

Установка Astra Linux

KICS for Networks 4.0.1 работает под управлением ОС Astra Linux Special Edition v.1.7 Smolensk

Для выполнения установки ОС Astra Linux Special Edition v.1.7 выполните следующие шаги:

- Подключите установочный диск «smolensk-1.7» к серверу KICS for Networks и загрузитесь с накопителя
- Выбрать язык интерфейса установки ОС Astra Linux Special Edition v.1.7, который вам удобен.
- Выбираем «Графическая установка» и жмем «Enter».



Принимаем лицензионное соглашение нажатием кнопки «Продолжить»



Лицензия

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ДЛЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ ПО ИСПОЛЬЗОВАНИЮ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SPECIAL EDITION

ВНИМАНИЕ! Прочтите внимательно нижеизложенное Лицензионное соглашение, прежде чем устанавливать, копировать или иным образом использовать приобретенный Программный продукт. Любое использование приобретенного Программного продукта, в том числе его установка и копирование, означает согласие с условиями приведенного ниже Лицензионного соглашения.

Настоящее Лицензионное соглашение для конечного пользователя (СОГЛАШЕНИЕ) является юридическим соглашением между Вами (физическим или юридическим лицом) (ПОЛЬЗОВАТЕЛЕМ) и открытым акционерным обществом «Научно-производственное объединение Русские базовые информационные технологии» (ПРАВООБЛАДАТЕЛЕМ), которое является разработчиком Операционной системы специального назначения «Astra Linux Special Edition» (ПРОГРАММНЫЙ ПРОДУКТ). Устанавливая, копируя или иным образом используя ПРОГРАММНЫЙ ПРОДУКТ, ПОЛЬЗОВАТЕЛЬ тем самым соглашается с положениями настоящего СОГЛАШЕНИЯ. Если ПОЛЬЗОВАТЕЛЬ не согласен с положениями настоящего СОГЛАШЕНИЯ, ПРАВООБЛАДАТЕЛЬ отказывает ему в праве на любое использование ПРОГРАММНОГО ПРОДУКТА. В этом случае ПОЛЬЗОВАТЕЛЬ не имеет права устанавливать, копировать или иным образом использовать ПРОГРАММНЫЙ ПРОДУКТ, а также вправе вернуть ПРОГРАММНЫЙ ПРОДУКТ организации, у которой его приобрел, при условии целостности (отсутствия признаков вскрытия) товарной упаковки.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ПРОГРАММНЫЙ ПРОДУКТ охраняется авторским правом, международными соглашениями о защите интеллектуальной собственности и действующим законодательством Российской Федерации. Соответствие ПРОГРАММНОГО ПРОДУКТА требованиям безопасности информации подтверждается сертификатом, оформленным согласно действующего законодательства Российской Федерации.

Снимок экрана

Справка

Продолжить

Выбираем «горячие клавиши» переключения раскладки клавиатуры нажимаем кнопку

«Продолжить»



Настройка клавиатуры

Вам нужно указать способ переключения клавиатуры между национальной раскладкой и стандартной латинской раскладкой.

Наиболее эргономичным способом считаются правая клавиша Alt или CapsLock (в последнем случае для переключения между заглавными и строчными буквами используется комбинация Shift+CapsLock). Ещё одна популярная комбинация: Alt+Shift; заметим, что в этом случае комбинация Alt+Shift потеряет своё привычное действие в Emacs и других, использующих её, программах.

Не на всех клавиатурах есть перечисленные клавиши.

Способ переключения между национальной и латинской раскладкой:

правый Alt (AltGr)
правый Control
правый Shift
правая клавиша с логотипом
клавиша с меню
Alt+Shift
Control+Shift
Control+Alt
Alt+Caps Lock
левый Control+левый Shift
левый Alt

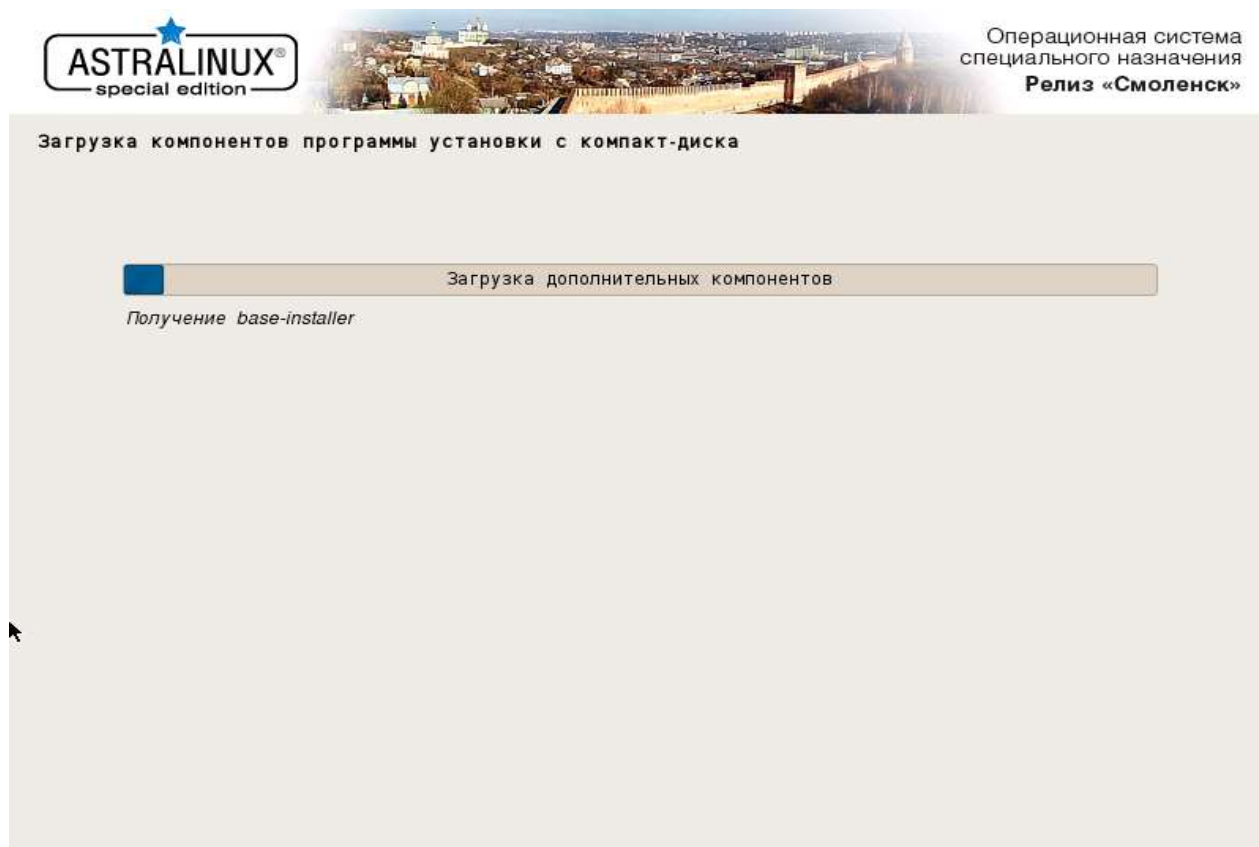
Снимок экрана

Справка

Вернуться

Продолжить

Ожидаем завершения загрузки компонентов системы



Указываем имя узла KICS for Networks (Например, kics4net-host-1), жмем «Продолжить»



Указываем имя учетной записи администратора (Например, kics), жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Настройка учётных записей пользователей и паролей

Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.

