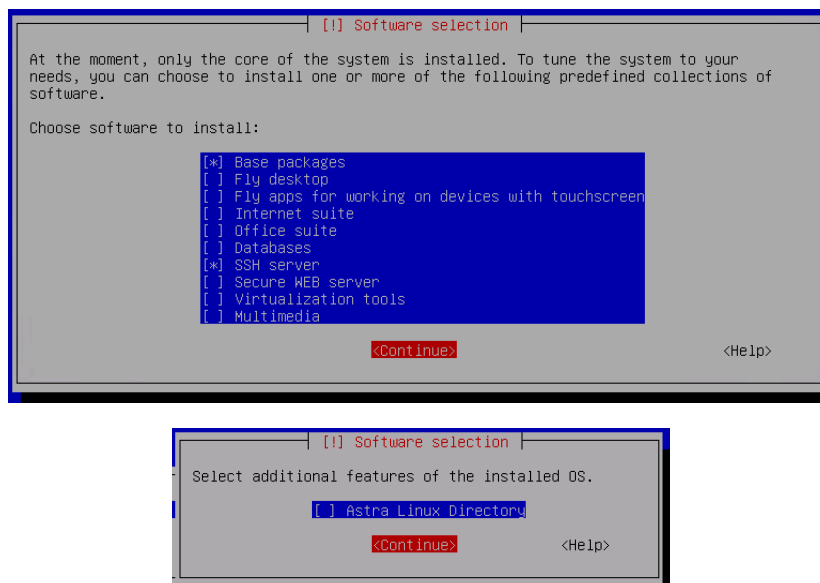
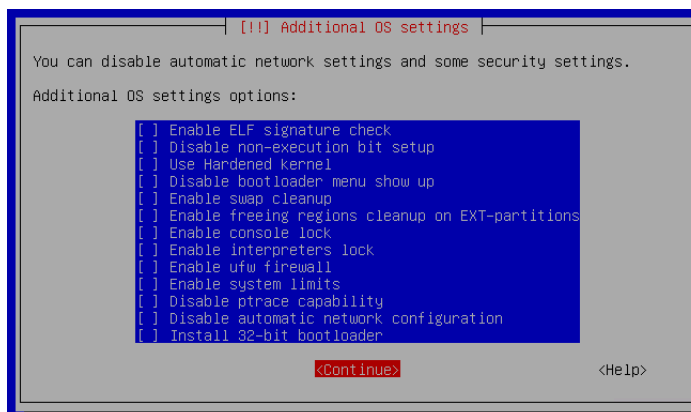
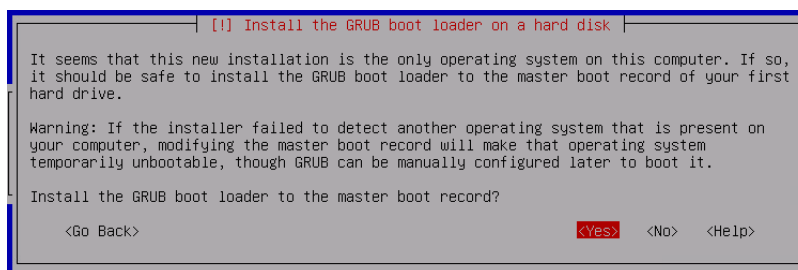
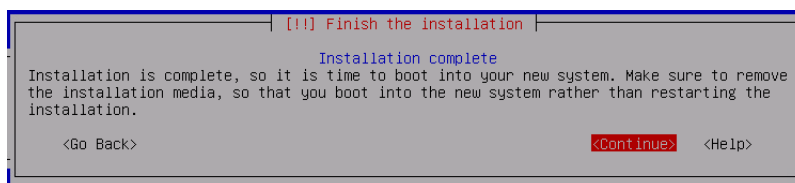


Рисунок 15 – Выбор дополнительного ПО при установке ОС Astra Linux 1.6SE



В результате чего произойдет установка минимально требуемого набора инструментов и функций ОС Astra Linux 1.6SE, что существенно сэкономит время установки и место на диске

Шаг 2. Снять выделения со всех дополнительных настроек**Рисунок 16 – Дополнительные настройки ОС****Шаг 3.** Установить модуль GRUB и указать для него пароль**Рисунок 17 – Установка модуля GRUB****Шаг 4.** При появлении сообщения Installation complete, прежде чем нажимать Continue, необходимо извлечь диск из привода**Рисунок 18 – Окончание установки**

