



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ
«НОВЫЕ ТЕХНОЛОГИИ»
Версия: 2.1.58**

Руководство по установке

RU.33654484.0001-01 91 02

Листов 36

АННОТАЦИЯ

Настоящий документ является руководством по установке изделия Программный комплекс «Система контроля действий поставщиков ИТ-услуг «Новые Технологии» (далее – СКДПУ НТ).

Данный документ содержит сведения о назначении и условиях применения СКДПУ НТ. Документ содержит описание действий по установке СКДПУ НТ, а также настройке необходимых компонентов среды функционирования.

СОДЕРЖАНИЕ

1 Условия функционирования.....	4
1.1 Общие сведения.....	4
1.2 Оценка объема хранилища данных.....	4
1.3 Сервисы СКДПУ НТ и среда функционирование.....	4
1.4 Требования к техническим и программным средствам.....	5
1.5 Настройка сети.....	6
2 Установка ОС Astra Linux 1.6SE.....	8
2.1 Начало процесса установки ОС Astra Linux 1.6SE.....	8
2.2 Разметка диска ОС Astra Linux 1.6SE под установку СКДПУ НТ.....	11
2.3 Процесс установки ОС Astra Linux 1.6SE.....	18
2.4 Настройка ОС Astra Linux 1.6SE.....	19
3 Установка СКДПУ НТ.....	21
3.1 Проверка целостности дистрибутива СКДПУ НТ.....	21
3.2 Процесс установки СКДПУ НТ.....	21
3.3 Фиксация контрольных сумм исполняемых файлов СКДПУ НТ.....	23
4 Начало работы с СКДПУ НТ.....	25
4.1 Доступ к СКДПУ НТ.....	25
4.1.1 Доступ к консоли администрирования.....	25
4.1.2 Доступ к веб-интерфейсу СКДПУ НТ.....	25
4.2 Настройка источников данных.....	26
4.3 Добавление файла лицензии.....	28
4.4 Обновление СКДПУ НТ.....	29
4.5 Настройка подключения к почтовому серверу.....	30
4.6 Включение режима ЗПС ОС Astra Linux 1.6SE.....	30
4.7 Встроенные правила сетевого фильтра.....	30
Перечень сокращений.....	31
Перечень рисунков.....	34
Перечень таблиц.....	35
История изменений.....	36

1 УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ

1.1 Общие сведения

СКДПУ НТ представляет собой серверное приложение, функционирующее на UNIX-платформе, реализованной в виде сервера под управлением ОС Astra Linux 1.6SE. Пользовательский интерфейс СКДПУ НТ реализован в форме веб-интерфейса, доступного через браузер.

Браузер должен быть установлен перед началом работы с СКДПУ НТ. Для корректной работы СКДПУ НТ рекомендуется в настройках браузера разрешить выполнение javascript и сохранение файлов cookies.

СКДПУ НТ имеет информационное сопряжение с веб-сервером HTTP Apache и СУБД PostgreSQL для обеспечения передачи и хранения данных.

1.2 Оценка объема хранилища данных

Рекомендуется использовать быстродействующее хранилище емкостью не менее 30 ГБ для области `/var/log/`, так как там хранятся лог файлы системы.

Объем места для хранения данных пользовательских сессий целевых систем рекомендуется оценивать с помощью пилотного проекта на реальных площадках, поскольку средний объем данных в сеансе зависит от сценариев использования и его сложно оценить заранее.



Рекомендуется планировать развертывание СКДПУ НТ с учетом возможности увеличения объема памяти, необходимого для хранения данных пользовательских сессий целевых систем

Если объем обрабатываемых пользовательских сессий целевых систем будет превышать отметку в 10000 сессий в день, то рекомендуется использовать накопители с высокими показателями пропускной способности для системы и хранилища с высоким IOPS для системы и хранилища, то есть RAID10 с 6+ дисков SAS или SSD.

Рекомендуется планировать inode с файловыми системами ext3 и ext4 или использовать файловую систему XFS для области `skdpu-nt-data`.

Для хранения 1 млн сеансов 50/50 RDP (без видеозаписей) и SSH требуется около 100 ГБ объема хранилища (с индексами).

1.3 Сервисы СКДПУ НТ и среда функционирования

таблица 1 содержит информацию о перечне сервисов СКДПУ НТ и среде функционирования с описанием выполняемых ими функций.

Таблица 1 – Перечень сервисов

Наименование сервиса	Описание
СКДПУ НТ	

Наименование сервиса	Описание
analysed	Оповещение о поступлении на обработку новых данных пользовательских сессий и проведение анализа на предмет наличия признаков аномального поведения пользователей шлюзов доступа. Регистрация обнаруженных инцидентов
collectd	Обработка полученных данных пользовательских сессий целевых систем от доступных шлюзов доступа, регистрация обнаруженных событий
indexd	Индексирование данных пользовательских сессий целевых систем, поступающих от шлюзов доступа, и их размещение в среде функционирования в виде текстовых файлов
enrichd	Регистрация событий безопасности, получаемых от систем сторонних производителей
jobrunnerd	Генерирование отчетов, структура которых соответствует предварительно выбранным шаблонам, и их отправка по электронной почте в соответствии с выбранными профилями выполнения
Среда функционирования	
Брокер сообщений RabbitMQ	Организация надежного информационного обмена сообщениями между подсистемами СКДПУ НТ. Обеспечение высокой надежности сохранения обрабатываемых данных и распределение нагрузки в процессе анализа большого объема данных
Syslog-NG	Прием данных пользовательских сессий целевых систем, а также генерация записей файлов журналов событий СКДПУ НТ
БД PostgreSQL	Обеспечение хранения индексируемых данных пользовательских сессий целевых систем, инцидентов, а также метаданных отчетов
Почтовый сервер SMTP	Доставка отчетов и оповещений уполномоченным лицам

1.4 Требования к техническим и программным средствам

В [таблице 2](#) содержатся минимальные характеристики программного и аппаратного обеспечения для развертывания сервера СКДПУ НТ.

[Таблица 2](#) – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ НТ

Компонент	Описание
Процессор	Архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA

Компонент	Описание
Интерфейсы	Интерфейс для подключения к LAN
ОС	ОС Astra Linux 1.6SE
Веб-сервер	HTTP Apache 2.4
База данных	СУБД PostgreSQL версии 9.6
Брокер сообщений	RabbitMQ версии 3.6
Другое ПО	Интерпретаторы языка программирования Python 3.5
	Библиотеки Python, обеспечивающие удовлетворение зависимостей для *.py части ПО
	Набор библиотек и средств в составе Erlang OTP версии 19.2

1.5 Настройка сети

СКДПУ НТ необходимо получать события системного журнала от Шлюзов доступа по протоколу syslog и отправлять уведомления по электронной почте. Пользователям СКДПУ НТ также необходимо получить доступ к веб-интерфейсу СКДПУ НТ со своих рабочих станций.



Рекомендуется настроить подключение к серверу NTP, чтобы синхронизировать системное время для корректной работы механизмов отчетности и анализа

В целях корректного функционирования СКДПУ НТ необходимо установить разрешения на сетевые соединения (см. [таблицу 3](#)).