Имя учётной записи администратора:

Задаем пароль для учетной записи, жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Настройка учётных записей пользователей и паролей

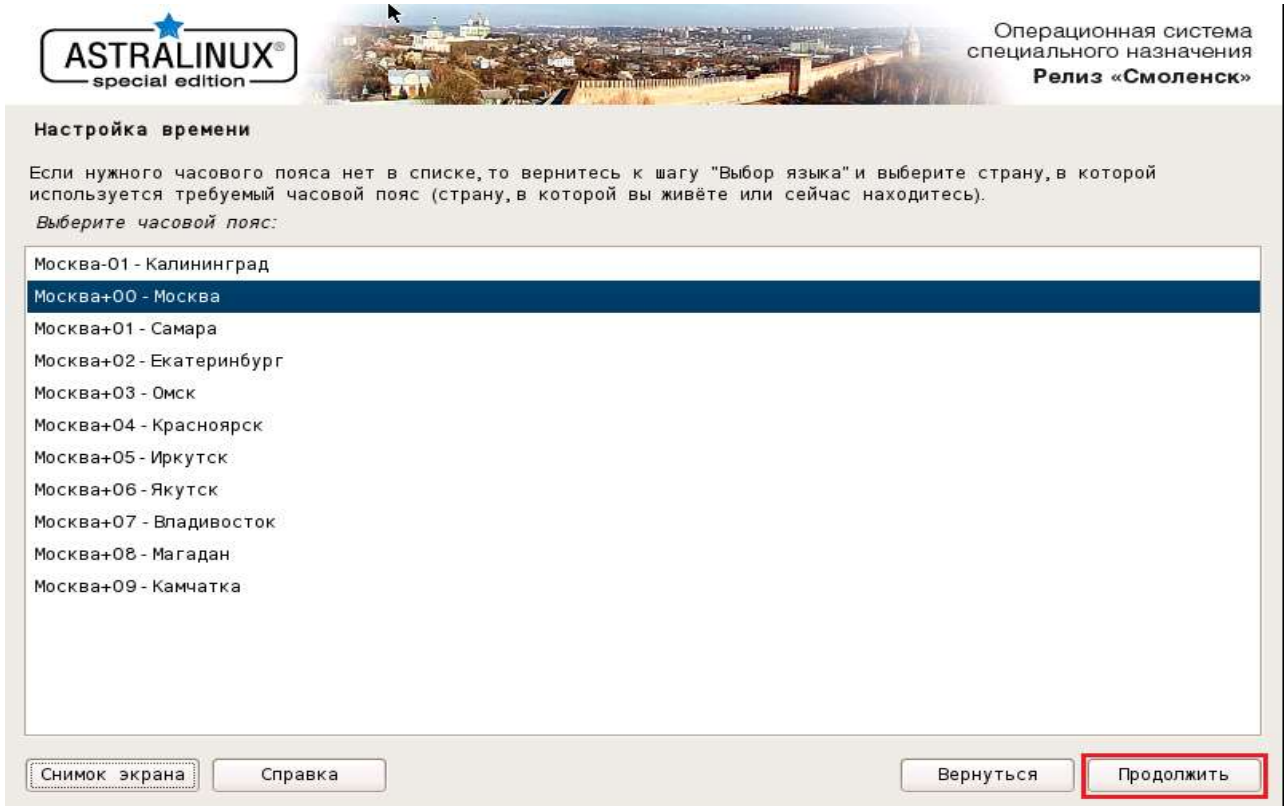
Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Введите пароль для нового администратора:

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.

Введите пароль ещё раз:

Выбираем часовой пояс «Москва», жмем кнопку «Продолжить»



Выбираем автоматический метод разметки всего диска. Жмем «Продолжить» (Диск может размечен иначе по Вашему усмотрению, под пользовательский каталог «/home» 10Гб, оставшееся место выделяем под корневой каталог «/»). Жмем «Продолжить».

Разметка дисков

Программа установки может провести вас через процесс разметки диска (предлагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.

Если выбрать использование инструмента управления разметкой всего диска, то далее вас попросят указать нужный диск.

Метод разметки:

Авто - использовать весь диск

Авто - использовать весь диск и настроить LVM

Авто - использовать весь диск с защитным преобразованием на LVM

Вручную

Снимок экрана

Справка

Вернуться

Продолжить

Выбираем наш HDD, Жмем «Продолжить»

Разметка дисков

Заметим, что все данные на выбранном диске будут стёрты, но не ранее чем вы подтвердите, что действительно хотите сделать изменения.

Выберите диск для разметки:

SCSI3 (0,0,0) (sda) - 64.4 GB VMware, VMware Virtual S

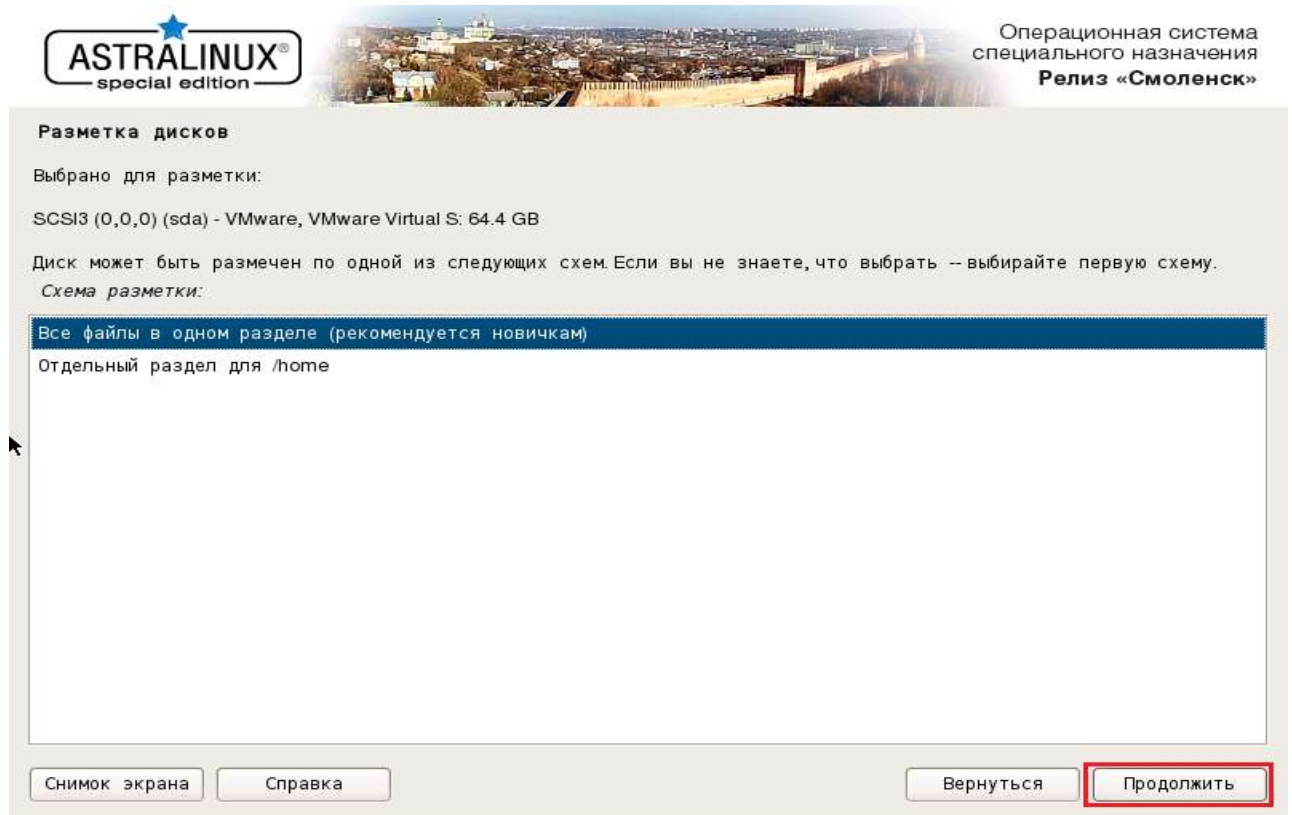
Снимок экрана

Справка

Вернуться

Продолжить

Выбираем «Все файлы в одном разделе» (При необходимости раздел «/home» можно сделать отдельно), жмем «Продолжить».



Завершаем разметку диска, жмем «Продолжить»



Разметка дисков

Перед вами список настроенных разделов и их точек монтирования. Выберите раздел, чтобы изменить его настройки (тип файловой системы, точку монтирования и так далее), свободное место, чтобы создать новый раздел, или устройство, чтобы создать на нём новую таблицу разделов.

Автоматическая разметка
Настройка программного RAID
Настройка менеджера логических томов (LVM)
Настроить защитное преобразование для томов
Настроить тома iSCSI

▽ SCSI3 (0,0,0) (sda) - 64.4 GB VMware, VMware Virtual S

>	#1	первичн.	60.1 GB	B	f	ext4	/
>	#5	логичес.	4.3 GB		f	подк	подк

Отменить изменения разделов

Закончить разметку и записать изменения на диск

Снимок экрана

Справка

Справка

Вернуться

Продолжить

Выбираем «Записать изменения на диск - ДА», жмем «Продолжить»



Разметка дисков

Если вы продолжите, то изменения, перечисленные ниже, будут записаны на диски. Или же вы можете сделать все изменения вручную.

На этих устройствах изменены таблицы разделов:
SCSI3 (0,0,0) (sda)

Следующие разделы будут отформатированы:
раздел #1 на устройстве SCSI3 (0,0,0) (sda) как ext4
раздел #5 на устройстве SCSI3 (0,0,0) (sda) как подк

Записать изменения на диск?

☐ Нет

☒ Да

Снимок экрана

Справка

Продолжить

Ожидаем завершения базовой установки



Выбираем компоненты, необходимые для установки: “Графический интерфейс Fly”, “Средства работы с Интернет”, “Консольные утилиты”, “Средства фильтрации сетевых пакетов ufw”, “Средства удалённого подключения ssh”

Выбирать службу ALD не требуется, жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Выбор и установка программного обеспечения

Выберите дополнительные функции устанавливаемой ОС.