Установщик закончит установку и произведет перезагрузку. После чего загрузка системы выведет Вам запрос:

```
Astra Linux SE 1.6 (smolensk)
tty1
astra login: ntadmin
Password:
Integrity level: 63
wabadmin@astra:~$ _
```

Рисунок 19 – Ввод логина ОС Astra Linux 1.6SE**3.4 Настройка ОС Astra Linux 1.6SE**

Перед установкой СКДПУ необходимо осуществить настройку сетевого интерфейса ОС Astra Linux 1.6SE:

Шаг 1. Авторизоваться под созданным ранее пользователем wabadmin



Для Integrity level указать значение 63

Шаг 2. Повысить привилегии командой `sudo -i`

Шаг 3. Внести изменения в сетевые настройки

```
vim /etc/network/interfaces
```

для статического адреса необходимо указать IP-адрес сервера СКДПУ, маску подсети и шлюз:

```
auto eth0
iface eth0 inet static
address <ip_СКДПУ>
netmask <маска_подсети>
gateway <шлюз>
```

для DHCP:

```
auto eth0
iface eth0 inet dhcp
```

Шаг 4. Сохранить файл `/etc/network/interfaces`

Шаг 5. Перезапустить сервис `networking`

```
/etc/init.d/networking restart
```

Шаг 6. Проверить получение интерфейсом IP-адреса по команде `ip a`

```
root@astra:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d7:13:c1 brd ff:ff:ff:ff:ff:ff
    inet 10.100.52.82/22 brd 10.100.55.255 scope global eth0
        valid_lft forever preferred_lft forever
root@astra:~# !
```

Рисунок 20 – Получение ip-адреса

Шаг 7. Добавить сервис SSH в автозагрузку и запустить:

```
systemctl enable ssh
systemctl start ssh
```

4.4 ПОРЯДОК РАЗВЕРТЫВАНИЯ СКДПУ

Перед установкой СКДПУ необходимо авторизоваться под учетной записью `wabadmin`, предварительно убедившись, что в ОС Astra Linux 1.6SE создана учетная запись `wabadmin`, и повысить привилегии командой `sudo -i`.

4.1 Проверка целостности дистрибутива СКДПУ

Проверка целостности файлов дистрибутива СКДПУ производится путем подсчета контрольных сумм файлов дистрибутива СКДПУ по алгоритму «Уровень-3, программно» программой фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0», имеющей сертификат соответствия требованиям по безопасности информации №680.

Необходимо выполнить следующие шаги:

Шаг 1. Вставить носитель с дистрибутивом СКДПУ в дисковод

Шаг 2. Получить права учетной записи `root`

Шаг 3. Зафиксировать исходное состояние контролируемых файлов

```
ufix -jR -Idoc* /media/cdrom/* > /home/wabadmin/skdpu.txt
ufix -e /home/wabadmin/skdpu.txt /home/wabadmin/skdpu.prj
```

Шаг 4. Печать файла отчета в файл формата `html` с помощью команды

```
ufix -h /home/wabadmin/skdpu.prj /home/wabadmin/skdpu_дата.html
```

Шаг 5. Сверка контрольных сумм, указанных в файле отчета `skdpu_дата.html`, с контрольными суммами, указанными в Формуляре (см. таблица 3).

4.2 Установка СКДПУ

Установка СКДПУ должна происходить от имени суперпользователя осуществляется следующим образом:

Шаг 1. Добавить дистрибутивные носители ОС Astra Linux 1.6SE в настройки пакетного менеджера с помощью команды

```
apt-cdrom add
```

Шаг 2. Убедиться, что в настройках `/etc/apt/sources.list` есть записи о добавленных дисках, выполнив команду

```
cat /etc/apt/sources.list
```



В содержимом должны присутствовать записи о двух дисках дистрибутива ОС Astra Linux 1.6SE

- Шаг 3.** Вставить диск с дистрибутивом СКДПУ в дисковод и добавить его в настройки пакетного менеджера командой

```
apt-cdrom add
```

- Шаг 4.** Запустить скрипт установки `/mount/cdrom/autostart.sh`

- Шаг 5.** При успешном завершении будет предложено закончить установку вводом следующей команды

```
LANG=en_US.utf8 apt-get install -o Dpkg::options::="--force-conffold" skdpu
```

- Шаг 6.** Перезапустить систему командой `reboot`

При успешной установке СКДПУ должен быть доступен по IP-адресу сервера `https://<IP-сервера>`



Доступ через веб-интерфейс осуществляется под учетной записью администратора `admin` с паролем по умолчанию `admin`

При успешной установке СКДПУ готова к использованию сразу после перезагрузки, дальнейшее конфигурирование выполняется посредством веб-интерфейса СКДПУ в соответствии с RU.33654484.0004-02 91 01.