Таблица 3 – Перечень настроек портов брандмауэра

Номер порта	Протокол прикладного уровня	Протокол транспортного уровня	Примечания
22	SSH	TCP	Доступ к консоли администрирования СКДПУ НТ
25	SMTP	TCP	Сетевое взаимодействие с почтовым сервером для отправки уведомлений
53	DNS	TCP, UDP	Сетевое взаимодействие с серверами DNS
80	HTTP	TCP	Доступ к веб-интерфейсу СКДПУ НТ
123	NTP	UDP	Синхронизация системного времени
389	LDAP	TCP, UDP	Обеспечение внешней авторизации с помощью службы каталогов LDAP
443	HTTPS	TCP	Доступ к веб-интерфейсу СКДПУ НТ
465	SMTP с проверкой подлинности	TCP	Сетевое взаимодействие с почтовым сервером для отправки уведомлений
514	syslog	TCP, UDP	Сетевое взаимодействие для отправки логов в формате syslog

Номер порта	Протокол прикладного уровня	Протокол транспортного уровня	Примечания
515	syslog	TCP, UDP	Сетевое взаимодействие для отправки логов в формате syslog
587	SMTP+STARTTLS	TCP	Сетевое взаимодействие с почтовым сервером для отправки уведомлений
636	LDAPS	TCP	Обеспечение внешней авторизации с помощью службы каталогов LDAP

2 УСТАНОВКА ОС ASTRA LINUX 1.6SE

Для установки программного обеспечения подготовьте ОС и программное и аппаратное обеспечение с минимальными характеристиками для развертывания сервера.

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

2.1 Начало процесса установки ОС Astra Linux 1.6SE

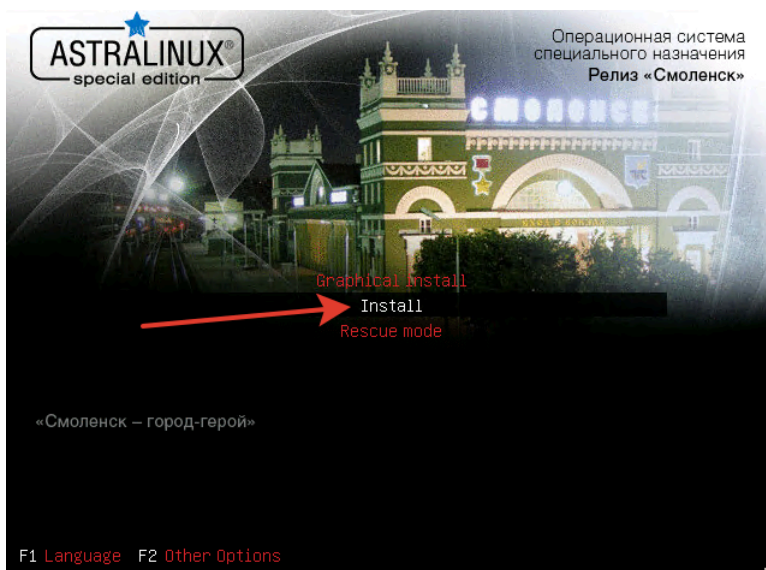
Шаг 1. Установить носитель в устройство считывания дисков.

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.

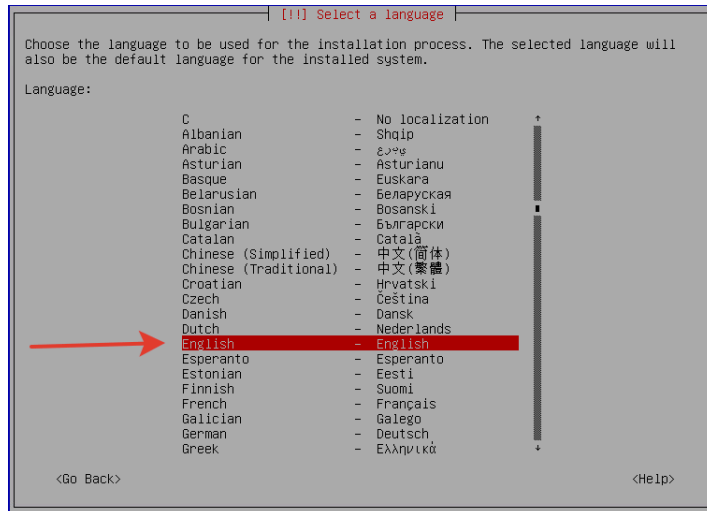
Шаг 3. В появившемся интерфейсе автозагрузки выбирать язык English



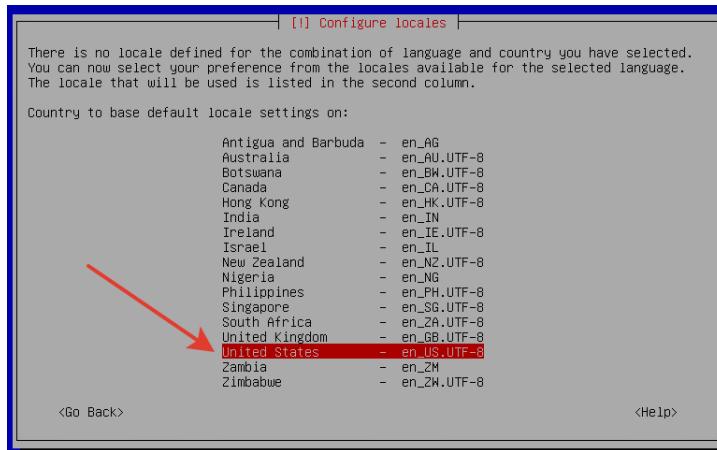
Шаг 4. Выбрать в меню вариант *Установка без графического интерфейса* **Install**



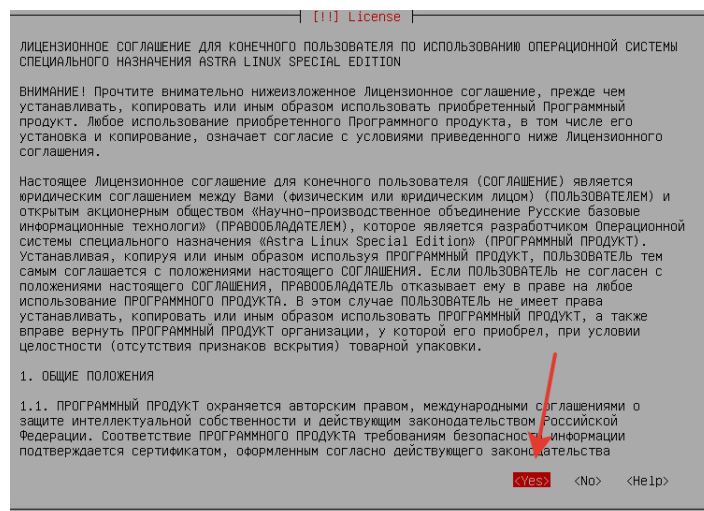
Шаг 5. Выбрать язык



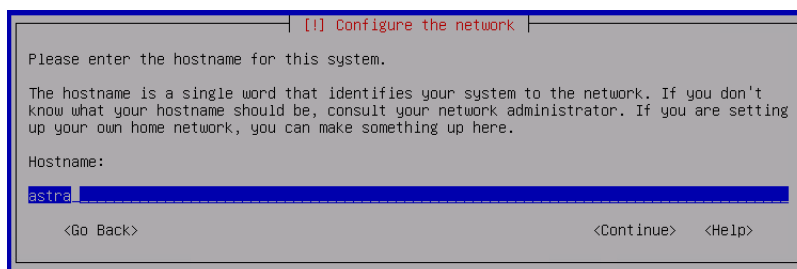
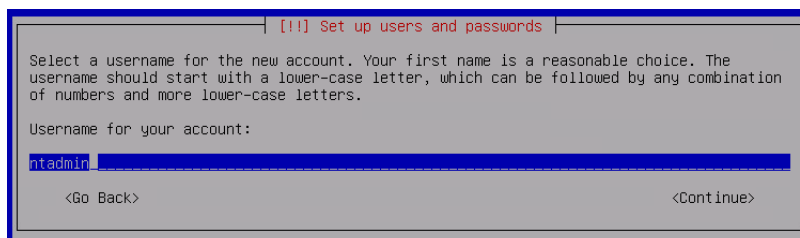
Шаг 6. Сконфигурировать локализацию