☐ Служба ALD

Снимок экрана

Справка

Продолжить

Ожидаем завершения установки ОС



Операционная система
специального назначения
Релиз «Смоленск»

Выбор и установка программного обеспечения

Выбор и установка программного обеспечения

Скачивается файл 259 из 1139 (осталось 30с)

Убираем все пункты, жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Дополнительные настройки ОС

Вы можете настроить параметры безопасности ОС и отключить автоматическую настройку сети. Мандатный контроль целостности процессов ОС по умолчанию включен и после настройки ОС администратором необходимо включить мандатный контроль целостности ФС и режим ЗПС. Для управления МКЦ могут использоваться программы fly-admin-smc, astra-mic-control, set-fs-ilev, unset-fs-ilev.

Дополнительные настройки ОС

- ☒ Включить режим замкнутой программной среды
- ☐ Запретить установку бита исполнения
- ☐ Использовать по умолчанию ядро Hardened
- ☐ Запретить вывод меню загрузчика
- ☐ Включить очистку разделов страничного обмена
- ☐ Включить очистку освобождаемых областей для EXT-разделов
- ☐ Включить блокировку консоли
- ☐ Включить блокировку интерпретаторов
- ☐ Включить межсетевой экран ufw
- ☐ Включить системные ограничения ulimits
- ☐ Отключить возможность трассировки ptrace
- ☐ Отключить автоматическую настройку сети
- ☐ Установить 32-битный загрузчик

Снимок экрана

Справка

Продолжить

Выбираем «Установить системный загрузчик GRUB - ДА», жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Установка системного загрузчика GRUB на жёсткий диск

Похоже, что данная система будет единственной на этом компьютере. Если это действительно так, то можно спокойно устанавливать системный загрузчик GRUB в основную загрузочную запись первого жёсткого диска.

Внимание! Если программе установки не удалось обнаружить другую операционную систему, имеющуюся на компьютере, то изменение основной загрузочной записи приведёт к тому, что эту операционную систему некоторое время нельзя будет загрузить. Позднее можно будет настроить GRUB для её загрузки.

Установить системный загрузчик GRUB в главную загрузочную запись?

☐ Нет

☒ Да

Снимок экрана

Справка

Вернуться

Продолжить

Задаем дважды пароль для GRUB, жмем «Продолжить»



Операционная система
специального назначения
Релиз «Смоленск»

Установка системного загрузчика GRUB на жёсткий диск

Системный загрузчик GRUB обладает многими мощными интерактивными свойствами, которые могут быть использованы для несанкционированного доступа к системе, если неизвестный пользователь получит доступ к машине перед загрузкой. Чтобы защититься от этого, вы можете задать пароль, который нужно будет ввести для редактирования меню или для входа в режим командной строки GRUB. По умолчанию, любому пользователю разрешено запускать любой пункт меню без пароля.

Введите пароль для GRUB.
Пароль для GRUB:

Снимок экрана

Справка

Вернуться

Продолжить

Жмем «Продолжить» для перезагрузки машины



Операционная система
специального назначения
Релиз «Смоленск»

Завершение установки



Установка завершена

Установка завершена, пришло время загрузить вашу новую систему. Извлеките установочные носители, чтобы система смогла загрузиться.

Снимок экрана

Справка

Вернуться

Продолжить

Важно!!! Если предполагается одновременное развертывание «Серверной» и «Сенсорной» части KICS for Networks с помощью «deploy script», то Логин/Пароль пользователя на машинах, под которым запускает установка KICS for Networks, должны быть одинаковыми.

Для дальнейшей корректной работы KICS for Network требуется обновление версии OS с 1.7.0 до 1.7.3:

В интерфейс системы копируем файлы: 1.7.0-11.06.2021_12.40.iso и repository-update.iso, располагаем их в любой удобной вам директории.

Выполняем обновление системы командой:

```
sudo astra-update -A </нумь/1.7.0-11.06.2021_12.40.iso> </нумь/ repository-update.iso>
```

После обновления перезагружаем систему командой:

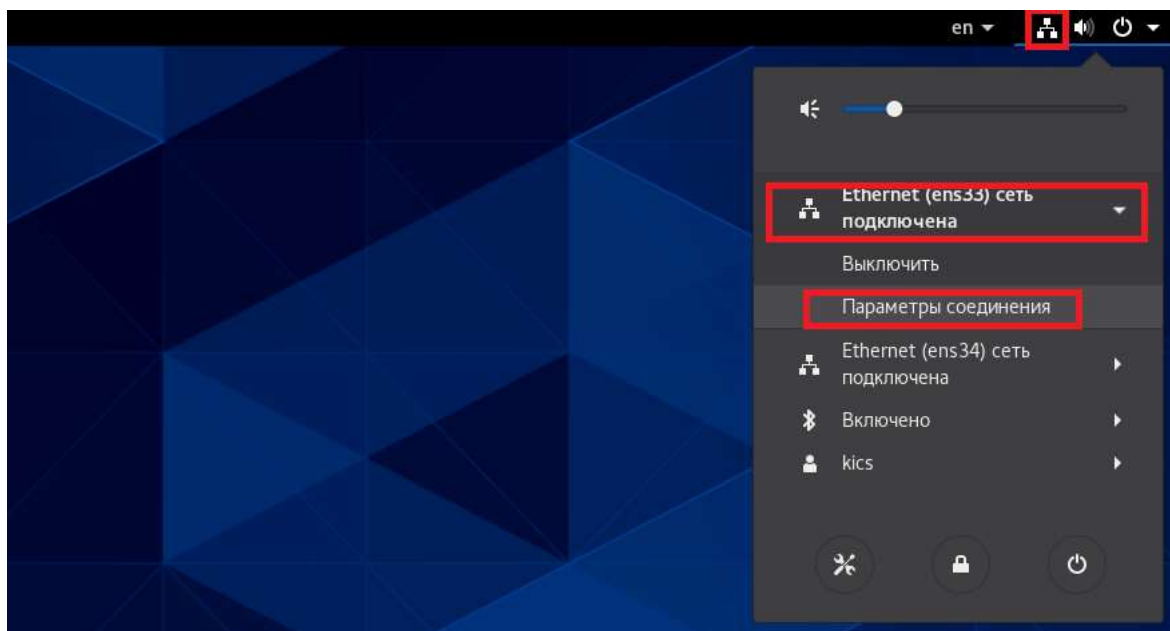
```
sudo reboot
```

Настройка сетевых параметров CentOS 8 Stream(Astra Linux).

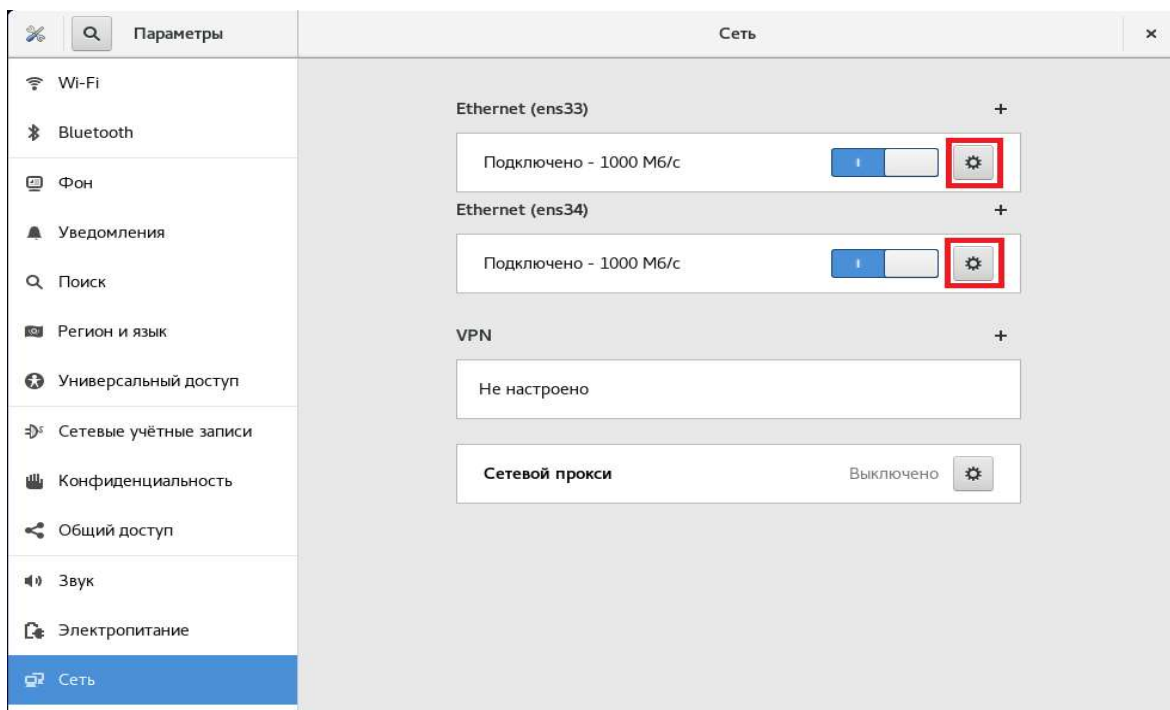
Настройка интерфейсов для Astra Linux отличается только интерфейсом ОС,

