UDV NTA Network Traffic Analyzer v.1.0

Инструкция по установке

cyberlympha.ru | support@cyberlympha.com

Содержание

1. Общая информация

В документе приведены общие инструкции для установки UDV NTA уровней Sensor и Management в операционной системе Альт Сервер 10 SP. Команды, которые отличаются для разных уровней развертывания, также приведены в общих инструкциях.

2. Справочная информация

В этом разделе:

2.1. Системные требования для установки и работы Комплекса

Требования для установки Комплекса

Минимальные системные требования для установки Комплекса приведены в таблице ниже (Таблица 1. Системные требования для установки Комплекса)

Табл. 1. Системные требования для установки Комплекса

	КОМПЛЕКС УРОВНЯ MANAGEMENT	КОМПЛЕКС УРОВНЯ SENSOR
Процессор	• 3,1 ГГц • 20 логических ядер	• 2,4 ГГц • 16 логических ядер
ОЗУ	64 ГБ	32 ГБ
Диск [1]	• 1 ТБ • SSD • аппаратный RAID	• 512 ГБ • SSD
Материнская плата	Поддержка UEFI	
Операционная система [2]	Альт СП релиз 10 версия 2	

> **Внимание:**
>
> Текущие системные требования актуальны при развертывании Комплекса в средах виртуализации.

Требования к клиентским обозревателям

Поддерживаемые обозреватели (браузеры):

- браузеры семейства Chromium (Google Chrome, Microsoft Edge, Яндекс.Браузер) версии 116 и выше;
- Mozilla Firefox версии 117 и выше.

1. Не включая объем для хранения копии сетевого трафика.
2. ОС не входит в комплект поставки Комплекса и приобретается отдельно.

Требования к разрешению экрана

Минимальное разрешение экрана для работы в веб-интерфейсе Комплекса — `1366x768`.

2.2. Архитектура UDV NTA

В UDV NTA реализован механизм, предоставляющий возможности по выстраиванию двух уровней иерархии. Каждый уровень иерархии представлен отдельным вариантом исполнения.

- UDV NTA уровня Sensor — обладает набором функций по глубокой инспекции пакетов до уровня приложений, анализу переданных команд по сети, хранению копии сетевого трафика, а также файлов, переданных по сети. Не имеет веб-интерфейса. Управление сенсорами выполняет Комплекс уровня Management
- UDV NTA уровня Management — обладает набором функций по хранению, индексации и визуализации метаданных сетевого трафика, а также возможностью анализа и корреляции событий безопасности и настройки правил обнаружения вторжений. Управляет сенсорами: отправляет им команды и обновления баз правил, а также получает с них оперативные данные.

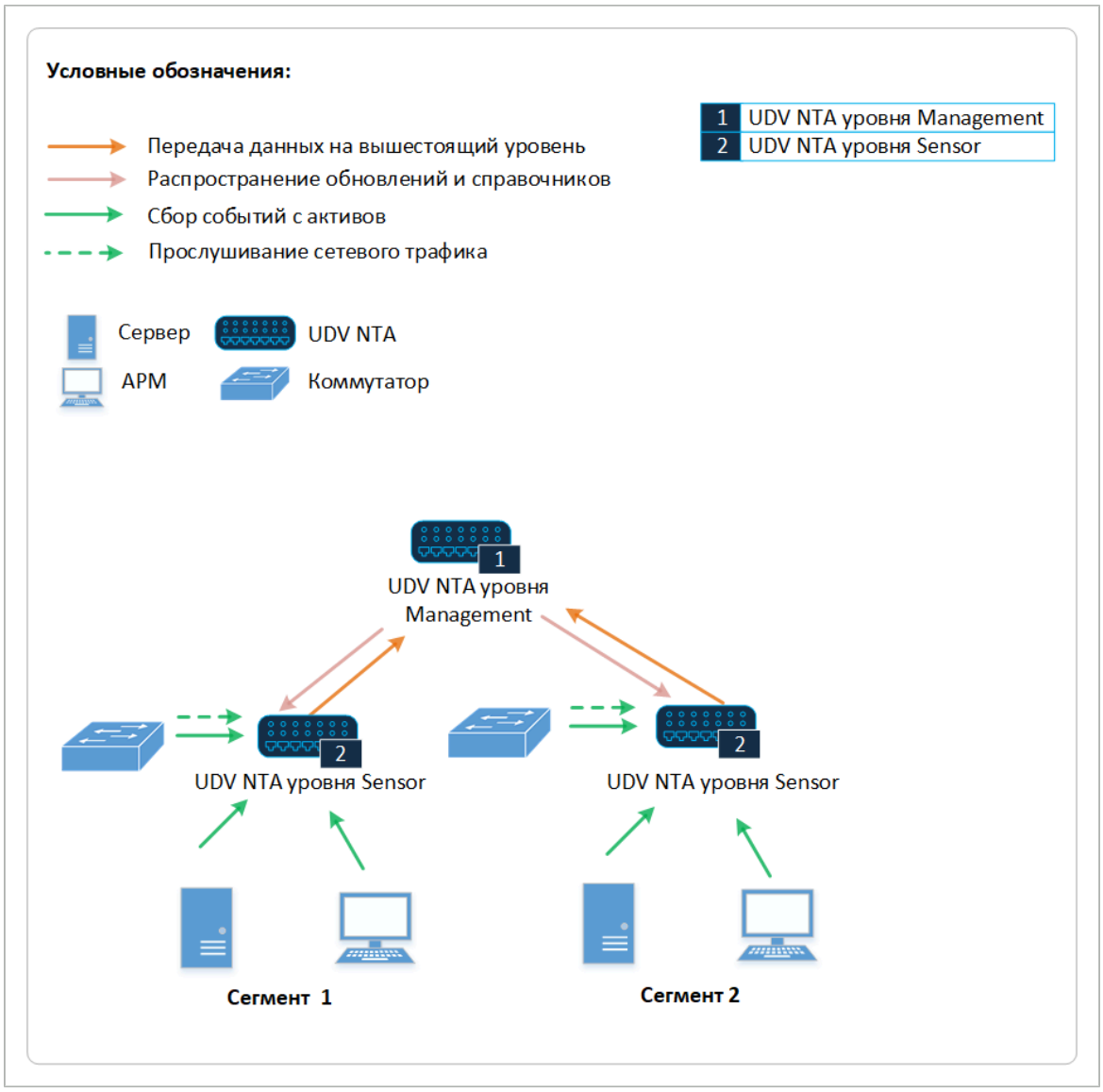

Рис. 1. Структурная схема иерархии

Порядок передачи информации по иерархии Комплексов

Предусмотрен следующий порядок взаимодействия между уровнями иерархии:

- Sensor → Management — передача оперативных данных (выявленные активы, метаданные сетевого трафика, полученные события ИБ).
- Management → Sensor — передача управляющих команд, обновлений, справочников (решающих правил).

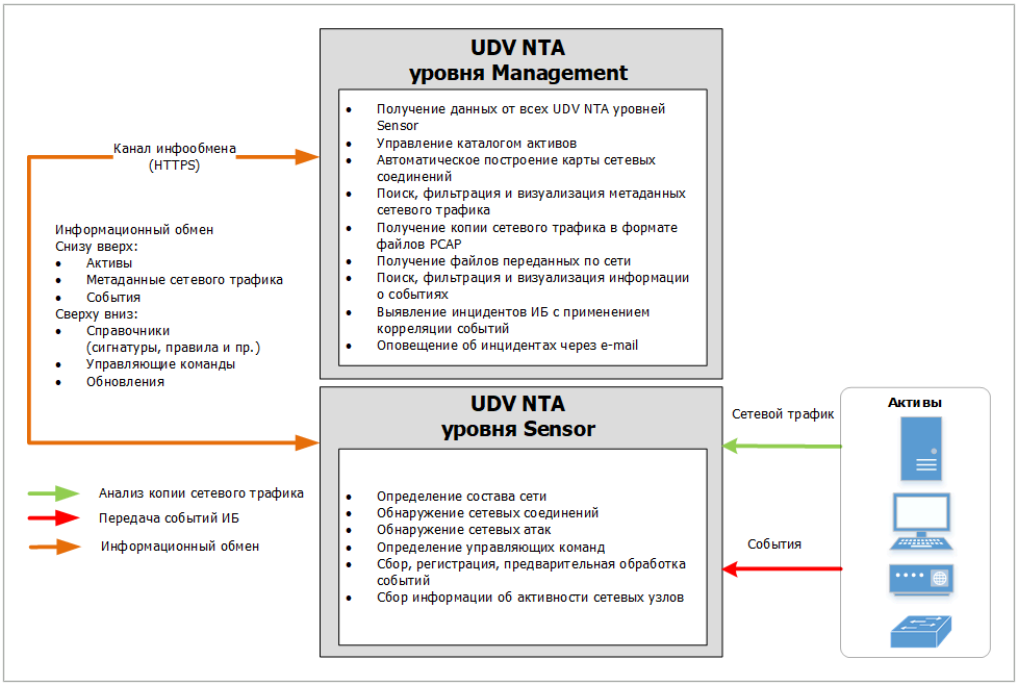

Рис. 2. Схема информационных потоков на различных уровнях иерархии

2.3. Назначение и основные функции

Назначение

Комплекс предназначен для выявления и расследования инцидентов, проактивного поиска угроз и контроля соблюдения политик информационной безопасности на основе анализа копии сетевого трафика.

Основные функции

1. Анализ сетевого трафика:
    - разбор протоколов до уровня L7;
    - запись и хранение копий сетевого трафика в формате PCAP для ретроспективного анализа;
    - хранение и анализ файлов, передаваемых в рамках сетевых сессий, с проверкой их на вредоносное ПО.
2. Обнаружение угроз:
    - сигнатурное обнаружение вторжений с помощью встроенных правил;
    - выявление атак на основе экспертных правил и методов машинного обучения.
3. Работа с инцидентами:
    - агрегация событий, корреляция данных и формирование инцидентов;
    - мониторинг через панели визуализации.
4. Выявление скрытых узлов:
    - обнаружение несанкционированных устройств в сети.

3. Установка и настройка сертифицированной ОС Альт Сервер 10 SP

В этом разделе:

Для установки и настройки сертифицированной ОС Альт Сервер 10 SP выполните следующие инструкции:

- Установка сертифицированной ОС Альт Сервер 10 SP
- Настройка сертифицированной ОС Альт Сервер 10 SP

Для увеличения производительности системы сбора внешних событий в ходе установки сертифицированной ОС Альт Сервер 10 SP необходимо выполнить разделение диска на логические разделы. При необходимости настройки логических разделов выполните следующие инструкции:

- Установка сертифицированной ОС Альт Сервер 10 SP с разделением диска на логические разделы
- Настройка сертифицированной ОС Альт Сервер 10 SP

3.1. Файлы, необходимые для установки ОС Альт Сервер 10 SP

Для установки ОС Альт Сервер 10 SP необходимы следующие файлы:

1. Дистрибутив ОС Альт Сервер 10 SP.
2. Архив репозитория `nta-1.0.tar`.

3.2. Установка сертифицированной ОС Альт Сервер 10 SP

Для установки ОС Альт Сервер:

1. Подключите ISO-образ ОС Альт Сервер `alt-sp-server-[дата версии]-x86_64.iso`.
   - **Результат шага:** окно установки откроется автоматически или по нажатию любой клавиши.
2. Выберите пункт меню **Rescue LiveCD** и нажмите клавишу **Enter**.

Рис. 3. Загрузка платформы в режиме Rescue LiveCD

- **Результат шага:** появится оболочка bash LiveCD ОС Альт Сервер.

3. Для подготовки к разметке дискового пространства:

   а. Просмотрите наименование диска, для которого будет выполняться разметка дискового пространства:

   ```
   fdisk -lu
   ```

   > Внимание:
   >
   > Разметка дискового пространства для установки ОС Альт Сервер должна выполняться на пустом и не размеченном ранее диске.

   Пример

   Результат команды:

   ```
   Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
   Disk model: Virtual disk
   Units: sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disklabel type: gpt
   Disk identifier: 9E3B26FD-87A0-438D-9E66-124AD43F1000
   ```

   где `/dev/sda` — наименование диска.

   б. Создайте переменную `D` и присвойте ей наименование диска, для которого будет выполняться разметка дискового пространства:

   ```
   D=[наименование_диска]
   ```

   Пример

Создание переменной `D` с наименованием диска `/dev/sda`:

```
D=/dev/sda
```

в. Создайте дисковые разделы. Для этого:

- Создайте переменную `V` и присвойте ей в качестве значения переменную `${D}` и номер третьего раздела диска:

```
V=${D}3
```

- Последовательно введите следующие команды для создания дисковых разделов:

```
wipefs -a $D
parted $D mktable gpt
parted $D mkpart primary 1MiB 255MiB set 1 esp on
parted $D mkpart primary 256MiB 260MiB set 2 bios_grub on
parted $D mkpart primary 261MiB 100% set 3 lvm on
blockdev --flushbufs $D
```

г. Просмотрите наименования созданных разделов диска:

```
fdisk -lu
```

Пример

Результат команды:

```
Device       Start       End   Sectors  Size Type
/dev/sda1     2048    522239    520192  254M EFI System
/dev/sda2   524288    532479      8192    4M BIOS boot
/dev/sda3   534528  78125055  77590528   37G Linux LVM
```

где `p1`, `p2`, `p3` — наименования созданных разделов диска `/dev/nvme0n1`.