Перед началом работы необходимо убедиться, что запущены следующие сервисы: `postgresql, rabbitmq, apache2`

Если требуется изменить IP-адрес для системы, возможно исправить его в `/etc/network/interfaces` и перезагрузить систему командой `reboot`.

4.3 Фиксация контрольных сумм исполняемых файлов СКДПУ

После установки СКДПУ необходимо зафиксировать контрольные суммы исполняемых файлов СКДПУ, которые должны подвергаться периодическому контролю в процессе эксплуатации СКДПУ.

Фиксация контрольных сумм исполняемых файлов СКДПУ производится путем подсчета контрольных сумм исполняемых файлов СКДПУ по алгоритму «Уровень-3, программно» программой фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0», имеющей сертификат соответствия требованиям по безопасности информации №680.

Фиксация исходного состояния исполняемых файлов СКДПУ осуществляется следующим образом:

- Шаг 1.** Авторизоваться в консоли администрирования СКДПУ под учетной записью `wabadmin` и получить права суперпользователя (см. [Администрирование ОС после установки](#))

Шаг 2. Зафиксировать исходное состояние контролируемых файлов

```
ufix -jR /opt/skdpu/scripts/* /opt/wab/bin/* /opt/wab/sbin/* /  
opt/wab/lib/* > /home/wabadmin/skdpu_inst.txt  
ufix -e /home/wabadmin/skdpu_inst.txt /home/wabadmin/  
skdpu_inst.prj
```

Шаг 3. Печать файла отчета в файл формата html с помощью команды

```
ufix -h /home/wabadmin/skdpu_inst.prj /home/wabadmin/  
skdpu_inst.html
```

5 ДОСТУП К СКДПУ

5.1 Администрирование ОС после установки

При доступе к консоли администрирования СКДПУ по протоколу SSH необходимо указывать порт 2242.

Порядок получения доступа к учетной записи root после установки СКДПУ следующий:

- Шаг 1.** Ввести логин `wabadmin` с паролем по умолчанию `!QAZ2wsx`
- Шаг 2.** Выполнить команду `super` для доступа к учетной записи `wabsuper`
- Шаг 3.** Ввести пароль по умолчанию `!QAZ2wsx`
- Шаг 4.** Выполнить команду `sudo -i` для доступа к учетной записи `root`
- Шаг 5.** Ввести пароль по умолчанию `!QAZ2wsx`



При первоначальном входе в систему, необходимо изменить пароли пользователей консоли `wabadmin` и `wabsuper` с помощью команды `passwd`

Для выполнения требований разграничения полномочий, значения паролей пользователей `wabadmin` и `wabsuper` не должны совпадать. Новые пароли необходимо выбирать согласно требованиям парольной политики, а после успешной замены надежно и безопасно сохранить. В случае утери паролей их восстановление значительно затруднено и в результате может потребоваться переустановка ОС.

5.2 Доступ к веб-интерфейсу СКДПУ

Для доступа к веб-интерфейсу необходимо выполнить следующую последовательность действий:

- Шаг 1.** Открыть веб-браузер.

Шаг 2. В адресной строке веб-браузера ввести следующее значение: *https://skdpu_ip_address*, где *skdpu_ip_address* – IP-адрес СКДПУ.



Веб-браузер должен быть настроен для принятия файлов cookies и запуска JavaScript.

В окне веб-браузера появится окно авторизации пользователя СКДПУ (см. рисунок 21).