Для работы KICS for Networks необходимо как минимум 2 интерфейса:

- MGMT – менеджмент интерфейс необходим для подключения к Web интерфейсу решения, поэтому IP адрес выбирается исходя из карты IP адресов конкретной площадки с учетом, чтобы все заинтересованные пользователи могли иметь к нему доступ. Данный порт так же может быть задействован для связи с сенсорами на удаленных площадках (для этого все сенсоры должны быть доступны для этой сети), но Вы так же можете выделить взаимодействие с сенсорами в отдельную подсеть.
- SPAN – интерфейс на который подается копия трафика с коммутаторов. Для конфигурации интерфейсов переходим в сетевые настройки CentOS8 Stream

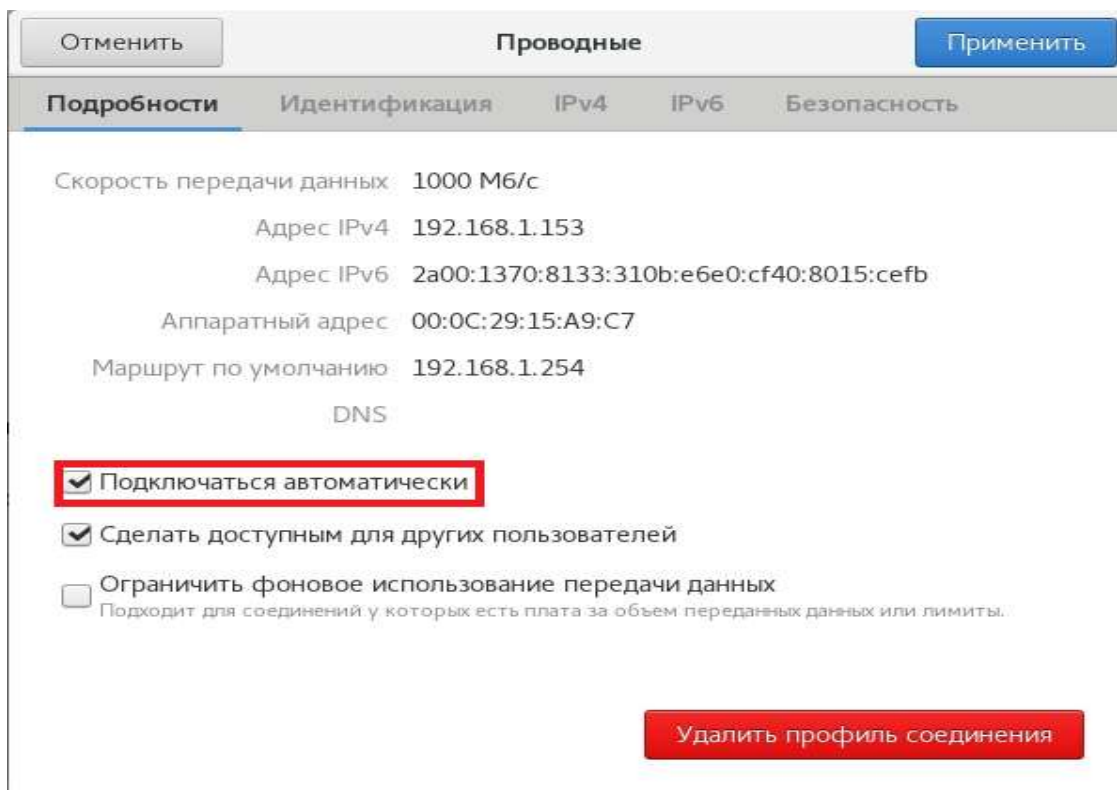


- Настраиваем сетевые интерфейсы для MGMT и SPAN(Количество сетевых интерфейсов SPAN зависит от количества точек съема трафика)



1. Настройка MGMT интерфейс:

- Устанавливаем флаг «Подключаться автоматически»



- Настраиваем имя интерфейса (например, «MGMT»), выбираем MAC, соответствующий интерфейсу

Отменить Проводные Применить

Подробности Идентификация IPv4 IPv6 Безопасность

Название MGMT

MAC-адрес 00:0C:29:15:A9:C7 (ens33)

Клонированный адрес

MTU автоматический

- Выбираем метод IPv4 – «Вручную». Настраиваем IP адрес для MGMT интерфейса.

Отменить Проводные Применить

Подробности Идентификация IPv4 IPv6 Безопасность

Метод IPv4 ☐ Автоматический (DHCP) ☐ Только для локальной сети ☒ Вручную ☐ Выключить

Адреса

Адрес	Маска сети	Шлюз
192.168.1.153	255.255.255.0	192.168.1.254

DNS Автоматический

Отделяйте IP-адреса запятыми

Маршруты Автоматический

Адрес	Маска сети	Шлюз	Метрика

- Отключаем IPv6. Жмем кнопку «Применить»

Отменить

Проводные

Применить

ПодробнееИдентификацияIPv4IPv6Безопасность

Метод IPv6

☐ Автоматический

☐ Автоматический, только DHCP

☐ Только для локальной сети

☐ Вручную

☒ Выключить

DNS

Автоматический

Отделяйте IP-адреса запятыми

Маршруты

Автоматический

Адрес	Префикс	Шлюз	Метрика
			×

☐ Использовать это подключение только для ресурсов в этой сети

2. Настройка SPAN интерфейс:

- Устанавливаем флаг «Подключаться автоматически»

Отменить **Проводные** Применить

Подробности Идентификация IPv4 IPv6 Безопасность

Аппаратный адрес 00:0C:29:15:A9:D1

Последнее использование Никогда

☒ Подключаться автоматически

☒ Сделать доступным для других пользователей

☐ Ограничить фоновое использование передачи данных
Подходит для соединений у которых есть плата за объем переданных данных или лимиты.

Удалить профиль соединения

- Настраиваем имя интерфейса (например, «SPAN»), выбираем MAC, соответствующий интерфейсу

Отменить **Проводные** Применить

Подробности **Идентификация** IPv4 IPv6 Безопасность

Название SPAN

MAC-адрес 00:0C:29:15:A9:D1 (ens34)

Клонированный адрес

MTU автоматический - +

- Отключаем IPv4..

The screenshot shows the 'Сетевые адаптеры' (Network Adapters) window with the 'Проводные' (Wired) tab selected. The 'IPv4' sub-tab is active. In the 'Метод IPv4' (IPv4 Method) section, the 'Автоматический (DHCP)' (Automatic (DHCP)) radio button is selected. The 'Только для локальной сети' (Only for this network) radio button is also selected. The 'Выключить' (Disable) radio button is highlighted with a red rectangle. Below this, the 'DNS' section shows 'Автоматический' (Automatic) selected. The 'Маршруты' (Routes) section shows 'Автоматический' (Automatic) selected. At the bottom, there is a checkbox labeled 'Использовать это подключение только для ресурсов в этой сети' (Use this connection only for resources in this network).

Отменить Проводные Применить

Подробности Идентификация IPv4 IPv6 Безопасность

Метод IPv4

☐ Автоматический (DHCP) ☐ Только для локальной сети

☐ Вручную ☒ Выключить

DNS Автоматический

Отделяйте IP-адреса запятыми

Маршруты Автоматический

Адрес	Маска сети	Шлюз	Метрика

☐ Использовать это подключение только для ресурсов в этой сети

- Отключаем IPv6. Жмем кнопку «Применить»

Отменить

Проводные

Применить

ПодробнееИдентификацияIPv4IPv6Безопасность

Метод IPv6

☐ Автоматический

☐ Автоматический, только DHCP

☐ Только для локальной сети

☐ Вручную

☒ Выключить

DNS

Автоматический

Отделяйте IP-адреса запятыми

Маршруты

Автоматический

Адрес

Префикс

Шлюз

Метрика

×

☐ Использовать это подключение только для ресурсов в этой сети

Настройка и установка пакетов Astra Linux

Вместе с дистрибутивом предоставляется текстовый файл с перечнем команд по установке необходимых пакетов (kics4net_preparing)

Для корректной работы компонентов KICS for Networks 4.0.x необходимо провести некоторые настройки и установить пакеты из файла дистрибутива 1.7.0-11.06.2021_12.40.iso командами из kics4net_preparing.