д. Создайте переменную `V` и присвойте ей в качестве значения переменную `${D}` и наименование одного из созданных разделов диска следующим образом:

```
V=${D}[наименование_раздела]
```

Пример

Создание переменной `V` с наименованием подраздела `p3`:

```
V=${D}p3
```

е. Последовательно введите следующие команды для настройки физических разделов диска:

```
pvcreate $V
vgcreate datapk $V
lvcreate -l 100%FREE -n rootfs datapk
blockdev --flushbufs $D
reboot
```

```
[root@localhost /]# D=/dev/sda
[root@localhost /]# wipefs -a $D
[root@localhost /]# parted $D mktable gpt
Information: You may need to update /etc/fstab.

[root@localhost /]# parted $D mkpart primary 1MiB 255MiB set 1 esp on
Information: You may need to update /etc/fstab.

[root@localhost /]# parted $D mkpart primary 256MiB 260MiB set 2 bios_grub on
Information: You may need to update /etc/fstab.

[root@localhost /]# parted $D mkpart primary 261MiB 100% set 3 lvm on
Information: You may need to update /etc/fstab.

[root@localhost /]# blockdev --flushbufs $D
[root@localhost /]# V=${D}3
[root@localhost /]# pvcreate $V
  Physical volume "/dev/sda3" successfully created.
[root@localhost /]# vgcreate datapk $V
  Volume group "datapk" successfully created
[root@localhost /]# lvcreate -l 100%FREE -n rootfs datapk
  Logical volume "rootfs" created.
[root@localhost /]# blockdev --flushbufs $D
[root@localhost /]# reboot
```

Рис. 4. Команды для подготовки диска к установке ОС Альт Сервер

- **Результат шага:** выполнена подготовка к разметке дискового пространства ОС Альт Сервер. Платформа будет перезагружена.

4. После перезагрузки выберите пункт меню **Install ALT SP Server** и нажмите клавишу **Enter**.

Рис. 5. Окно установки ОС Альт Сервер

- **Результат шага:** появится окно **Язык**.

5. Если после выбора пункта меню **Install ALT SP Server** отображается пустой экран и установка не начинается, необходимо отключить загрузку видеодрайверов. Для этого:

а. Выберите пункт меню **Install ALT SP Server** и нажмите клавишу **E**.

Рис. 6. Экран выбора действия после монтирования образа ОС Альт Сервер

б. Добавьте параметр `nomodeset` перед строкой, начинающейся на `$EFI_BOOTARGS`, как указано на рисунке ниже.

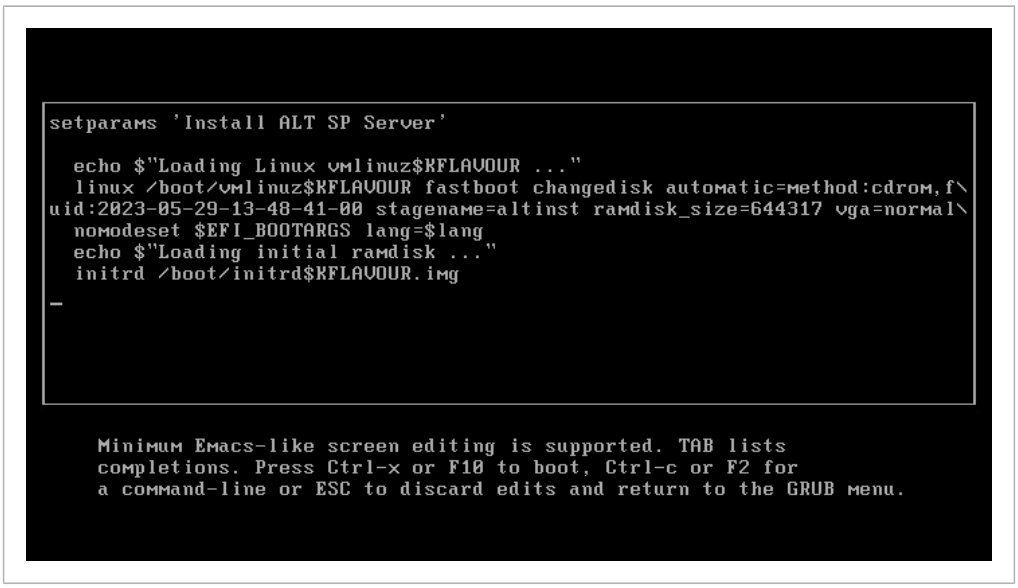

Рис. 7. Добавление параметра «nomodeset»

в. Нажмите клавишу **F10** или сочетание клавиш **CTRL + X**.

- **Результат шага:** установка будет запущена с новыми параметрами.

6. В окне **Язык** настройте язык и раскладку клавиатуры. Для этого:

а. Выберите язык **Русский**.

б. Установите способ переключения раскладки **Клавиши Alt и Shift одновременно**.

в. Нажмите **Далее**.

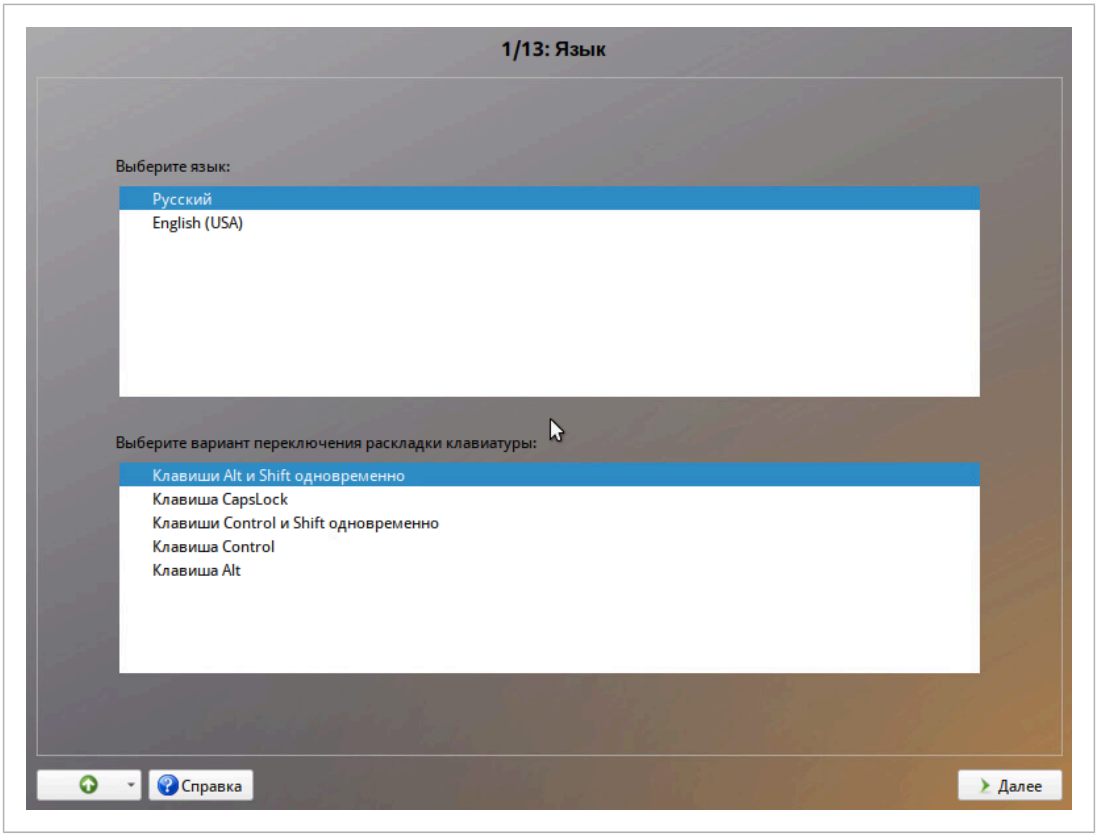

Рис. 8. Окно настройки языка и раскладки клавиатуры ОС Альт Сервер

- **Результат шага:** появится окно **Подтверждение согласия**.

7. Ознакомьтесь с лицензионным соглашением. Установите чекбокс **Да, я согласен с условиями** и нажмите **Далее**.

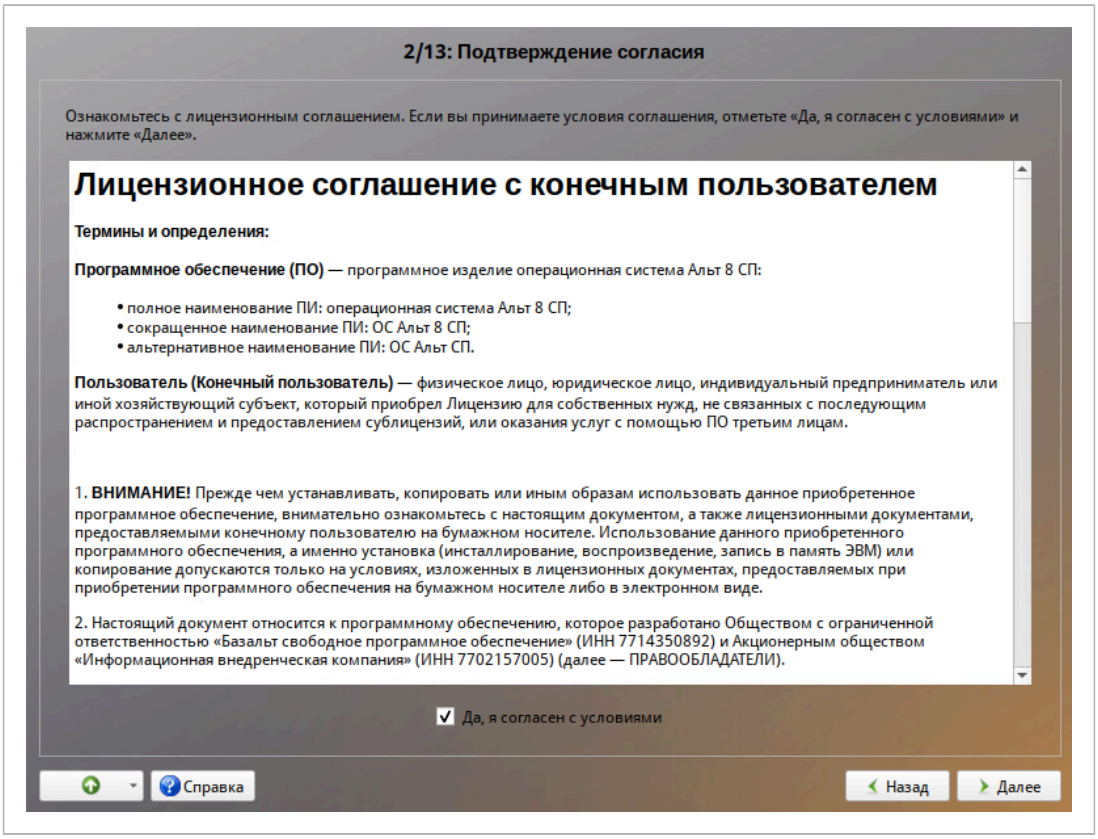

Рис. 9. Окно лицензионного соглашения установки ОС Альт Сервер

- **Результат шага:** появится окно **Дата и время**.

8. В окне **Дата и время** выберите текущий регион и часовой пояс и нажмите **Далее**.

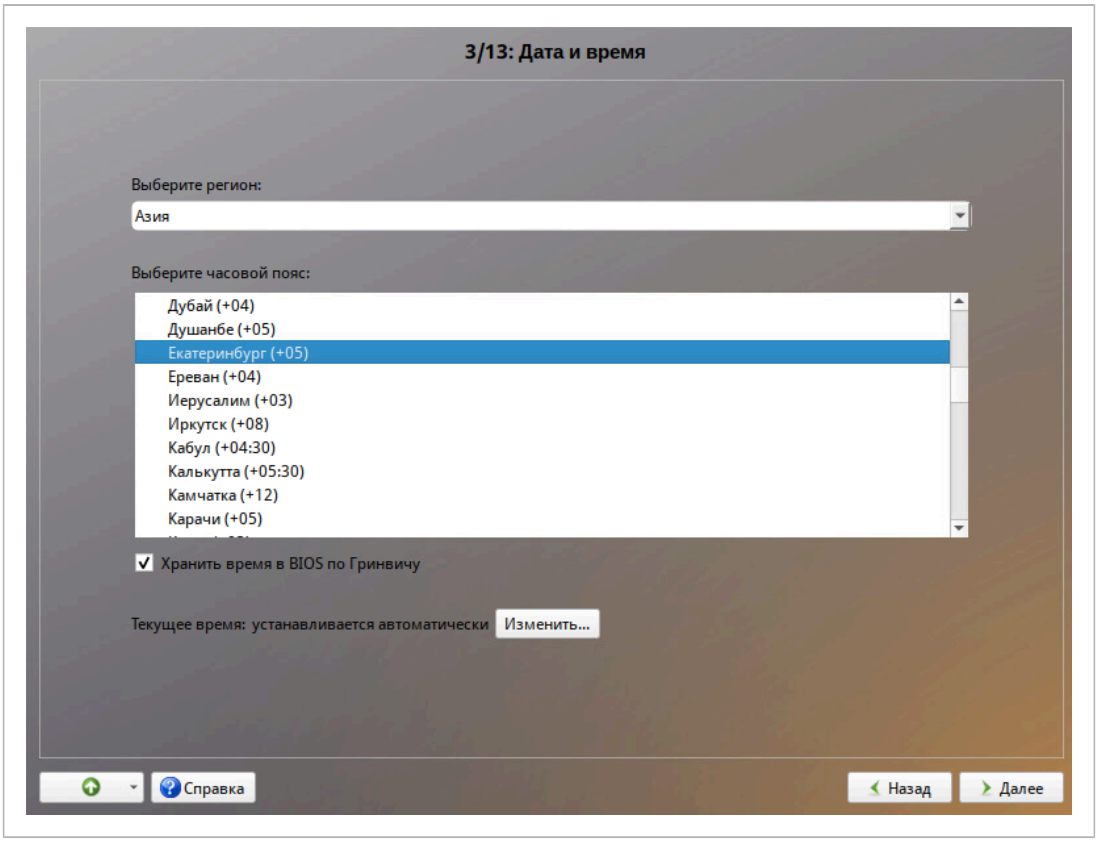

Рис. 10. Окно «Дата и время»

- **Результат шага:** появится окно **Подготовка диска**.