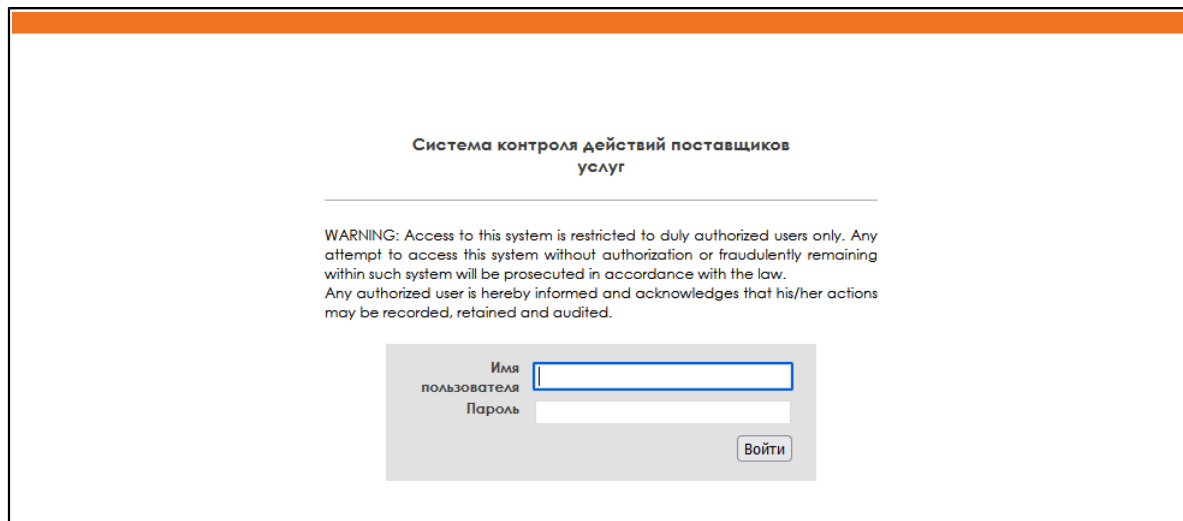


Рисунок 21 – Страница входа

Шаг 3. Для получения доступа к веб-интерфейсу пользователя в окне авторизации необходимо указать имя пользователя (логин) в поле **Имя пользователя** и пароль в поле **Пароль**, предоставленные администратором СКДПУ.

Шаг 4. Нажать кнопку **Войти**.

Если вход в систему будет выполнен успешно, то на экране отобразится главная страница СКДПУ.

В боковом меню представлены доступные действия. Содержимое бокового меню зависит от профиля пользователя и от назначенных прав доступа

5.3 Настройка подключения к почтовому серверу

Для осуществления отправки уведомлений и отчетов уполномоченным лицам необходимо настроить подключение к почтовому серверу

Шаг 1. Перейти в раздел веб-интерфейса **Система > Почтовый сервер**

Шаг 2. Заполнить необходимые параметры подключения.



При необходимости следует задать IP адрес DNS-сервера в разделе веб-интерфейса **Система > Сеть**

5.4 Добавление файла лицензии

По умолчанию СКДПУ функционирует в режиме демонстрации. Чтобы это исправить, необходимо загрузить файл лицензии

Шаг 1. Перейти в раздел **Конфигурация > Лицензия**

Шаг 2. Получить контекст-файл, нажав на **Скачать контекст-файл**

Шаг 3. Связаться с технической поддержкой и передать полученный контекст-файл специалисту технической поддержки

Шаг 4. Получить от специалиста технической поддержки файл лицензии

Шаг 5. Загрузить полученный файл лицензии нажатием на **Обзор** с последующим выбором файла лицензии

Шаг 6. Обновить лицензию нажатием на **Обновить лицензию**

5.5 Включение режима ЗПС ОС Astra Linux 1.6SE

Если планируется применять режим ЗПС, то его необходимо включить в разделе мониторинга операционной системы ОС Astra Linux 1.6SE и проверить, что все необходимые компоненты СКДПУ успешно обрабатывают без ошибок в мониторинге ЗПС.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

AMQP	Advanced Message Queuing Protocol — открытый протокол прикладного уровня для передачи сообщений между компонентами системы. Основная идея состоит в том, что отдельные подсистемы (или независимые приложения) могут обмениваться произвольным образом сообщениями через AMQP-брокер, который осуществляет маршрутизацию, возможно гарантирует доставку, распределение потоков данных, подписку на нужные типы сообщений.
API	Application Programming Interface — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
CLI	Command-Line Interface — разновидность текстового интерфейса (TUI) между человеком и компьютером, в котором инструкции компьютеру даются в основном путём ввода с клавиатуры текстовых строк (команд), в UNIX-системах возможно применение мыши.
CSV	Comma-Separated Values - текстовый формат, предназначенный для представления табличных данных.
DHCP	Dynamic Host Configuration Protocol — прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.
DNS	Domain Name System «система доменных имён» — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись).
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	HyperText Transfer Protocol Secure - расширение протокола HTTP, поддерживающее шифрование.
IPTABLES	Утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux, начиная с версии 2.4.
JSON	JavaScript Object Notation — текстовый формат обмена данными, основанный на JavaScript.