Подключение установочного диска

Способ №1

- Подключить 1.7.0-11.06.2021_12.40.iso в качестве CD-ROM используя Remote Media

Способ №2 - Создание локального репозитория

- Подключить 1.7.0-11.06.2021_12.40.iso в качестве CD-ROM используя команду *mount*

```
sudo mount /путь/1.7.0-11.06.2021_12.40.iso /media/cdrom
```

- Создать папку (рекомендуется в /tmp)

```
sudo mkdir /tmp/mnt/
```

- Открыть Midnight Commander и скопировать все содержимое CDROM в папку /tmp/mnt

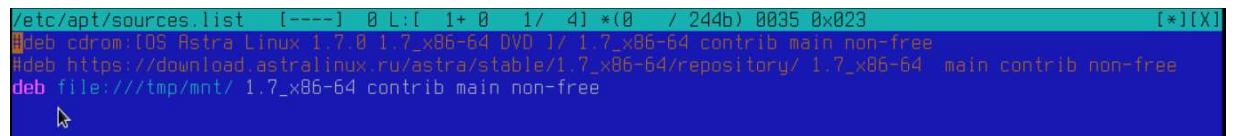
```
sudo mc
```

- Отредактировать файл /etc/apt/source.list

```
sudo mcedit /etc/apt/source.list
```

Закомментировать ссылку на CDROM

Добавить ссылку на /tmp/mnt



```
/etc/apt/sources.list [----] 0 L:[ 1+ 0 1/ 4] *(0 / 244b) 0035 0x023 [*][X]
#deb cdrom:[05 Astra Linux 1.7.0 1.7_x86-64 DVD 1/ 1.7_x86-64 contrib main non-free
#deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository/ 1.7_x86-64 main contrib non-free
deb file:///tmp/mnt/ 1.7_x86-64 contrib main non-free
```

- Отключить CDROM

```
sudo umount /media/cdrom
```

- Обновить информацию о репозиториях

```
sudo apt update
```

```
kics@kics4net-host-1:/tmp$ sudo apt update
Пол:1 file:/tmp/mnt 1.7_x86-64 InRelease
Игн:1 file:/tmp/mnt 1.7_x86-64 InRelease
Пол:2 file:/tmp/mnt 1.7_x86-64 Release [5 766 B]
Игн:3 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD 1.7_x86-64 InRelease
Сущ:4 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD 1.7_x86-64 Release
Пол:2 file:/tmp/mnt 1.7_x86-64 Release [5 766 B]
Пол:5 file:/tmp/mnt 1.7_x86-64 Release.gpg [833 B]
Пол:5 file:/tmp/mnt 1.7_x86-64 Release.gpg [833 B]
Пол:7 file:/tmp/mnt 1.7_x86-64/contrib amd64 Packages [2 156 B]
Пол:8 file:/tmp/mnt 1.7_x86-64/main amd64 Packages [1 139 kB]
Пол:9 file:/tmp/mnt 1.7_x86-64/non-free amd64 Packages [45,3 kB]
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
kics@kics4net-host-1:/tmp$
```

Далее перейти в директорию где лежит `kics4net_preparing` и выдать ему права на выполнение командой :

```
sudo chmod +x kics4net_preparing
```

- Запустить файл на исполнение командой

```
sudo /путь/kics4net_preparing
```

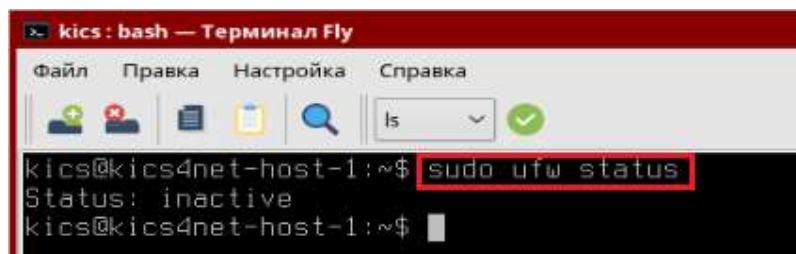
- Перезагрузить ОС

```
sudo reboot
```

С требованиями также можно ознакомиться по ссылке:

<https://support.kaspersky.com/help/KICSforNetworks/4.0/ru-RU/102347.htm>

Проверим статус работы межсетевого экрана, активируем если отключен – «**sudo ufw status**»,



```
kics@kics4net-host-1:~$ sudo ufw status
Status: inactive
kics@kics4net-host-1:~$
```

Активируем межсетевой экран «**sudo ufw enable**», проверяем включенные правила – «**sudo ufw status verbose**»

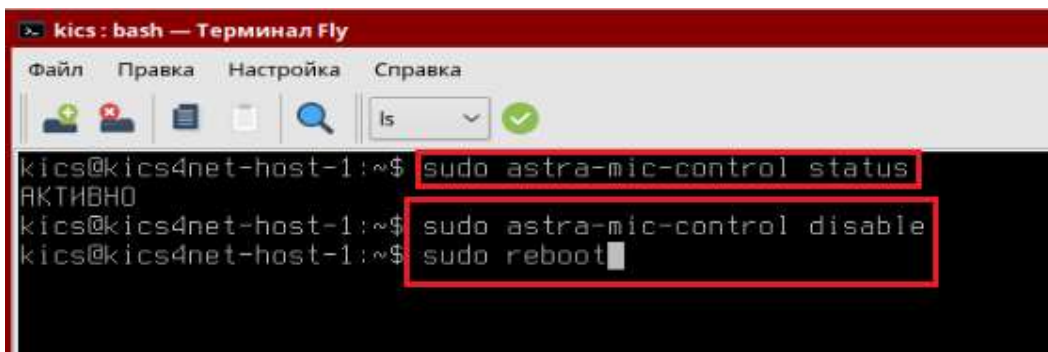
```
kics : bash — Терминал Fly
Файл  Правка  Настройка  Справка
[Icons]  [Is]  [Checkmark]
kics@kics4net-host-1:~$ sudo ufw enable
Firewall is active and enabled on system startup
kics@kics4net-host-1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
kics@kics4net-host-1:~$
```

Для возможности администрирования сервера разрешим использование SSH на межсетевом экране – «**sudo ufw allow ssh**» и проверяем статус

```
kics : bash — Терминал Fly
Файл  Правка  Настройка  Справка
[Icons]  [Is]  [Checkmark]
kics@kics4net-host-1:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
kics@kics4net-host-1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
```

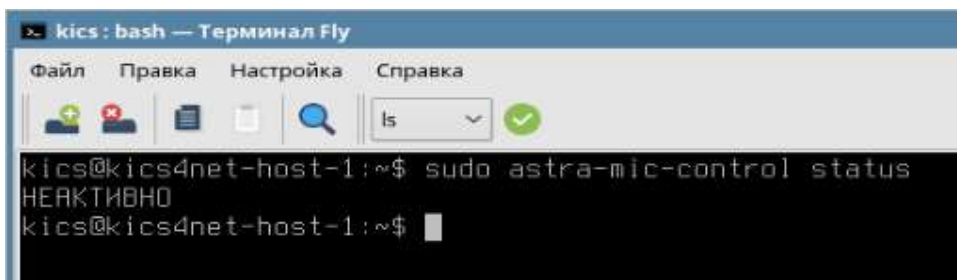
Активируем службу – «**sudo systemctl start ssh**», добавляем в автозагрузку – «**sudo systemctl enable ssh**»

A terminal window titled "kics : bash — Терминал Fly" with a menu bar (Файл, Правка, Настройка, Справка) and a toolbar. The terminal shows the following commands and output:

```
kics@kics4net-host-1:~$ sudo astra-mic-control status
АКТИВНО
kics@kics4net-host-1:~$ sudo astra-mic-control disable
kics@kics4net-host-1:~$ sudo reboot
```