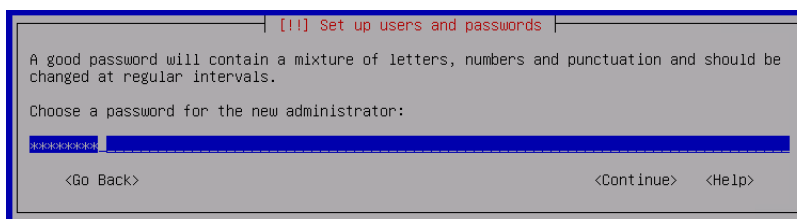
Шаг 7. Принять лицензионное соглашение



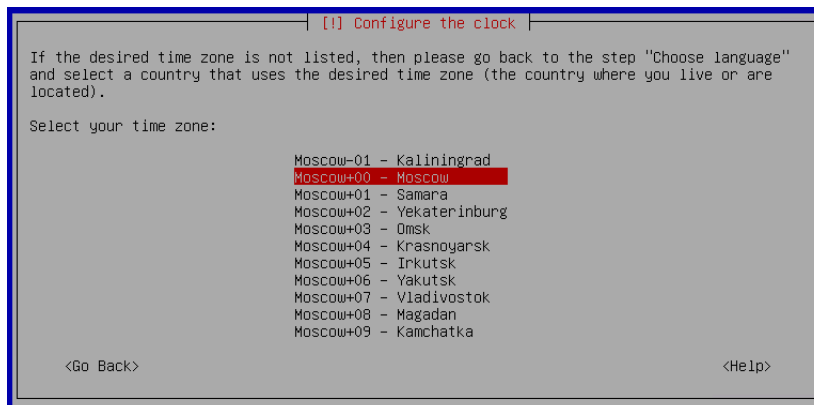
Шаг 8. Выбрать раскладку клавиатуры

Шаг 9. После загрузки первичных пакетов ввести имя хоста `astra`, `skdpu-nt` или хостнейм, используемый в организацииШаг 10. Создать пользователя `ntadmin` и задать для него пароль `ntadmin!`

Шаг 11. Подтвердить пароль повторным вводом



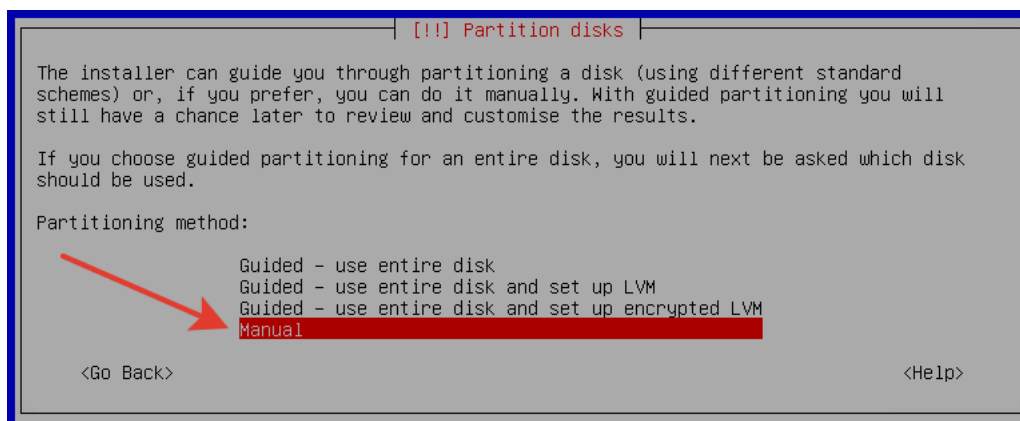
Шаг 12. Выбрать часовой пояс



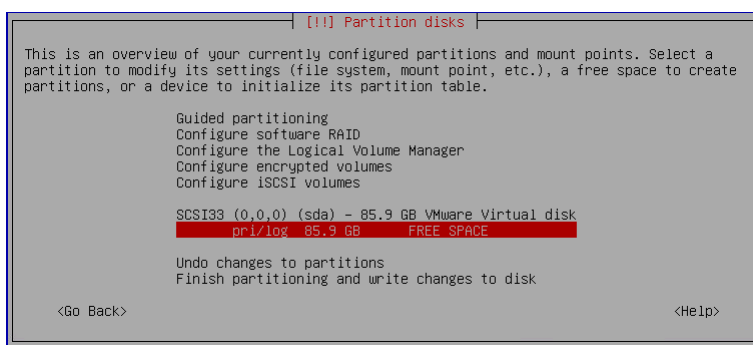
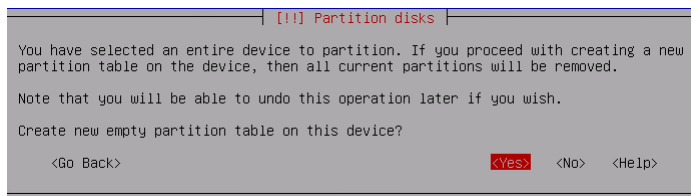
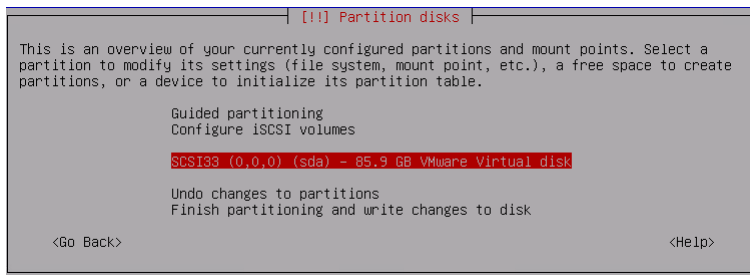
2.2 Разметка диска ОС Astra Linux 1.6SE под установку СКДПУ НТ

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

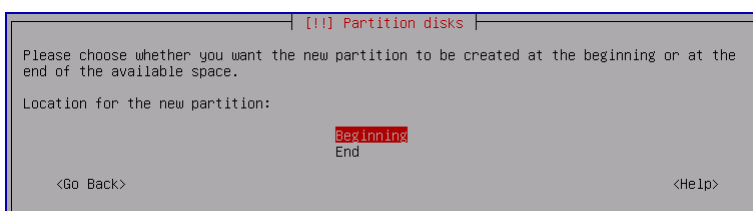
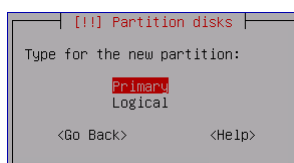
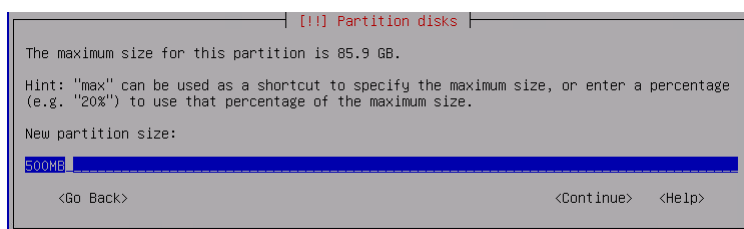
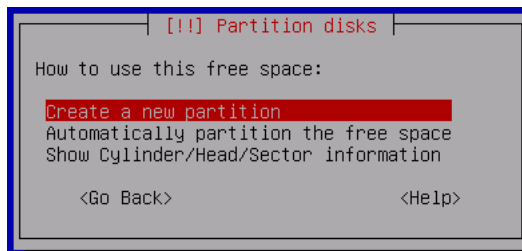
Шаг 1. Выбрать ручной режим разметки