JWT	JSON Web Token (JWT) — это открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON.
LAN	Local Area Network (локальная компьютерная сеть)
LVM	Logical Volume Manager — подсистема операционных систем Linux и OS/2, позволяющая использовать разные области одного жёсткого диска и/или области с разных жёстких дисков как один логический том.
NTLM	NT LAN Manager — протокол сетевой аутентификации, разработанный фирмой Microsoft для Windows NT.
OCR	Optical character recognition - механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные - последовательность кодов, использующихся для представления символов в компьютере (например, в текстовом редакторе).
RDP	Remote Desktop Protocol, протокол удаленного рабочего стола
REST	Representational State Transfer — архитектурный стиль взаимодействия компонентов распределённого приложения в сети. REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределённой гипермедиа-системы.
RFB	Remote FrameBuffer — простой клиент-серверный сетевой протокол прикладного уровня для удалённого доступа к графическому рабочему столу компьютера, используемый в VNC.
RFC	Request for Comments, рабочее предложение – стандарты Интернета в части реализаций.
RLOGIN	Remote LOGIN (удалённый вход в систему)
SCP	Secure Copy Protocol — утилита и протокол копирования файлов между компьютерами, использующий, в отличие от утилиты RCP, в качестве транспорта не RSH, а зашифрованный SSH.
SFTP	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты — это широко используемый сетевой протокол,

	предназначенный для передачи электронной почты в сетях TCP/IP.
SSH	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
SSL	Secure Sockets Layer (уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
SSO	Single Sign-On — технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации.
TACACS+	TACACS+ (Terminal Access Controller Access Control System plus) — сеансовый протокол, результат дальнейшего усовершенствования TACACS, предпринятого Cisco.
TCP	Transmission Control Protocol (TCP, протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.
TELNET	TErminaL NETwork - сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP)
TLS	Transport Layer Security — протокол защиты транспортного уровня
UTF-8	Unicode Transformation Format, 8-bit — «формат преобразования Юникода, 8-бит» — распространённый стандарт кодирования символов, позволяющий более компактно хранить и передавать символы Юникода, используя переменное количество байт (от 1 до 4), и обеспечивающий полную обратную совместимость с 7-битной кодировкой ASCII. Стандарт UTF-8 официально закреплён в документах RFC 3629 и ISO/IEC 10646 Annex D.
VNC	Virtual Network Computing - система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).
APM	Автоматизированное рабочее место

ЗПС	Закрытая программная среда
ОС	Операционная система
ПО	Программное обеспечение

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Выбор языка установки.....	8
Рисунок 2 – Выбор текстового режима установки.....	8
Рисунок 3 – Выбор языка установки.....	9
Рисунок 4 – Выбор параметров локализации.....	9
Рисунок 5 – Лицензионное соглашение ОС.....	9
Рисунок 6 – Выбор раскладки клавиатуры.....	10
Рисунок 7 – Задание имени хоста.....	10
Рисунок 8 – Создание пользователя.....	11
Рисунок 9 – Подтверждение пароля.....	11
Рисунок 10 – Задание часового пояса.....	11
Рисунок 11 – Разметка дискового пространства.....	12
Рисунок 12 – Создание загрузочной области.....	13
Рисунок 13 – Создание LVM.....	13
Рисунок 14 – Запуск процесса разбиения диска с установленными параметрами.....	15
Рисунок 15 – Выбор дополнительного ПО при установке ОС Astra Linux 1.6SE.....	15
Рисунок 16 – Дополнительные настройки ОС.....	16
Рисунок 17 – Установка модуля GRUB.....	16
Рисунок 18 – Окончание установки.....	16
Рисунок 19 – Ввод логина ОС Astra Linux 1.6SE.....	16
Рисунок 20 – Получение ip-адреса.....	17
Рисунок 21 – Страница входа.....	22

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Основные возможности СКДПУ.....	3
Таблица 2 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ.....	5
Таблица 3 – Пример разметки разделов.....	14