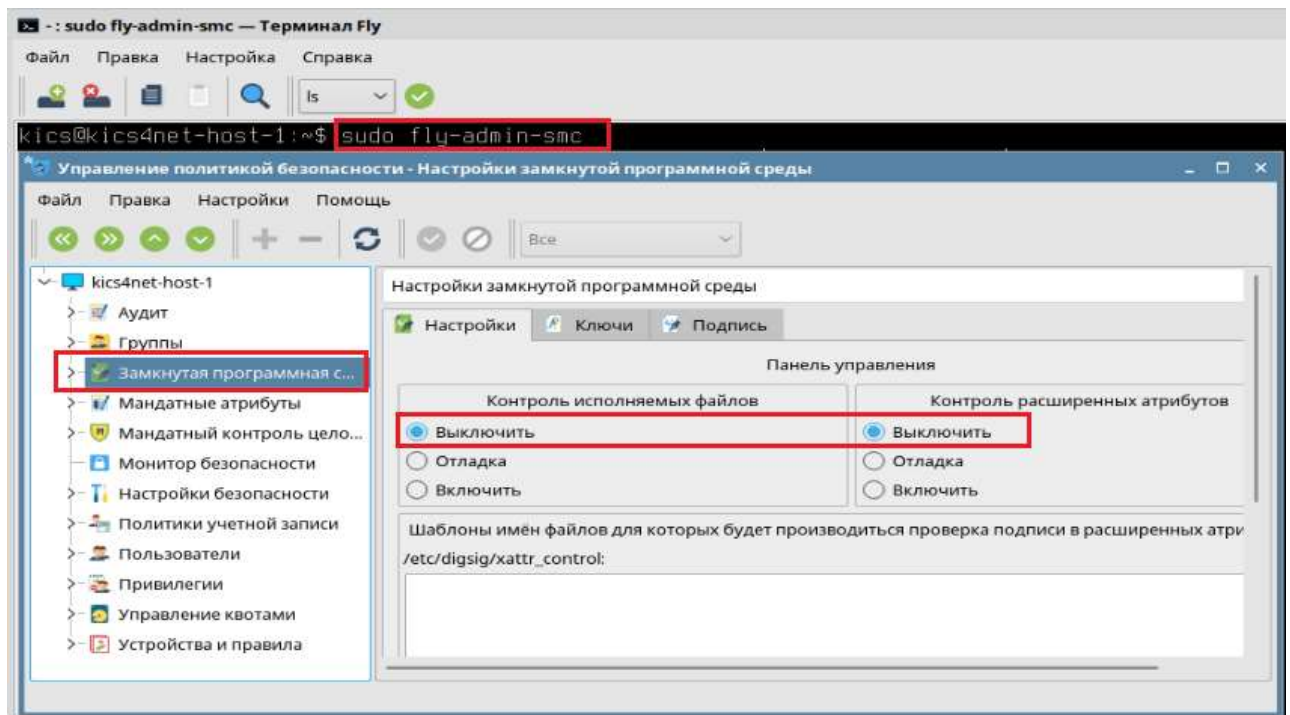
The first two lines of the output are highlighted with red boxes.

Повторно проверяем статус

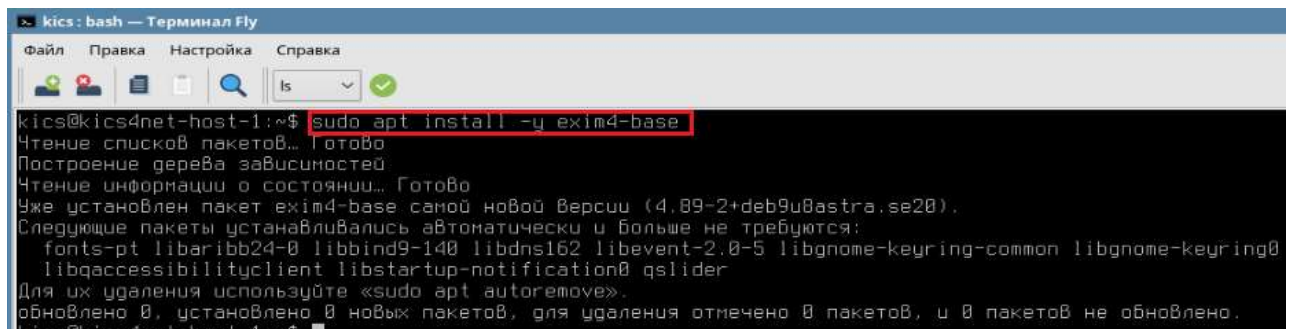
A terminal window titled "kics : bash — Терминал Fly" with a menu bar (Файл, Правка, Настройка, Справка) and a toolbar. The terminal shows the following commands and output:

```
kics@kics4net-host-1:~$ sudo astra-mic-control status
НЕАКТИВНО
kics@kics4net-host-1:~$
```

Проверяем статус механизма замкнутой среды, при необходимости отключаем «**sudo fly-admin-smc**»



Если планируется передача событий на почту, то необходимо установить почтовый сервер (Например, exim) – «`sudo apt install -y exim4-base`»



Настройка синхронизации времени ОС

Синхронизация времени настраивается для автоматической корректировки времени ОС для исключения некорректной метки времени событиям, которые фиксируются в KICS for Networks и ошибок в работе системы. **Все сенсоры должны синхронизироваться по тому же времени, что и сервер!!!**

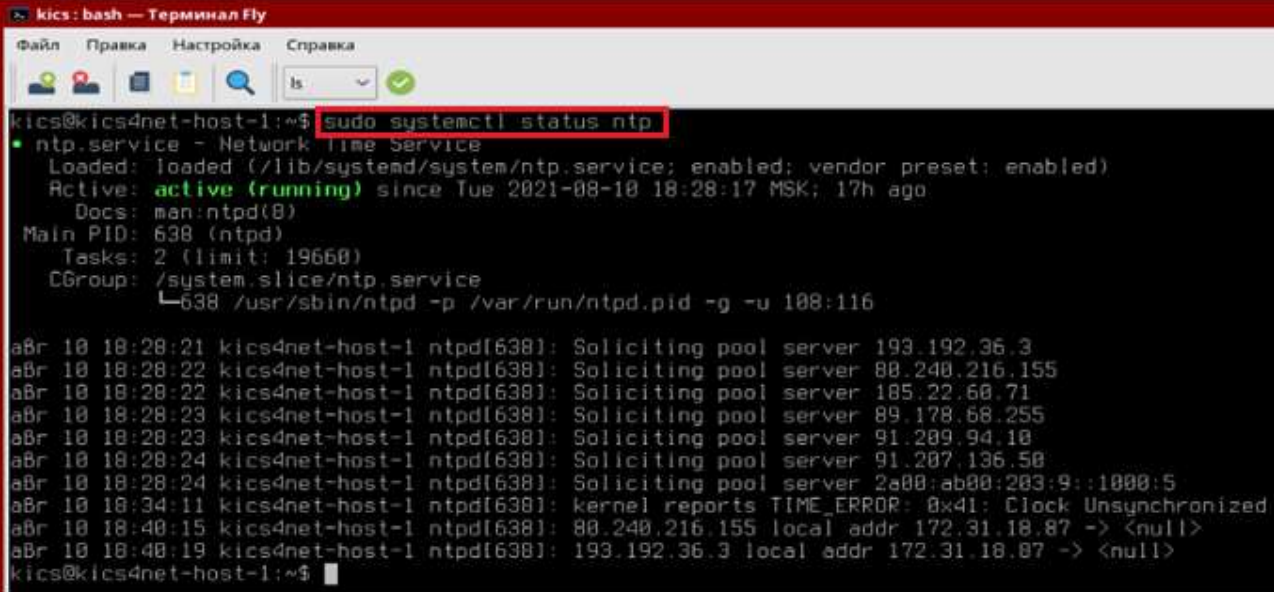
Синхронизация времени Astra Linux

В версии Kaspersky Industrial CyberSecurity for Networks 4.0.1 не применяется команда автоматического включения синхронизации времени Сервера с узлами, на которых установлены сенсоры. Для синхронизации времени требуется выполнить действия по настройке программных средств из состава операционной системы на всех узлах с установленными компонентами программы.

С информацией по настройке так же можно ознакомиться по ссылке:

<https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361687#id>

Проверяем статус службы ntp – «`sudo systemctl status ntp`»



```
kics@kics4net-host-1:~$ sudo systemctl status ntp
• ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-08-10 18:28:17 MSK; 17h ago
     Docs: man:ntpd(8)
   Main PID: 638 (ntpd)
    Tasks: 2 (limit: 19660)
   CGroup: /system.slice/ntp.service
           └─638 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 108:116

aBr 10 18:28:21 kics4net-host-1 ntpd[638]: Soliciting pool server 193.192.36.3
aBr 10 18:28:22 kics4net-host-1 ntpd[638]: Soliciting pool server 80.240.216.155
aBr 10 18:28:22 kics4net-host-1 ntpd[638]: Soliciting pool server 185.22.60.71
aBr 10 18:28:23 kics4net-host-1 ntpd[638]: Soliciting pool server 89.178.68.255
aBr 10 18:28:23 kics4net-host-1 ntpd[638]: Soliciting pool server 91.209.94.10
aBr 10 18:28:24 kics4net-host-1 ntpd[638]: Soliciting pool server 91.207.136.50
aBr 10 18:28:24 kics4net-host-1 ntpd[638]: Soliciting pool server 2a00:ab00:203:9::1000:5
aBr 10 18:34:11 kics4net-host-1 ntpd[638]: kernel reports TIME_ERROR: 0x41: Clock Unsynchronized
aBr 10 18:40:15 kics4net-host-1 ntpd[638]: 80.240.216.155 local addr 172.31.18.87 -> <null>
aBr 10 18:40:19 kics4net-host-1 ntpd[638]: 193.192.36.3 local addr 172.31.18.87 -> <null>
kics@kics4net-host-1:~$
```