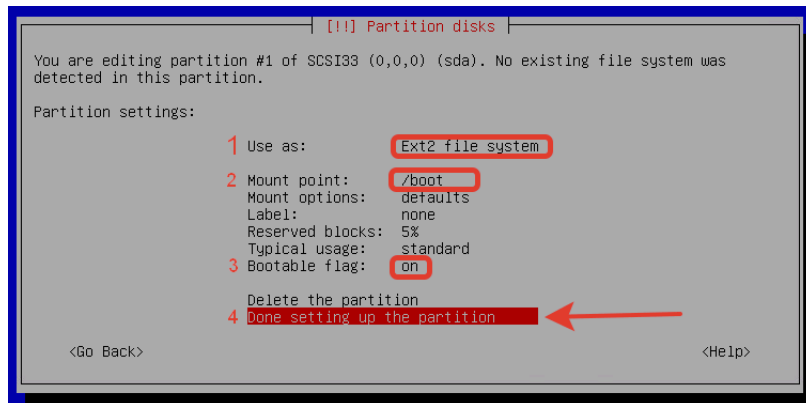
Шаг 2. Выбрать область для разметки



Шаг 3. Создать новую партицию размером 500 Мб

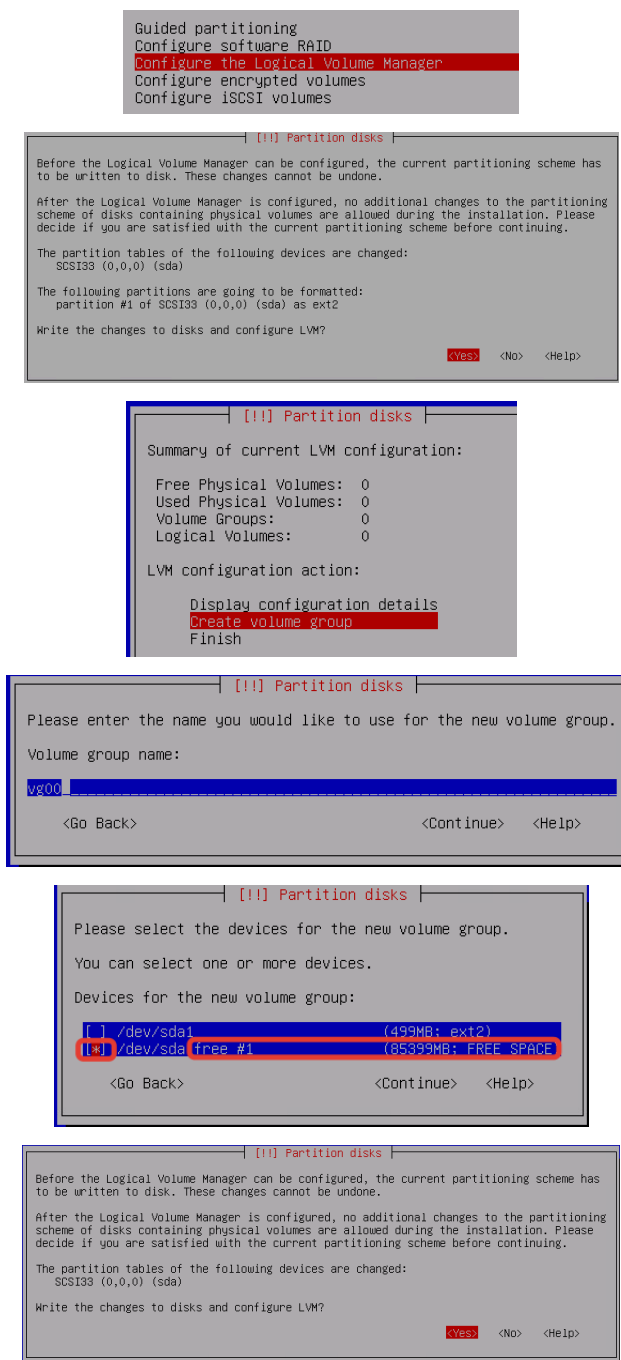


Шаг 4. Создать в главной партии физический раздел /boot – 500МВ, файловой системой ext2 и точкой монтирования /boot.



Обязательно проставьте флаг автозагрузки.

Шаг 5. Создать LVM с названием `vg00`. В качестве места создания обязательно ставим отметку напротив незанятого пространства.



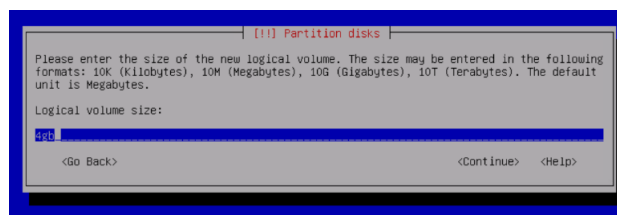
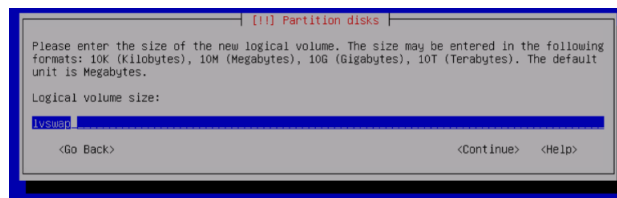
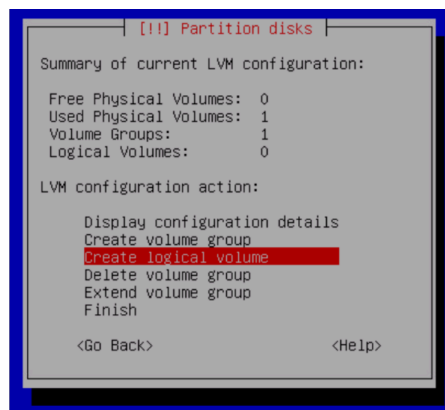
Шаг 6. Внутри LVM создать логические партиции (пример см. [таблицу 4](#))

Таблица 4 – Пример разметки разделов

Имя раздела	Размер	Точка монтирования	Тип файловой системы
/boot	500 MB	/boot	Ext2, флаг автозагрузки
Логические разделы LVM <code>vg00</code>			
lvroot	15 GB	/	Ext3 или Ext4

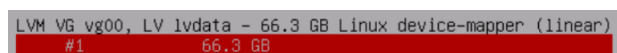
Имя раздела	Размер	Точка монтирования	Тип файловой системы
lvvar	15 GB	/var	Ext3 или Ext4
lvopt	15 GB	/opt	Ext3 или Ext4
lvswap	4 GB	-	Swap area
lvfree	100 MB	-	Do not use
lvdata	все оставшееся место	/opt/skdpu-nt-data	Ext4

Шаг 1. Создание логического тома, вводим название и размер



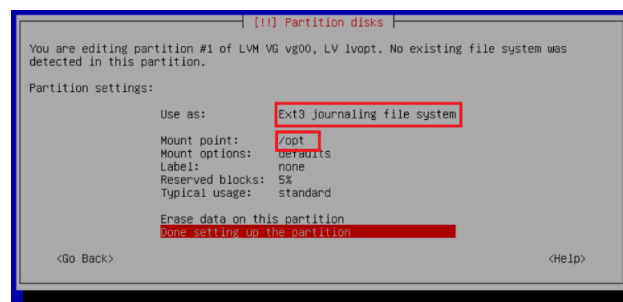
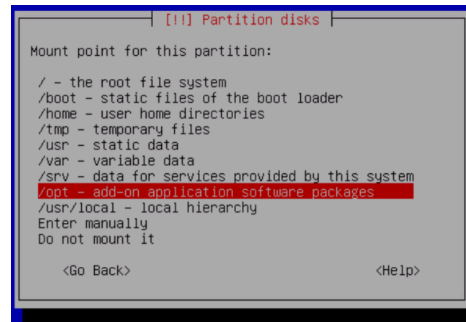
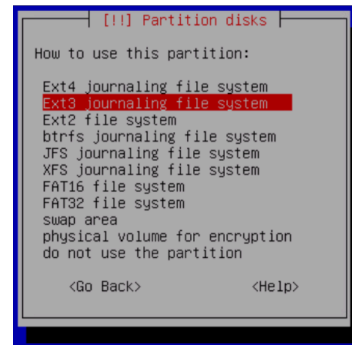
Аналогично создаются все необходимые тома.