9. Выполните разметку дискового пространства. Для этого:

   a. В поле **Выберите профиль** установите чекбокс **Вручную** и нажмите **Далее**.

   - **Результат шага:** появится окно с разделами диска.

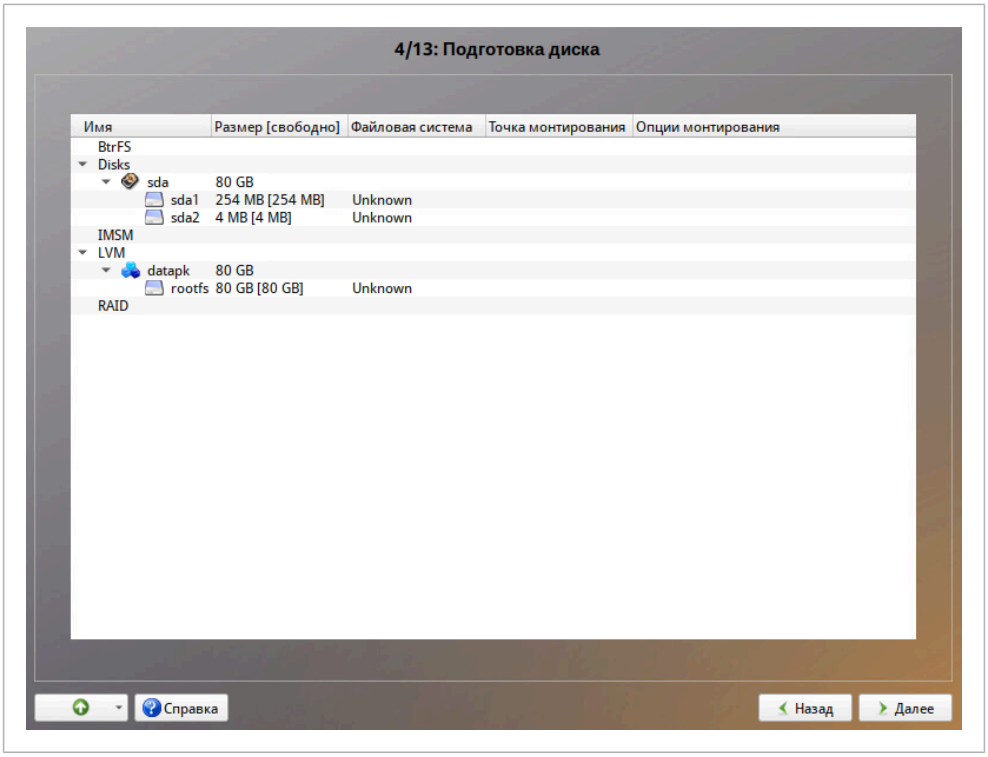

Рис. 11. Окно «Подготовка диска»

б. В раскрывающемся списке **Disks** выберите настроенный ранее раздел диска (например, `nvme0n1p1` или `sda1`) и нажмите **Изменить точку монтирования**.

в. В новом окне выберите **Файловая система FAT32** и нажмите **OK**.

г. В новом окне оставьте поле **Метка тома** пустым и нажмите **OK**.

д. В следующем окне убедитесь, что в поле **Точка монтирования** указано **/boot/efi**, и нажмите **OK**.

- **Результат шага:** появится окно с разделами диска.

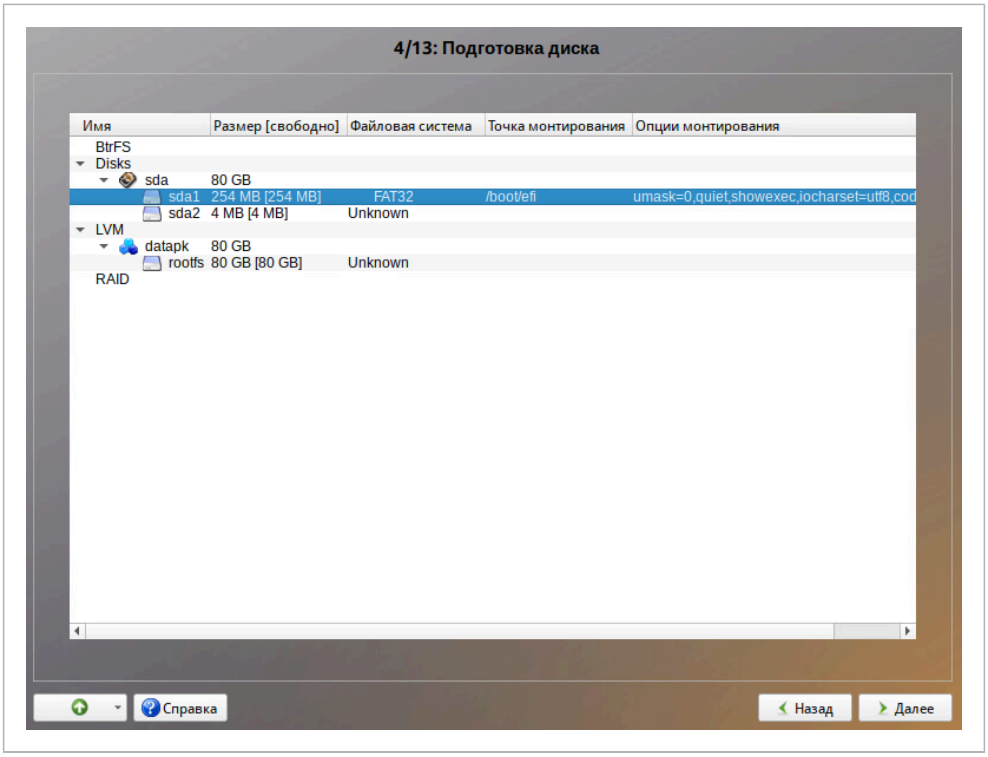

Рис. 12. Окно «Подготовка диска» (форматирование раздела на примере sda1)

е. В раскрывающемся списке **LVM** выберите **rootfs** и нажмите **Создать файловую систему**.

ж. В новом окне выберите **Файловая система XFS** и нажмите **OK**.

> Внимание:
>
> Необходимо создавать разделы объемом не более 500 ГБ при разметке дискового пространства в файловой системе xfs на ОС Альт Сервер. При необходимости объем можно увеличить после завершения установки.

з. В новом окне оставьте поле **Метка тома** пустым и нажмите **OK**.

и. В следующем окне убедитесь, что в поле **Точка монтирования** указано **/**, и нажмите **OK**.

- **Результат шага:** появится окно подготовки диска со списком томов в созданной группе.

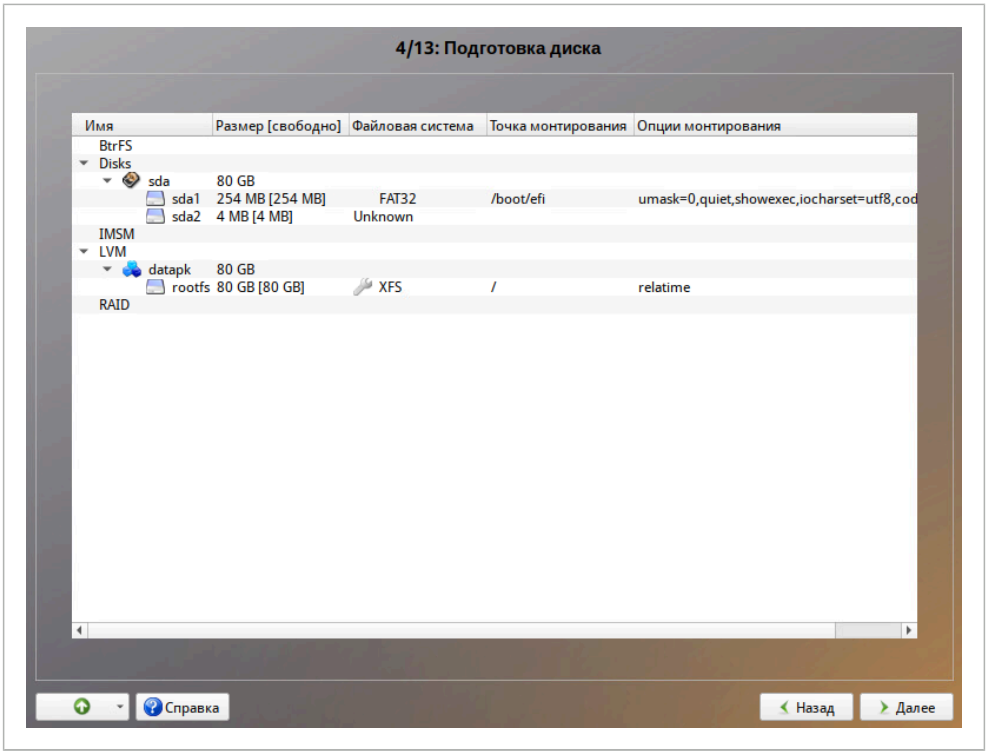

Рис. 13. Окно «Подготовка диска» (форматирование раздела rootfs)

к. Для применения настроек нажмите **Далее**.

л. Во всплывающем окне для продолжения нажмите **ОК**.

- **Результат шага:** начнется установка ОС Альт Сервер.

10. Дождитесь окончания установки ОС Альт Сервер.
    - **Результат шага:** появится окно **Установка загрузчика**.
11. Убедитесь, что в поле **Устройство:** выбрано устройство **EFI** для установки загрузчика. При необходимости установите пароль на вход в загрузчик. Нажмите **Далее**.

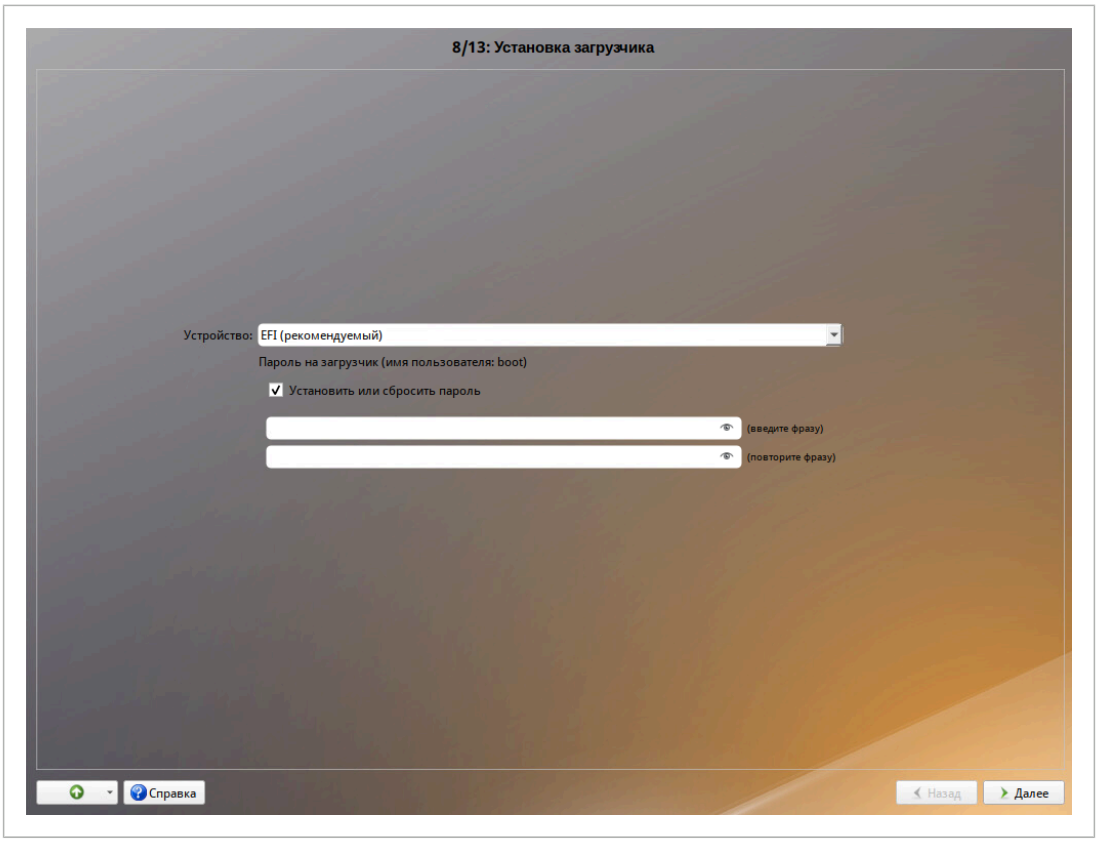

Рис. 14. Окно «Установка загрузчика»

- **Результат шага:** появится окно **Настройка сети**.