Если служба не запущена, активируем её автоматический запуск при старте и запускаем её -

«`sudo systemctl enable ntp`», «`sudo systemctl start ntp`»

```
kics@kics4net-host-1:~$ sudo systemctl start ntp
kics@kics4net-host-1:~$ sudo systemctl enable ntp
Synchronizing state of ntp.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ntp
kics@kics4net-host-1:~$
```

При наличии собственного сервера NTP необходимо добавить его в конфигурацию службы ntp –

«**sudo kate /etc/ntp.confclear**»

```
~: sudo kate — Терминал Fly
Файл Правка Настройка Справка
kics@kics4net-host-1:~$ sudo kate /etc/ntp.conf
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
trying to load "/usr/lib/x86_64-linux-gnu/qt5/plugins/kf5/kio/file.so" from "/usr/lib/x86_64-linux-

ntp.conf — Kate
Файл Правка Вид Закладки Сеанс Сервис Настройка Справка
ntp.conf
# Access control configuration: see /usr/share/doc/ntp-doc/html/acctopt.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.
# By default, exchange time with everybody, but don't allow configuration.
# Local users may interrogate the ntp server more closely.
# Needed for adding pool entries
# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
# restrict 192.168.123.0 mask 255.255.255.0 notrust
# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
# broadcast 192.168.123.255
# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines. Please do this only if you trust everybody on the network!
# disable auth
# broadcastclient
pool 0.debian.pool.ntp.org iburst
server 192.168.10.50 iburst
Строка: 1, столбец: 1
ВСТАВКА Отступы: 4 UTF-8 Normal
Поиск и замена
```

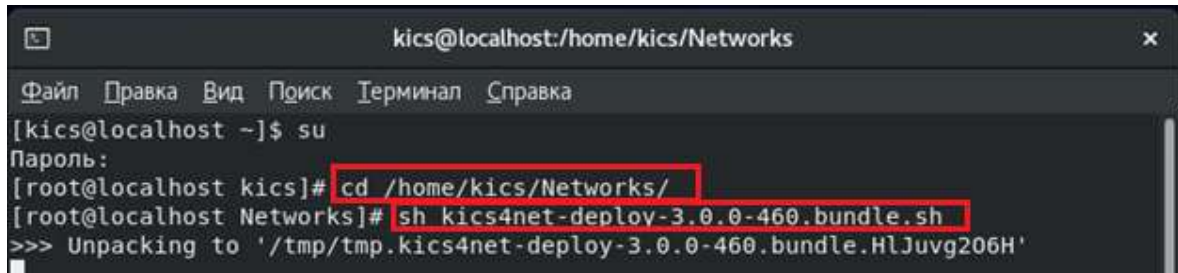
Сохраняем, закрываем и перезапускаем службу ntp – «**sudo systemctl restart ntp**», проверяем статус. Для успешной синхронизации так же должен быть доступен 123 порт.

```
kics@kics4net-host-1:~$ sudo systemctl restart ntp
kics@kics4net-host-1:~$ sudo systemctl status ntp
• ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-08-11 12:53:46 MSK; 2s ago
     Docs: man:ntpd(8)
   Process: 86734 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
  Main PID: 86740 (ntpd)
    Tasks: 2 (limit: 19660)
   CGroup: /system.slice/ntp.service
           └─86740 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 108:116

aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: leapsecond file ('/usr/share/zoneinfo/leap-seconds.list'):
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: Listen and drop on 0 v6wildcard [::]:123
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: Listen and drop on 1 v4wildcard 0.0.0.0:123
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: Listen normally on 2 lo 127.0.0.1:123
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: Listen normally on 3 eth0 172.31.18.87:123
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: Listening on routing socket on fd #20 for interface updates
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
aBr 11 12:53:46 kics4net-host-1 ntpd[86740]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
aBr 11 12:53:46 kics4net-host-1 systemd[1]: Started Network Time Service.
aBr 11 12:53:47 kics4net-host-1 ntpd[86740]: Soliciting pool server 46.17.46.226
kics@kics4net-host-1:~$
```


Установку KICS for Networks проводим под root (CentOS Stream),
sudo (Astra Linux).

Переходим в директорию, где лежат дистрибутивы и запускаем скрипт «kics4net-4.0.0-388.x86_64.rpm»



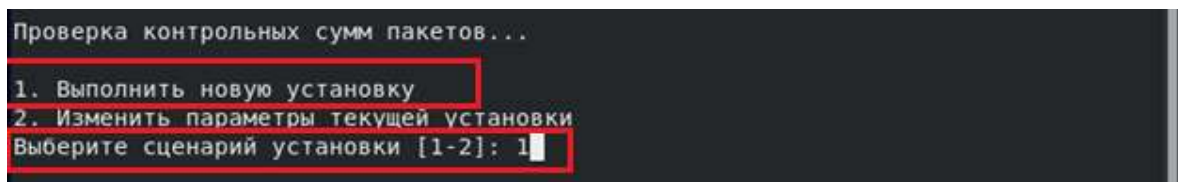
```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
[kics@localhost ~]$ su
Пароль:
[root@localhost kics]# cd /home/kics/Networks/
[root@localhost Networks]# sh kics4net-deploy-3.0.0-460.bundle.sh
>>> Unpacking to '/tmp/tmp.kics4net-deploy-3.0.0-460.bundle.HlJuvvg206H'
```

Выбираем язык меню скрипта:



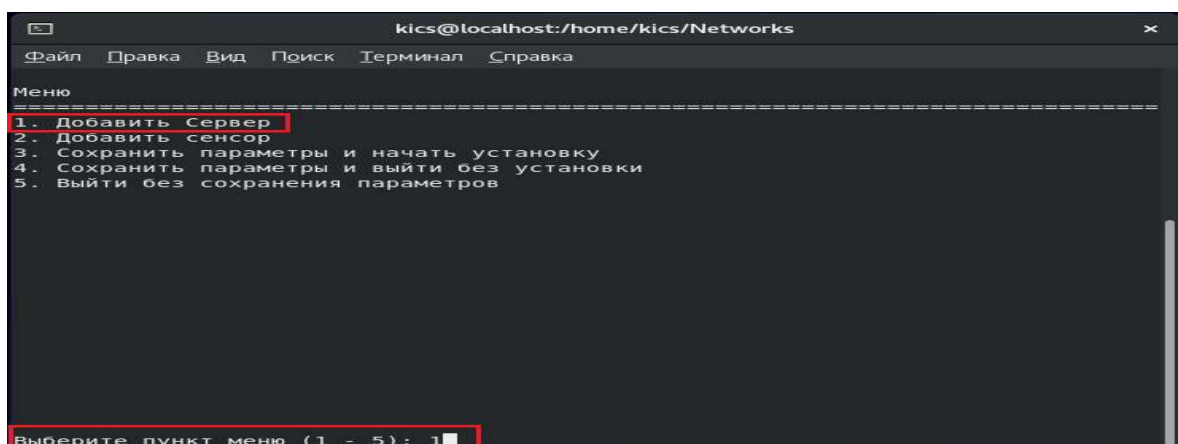
```
>>> Unpacking to '/tmp/tmp.kics4net-deploy-3.0.0-460.bundle.HlJuvvg206H'
1. English
2. Русский
Choose language [1-2]: 2
```

Выполняем новую установку, если ранее решение не устанавливалось:



```
Проверка контрольных сумм пакетов...
1. Выполнить новую установку
2. Изменить параметры текущей установки
Выберите сценарий установки [1-2]: 1
```

Добавляем новый сервер, выбираем пункт «1»:



```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
Меню
=====
1. Добавить Сервер
2. Добавить сенсор
3. Сохранить параметры и начать установку
4. Сохранить параметры и выйти без установки
5. Выйти без сохранения параметров
Выберите пункт меню (1 - 5): 1
```

Если предполагается распределенная установка обязательно указываем IP MGMT интерфейса (Например: 192.168.1.153) для сервера и сенсоров. В противном случае могут возникнуть проблемы с последующем подключением сенсоров к серверу KICS for Networks. Если используется инсталляция только с 1 сервером (all in one), то указываем localhost– «127.0.0.1».