Шаг 2. Для перехода в настройки выбора файловой системы и точки монтирования выбираем строку с размером партии

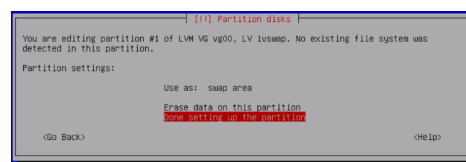
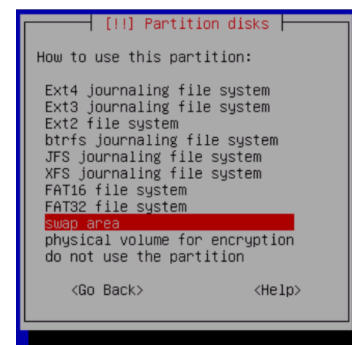


Разметка lvm для разделов lvroot, lvvar и lvopt настраивается аналогично.

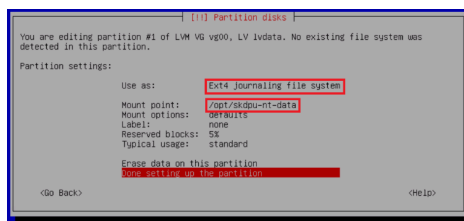
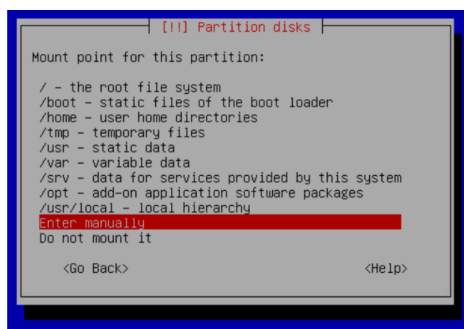
Шаг 3. Выбор файловой системы и точки монтирования:



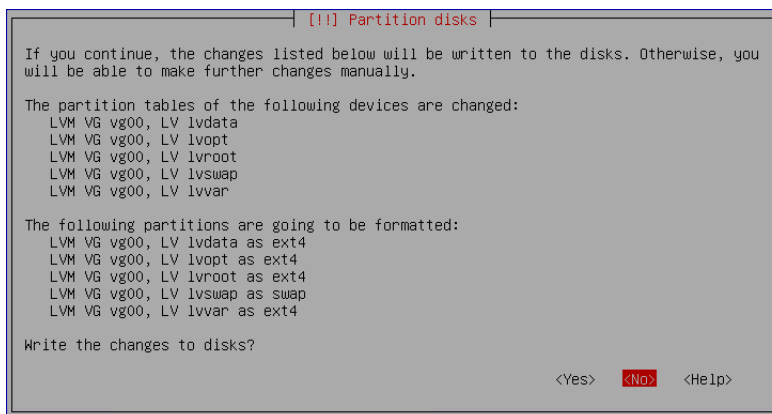
Для раздела `lvswap` из списка выбираем из списка `swap area` без точки монтирования.



Для раздела `lvdata` выбираем файловую систему `Ext4` из списка, аналогично предыдущим, точку монтирования задаем вручную.



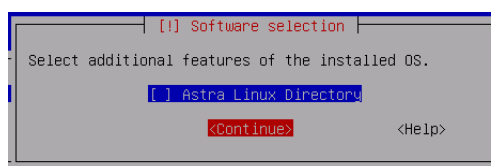
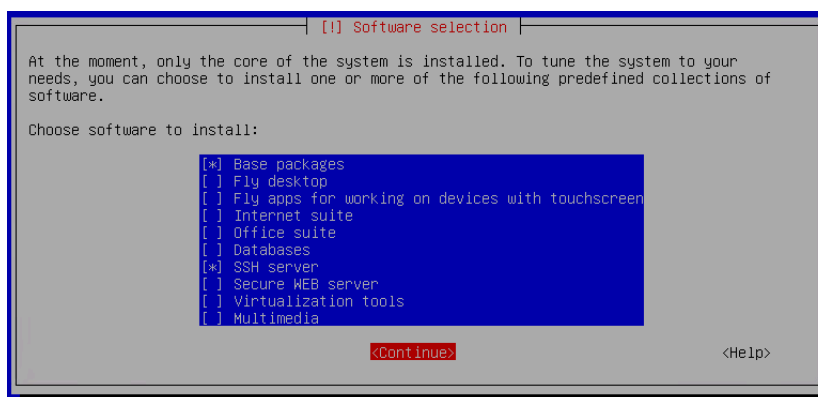
Шаг 7. После создания и задания параметров логических разделов выбираем **Finish ... and write to disk** и запускаем программу разметки диска по принятым параметрам.



Далее ждем установки основных пакетов ОС Astra Linux 1.6SE.

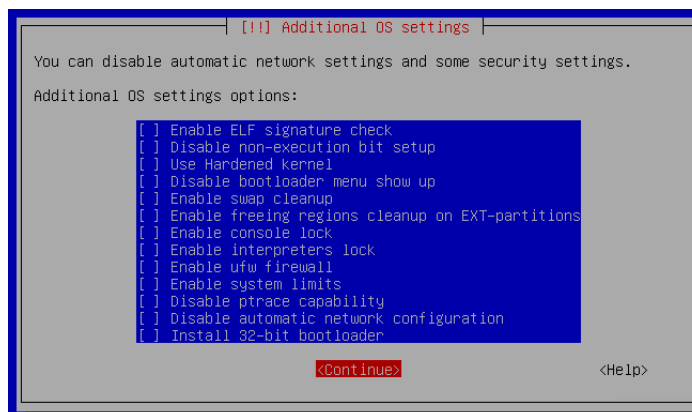
2.3 Процесс установки ОС Astra Linux 1.6SE

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

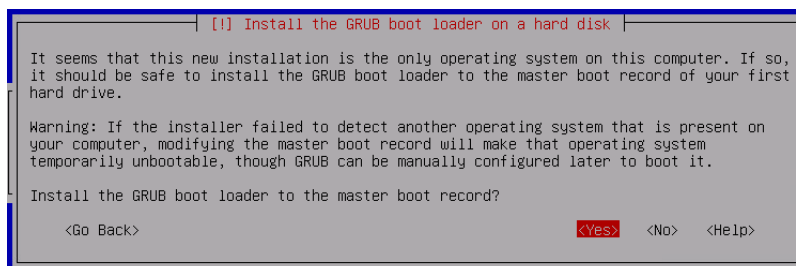


В результате чего произойдет установка минимально требуемого набора инструментов и функций ОС Astra Linux 1.6SE, что существенно сэкономит время установки и место на диске

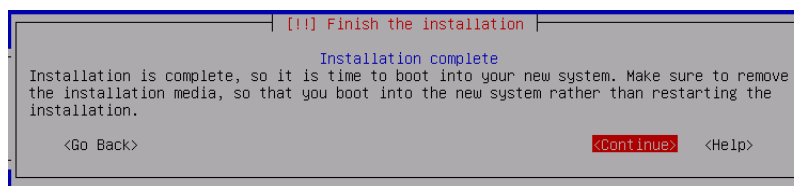
Шаг 2. Снять выделения со всех дополнительных настроек



Шаг 3. Установить загрузчик GRUB и указать для него пароль



Шаг 4. При появлении сообщения **Installation complete**, прежде чем нажимать **Continue**, необходимо извлечь диск из привода



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

```
Astra Linux SE 1.6 (smolensk)
tty1
astra login: _
```

2.4 Настройка ОС Astra Linux 1.6SE

При необходимости, для обновления СКДПУ НТ следует выполнить следующие шаги:

Шаг 1. Авторизоваться под созданным ранее пользователем **ntadmin**

i | Для **Integrity level** указать значение 63

Шаг 2. Получить права суперпользователя через `sudo -i`.

Шаг 3. Внести изменения в сетевые настройки

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

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

```
auto eth0
iface eth0 inet static
address <ip_ПК_СКДПУ_НТ>
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`

```
systemctl restart networking.service
```

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:~# !
```

Шаг 7. Добавить сервис SSH в автозагрузку и запустить:

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



Инструкции по установке обновлений ОС Astra Linux 1.6SE поставляются совместно с дисками обновлений

3 УСТАНОВКА СКДПУ НТ

Перед установкой СКДПУ НТ необходимо авторизоваться под учетной записью `ntadmin`, предварительно убедившись, что в ОС Astra Linux 1.6SE создана учетная запись `ntadmin` командой `w`.