12. Выполните настройку сетевых интерфейсов. Для этого:

> Подсказка:
>
> Интерфейс для прослушивания копии сетевого трафика не требуется настраивать на этапах установки и настройки ОС.

а. В поле **Имя компьютера:** введите сетевое имя для UDV NTA.

б. В поле **Интерфейсы** выберите сетевой интерфейс, который будет использоваться для управления UDV NTA.

> Прим.:
>
> Чтобы узнать, в какой сетевой интерфейс физически подключен интернет-кабель, при выборе сетевого интерфейса просмотрите его описание: если указан статус провод подсоединен, значит кабель подключен к выбранному интерфейсу.

в. В поле **Конфигурация** выберите **Вручную**.

г. В поле **IP** введите IP-адрес интерфейса и выберите маску для интерфейса управления. Нажмите **Добавить**.

д. В поле **Шлюз по умолчанию** введите IP-адрес шлюза для интерфейса управления.

е. В поле **DNS-серверы** введите адреса DNS-серверов для интерфейса управления.

> Прим.:
>
> Интерфейс для прослушивания копии сетевого трафика настраивать не требуется.

ж. Нажмите **Далее**.

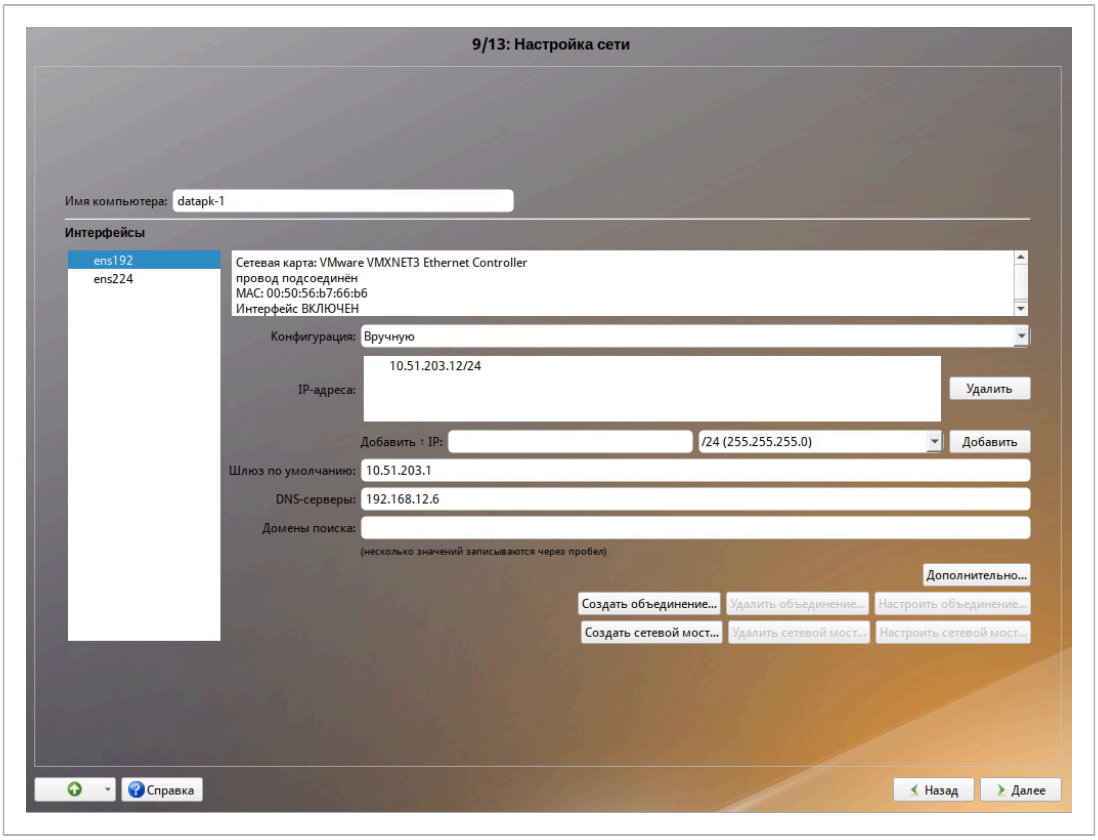

Рис. 15. Окно «Настройка сети»

- **Результат шага:** появится окно **Администратор системы**.

13. Введите и подтвердите новый пароль администратора `root`. Нажмите **Далее**.

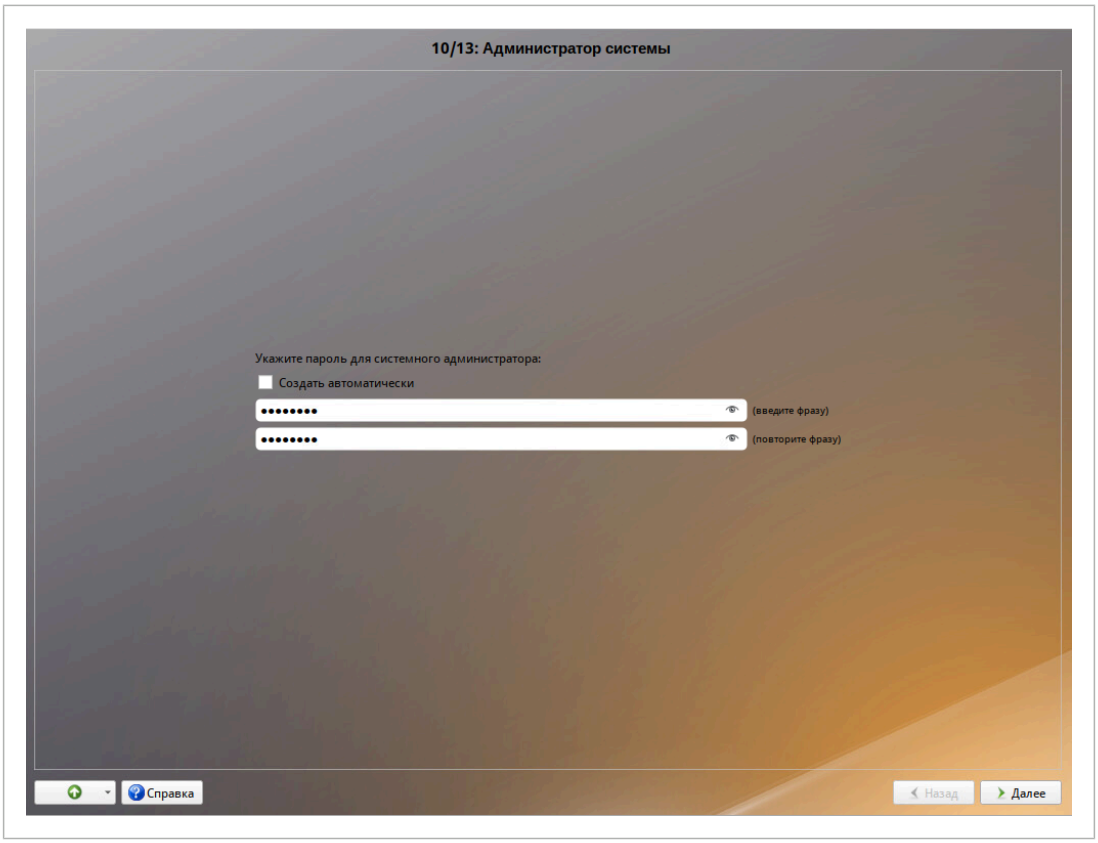

Рис. 16. Окно «Администратор системы»

- **Результат шага:** появится окно **Системный пользователь**.

14. Выполните настройку новой учетной записи пользователя с правами администратора. Для этого:
    a. Введите имя (логин) пользователя `nta`.
    б. Введите и подтвердите новый пароль пользователя.
    в. Нажмите **Далее**.

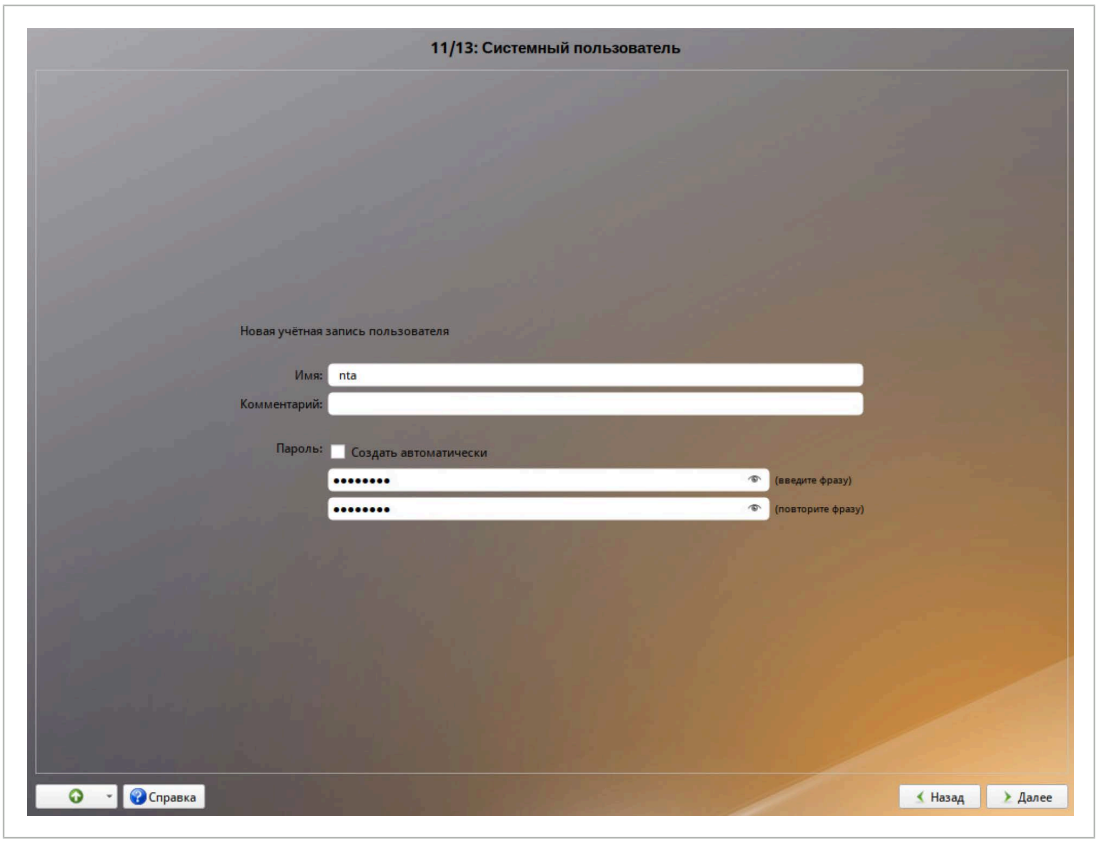

Рис. 17. Окно «Системный пользователь»

- **Результат шага:** появится окно **Завершение установки**.

15. Нажмите **Завершить** и дождитесь перезагрузки ОС Альт Сервер.

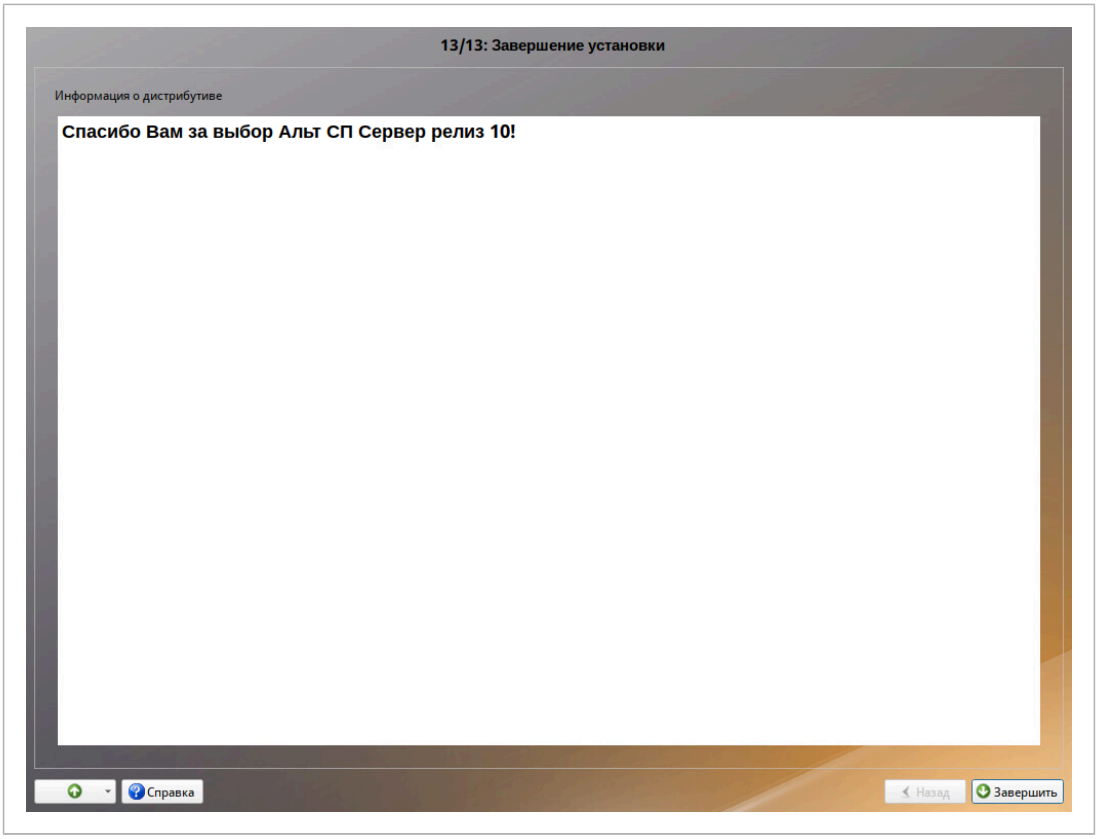

Рис. 18. Окно «Завершение установки»

- **Результат шага:** ОС Альт Сервер будет установлена и перезагружена. Появится строка для ввода логина.