Если планируется интеграция с KSC, подтверждаем установку агента администрирования «Y».
Активируем синхронизацию времени между сервером и сенсорами для распределенной установки «Y».(Для инсталляции all in one выбираем «N»)

```
kics@localhost:/home/kics/Networks
Файл  Правка  Вид  Поиск  Терминал  Справка
Добавление Сервера (чтобы вернуться в предыдущее меню, нажмите ENTER без ввода значения)
=====
Введите IP-адрес узла для установки: 192.168.1.153
Добавить функциональность взаимодействия программы с Kaspersky Security Center (y/n)? y
Включить синхронизацию времени между Сервером и сенсорами (y/n)? y
```

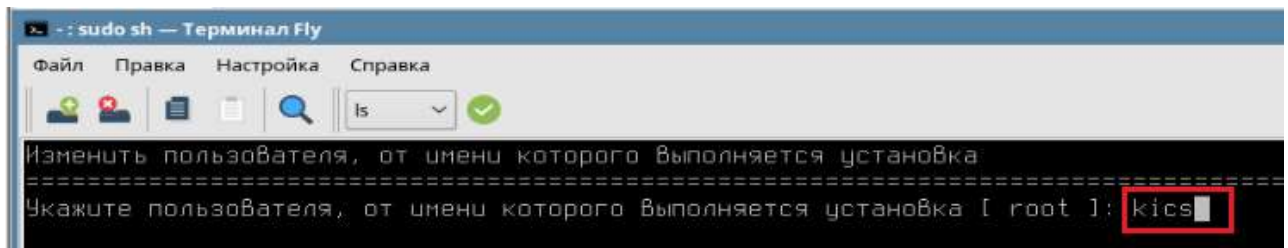
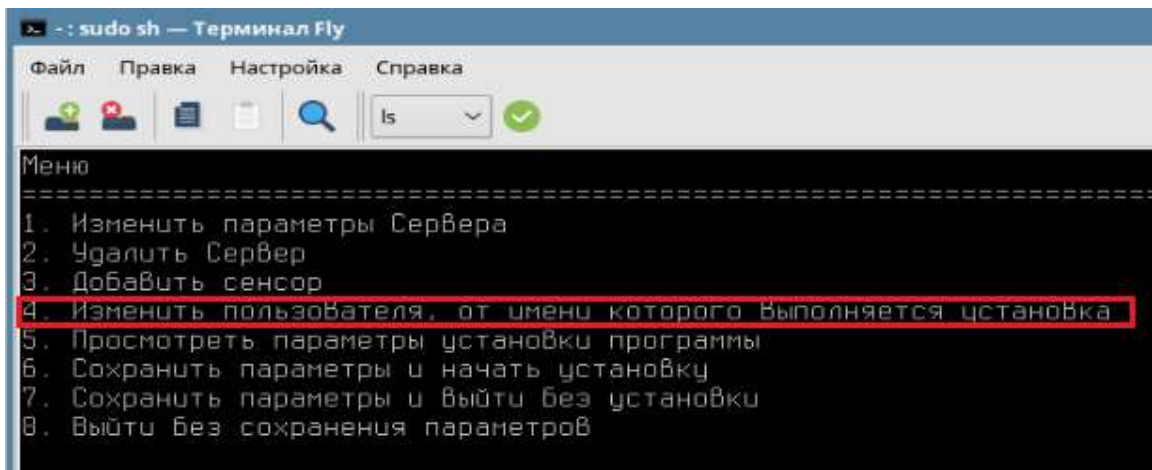
Добавляем сенсор, выбираем пункт «3» (добавление сенсора не требуется, если используется инсталляция с 1 сервером (all in one)):

```
kics@localhost:/home/kics/Networks
Файл  Правка  Вид  Поиск  Терминал  Справка
Меню
=====
1. Изменить параметры Сервера
2. Удалить Сервер
3. Добавить сенсор
4. Изменить пользователя, от имени которого выполняется установка
5. Просмотреть параметры установки программы
6. Сохранить параметры и начать установку
7. Сохранить параметры и выйти без установки
8. Выйти без сохранения параметров
=====
Выберите пункт меню (1 - 8): 3
```

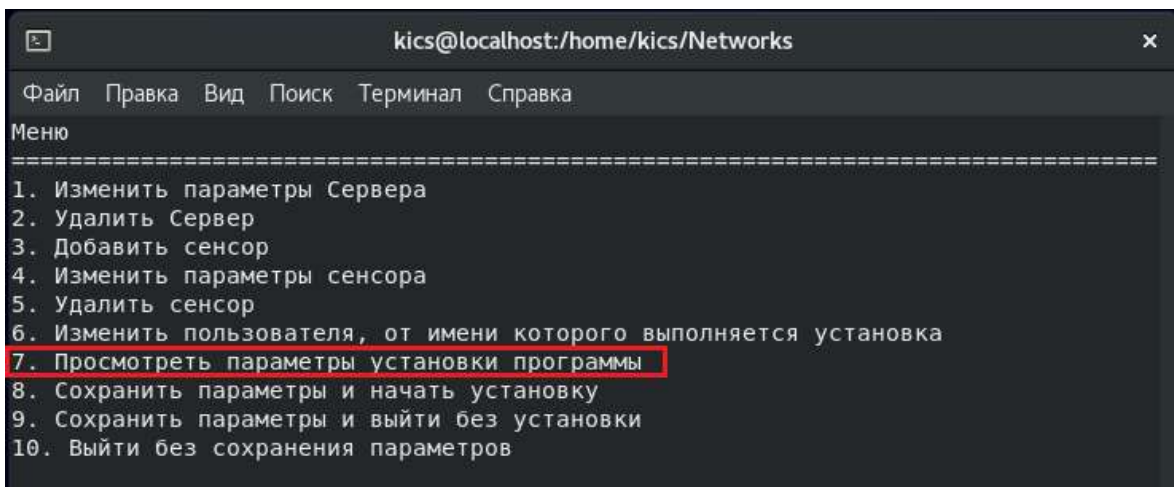
Указываем IP адрес сенсора, настроенный на MGMT интерфейс:

```
kics@localhost:/home/kics/Networks
Файл  Правка  Вид  Поиск  Терминал  Справка
Добавление сенсора (чтобы вернуться в предыдущее меню, нажмите ENTER без ввода значения)
=====
Введите IP-адрес узла для установки: 192.168.1.197
```

При установке на Astra Linux изменяем пользователя с root на администратора (Например, kics)



Проверяем настройки указанные ранее, выбираем пункт «7» - Просмотреть параметры установки программы:



```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
Просмотр параметров установки программы
=====
Пользователь, от имени которого выполняется установка: root
Синхронизация времени между Сервером и сенсорами: включено
[Сервер] (192.168.1.153)
    Аппаратный таймер наблюдения: выключено
    Взаимодействие программы с Kaspersky Security Center: включено
    Повторное создание базы данных: выключено
    Имя узла, на котором запущен публичный gRPC-сервер: localhost
    Создать новые сертификаты: включено
[Сенсор] (192.168.1.197)
    Аппаратный таймер наблюдения: выключено
```

Приступаем к установке, выбираем пункт «8» - Сохранить параметры и начать установку:

```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
Меню
=====
1. Изменить параметры Сервера
2. Удалить Сервер
3. Добавить сенсор
4. Изменить параметры сенсора
5. Удалить сенсор
6. Изменить пользователя, от имени которого выполняется установка
7. Просмотреть параметры установки программы
8. Сохранить параметры и начать установку
9. Сохранить параметры и выйти без установки
10. Выйти без сохранения параметров
```

Вводим пароль (2 раза) для пользователя, под которым проводим установку KICS for Networks

```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
1. Изменить параметры Сервера
2. Удалить Сервер
3. Добавить сенсор
4. Изменить параметры сенсора
5. Удалить сенсор
6. Изменить пользователя, от имени которого выполняется установка
7. Просмотреть параметры установки программы
8. Сохранить параметры и начать установку
9. Сохранить параметры и выйти без установки
10. Выйти без сохранения параметров

Выберите пункт меню (1 - 10): 8
SSH password:
BECOME password(defaults to SSH password):
```

Ждем завершения установки. При успешной установке графа «failed = 0», для каждого узла.

```
kics@localhost:/home/kics/Networks
Файл Правка Вид Поиск Терминал Справка
skipping: [192.168.1.197]
changed: [192.168.1.153]

TASK [Persist firewall configuration (CentOS 8 specific)] *****
changed: [192.168.1.197]
changed: [192.168.1.153]

PLAY [127.0.0.1] *****

TASK [Delete temporary certificates dir on a deployer host] *****
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1 : ok=5 changed=3 unreachable=0 failed=0 s
kipped=0 rescued=0 ignored=0
192.168.1.153 : ok=137 changed=69 unreachable=0 failed=0 s
kipped=77 rescued=0 ignored=6
192.168.1.197 : ok=107 changed=46 unreachable=0 failed=0 s
kipped=97 rescued=0 ignored=6

Установка Kaspersky Industrial CyberSecurity for Networks выполнена успешно.
Deployment duration: 04m:22s
>>> Deleting '/tmp/tmp.kics4net-deploy-3.0.0-460.bundle.7bXeaD8Gz9'
[root@localhost Networks]#
```