3.1 Проверка целостности дистрибутива СКДПУ НТ

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

Необходимо выполнить следующие шаги:

Шаг 1. Вставить носитель с дистрибутивом СКДПУ НТ в дисковод, смонтировать диск

Шаг 2. Получить права суперпользователя через `sudo -i`.

Шаг 3. Зафиксировать исходное состояние контролируемых файлов, расположенных в директории `/media/cdrom/repo/` командами

```
ufix -jR /media/cdrom/repo/* > /home/ntadmin/skdpu_nt.txt
ufix -e /home/ntadmin/skdpu_nt.txt /home/ntadmin/skdpu_nt.prj
```

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

```
ufix -h /home/ntadmin/skdpu_nt.prj /home/ntadmin/
skdpu_nt_data.html
```

Шаг 5. Сверка контрольных сумм, указанных в файле отчета `skdpu_nt.html`, с контрольными суммами, указанными в Формуляре в таблице 3.

3.2 Процесс установки СКДПУ НТ

Для установки СКДПУ НТ необходимо выполнить следующие шаги:

Шаг 1. Произвести вход по SSH на сервер СКДПУ НТ под пользователем `ntadmin`

Шаг 2. Повысить права доступа до суперпользователя с помощью команды `sudo -i`

Шаг 3. Вставить диск с дистрибутивом ОС Astra Linux 1.6SE

- Шаг 4. Добавить дистрибутивные носители ОС Astra Linux 1.6SE в настройки пакетного менеджера с помощью команды

```
apt-cdrom add
```

```
root@astral6-1:~# apt-cdrom add
Using CD-ROM mount point /media/cdrom/
Unmounting CD-ROM...
Waiting for disc...
Please insert a Disc in the drive and press [Enter]
Mounting CD-ROM...
Identifying... [802e821308ebcaedca97ac0ccc9934fd-2]
Scanning disc for index files...
Found 3 package indexes, 0 source indexes, 0 translation indexes and 1 signatures
This disc is called:
'OS Astra Linux 1.6 smolensk - amd64 DVD '
Copying package lists...gpgv: Signature made Wed 20 Jun 2018 06:52:14 PM MSK
gpgv:         using RSA key 7A7A24A559D1F7A9C9FA1F9A7DB1E284F89C2962
gpgv: Good signature from "JSC RPA RusBITech (REPOSITORY RBT KEY 2018) <mail@rusbitech.ru>"
Reading Package Indexes... Done
Writing new source list
Source list entries for this disc are:
deb cdrom:[OS Astra Linux 1.6 smolensk - amd64 DVD ]/ smolensk contrib main non-free
Unmounting CD-ROM...
Repeat this process for the rest of the CDs in your set.
root@astral6-1:~#

root@astral6-1:~# apt-cdrom add
Using CD-ROM mount point /media/cdrom/
Unmounting CD-ROM...
Waiting for disc...
Please insert a Disc in the drive and press [Enter]
Mounting CD-ROM...
Identifying... [fe085f71241f1665e30906belc7fb9d9-2]
Scanning disc for index files...
Found 3 package indexes, 0 source indexes, 0 translation indexes and 1 signatures
Found label 'OS Astra Linux 1.6 smolensk-devel - amd64 DVD'
This disc is called:
'OS Astra Linux 1.6 smolensk-devel - amd64 DVD'
Copying package lists...gpgv: Signature made Wed 20 Jun 2018 07:04:31 PM MSK
gpgv:         using RSA key 7A7A24A559D1F7A9C9FA1F9A7DB1E284F89C2962
gpgv: Good signature from "JSC RPA RusBITech (REPOSITORY RBT KEY 2018) <mail@rusbitech.ru>"
Reading Package Indexes... Done
Writing new source list
Source list entries for this disc are:
deb cdrom:[OS Astra Linux 1.6 smolensk-devel - amd64 DVD]/ smolensk contrib main non-free
Unmounting CD-ROM...
Repeat this process for the rest of the CDs in your set.
root@astral6-1:~#
```

- Шаг 5. Убедиться, что в настройках `/etc/apt/sources.list` есть записи о добавленных дисках, выполнив команду

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

```
root@astral6-1:~# vi /etc/apt/sources.list
root@astral6-1:~# cat /etc/apt/sources.list
deb cdrom:[OS Astra Linux 1.6 smolensk-devel - amd64 DVD]/ smolensk contrib main non-free
deb cdrom:[OS Astra Linux 1.6 smolensk - amd64 DVD ]/ smolensk contrib main non-free
```



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

- Шаг 6. Вставить диск с дистрибутивом СКДПУ НТ в дисковод и добавить в `/etc/apt/sources.list` запись вида:

```
deb file:///media/cdrom/repo ./
```

- Шаг 7. Сохранить изменения

Шаг 8. Выполнить команду

```
mount /dev/cdrom
apt-get update
```

Шаг 9. При отсутствии ошибок произвести установку СКДПУ НТ

```
apt-get install skdpu-nt
```



При установке apt подсистема может просить предоставлять необходимые диски с пакетами ОС Astra Linux 1.6SE.

Шаг 10. После окончания установки СКДПУ НТ проверить работу сервисов СКДПУ НТ с помощью команды

```
/opt/skdpu-nt/bin/nt-status
```

```
Server: skdpunt-test1
Uptime: 110 days, 19:25:01.564547
Load averages: 6.03 6.11 6.05
CPU: 6 cores detected
      0      1.0      1.0
      1      3.0      1.0
      2      0.0      0.0
      3     65.0      0.0
      4      0.0      0.0
      5     58.0      1.0
Total memory: 7.7GB
Available: 2.65GB
Used: 5.04GB 65.5%
Swap: 2.0GB
Free: 803.53MB 60.7%
Filesystem: /
Total: 76.27GB
Used: 63.27GB 87.4%
Process: analysed is running (389)
CPU usage: 0.0%
Memory usage: 604.93MB
Process: jobrunnerd is running (10537)
CPU usage: 0.0%
Memory usage: 851.0MB
Process: indexd is running (13225)
CPU usage: 0.0%
Memory usage: 161.62MB
Process: collectd is running (13100)
CPU usage: 0.0%
Memory usage: 288.5MB
Process: enrichd is running (13922)
CPU usage: 0.0%
Memory usage: 299.46MB
Syslog listener status: enabled
```

3.3 Фиксация контрольных сумм исполняемых файлов СКДПУ НТ

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

Фиксация контрольных сумм исполняемых файлов СКДПУ НТ производится путем подсчета контрольных сумм исполняемых файлов СКДПУ НТ по алгоритму «Уровень-3, программно» программой фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0».

Фиксация исходного состояния исполняемых файлов СКДПУ НТ осуществляется следующим образом:

Шаг 1. Получить права суперпользователя через последовательное выполнение команд `super` и `sudo -i`.

Шаг 2. Зафиксировать исходное состояние исполняемых файлов

```
ufix -jR -I*__pycache__* /opt/skdpu-nt/bin/* /opt/skdpu-nt/lib/*  
> /home/ntadmin/skdpu_nt_inst.txt  
ufix -e /home/ntadmin/skdpu_nt_inst.txt /home/ntadmin/  
skdpu_nt_inst.prj
```

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

```
ufix -h /home/ntadmin/skdpu_nt_inst.prj /home/ntadmin/  
skdpu_nt_inst_data.html
```

4 НАЧАЛО РАБОТЫ С СКДПУ НТ

i Перед началом работы необходимо убедиться с помощью команды `systemctl status`, что запущены следующие сервисы: `postgresql`, `rabbitmq`, `apache2`

4.1 Доступ к СКДПУ НТ

4.1.1 Доступ к консоли администрирования

Учетная запись `ntadmin` - это учетная запись с низкими правами, которой разрешен вход в консоль и вход по протоколу SSH на сервер СКДПУ НТ.