Если после установки требуется изменить настройки сетевых интерфейсов, перейдите к разделу «Настройка сетевых интерфейсов в терминале Комплекса». Если после установки требуется изменить сетевое имя Комплекса, перейдите к разделу «Изменение сетевого имени Комплекса».

3.3. Настройка сертифицированной ОС Альт Сервер 10 SP

1. Подключитесь к виртуальной машине UDV NTA по протоколу SSH:

   а. Откройте программу-клиент SSH.

   б. Выполните команду для подключения к UDV NTA и нажмите клавишу **Enter**:

   ```
   ssh nta@[ip_addr]
   ```

   Где `[ip_addr]` — IP-адрес сетевого интерфейса управления UDV NTA.

   в. Введите пароль созданной учетной записи, нажмите клавишу **Enter** для подключения.

   > Прим.:
   >
   > При вводе пароль отображаться не будет.

г. Повысьте привилегии, выполнив команду для смены учетной записи на `root`:

```
su -
```

д. Введите пароль учетной записи `root` и нажмите клавишу **Enter**.

> Прим.:
>
> При вводе пароль отображаться не будет.

- **Результат шага:** выполнен вход в операционную систему под учетной записью `root` по протоколу SSH.

2. При наличии доступа в сеть Интернет установите и обновите необходимое ПО и ядро ОС Альт Сервер следующим способом:

> Подсказка:
>
> Для установки и обновления компонентов ОС Альт Сервер при отсутствии доступа в сеть Интернет см. раздел «Обновление компонентов ОС Альт Сервер без доступа в Интернет». После обновления без использования сети Интернет сразу перейдите к шагу 3.

а. Добавьте репозиторий пакетов и установите пакет `sudo`. Для этого:

- Скопируйте сертифицированный образ ОС Альт Сервер в директорию `/home/nta`.
- Смонтируйте образ ОС Альт Сервер, выполнив команду:

```
mount -o loop /home/nta/alt-sp-server-[дата версии]-x86_64.iso /media/ALTLinux
```

- Добавьте образ ОС Альт Сервер в качестве репозитория пакетов, выполнив команду:

```
apt-cdrom --no-mount -d=/media/ALTLinux add
```

- Установите пакет `sudo`, выполнив команду:

```
apt-get update && apt-get install sudo -y
```

б. Удалите все текущие репозитории:

```
apt-repo rm all
```

в. Откройте для редактирования конфигурационный файл со ссылками на репозитории:

```
mcedit /etc/apt/sources.list.d/altsp.list
```

г. Раскомментируйте репозитории (либо все с `http`, либо все с `ftp` в адресе), удалив символ `#`:

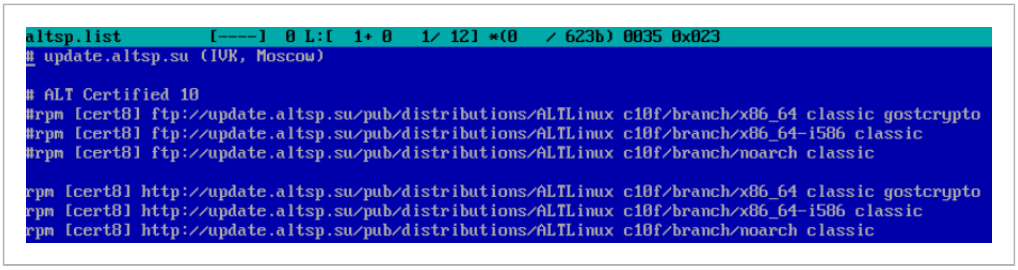

Рис. 19. Включение репозиториев ОС Альт Сервер по протоколу HTTP

ОСТОРОЖНО:

Может быть выбран только один тип репозиториев (`http` либо `ftp`), иначе попытки обновления ОС Альт Сервер будут неудачны.

д. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.

е. Выполните обновление ПО в составе ОС Альт Сервер:

```
apt-get update && apt-get dist-upgrade -y && update-kernel -y
```

Внимание:

Если при выполнении команды будут возникать ошибки вида `Невозможно получить [наименование_пакета], Bizzare error ...`, выполните команду повторно. При повторном возникновении ошибок обратитесь в сервисный центр «Базальт СПО».

- **Результат шага:** ПО и ядро ОС Альт Сервер обновлены до актуальной версии.

ж. Выполните перезагрузку ОС Альт Сервер:

```
shutdown -r now
```

- **Результат шага:** ОС Альт Сервер перезагружена.

з. Повторно выполните вход в ОС Альт Сервер под учетной записью `root`.

3. Настройте доступ по протоколу SSH:

а. Откройте конфигурационный файл `sshd_config`:

```
mcedit /etc/openssh/sshd_config
```

б. Раскомментируйте следующие параметры, удалив символ `#`:

```
GSSAPIAuthentication no
UseDNS no
```

> Прим.:
>
> В конфигурационном файле `sshd_config` можно также настроить доступ к комплексу по протоколу SSH для учетной записи суперпользователя. Для этого необходимо раскомментировать параметр `PermitRootLogin without-password` и изменить его на `PermitRootLogin yes`, но делать это не рекомендуется.

в. Закройте конфигурационный файл `sshd_config` с сохранением изменений.

г. Для применения новых настроек перезапустите службу SSH:

```
systemctl restart sshd
```

4. > Внимание:
   >
   > При работе в учетной записи `nta` может потребоваться использование `sudo` для выполнения некоторых команд. Для добавления возможности использования `sudo`:
   >
   > a. Откройте для редактирования конфигурационный файл `sudoers`, выполнив команду:
   >
   > ```
   > mcedit /etc/sudoers
   > ```
   >
   > b. В поле `User privilege specification` добавьте запись:
   >
   > ```
   > nta ALL=(ALL:ALL) ALL
   > ```
   >
   > c. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.

Для применения настроек выполните повторный вход в учетную запись `nta` по протоколу SSH.

5. Настройте синхронизацию времени. Для этого:

а. Откройте для редактирования конфигурационный файл `chrony.conf`:

```
mcedit /etc/chrony.conf
```

б. Удалите или закомментируйте строку `pool pool.ntp.org iburst`. Добавьте адреса существующих NTP-серверов, добавив для каждого сервера следующую строку:

```
server [IP-адрес_NTP-сервера] iburst
```

Рис. 20. Файл конфигурации службы chronyd

в. Сохраните и закройте файл.

г. Запустите службу `chronyd`. Добавьте в автозагрузку ОС Альт Сервер:

```
systemctl enable chronyd
```

д. Выполните команду для перезапуска службы `chronyd`:

```
systemctl restart chronyd
```

е. Выполните команду для проверки синхронизации времени:

```
chronyc sources
```

```
[root@NTA ~]# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* ntp.ix.ru                     1   8     2   689    -87us[ -199us] +/- 2196us
```

Рис. 21. Пример корректного вывода команды chronyc sources

Прим.:

При выводе команды должны присутствовать адреса NTP-серверов, указанные в конфигурационном файле `chrony.conf`.

- **Результат шага:** выполнена настройка службы `chronyd` для синхронизации времени UDV NTA.

Прим.:

Вы можете позже настроить Management в качестве NTP-сервера для Sensor — см. раздел «Настройка Комплекса уровня Management в качестве NTP-сервера для сенсоров».

6. Измените настройки ядра ОС в конфигурационном файле `99-datapk.conf`. Для этого:

а. Откройте файл `99-datapk.conf` на редактирование:

```
mcedit /etc/sysctl.d/99-datapk.conf
```

Прим.:

Если файл `99-datapk.conf` изначально отсутствовал в директории `/etc/sysctl.d`, он будет создан.

б. Добавьте в файл следующие строки:

```
net.ipv6.conf.all.disable_ipv6 = 1
vm.max_map_count=262144
net.core.rmem_default=16777216
net.core.rmem_max=16777216
```

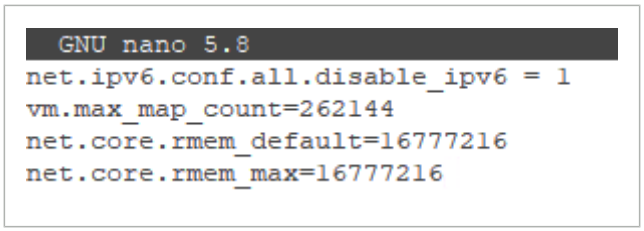

Рис. 22. Создание конфигурационного файла 99-datapk.conf

в. Примените новые настройки по команде:

```
sysctl -p /etc/sysctl.d/99-datapk.conf
```

г. Убедитесь, что настройки в конфигурационном файле `99-datapk.conf` соответствуют заданным:

```
sysctl -a | grep -P 'net.ipv6.conf.all.disable_ipv6|vm.max_map_count|
net.core.rmem_default|net.core.rm em_max'
```

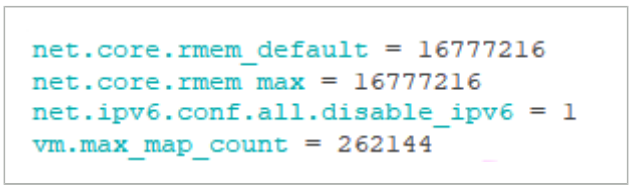

Рис. 23. Корректный вывод значений конфигурационного файла 99-datapk.conf

- **Результат шага:** настроен конфигурационный файл для управления параметрами ядра.

4. Установка и запуск Комплекса в настроенной ОС Альт Сервер

В этом разделе:

> Прим.:
>
> Инструкции, приведенные в этом разделе, актуальны для установки Комплекса на сертифицированную версию ОС Альт Сервер.

Порядок установки и запуска Комплекса уровня Sensor приведен в разделе «Установка и запуск UDV NTA уровня Sensor».

Порядок установки Комплекса уровня Management приведен в разделе «Установка и запуск UDV NTA уровня Management».

Порядок установки Комплекса уровня Management и Sensor на одном аппаратном средстве приведен в разделе «Установка и запуск UDV NTA уровня Management и Sensor на одном аппаратном средстве».

4.1. Установка и запуск UDV NTA уровня Management

Для установки и запуска Management:

1. С помощью приложения для обмена файлами по протоколу SFTP скопируйте все файлы дистрибутива UDV NTA в директорию `/home/nta` операционной системы.
2. Выполните вход в ОС под учетной записью администратора системы `root`.
3. Распакуйте архив `nta-1.0.tar`, выполнив команду:

```
tar -xvf /home/nta/nta-1.0.tar -C /var/opt
```

4. Создайте конфигурационный файл репозитория, выполнив команду:

```
mcedit /etc/apt/sources.list.d/dptk.list
```

5. Скопируйте в созданный конфигурационный файл следующее содержимое:

```
#NTA
rpm file:/var/opt/release-3.0-rc/nta noarch classic
rpm file:/var/opt/release-3.0-rc/nta x86_64 classic
rpm file:/var/opt/release-3.0-rc/zeek noarch classic
rpm file:/var/opt/release-3.0-rc/zeek x86_64 classic

#Ours
rpm file:/var/opt/release-3.0-rc/ours noarch classic
rpm file:/var/opt/release-3.0-rc/ours x86_64 classic
#Third
```

```
rpm file:/var/opt/release-3.0-rc/third noarch classic
rpm file:/var/opt/release-3.0-rc/third x86_64 classic
#Tools
rpm file:/var/opt/release-3.0-rc/tools noarch classic
rpm file:/var/opt/release-3.0-rc/tools x86_64 classic
```

6. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
7. Смонтируйте образ ОС Альт Сервер:

   а. Скопируйте сертифицированный образ ОС Альт Сервер в директорию `/home/nta`

   б. Смонтируйте образ ОС Альт Сервер, выполнив команду:

   ```
   mount -o loop /home/nta/alt-sp-server-[дата версии]-x86_64.iso /media/ALTLinux
   ```

   в. Добавьте образ ОС Альт Сервер в качестве репозитория пакетов, выполнив команду:

   ```
   apt-cdrom --no-mount -d=/media/ALTLinux add
   ```

8. Обновите репозиторий, выполнив команду:

   ```
   apt-get update
   ```

   - **Результат шага:** репозиторий успешно обновлен.

9. Выполните установку Management командой:

   ```
   apt-get install udv-nta-corp -y
   ```

   > Прим.:
   >
   > При необходимости установки модуля управления внешними событиями дополнительно выполните команду:
   >
   > ```
   > apt-get install udv-external-events-system -y
   > ```

10. Откройте файл `manager.env` Management, выполнив команду:

    ```
    mcedit /usr/share/udv/datapk/manager.env
    ```

11. Укажите IP-адрес Management в значении переменной `HOST_IP`.
12. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
13. Перезагрузите UDV NTA, выполнив команду:

    ```
    shutdown -r now
    ```

14. Дождитесь перезагрузки UDV NTA и выполните повторный вход в ОС под учетной записью администратора системы `root`.
15. Настройте межсетевой экран `iptables`. Для этого:

    а. Убедитесь, что межсетевой экран `efw` не запущен и не будет конфликтовать с `iptables`:

    ```
    cat /etc/net/ifaces/default/options | grep CONFIG_FW
    ```

> Прим.:
>
> Значение параметра `CONFIG_FW` должно быть **no**.

б. Откройте для редактирования конфигурационный файл `iptables` с правилами межсетевого экранирования:

```
mcedit /etc/sysconfig/iptables
```

в. Добавьте правила межсетевого экрана в конфигурационный файл `iptables`:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 20085 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 20044 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 20104 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 16379 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 19091 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 15673 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

г. Подтвердите сохранение изменений и нажмите кнопку **Выход**.

д. Выполните запуск службы `iptables` и добавьте в автозагрузку:

```
systemctl enable --now iptables
```

16. Перезагрузите UDV NTA, выполнив команду:

```
shutdown -r now
```

17. Дождитесь перезагрузки UDV NTA и выполните повторный вход в ОС под учетной записью администратора системы `root`.
18. Убедитесь, что все сервисы UDV NTA запущены (имеют статус `active`), выполнив команду:

```
systemctl list-units 'udv-*' --all
```

- **Результат шага:** сервисы UDV NTA успешно запущены, отсутствуют ошибки в ходе их работы.

19. Проверьте возможность подключения к Management по протоколу HTTPS. Для этого:
    a. Откройте веб-браузер на клиентской машине.
    б. Введите адрес для подключения в веб-интерфейсу в формате `https://[IP-адрес]`, где `[IP-адрес]` — IP-адрес интерфейса управления Management.

- **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.

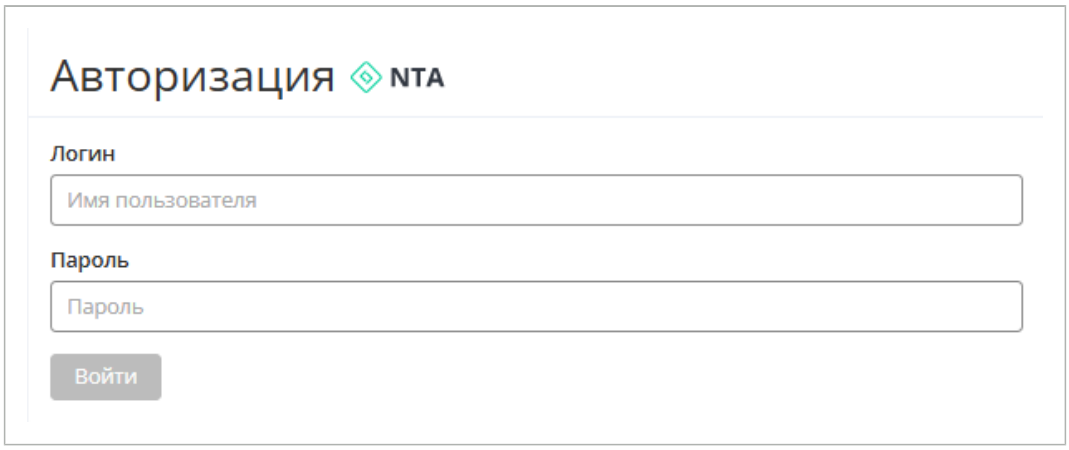

Рис. 24. Окно входа в веб-интерфейс UDV NTA

20. Если в веб-браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для веб-браузера):
    a. Нажмите на кнопку **Дополнительные**.

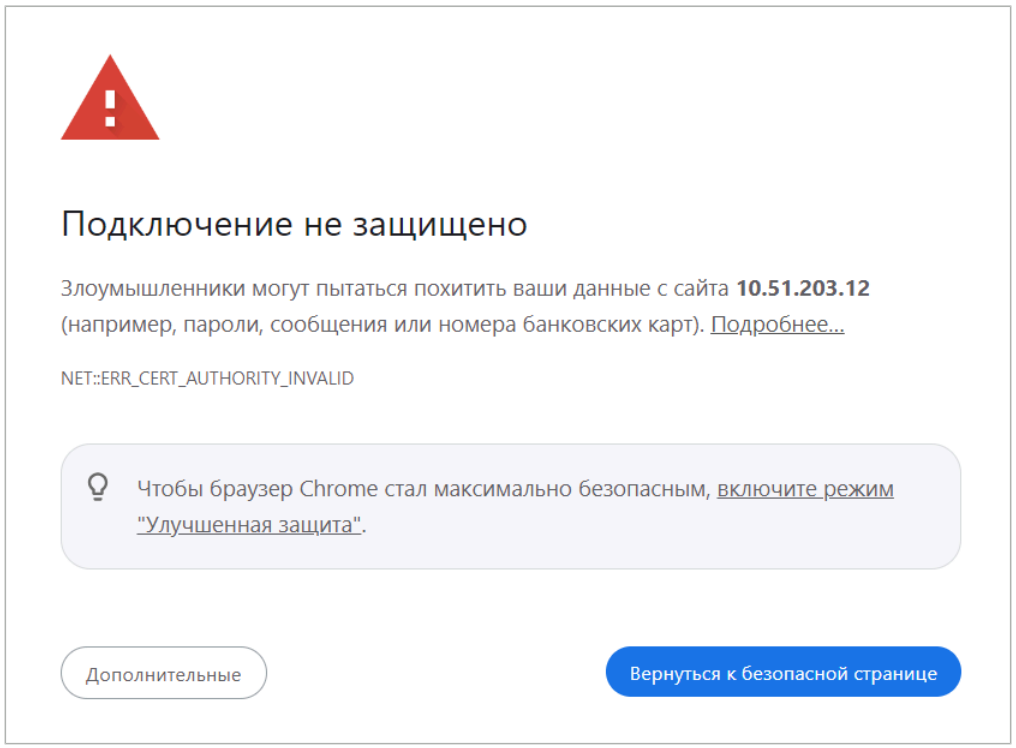

Рис. 25. Окно предупреждения о незащищенном подключении

- **Результат шага:** открыты дополнительные настройки для подключения к веб-интерфейсу UDV NTA в браузере.

6. Для продолжения подключения к UDV NTA нажмите ссылку `Перейти на сайт [IP-адрес] (небезопасно)`.

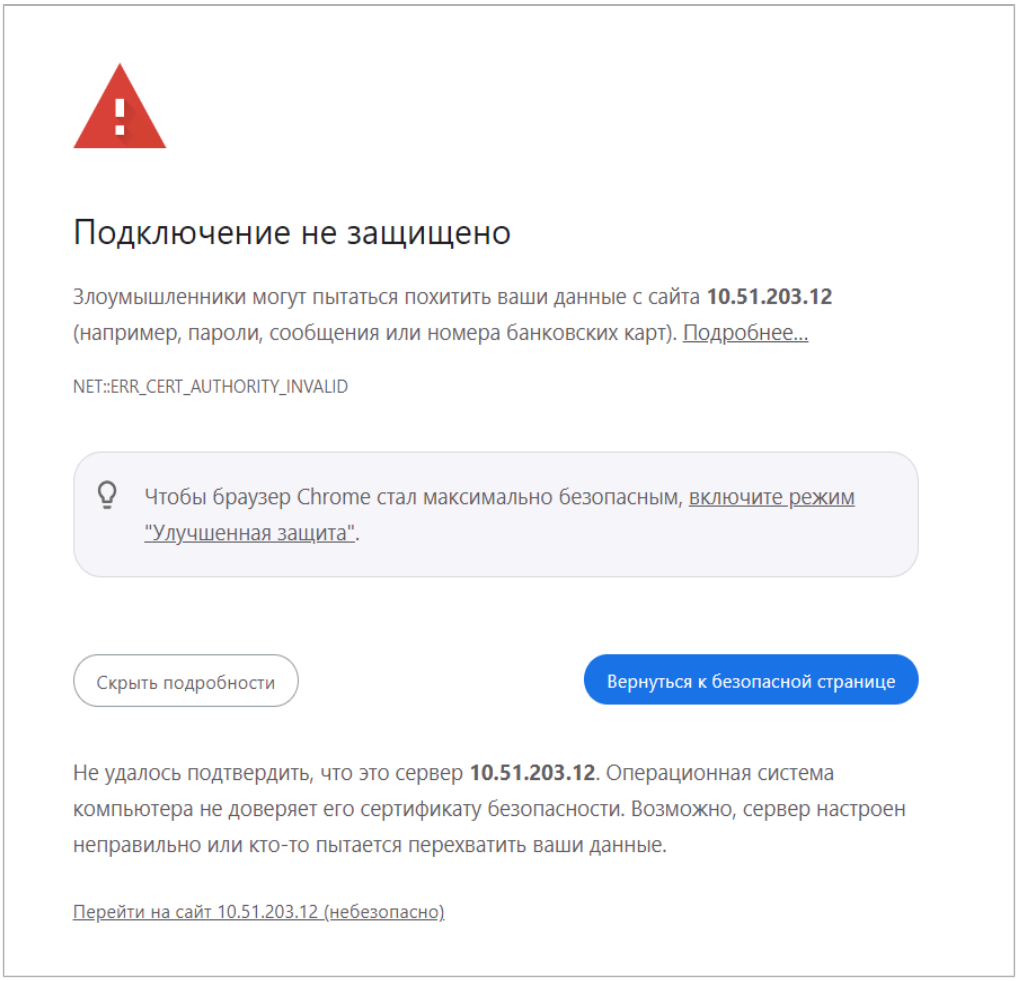

Рис. 26. Подключение к UDV NTA по HTTPS

- **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.

Для возможности сбора данных с объектов защиты установите UDV NTA уровня Sensor и подключите их к UDV NTA уровня Management согласно инструкции в разделе «Установка и запуск UDV NTA уровня Sensor».

> Внимание:
>
> UDV NTA уровня Sensor и UDV NTA уровня Management разных версий невозможно подключить друг к другу.

См. также

Подключение к веб-интерфейсу по протоколу HTTPS

4.2. Установка и запуск UDV NTA уровня Sensor

> Внимание:
>
> UDV NTA уровня Sensor и UDV NTA уровня Management разных версий невозможно подключить друг к другу.

Для установки и запуска Sensor:

1. С помощью приложения для обмена файлами по протоколу SFTP скопируйте все файлы дистрибутива UDV NTA в директорию `/home/nta` операционной системы.
2. Выполните вход в ОС под учетной записью администратора системы `root`.
3. Распакуйте архив `nta-1.0.tar`, выполнив команду:

```
tar -xvf /home/nta/nta-1.0.tar -C /var/opt
```

4. Создайте конфигурационный файл репозитория, выполнив команду:

```
mcedit /etc/apt/sources.list.d/dptk.list
```

5. Скопируйте в созданный конфигурационный файл следующее содержимое:

```
#NTA
rpm file:/var/opt/release-3.0-rc/nta noarch classic
rpm file:/var/opt/release-3.0-rc/nta x86_64 classic
rpm file:/var/opt/release-3.0-rc/zeek noarch classic
rpm file:/var/opt/release-3.0-rc/zeek x86_64 classic

#Ours
rpm file:/var/opt/release-3.0-rc/ours noarch classic
rpm file:/var/opt/release-3.0-rc/ours x86_64 classic
#Third
rpm file:/var/opt/release-3.0-rc/third noarch classic
rpm file:/var/opt/release-3.0-rc/third x86_64 classic
#Tools
rpm file:/var/opt/release-3.0-rc/tools noarch classic
rpm file:/var/opt/release-3.0-rc/tools x86_64 classic
```

6. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
7. Смонтируйте образ ОС Альт Сервер:

    а. Скопируйте сертифицированный образ ОС Альт Сервер в директорию `/home/nta`

    б. Смонтируйте образ ОС Альт Сервер, выполнив команду:

    ```
    mount -o loop /home/nta/alt-sp-server-[дата версии]-x86_64.iso /media/ALTLinux
    ```

    в. Добавьте образ ОС Альт Сервер в качестве репозитория пакетов, выполнив команду:

    ```
    apt-cdrom --no-mount -d=/media/ALTLinux add
    ```

8. Обновите репозиторий, выполнив команду:

```
apt-get update
```

    - **Результат шага:** репозиторий успешно обновлен.