Учетная запись `ntsuper` является более привилегированной, и для данной учетной записи разрешено повышение прав до суперпользователя через последовательное выполнение команд `super` и `sudo -i`.

Перечисленные учетные записи обладают следующими паролями по умолчанию:

- `ntadmin` с паролем `ntadmin!`
- `ntsuper` с паролем `ntsuper!`

Чтобы получить права суперпользователя в консоли администрирования СКДПУ НТ, необходимо производить авторизацию следующим образом:

Шаг 1. Произвести вход в консоль ОС под пользователем `ntadmin`

Шаг 2. Повысить права доступа до пользователя `ntsuper` с помощью команды `super`.

Шаг 3. Выполнить команду `sudo -i` для доступа к учетной записи суперпользователя

i Данный порядок действует как для локального доступа непосредственно к серверу СКДПУ НТ, так и при доступе по сети (по протоколу SSH).

При первом входе ОС будет требовать замены паролей по умолчанию на новые. Необходимо изменить пароли для учетных записей и надежно сохранить новые пароли, так как их аварийный сброс будет представлять сложность и требовать остановки функционирования системы.


i При необходимости, пароли можно поменять штатно при помощи команды `passwd` в консоли ОС.

4.1.2 Доступ к веб-интерфейсу СКДПУ НТ

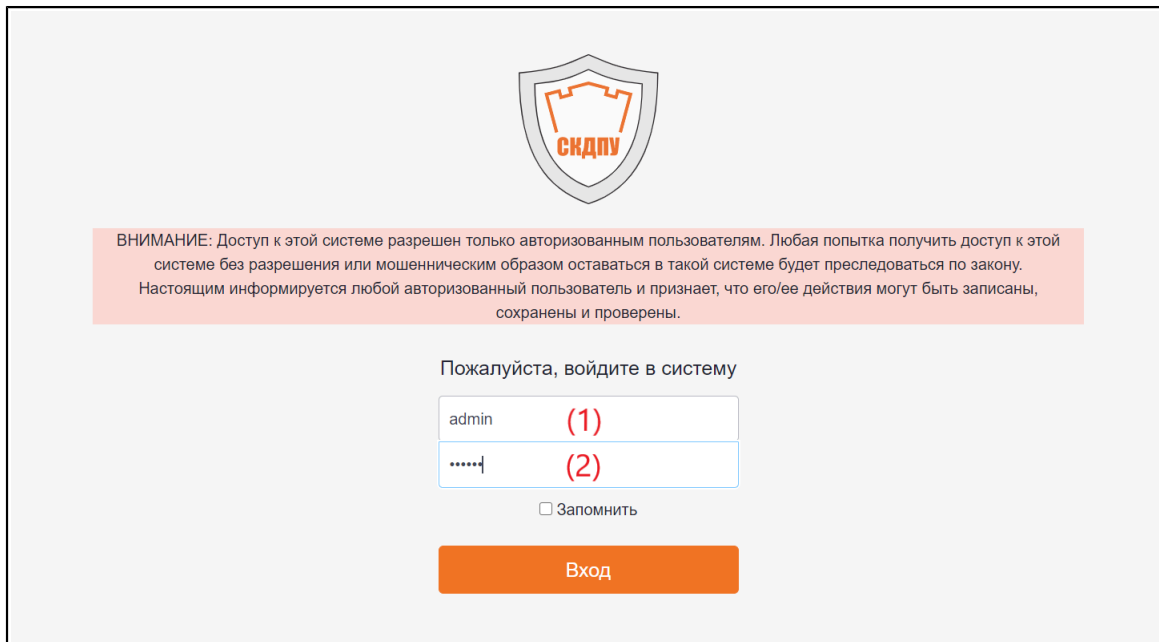
Для доступа к веб-интерфейсу необходимо выполнить следующую последовательность действий:

Шаг 1. Открыть веб-браузер.

Шаг 2. В адресной строке веб-браузера ввести адрес сервера СКДПУ НТ.

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

В окне веб-браузера появится окно ввода логина и пароля пользователя СКДПУ НТ (см. [раздел 4.1.2](#)).



ВНИМАНИЕ: Доступ к этой системе разрешен только авторизованным пользователям. Любая попытка получить доступ к этой системе без разрешения или мошенническим образом оставаться в такой системе будет преследоваться по закону. Настоящим информируется любой авторизованный пользователь и признает, что его/ее действия могут быть записаны, сохранены и проверены.

Пожалуйста, войдите в систему

admin (1)

..... (2)

Запомнить

Вход

Рисунок 1 – Форма ввода логина и пароля

Шаг 3. Для получения доступа к веб-интерфейсу пользователя в окне авторизации необходимо указать имя пользователя (логин) в поле (1) и пароль в поле (2), предоставленные администратором СКДПУ НТ.

Шаг 4. Нажать кнопку **Вход**.

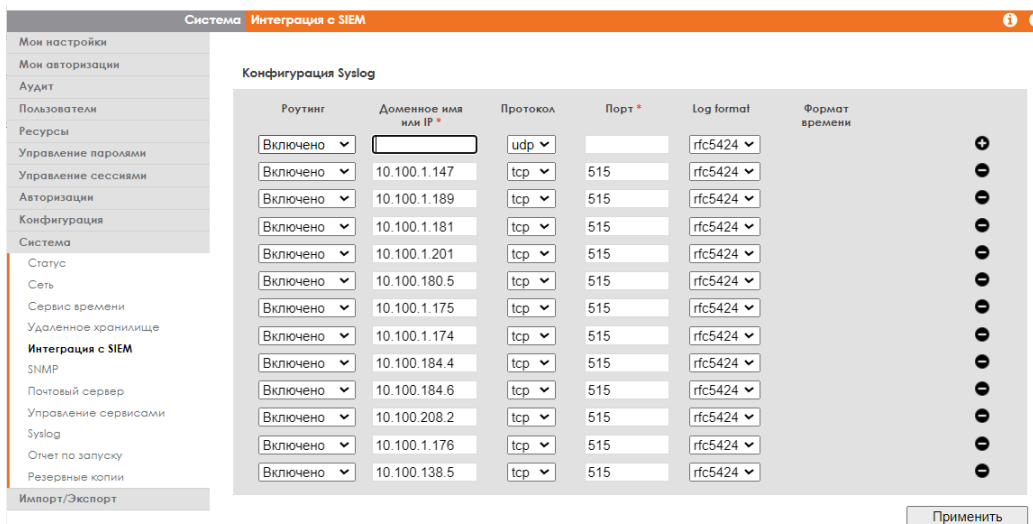
После успешного прохождения процесса авторизации загружается основной интерфейс СКДПУ НТ.

4.2 Настройка источников данных

Сначала производим настройки на Шлюзе доступа:

Шаг 1. Авторизоваться в веб-интерфейсе Шлюза доступа.

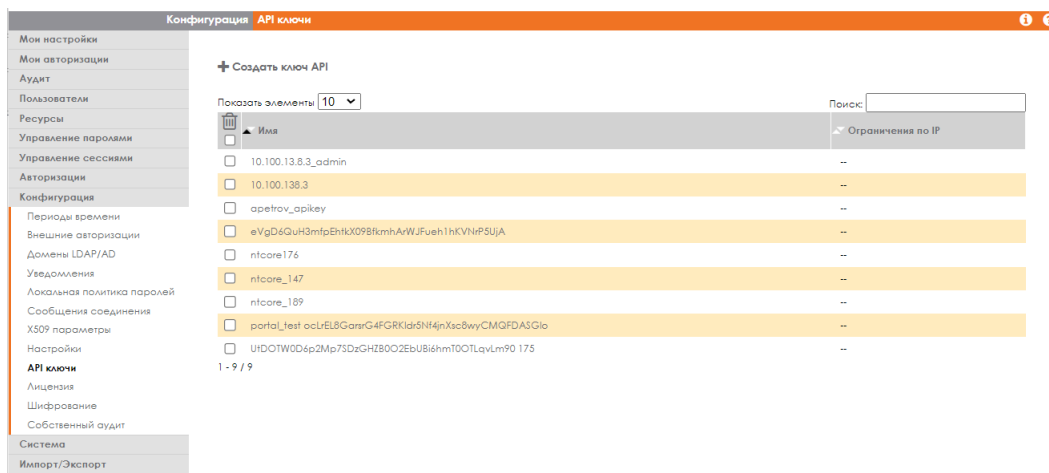
Шаг 2. Перейти в раздел Система > Интеграция с SIEM



Шаг 3. В верхней строке ввести IP-адрес СКДПУ НТ, Протокол `tcp`, Порт `515`, формат логгирования `rfc5424` и нажать кнопку **+**. (Подробнее см. [СКДПУ] Руководство администратора)

Шаг 4. Сохранить настройки нажатием на **Применить**.

Шаг 5. Перейти в раздел Конфигурация > API ключи



Шаг 6. Создать API-ключ для доступа к Шлюзу доступа, скопировав его для дальнейшей настройки.

Далее производится настройка в СКДПУ НТ.

Шаг 1. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 2. Перейти в раздел Компоненты > Шлюзы.

Шаг 3. Выбрать интересующий Шлюз доступа из перечня.

Шаг 4. В поле **Адрес** ввести URL Шлюза доступа, в поле **Имя пользователя** ввести учетную запись `admin`, скопированный ранее API-ключ ввести в поле **Ключ API** и поле **Подтверждение токена**.

Адрес
https://skdpu_adress

Имя пользователя
admin

Пароль
Пароль установлен

Подтверждение пароля

Сбросить

Ключ API
Токен API установлен

Подтверждение токена

Сбросить

Шаг 5. Для сохранения внесенных изменений необходимо нажать **Сохранить**.

При успешном изменении параметров шлюза появится оповещение

Данные шлюза обновлены ✕

В карточке шлюза нажимаем кнопку **Проверка соединения**, если все настроено правильно, то кнопка сменится на **OK**, в противном случае процесс настройки надо повторить заново.

4.3 Добавление файла лицензии

Чтобы загрузить переданный файл лицензии необходимо:

Шаг 1. Войти в консоль администрирования под учетной записью `ntadmin`.

Шаг 2. Получить права суперпользователя.

Шаг 3. Скопировать предоставленный файл лицензии `<file.key>` на сервер СКДПУ НТ в директорию `/home/ntadmin/`, используя клиент или .

Шаг 4. Перенести файл лицензии командой

```
mv /home/ntadmin/<file.key> /opt/skdpu-nt/etc/license.key
```

Шаг 5. Перезапустить сервисы `apache2` и `gunicorn`

```
systemctl restart apache2  
systemctl restart gunicorn
```

Шаг 6. Авторизоваться в веб-интерфейсе СКДПУ НТ.

Шаг 7. Перейти в раздел **Настройки > Информация о лицензии**, где должны появиться сведения об установленной лицензии.

4.4 Обновление СКДПУ НТ

Для обновления СКДПУ НТ необходимо следующие шаги:

Шаг 1. Получить права суперпользователя в консоли администрирования СКДПУ НТ.

Шаг 2. Установить DVD-R носитель СКДПУ НТ в привод и смонтировать с помощью команды

```
apt-cdrom install
```

Шаг 3. Выполнить следующие команды

```
apt-get update  
apt-get install skdpu-nt
```

Шаг 4. Перезапустить сервер СКДПУ НТ

Шаг 5. Проверить работу сервисов СКДПУ НТ с помощью команды

```
/opt/skdpu-nt/bin/nt-status
```

```
Server: skdpunt-test1  
Uptime: 110 days, 19:25:01.564547  
Load averages: 6.03 6.11 6.05  
CPU: 6 cores detected  
    0      1.0      1.0  
    1      3.0      1.0  
    2      0.0      0.0  
    3     65.0      0.0  
    4      0.0      0.0  
    5     58.0      1.0  
Total memory: 7.7GB  
Available: 2.65GB  
Used: 5.04GB 65.5%  
Swap: 2.0GB  
Free: 803.53MB 60.7%  
Filesystem: /  
Total: 76.27GB  
Used: 63.27GB 87.4%  
Process: analysed is running (389)  
CPU usage: 0.0%  
Memory usage: 604.93MB  
Process: jobrunnerd is running (10537)  
CPU usage: 0.0%  
Memory usage: 851.0MB  
Process: indexd is running (13225)  
CPU usage: 0.0%  
Memory usage: 161.62MB  
Process: collectd is running (13100)  
CPU usage: 0.0%  
Memory usage: 288.5MB  
Process: enrichd is running (13922)  
CPU usage: 0.0%  
Memory usage: 299.46MB  
Syslog listener status: enabled
```

4.5 Настройка подключения к почтовому серверу

Описание сценария

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

Сценарий

Шаг 1. Перейти в раздел веб-интерфейса СКДПУ НТ **Настройки > Основные настройки > Почтовый сервер** под учетной записью администратора.

Шаг 2. Заполнить необходимые параметры подключения.



Почтовый сервер должен быть предварительно настроен

4.6 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 с помощью тестовой сессии проверить, что все необходимые компоненты СКДПУ НТ успешно обрабатывают без ошибок в мониторинге ЗПС.

4.7 Встроенные правила сетевого фильтра

У СКДПУ НТ есть собственный набор правил сетевой фильтрации, который по умолчанию включен сразу после установки. Чтобы отключить правила сетевого фильтра, используйте

```
/opt/skdpu-nt/bin/nt-network-filter disable
```

Тем не менее, рекомендуется оставить их включенными, чтобы избежать угроз безопасности.

Чтобы изменить набор активных правил, отредактируйте файл `/opt/skdpu-nt/etc/filter.enable`.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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.
LAN	Local Area Network — локальная компьютерная сеть.
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к каталогам) — протокол прикладного уровня для доступа к службе каталогов X.500
LDAPS	Lightweight Directory Access Protocol Secure — расширение протокола LDAP для поддержки шифрования в целях повышения безопасности
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.
NTP	Network Time Protocol — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.
RDP	Remote Desktop Protocol — протокол удаленного рабочего стола
SAS	Serial Attached SCSI — последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных, например, жёстких дисков и ленточных накопителей.
SATA	Serial Advanced Technology Attachment — последовательный интерфейс обмена данными с накопителями информации.

SCSI	Small Computer System Interface — набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами.
SIEM	Security information and event management — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) - управление информацией о безопасности, и SEM (Security event management) - управление событиями безопасности.
SMTP	Simple Mail Transfer Protocol (простой протокол передачи почты) — широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.
SSD	Solid-State Drive — компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти, альтернатива жёстким дискам (HDD).
SSH	Secure SHell (безопасная оболочка) — протокол защищенной передачи данных.
TCP	Transmission Control Protocol (протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.
UDP	User Datagram Protocol (протокол пользовательских датаграмм) — один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.
URL	Uniform Resource Locator (унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов.
XFS	High-performance journaling FileSystem — высокопроизводительная 64-битная журналируемая файловая система, созданная компанией Silicon Graphics для собственной операционной системы IRIX.
АРМ	Автоматизированное рабочее место
ЗПС	Закрытая программная среда
ОС	Операционная система
СУБД	Система управления базами данных

ФСТЭК

Федеральная служба по техническому и экспортному
контролю России

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Форма ввода логина и пароля.....	26
--	----

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Перечень сервисов.....	4
Таблица 2 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ НТ.....	5
Таблица 3 – Перечень настроек портов брандмауэра.....	6
Таблица 4 – Пример разметки разделов.....	14