9. Выполните установку Sensor командой:

```
apt-get install udv-datapk-dpi-sensor -y
```

> Прим.:
>
> При необходимости установки модуля управления внешними событиями дополнительно выполните команду:
>
> ```
> apt-get install udv-external-events-system -y
> ```

10. Настройте сетевой интерфейс для прослушивания трафика. Для этого:

    а. Если отсутствует, создайте директорию с наименованием сетевого интерфейса для прослушивания трафика (в примере ниже это `ens224`):

    ```
    mkdir /etc/net/ifaces/ens224
    ```

    б. Скопируйте файл конфигурации настроенного сетевого интерфейса управления `options` (в примере ниже это `ens192`) в созданную ранее директорию, выполнив команду:

    ```
    cp /etc/net/ifaces/ens192/options /etc/net/ifaces/ens224/
    ```

    в. Создайте новый файл `iplink` и добавьте в него команду переключения интерфейса в режим прослушивания всех пакетов (`promisc`), выполнив команду:

    ```
    echo promisc on > /etc/net/ifaces/ens224/iplink
    ```

    г. Перезагрузите сетевой сервис, выполнив команду:

    ```
    systemctl restart network
    ```

    ▸ **Результат шага:** сетевой интерфейс для прослушивания трафика переключен в режим прослушивания всех пакетов.

11. Откройте файл `sensor.env` Sensor, выполнив команду:

    ```
    mcedit /usr/share/udv/datapk/sensor.env
    ```

12. Укажите через запятую наименования сетевых интерфейсов для прослушивания сетевого трафика в переменной `LISTENING_INTERFACES`.
13. Укажите IP-адрес UDV NTA уровня Management в переменной `MANAGER_NODE_ADDRESS`.
14. Сохраните и закройте файл `sensor.env`.
15. Настройте разделы для хранения трафика и файлов. Для этого:

    а. Создайте файловые системы на разделах `pcaps` и `files`, последовательно выполнив команды:

    ```
    mkfs.xfs /dev/nta/pcaps
    mkfs.xfs /dev/nta/files
    ```

```
[root@nta-1 nta]# mkfs.xfs /dev/nta/pcaps
meta-data=/dev/nta/pcaps         isize=512    agcount=4, agsize=1293824 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=5175296, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
[root@nta-1 nta]# mkfs.xfs /dev/nta/files
meta-data=/dev/nta/files         isize=512    agcount=4, agsize=655360 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=2621440, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
```

Рис. 27. Создание файловых систем на разделах pcaps и files

б. Создайте директории для хранения трафика и файлов:

```
mkdir -p /usr/share/udv/zeek-wrapper/extracted_files
mkdir -p /var/cache/udv/stenographer/
```

в. Измените права на созданные директории:

```
chmod -R 777 /usr/share/udv/zeek-wrapper/extracted_files
chmod -R 777 /var/cache/udv/stenographer/
```

г. Добавьте следующие строки в конец файла `/etc/fctab` для автоматического подключени разделов при перезагрузке:

```
/dev/mapper/nta-files   /usr/share/udv/zeek-wrapper/extracted_files xfs defaults
 0   0
/dev/mapper/nta-pcaps   /var/cache/udv/stenographer xfs defaults    0   0
```

д. Сохраните и закройте файл `/etc/fctab`.

е. Подключите добавленные разделы на основе `/etc/fctab`:

```
mount -a
```

ж. Убедитесь, что необходимые разделы подключены:

```
df -h | grep -E "(pcaps|files)"
```

```
[root@nta-1 ~]# df -h | grep -E "(pcaps|files)"
/dev/mapper/nta-files    10G  104M  9.9G   2% /usr/share/udv/zeek-wrapper/extracted_files
/dev/mapper/nta-pcaps    20G  174M   20G   1% /var/cache/udv/stenographer
```

Рис. 28. Подключенные разделы «pcaps» и «files»

16. Настройте сетевой экран `iptables`. Для этого:

а. Убедитесь, что межсетевой экран `efw` не запущен и не будет конфликтовать с `iptables`:

```
cat /etc/net/ifaces/default/options | grep CONFIG_FW
```

> Прим.:
>
> Значение параметра `CONFIG_FW` должно быть **no**.

б. Откройте для редактирования конфигурационный файл `iptables` с правилами межсетевого экранирования:

```
mcedit /etc/sysconfig/iptables
```

в. Добавьте правила межсетевого экрана в конфигурационный файл `iptables`:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --dport 514 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 514 -j ACCEPT
-A INPUT -p udp -m udp --dport 515 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 515 -j ACCEPT
-A INPUT -p udp -m udp --dport 162 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

г. Подтвердите сохранение изменений и нажмите кнопку **Выход**.

д. Выполните запуск службы `iptables` и добавьте в автозагрузку:

```
systemctl enable --now iptables
```

17. Перезагрузите UDV NTA, выполнив команду:

```
shutdown -r now
```

18. Дождитесь перезагрузки UDV NTA и выполните повторный вход в ОС под учетной записью администратора системы `root`.
19. Убедитесь, что все сервисы UDV NTA запущены (имеют статус `active`), выполнив команду:

```
systemctl list-units 'udv-*' --all
```

- **Результат шага:** сервисы UDV NTA успешно запущены, отсутствуют ошибки в ходе их работы.

20. Убедитесь, что сенсор успешно подключился к UDV NTA уровня Management. Для этого убедитесь, что в журнале событий сервиса `udv-redis-sensor` отсутствуют ошибки:

```
journalctl -eu udv-redis-sensor.service
```

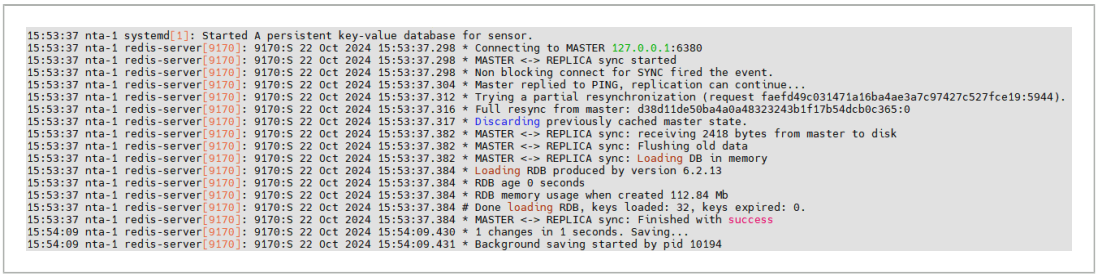

Рис. 29. Пример журнала событий «udv-redis-sensor» при успешном подключении сенсора

См. также

Подключение к веб-интерфейсу по протоколу HTTPS

4.3. Установка и запуск UDV NTA уровня Management и Sensor на одном аппаратном средстве

> Внимание:
>
> UDV NTA уровня Sensor и UDV NTA уровня Management разных версий невозможно подключить друг к другу.

Для установки и запуска UDV NTA уровня Management и Sensor:

1. С помощью приложения для обмена файлами по протоколу SFTP скопируйте все файлы дистрибутива UDV NTA в директорию `/home/nta` операционной системы.
2. Выполните вход в ОС под учетной записью администратора системы `root`.
3. Распакуйте архив `nta-1.0.tar`, выполнив команду:

```
tar -xvf /home/nta/nta-1.0.tar -C /var/opt
```

4. Создайте конфигурационный файл репозитория, выполнив команду:

```
mcedit /etc/apt/sources.list.d/dptk.list
```

5. Скопируйте в созданный конфигурационный файл следующее содержимое:

```
#NTA
rpm file:/var/opt/release-3.0-rc/nta noarch classic
rpm file:/var/opt/release-3.0-rc/nta x86_64 classic
rpm file:/var/opt/release-3.0-rc/zeek noarch classic
rpm file:/var/opt/release-3.0-rc/zeek x86_64 classic

#Ours
rpm file:/var/opt/release-3.0-rc/ours noarch classic
rpm file:/var/opt/release-3.0-rc/ours x86_64 classic
#Third
rpm file:/var/opt/release-3.0-rc/third noarch classic
rpm file:/var/opt/release-3.0-rc/third x86_64 classic
```

```
#Tools
rpm file:/var/opt/release-3.0-rc/tools noarch classic
rpm file:/var/opt/release-3.0-rc/tools x86_64 classic
```

6. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
7. Смонтируйте образ ОС Альт Сервер:

   а. Скопируйте сертифицированный образ ОС Альт Сервер в директорию `/home/nta`

   б. Смонтируйте образ ОС Альт Сервер, выполнив команду:

   ```
   mount -o loop /home/nta/alt-sp-server-[дата версии]-x86_64.iso /media/ALTLinux
   ```

   в. Добавьте образ ОС Альт Сервер в качестве репозитория пакетов, выполнив команду:

   ```
   apt-cdrom --no-mount -d=/media/ALTLinux add
   ```

8. Обновите репозиторий, выполнив команду:

   ```
   apt-get update
   ```

   - **Результат шага:** репозиторий успешно обновлен.

9. Выполните установку UDV NTA уровня Management и Sensor командой:

   ```
   apt-get install udv-nta-corp udv-datapk-dpi-sensor -y
   ```

   > Прим.:
   >
   > При необходимости установки модуля управления внешними событиями дополнительно выполните команду:
   >
   > ```
   > apt-get install udv-external-events-system -y
   > ```

10. Настройте сетевой интерфейс для прослушивания трафика. Для этого:

    а. Если отсутствует, создайте директорию с наименованием сетевого интерфейса для прослушивания трафика (в примере ниже это `ens224`):

    ```
    mkdir /etc/net/ifaces/ens224
    ```

    б. Скопируйте файл конфигурации настроенного сетевого интерфейса управления `options` (в примере ниже это `ens192`) в созданную ранее директорию, выполнив команду:

    ```
    cp /etc/net/ifaces/ens192/options /etc/net/ifaces/ens224/
    ```

    в. Создайте новый файл `iplink` и добавьте в него команду переключения интерфейса в режим прослушивания всех пакетов (`promisc`), выполнив команду:

    ```
    echo promisc on > /etc/net/ifaces/ens224/iplink
    ```

    г. Перезагрузите сетевой сервис, выполнив команду:

    ```
    systemctl restart network
    ```

▸ **Результат шага:** сетевой интерфейс для прослушивания трафика переключен в режим прослушивания всех пакетов.

11. Откройте файл `manager.env` UDV NTA уровня Management, выполнив команду:

```
mcedit /usr/share/udv/datapk/manager.env
```

12. Укажите IP-адрес UDV NTA уровня Management в значении переменной `HOST_IP`.
13. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
14. Откройте файл `sensor.env` UDV NTA уровня Sensor, выполнив команду:

```
mcedit /usr/share/udv/datapk/sensor.env
```

15. Укажите через запятую наименования сетевых интерфейсов для прослушивания сетевого трафика в переменной `LISTENING_INTERFACES`.
16. Сохраните и закройте файл `sensor.env`.
17. Настройте разделы для хранения трафика и файлов. Для этого:

    а. Создайте файловые системы на разделах `pcaps` и `files`, последовательно выполнив команды:

```
mkfs.xfs /dev/nta/pcaps
mkfs.xfs /dev/nta/files
```

```
[root@nta-1 nta]# mkfs.xfs /dev/nta/pcaps
meta-data=/dev/nta/pcaps         isize=512    agcount=4, agsize=1293824 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=5175296, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
[root@nta-1 nta]# mkfs.xfs /dev/nta/files
meta-data=/dev/nta/files         isize=512    agcount=4, agsize=655360 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=2621440, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
```

Рис. 30. Создание файловых систем на разделах pcaps и files

    б. Создайте директории для хранения трафика и файлов:

```
mkdir -p /usr/share/udv/zeek-wrapper/extracted_files
mkdir -p /var/cache/udv/stenographer/
```

    в. Измените права на созданные директории:

```
chmod -R 777 /usr/share/udv/zeek-wrapper/extracted_files
chmod -R 777 /var/cache/udv/stenographer/
```

    г. Добавьте следующие строки в конец файла `/etc/fctab` для автоматического подключени разделов при перезагрузке:

```
/dev/mapper/nta-files   /usr/share/udv/zeek-wrapper/extracted_files xfs defaults
 0   0
/dev/mapper/nta-pcaps   /var/cache/udv/stenographer xfs defaults    0   0
```

д. Сохраните и закройте файл `/etc/fctab`.

е. Подключите добавленные разделы на основе `/etc/fctab`:

```
mount -a
```

ж. Убедитесь, что необходимые разделы подключены:

```
df -h | grep -E "(pcaps|files)"
```

```
[root@nta-1 ~]# df -h | grep -E "(pcaps|files)"
/dev/mapper/nta-files    10G  104M  9.9G   2% /usr/share/udv/zeek-wrapper/extracted_files
/dev/mapper/nta-pcaps    20G  174M   20G   1% /var/cache/udv/stenographer
```

Рис. 31. Подключенные разделы «pcaps» и «files»

18. Настройте межсетевой экран `iptables`. Для этого:

а. Убедитесь, что межсетевой экран `efw` не запущен и не будет конфликтовать с `iptables`:

```
cat /etc/net/ifaces/default/options | grep CONFIG_FW
```

> Прим.:
>
> Значение параметра `CONFIG_FW` должно быть **no**.

б. Откройте для редактирования конфигурационный файл `iptables` с правилами межсетевого экранирования:

```
mcedit /etc/sysconfig/iptables
```

в. Добавьте правила межсетевого экрана в конфигурационный файл `iptables`:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -p udp -m udp --dport 514 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 514 -j ACCEPT
-A INPUT -p udp -m udp --dport 515 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 515 -j ACCEPT
-A INPUT -p udp -m udp --dport 162 -j ACCEPT
```

```
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

г. Подтвердите сохранение изменений и нажмите кнопку **Выход**.

д. Выполните запуск службы `iptables` и добавьте в автозагрузку:

```
systemctl enable --now iptables
```

19. Перезагрузите UDV NTA, выполнив команду:

```
shutdown -r now
```

20. Дождитесь перезагрузки UDV NTA и выполните повторный вход в ОС под учетной записью администратора системы `root`.
21. Убедитесь, что все сервисы UDV NTA запущены (имеют статус `active`), выполнив команду:

```
systemctl list-units 'udv-*' --all
```

- **Результат шага:** сервисы UDV NTA успешно запущены, отсутствуют ошибки в ходе их работы.

22. Проверьте возможность подключения к Management по протоколу HTTPS. Для этого:

а. Откройте веб-браузер на клиентской машине.

б. Введите адрес для подключения в веб-интерфейсу в формате `https://[IP-адрес]`, где `[IP-адрес]` — IP-адрес интерфейса управления Management.

- **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.

Рис. 32. Окно входа в веб-интерфейс UDV NTA

23. Если в веб-браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для веб-браузера):

а. Нажмите на кнопку **Дополнительные**.

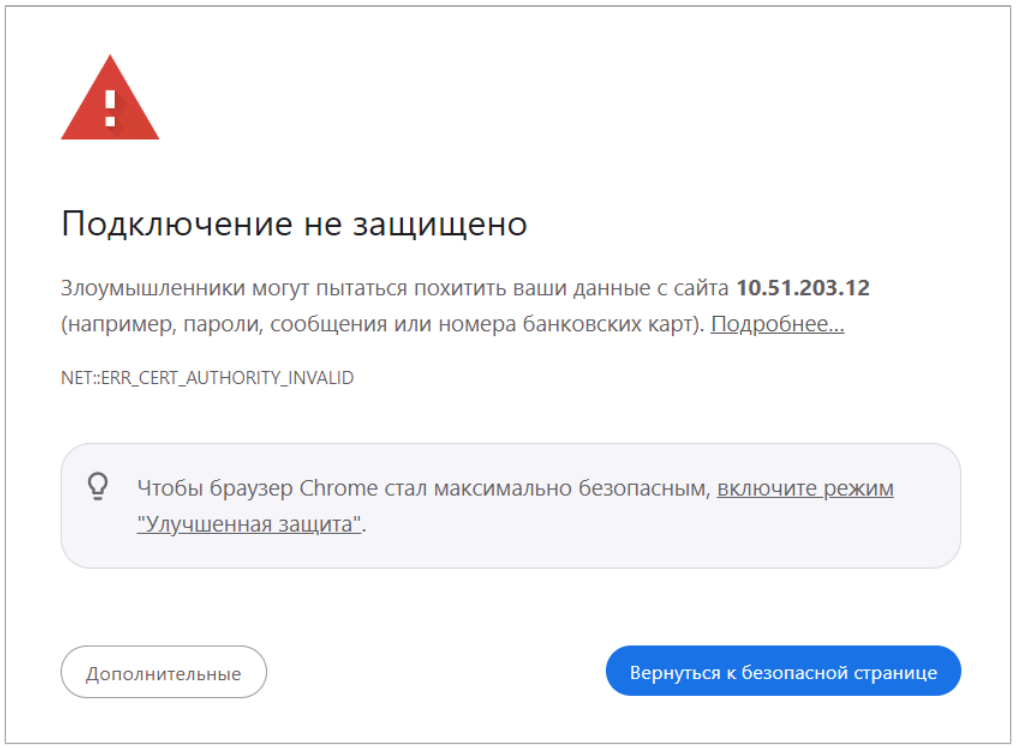

Рис. 33. Окно предупреждения о незащищенном подключении

▸ **Результат шага:** открыты дополнительные настройки для подключения к веб-интерфейсу UDV NTA в браузере.

б. Для продолжения подключения к UDV NTA нажмите ссылку `Перейти на сайт [IP-адрес] (небезопасно)`.

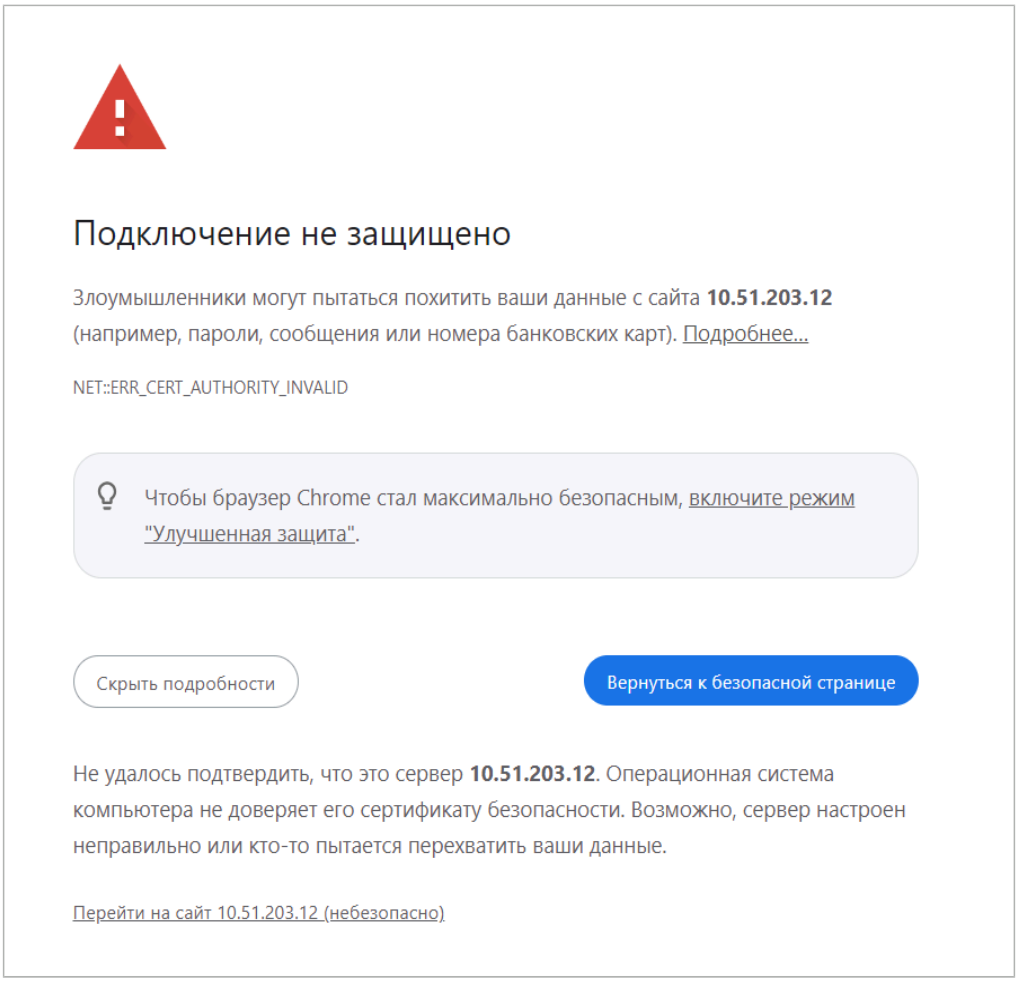

Рис. 34. Подключение к UDV NTA по HTTPS

- **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.

См. также

Подключение к веб-интерфейсу по протоколу HTTPS

5. Дополнительные настройки UDV NTA

В этом разделе:

В этом разделе приведены настройки, которые можно выполнить при необходимости на любой версии ОС Альт Сервер 10 после ее установки и развертывания всех уровней UDV NTA:

5.1. Создание единого виртуального интерфейса (bond) для прослушивания трафика с нескольких физических интерфейсов

В данной инструкции описано создание интерфейса `bond` в ОС Альт Сервер в режиме broadcast (mode=3). `Bonding` — это технология объединения нескольких физических интерфейсов в один логический `bond`-интерфейс для повышения надежности и производительности сетевых соединений.

Внимание:

Ограничения в использовании `bond`:

- **Конфликтующий трафик**. Наличие конфликтов трафика, таких как одинаковые IP- или MAC-адреса, может привести к потере пакетов или информации.
- **Невозможность различать трафик с разных интерфейсов**. Трафик с разных подчиненных интерфейсов обрабатывается как единое целое. Это усложняет анализ и мониторинг трафика, поскольку вся информация агрегирована, и отдельные потоки не видны.
- **Нагрузка на анализаторы трафика**. Использование `bond` может увеличить нагрузку на анализаторы трафика: `Zeek`, `Suricata`, `Steno`. При перегрузке этих служб возможна потеря пакетов или информации.

Прим.:

Инструкция не учитывает частные параметры оборудования и настройки систем эксплуатации.

Для создания интерфейса `bond`:

1. Если неизвестны имена сетевых интерфейсов, которые планируется объединить, отобразите все доступные сетевые интерфейсы с помощью одной из команд:

   ```
   ip link show
   ```

   или

   ```
   cat /proc/net/dev
   ```

2. Убедитесь, что сетевые интерфейсы, которые необходимо объединить, имеют одинаковые сетевые параметры (например, скорость, способ связи). Для этого введите команду:

   ```
   ethtool [iface_name]
   ```

   Где `[iface_name]` — наименование проверяемого сетевого интерфейса.

3. Остановите работу UDV NTA командой:

   ```
   systemctl stop udv-* --all
   ```

4. Перейдите в директорию `/etc/net/ifaces`:

   ```
   cd /etc/net/ifaces
   ```

5. Убедитесь, что в директории `/etc/net/ifaces` присутствуют директории сетевых интерфейсов, которые планируется объединить. Для этого введите команду:

   ```
   ls
   ```

6. Если в результате шага 5 не было необходимых директорий интерфейсов, создайте их по команде:

   ```
   mkdir [iface_name]
   ```

   Где `[iface_name]` — наименование интерфейса, который планируется объединять с другим.

7. Создайте каталог объединенного сетевого интерфейса `bond0`:

   ```
   mkdir /etc/net/ifaces/bond0
   ```

> Прим.:
>
> Номер `0` интерфейса `bond0` задан для примера.

8. Создайте файл с параметрами сетевого интерфейса `bond0` (команду ниже необходимо скопировать и вставить в командную строку целиком):

```
echo -e 'TYPE=bond\nONBOOT=yes\nBOOTPROTO=static
HOST="[iface_name_1] [iface_name_2]"\nBONDMODE=3
BONDOPTIONS="miimon=100"' \
> /etc/net/ifaces/bond0/options
```

   Где `[iface_name_1]` и `[iface_name_2]` — названия подключенных сетевых интерфейсов, которые необходимо объединить.

9. Включите у интерфейса режим `promiscuous` для прослушивания всех пакетов, создав файл `iplink`:

```
echo -e 'promisc on\narp on\nup' > /etc/net/ifaces/bond0/iplink
```

10. При необходимости задайте дополнительные параметры: например, параметр `MTU`, отвечающий за максимальный размер передаваемого по сети пакета данных:

```
echo 'mtu [INT]' >> /etc/net/ifaces/bond0/iplink
```

    Где `[INT]` — значение параметра `MTU` в байтах.

11. Для применения новых настроек перезапустите службу сети командой `systemctl restart network` или перезапустите ОС Альт Сервер командой `reboot`.
12. Для проверки корректности создания сетевого интерфейса выполните команду:

```
cat /proc/net/bonding/bond0
```

    - **Результат шага:** в выводе будут представлены настройки объединенного сетевого интерфейса `bond0` и сетевых интерфейсов `[iface_name_1]` и `[iface_name_2]`, которые были объединены.

13. Присвойте переменной `LISTENING_INTERFACES` в файле `sensor.env` в директории `/usr/share/udv/datapk/` значение созданного `bond`-интерфейса.
14. Запустите сервисы UDV NTA командой:

```
systemctl start udv-* --all
```

5.2. Уменьшение количества ложных срабатываний модулей анализа сетевых данных с использованием белого списка

Белый список — это метод управления сетевой безопасностью, при котором создается список разрешенных IP-адресов, доменов или приложений. Взаимодействия с этими ресурсами не активируют в модулях анализа сетевых данных компоненты, отвечающие за обнаружение определенных тактик и техник атак. Для ресурсов, не входящих в этот список, создаются события ИБ для дальнейшего анализа или блокировки администратором.

В UDV NTA файл с белым списком `general.dat` по умолчанию находится в директории `/usr/share/udv/zeek-wrapper/configs/`

Формат записей белого списка

Записи белого списка имеют следующий формат:

```
[option_name] [new_value]
```

Где:

- `[option_name]` — наименование переменной;
- `[new_value]` — значение переменной.

> Прим.:
>
> Между наименованием переменной и ее значением ставится пробел или табуляция.
>
> Если у переменной несколько значений, они разделяются запятой, без пробела.

Со списком основных переменных вы можете ознакомиться в разделе «Переменные файла белого списка» Руководства по эксплуатации UDV NTA.

Примеры записей:

Пример

```
BZAR::t1003_006_whitelist_orig_addrs 192.168.1.161,10.0.0.1
```

```
BZAR::t1003_006_whitelist_orig_subnets 192.168.1.0/24
```

```
BZAR::t1003_006_whitelist_orig_names example.com
```

```
DNS::whitelist_orig_names *.example.ru,*.dev
```